



Web Application Security Assessment

An assessment of the security of the Astley Jewellers'
web application

Isaac Basque-Rice

CMP319: Ethical Hacking 2

BSc Ethical Hacking Year 3

2021/22

CMP319 – Coursework 1: You should include Introduction, Procedure and Results, References Part 1, and Appendices part 1.

CMP319 – Coursework 2: You should include Abstract, Discussion, References Part 2, and Appendices part 2

Note that Information contained in this document is for educational purposes.

Abstract

The usage of web applications on the internet in the modern day is simply unavoidable, be it social media, administrative work such as online banking, or for online shopping, amongst a host of other uses. As a result of this, the security of the billions of daily internet users and the millions of organisations, groups, or individuals who choose to run a web app is of the utmost importance. If the security of any of these web applications are compromised the repercussions could be enormous, leaking personal information and credentials, losing a significant chunk of revenue, or being forced to close a business are all realistic issues for an organisation that has been compromised. As a result of this, Astley Jewellers' has asked a security professional to conduct a test of the security of their web application, and produce a report based on this assessment.

This report covers a full web application penetration test, making use of the OWASP Web Application Testing Methodology. The use of such a methodology is of paramount importance to ensure as thorough a test of the application as possible to remediate and mitigate any issues that may be present in said application.

During the assessment, the Astley Jewellers' website was found to contain a multitude of vulnerabilities, including but not limited to SQL Injection, Cross Site Scripting, weak or non-present cryptography, and weak password usage. The presence of these vulnerabilities, amongst others, allowed the tester administrative access and access to other users' accounts including the admin account. The report will outline recommended steps for a developer to take in securing the application to ensure any prospective attackers do not have the opportunity to gain such privileged access to the website.

Contents

1	Introduction	1
1.1	Background.....	1
1.1	Aims.....	1
2	Procedure and Results	3
1.2	Overview of Procedure	3
2.1	Information gathering.....	4
2.1.1	Fingerprint Web Server.....	4
2.1.2	Review Webserver Metafiles for Information Leakage.....	5
2.1.3	Enumerate Applications on Webserver.....	5
2.1.4	Review Webpage Content for Information Leakage	6
2.1.5	Identify Application Entry Points	7
2.1.6	Map Execution Paths Through Application	8
2.1.7	Fingerprint Web Application Framework	10
2.2	Configuration and Deployment Management Testing	12
2.2.1	Test Application Platform Configuration	12
2.2.2	Enumerate Infrastructure and Application Admin Interfaces	15
2.2.3	Test HTTP Strict Transport Security	16
2.3	Identity Management Testing.....	18
2.3.1	Test Role Definitions.....	18
2.3.2	Test User Registration Process	19
2.3.3	Testing for Weak or Unenforced Username Policy	21
2.4	Authentication Testing.....	23
2.4.1	Testing for Credentials Transported over Unencrypted Channels.....	23
2.4.2	Testing for Default Credentials.....	24
2.4.3	Testing for Weak Lock Out Mechanism	24
2.4.4	Testing for Weak Password Policy	25
2.5	Authorisation testing.....	27
2.5.1	Testing Directory Traversal File Include.....	27
2.6	Session Management Testing	28
2.6.1	Testing for Session Management Schema.....	28

2.6.2	Testing for Cookies Attributes	28
2.6.3	Testing for Session Fixation	29
2.6.4	Testing for Logout Functionality	31
2.7	Input Validation Testing	33
2.7.1	Testing for Reflected Cross Site Scripting	33
2.7.2	Testing for Stored Cross Site Scripting.....	33
2.7.3	Testing for SQL Injection.....	34
2.7.4	Testing for Incubated Vulnerability	35
2.8	Error Handling	37
2.8.1	Testing for Improper Error Handling	37
2.9	Cryptography.....	38
2.9.1	Testing for Weak Transport Layer Security.....	38
2.10	Business Logic Testing	39
2.10.1	Test Ability to Forge Requests	39
2.10.2	Test Number of Times a Function Can Be Used Limits	39
2.10.3	Test Upload of Unexpected File Types	39
3	Discussion.....	40
3.1	Source Code Analysis	40
3.1.1	Analysis	40
3.1.2	Results.....	40
3.2	Vulnerabilities Discovered and Countermeasures.....	42
3.2.1	Robots.txt vulnerability.....	42
3.2.2	Local File Inclusion vulnerability	43
3.2.3	Hidden source code vulnerability	43
3.2.4	Reversible cookie vulnerability	44
3.2.5	Cookie attributes vulnerability	44
3.2.6	Directory browsing vulnerability	45
3.2.7	User enumeration vulnerability.....	45
3.2.8	Unlimited login attempts.....	46
3.2.9	No HTTPS vulnerability.	46
3.2.10	File upload vulnerability.....	47

3.2.11	Cross Site Request Forgery (CSRF) vulnerability.....	48
3.2.12	PHP information disclosure vulnerability.....	48
3.2.13	SQL Injection vulnerability.....	49
3.2.14	Hidden guessable folder vulnerability.....	50
3.2.15	Brute-forceable Admin password.....	50
3.2.16	Generic issues.....	50
3.3	Overall Discussion.....	52
4	Future Work.....	53
	References part 1.....	54
	References part 2.....	55
1	<i>Appendices part 1</i>	59
4.1	<i>Appendix A – Omitted Methodology</i>	59
4.2	<i>Appendix B – Site Files and Data</i>	61
4.2.1	<i>Section 1 – Site URLs</i>	61
4.3	<i>Appendix C – Console Output</i>	73
4.3.1	<i>Section 1 – Dirb Output</i>	73
4.3.2	<i>Section 2 – Nikto Output</i>	75
4.4	<i>Appendix D - GUI Tool Output</i>	77
4.4.1	<i>OWASP Zap Scan Report Output</i>	77
	<i>Appendices part 2</i>	110
4.5	<i>Appendix A - Grep Results</i>	110

1 INTRODUCTION

1.1 BACKGROUND

In the modern world, a substantial internet presence is a requirement for any successful business, particularly during the recent coronavirus pandemic, the need for goods and services to be available online has arguably never been higher due to the fact people were unable to leave the house for the most part. Naturally, however, with the increase in internet-dependency also comes the increase in cybercrime.

According to a study conducted by several universities in the UK, including Abertay, “There was a reported 600% increase of phishing attacks in March 2020 [and] The World Economic Forum (WEF) reported that the pandemic led to a 50.1% increase in cyber-attacks” (Lallie et al., 2021).

Any organisation not adequately prepared for the eventuality of being a victim of a cybercrime may, and often will, find themselves with intensely serious issues on their hands, from the loss of customer or user data such as emails, passwords, payment information etc, which may lead to fines, to, in the most extreme cases, the inability to function at all for a certain period, or even indefinitely.

Preparation is, of course, key to avoiding this. To this end the owner of Astley Jewellers, Mr. Rick Astley, has contacted a penetration tester to test the security of his business’s website with the aim of producing a report on the tester’s findings, as well as ways of fixing any issues that may appear. The description given to the tester outlines the fact that the site was developed externally and handed off to Astley, and the fact it is “buggy but mostly functional”. Astley has provided valid user credentials for the tester and a virtual machine with the website hosted on it, so as not to disrupt normal usage.

1.1 AIMS

The aim of this test is to determine all vulnerabilities present within the web application and as previously mentioned, present them to the client in the form of a report. A penetration test is typically performed by the tester from the perspective of a malicious actor, or hacker, meaning the actions the tester will take are likely to be like the ones that would occur if a genuine attack were to take place. To this end the tester will be attempting to escalate their privileges on the application, attempt to steal as much user information as they possibly can, and ultimately, if possible, go as far as to deface the website, gain control of it in other ways, or prevent normal usage of the site.

To achieve this, the tester will make use of an industry standard methodology, whereby they will use a series of tools to achieve certain goals in a specific order to be as thorough as possible. Further information about this can be found In the Overview and Procedure section. This process is designed to uncover as many vulnerabilities in the application as possible, and the results can be used to provide suggestions with regards to countermeasures that the client can take to mitigate them.

2 PROCEDURE AND RESULTS

1.2 OVERVIEW OF PROCEDURE

In this case, the tester had decided to make use of the OWASP Web Application Security Testing methodology (OWASP, n.d.) Stable version 4.0. This methodology was chosen as it is from an accredited and reputable institution and provides a thorough pathway of steps for the tester, the stable version was chosen over the more up to date version because issues could arise in the methodology during the process of this test.

This methodology consists of the following steps:

1. Information Gathering
2. Configuration and Deployment Management Testing
3. Identity Management Testing
4. Authentication Testing
5. Authorisation Testing
6. Session Management Testing
7. Input Validation Testing
8. Error Handling
9. Cryptography
10. Business Logic Testing
11. Client-side Testing

Naturally there are areas of this methodology that do not fit within the scope of this test, due to the structure of the OWASP methodology, whereby each section has multiple subsections, the areas of omission are too great in number to list out here, as such there is an extra “omitted methodology” section to this document in Appendix A. The only whole section of the methodology omitted is Client-side testing, as the relevant contents of this section are covered elsewhere.

Throughout the duration of the test the tester made use of tools that were provided to them by the organisation they are a part of. This includes, but is not necessarily limited to, a Kali Linux virtual machine with most of the Required tools preinstalled, OWASP tools such as Mantra and Zap, and CyberChef.

2.1 INFORMATION GATHERING

2.1.1 Fingerprint Web Server

The concept of “Fingerprinting” a web server describes the process of identifying the software specification of the server that the target is running on. To achieve this, testers normally run a few automatic testing tools such as nmap, Nikto, and netcraft.

In this instance, the tester ran the nmap command, the industry standard network mapping software, with the -sV flag, which displayed the services running on the target host device.

```
root@kali:~# nmap -sV 192.168.1.20
Starting Nmap 7.91 ( https://nmap.org ) at 2021-11-09 04:44 EST
Nmap scan report for 192.168.1.20
Host is up (0.00081s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE  VERSION
21/tcp    open  ftp      ProFTPD 1.3.4c
80/tcp    open  http     Apache httpd 2.4.29 ((Unix) OpenSSL/1.0.2n PHP/5.6.34
mod_perl/2.0.8-dev Perl/v5.16.3)
443/tcp   open  ssl/http Apache httpd 2.4.29 ((Unix) OpenSSL/1.0.2n PHP/5.6.34
mod_perl/2.0.8-dev Perl/v5.16.3)
3306/tcp  open  mysql    MariaDB (unauthorized)
MAC Address: 00:15:5D:00:04:0C (Microsoft)
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.10 seconds
```

Figure 1, output for the command

As can be seen in the above image, the command shows that the target web server is running a Unix based system with four services

- File Transfer Protocol using ProFTPD on port 21
- Hypertext Transfer Protocol using Apache with OpenSSL, PHP, and Perl
 - HTTP on port 80
 - HTTPS on port 443
- MariaDB, a fork of MySQL, on port 3306

From this we can refine possibilities for exploitation in the later stages, of particular interest is the last service found in the list, MariaDB, which if improperly implemented could result in a vulnerability known as an SQL injection, which will be covered in a later section. In addition to this there may be vulnerabilities in the specific versions of the other services found on the target.

2.1.2 Review Webserver Metafiles for Information Leakage

This stage concerns the meta files of the website, i.e., the files that describe the site itself. The primary metafile of note in most sites is the “robots.txt” file, which specifies which files and directories should or should not be indexed by search engines. The robots.txt file for the client’s site is accessible by appending “/robots.txt” to the end of the URL.

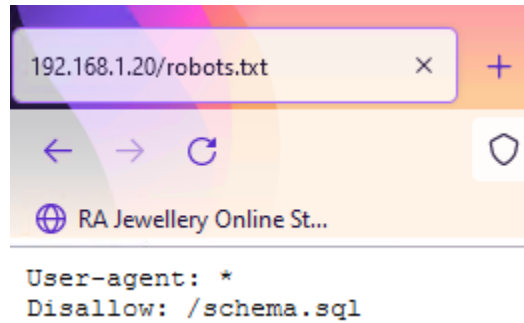


Figure 2, the robots.txt file

As can be seen above, the only disallowed page on the site currently is one entitled “schema.sql”, which when navigated to displays a plain text file with what appears to be the entire database schema for the site, which is a collection of objects associated with a database. This can be found in Appendix B.

2.1.3 Enumerate Applications on Webserver

This stage is fairly like the above fingerprinting section, whereby the tester was trying to determine what applications were present on the server, to see if there were any nonstandard ports being used etc. Because of this a similar scan was run, which can be seen in the image below.

```
root@kali:~# nmap -Pn -sT -sV -p0-65535 192.168.1.20
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2021-11-09 10:48 EST
Nmap scan report for 192.168.1.20
Host is up (0.0012s latency).
Not shown: 65532 closed ports
PORT      STATE SERVICE  VERSION
21/tcp    open  ftp      ProFTPD 1.3.4c
80/tcp    open  http     Apache httpd 2.4.29 ((Unix) OpenSSL/1.0.2n PHP/5.6.34 mod_perl/2.0.8-dev Perl/v5.16.3)
443/tcp   open  ssl/http Apache httpd 2.4.29 ((Unix) OpenSSL/1.0.2n PHP/5.6.34 mod_perl/2.0.8-dev Perl/v5.16.3)
3306/tcp  open  mysql    MariaDB (unauthorized)
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 27.02 seconds
```

Figure 3, a slightly more in-depth scan

No changes from the previous scan were detected despite the fact the scope of this scan was much wider, as a result the tester can say with a high degree of confidence that these are the only external services running on the web host server.

2.1.4 Review Webpage Content for Information Leakage

In some instances, web developers may accidentally leave comments and metadata on their projects that describe the inner workings of the project in more detail than perhaps is necessary or good from a security standpoint. Commenting code (for example) is best practise in many cases, however leaving them up publicly can cause some serious harm, this section is concerned with finding such pieces of code.

To search more efficiently here and throughout this section, the tester made use of a tool called HTTCCrack, which allowed them to download the entire user-viewable codebase of the site and view it in a code editor of their choice.

In this case, an apparent issue is that, when logged in, a User ID number and a “code”, which appears to be relevant session identification number that could possibly link into a later section of the test, is visible in the top left-hand corner of the page. This appears to be because in the source for the page these values are stored at the top, outside of the HTML tags, but still are displayed.



Figure 4, user ID and code as displayed on the site

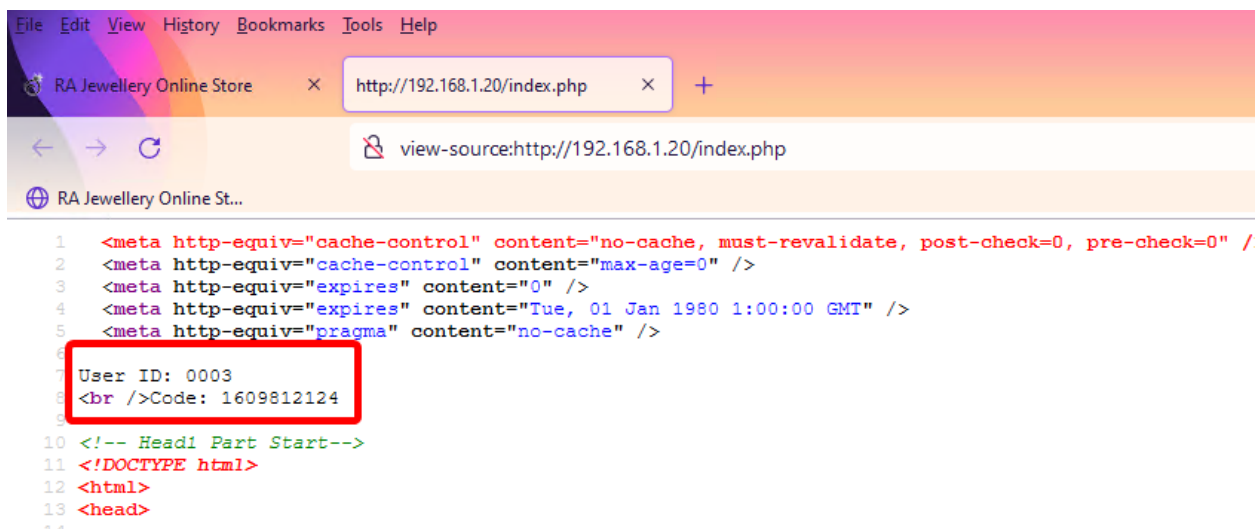


Figure 5, Similar values as seen in the source for the page

2.1.5 Identify Application Entry Points

During testing for this stage, it was necessary to gain information about all the entry points to the application, i.e., places in which it is possible to enter user data. In order to enumerate these input forms the tester conducted a manual search of the site. The places found by the tester where this is possible is as follows:

- Prior to Login:
 - Login Prompt:
 - Username
 - Password
 - Sign Up page:
 - Name
 - Surname
 - Username
 - Password

- Re-Password
- Email
- Billing Address
- Telephone
- Search Bar
- Post-Login
 - Change Profile
 - Name
 - Surname
 - Email
 - Billing Address
 - Telephone
 - View Products
 - Enter Quantity
 - Checkout
 - Credit Card

In addition to this, the standard purchasing procedure, as well as the login procedure, were both analysed using the network view in Firefox for POST and GET requests being served to the server. These requests are an essential part of web communication as they allow data to be transferred between the client and server devices, nothing out of the ordinary was found in this section.

2.1.6 Map Execution Paths Through Application

To understand the structure of the site and gain a full understanding of it, it was necessary to map it out. This was done through the usage of the OWASP Zap tool. This tool allows the user to find a full list of URLs associated with a specific domain, in our case <http://192.168.1.20>, using an inbuilt spidering tool. The tool found 456 URLs, which can be found in their entirety in Appendix B. In addition to this, a full report generated by the scan can be found in Appendix D

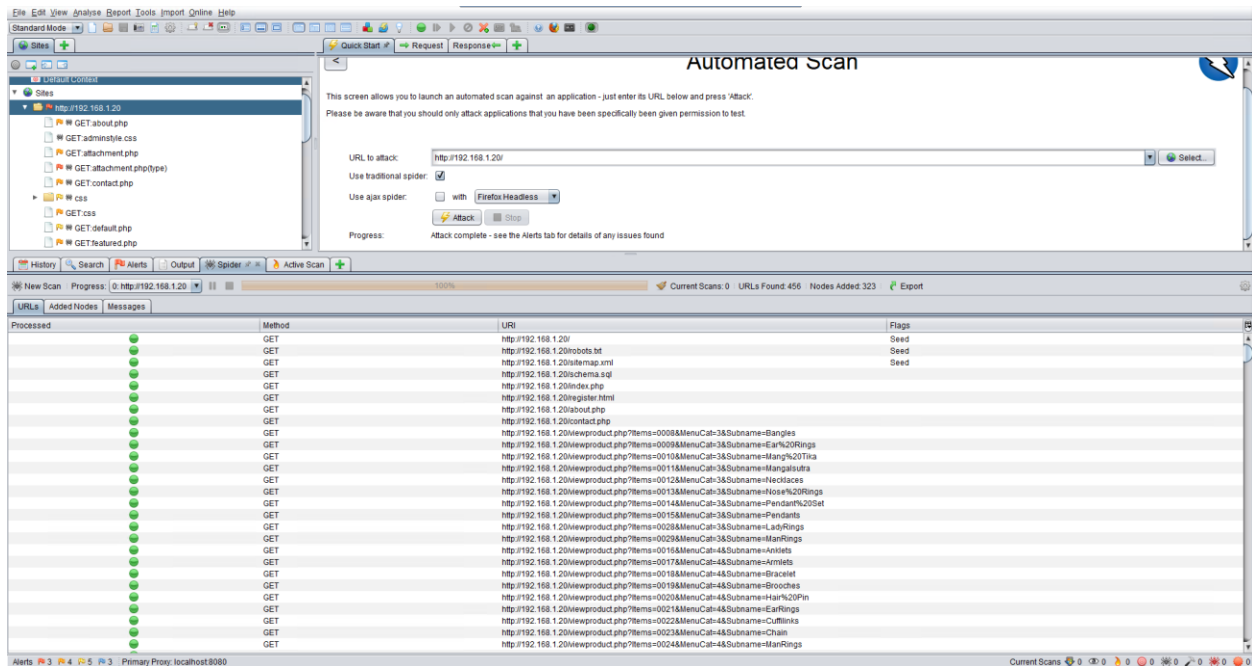


Figure 6, OWASP ZAP after use against the site

After this the tester conducted a brute force attack to further enumerate any possible hidden file, folders, URLs, and other elements within the scope of the site. The tester made use of two tools, Dirb and Nikto, the former is a shortened form of “dirbuster” which enumerates the files and folders etc, and the latter is a tool that discovers vulnerabilities on the server but is being used in this instance to provide wider coverage. The full results of this scan can be found in Appendix C sections 1 and 2 respectively.

```

— Scanning URL: http://192.168.1.20/ —
+ http://192.168.1.20/cgi-bin/ (CODE:403|SIZE:1038)
=> DIRECTORY: http://192.168.1.20/contact/
=> DIRECTORY: http://192.168.1.20/css/
=> DIRECTORY: http://192.168.1.20/font/
=> DIRECTORY: http://192.168.1.20/image/
=> DIRECTORY: http://192.168.1.20/includes/
+ http://192.168.1.20/index.php (CODE:200|SIZE:16618)
=> DIRECTORY: http://192.168.1.20/js/
+ http://192.168.1.20/phpinfo.php (CODE:200|SIZE:98418)
+ http://192.168.1.20/phpmyadmin (CODE:403|SIZE:1193)
=> DIRECTORY: http://192.168.1.20/pics/

```

Figure 7, Start section of dirb scan

2.1.7 Fingerprint Web Application Framework

A crucial step in the penetration testing process is fingerprinting the target, that is the process by which information is collected about the target system. Through the usage of the curl command the tester was able to determine issues within the framework, crucially the presence of the X-Powered-By header, which reveals the configuration of the server (seen in the figure below)

```

* Trying 192.168.1.20:80 ...
* Connected to 192.168.1.20 (192.168.1.20) port 80 (#0)
> GET / HTTP/1.1
> Host: 192.168.1.20
> User-Agent: curl/7.74.0
> Accept: */*
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 200 OK
< Date: Sun, 21 Nov 2021 16:51:45 GMT
< Server: Apache/2.4.29 (Unix) OpenSSL/1.0.2n PHP/5.6.34 mod_perl/2.0.8-dev Perl/v5.16.3
< X-Powered-By: PHP/5.6.34
< Set-Cookie: PHPSESSID=ogihv0m6252ic1hv1qljr6ku80; path=/
< Expires: Thu, 19 Nov 1981 08:52:00 GMT
< Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
< Pragma: no-cache
< Transfer-Encoding: chunked
< Content-Type: text/html; charset=UTF-8
<

```

Figure 8, curl being used to capture some headers, including x-powered-by

In addition to this, the previously-ran Nikto scan (seen in Appendix C) reveals other issues, the lack of X-XSS-Protection, X-Content-Type-Options, and anti-clickjacking headers, amongst other issues.

```
+ Server: Apache/2.4.29 (Unix) OpenSSL/1.0.2n PHP/5.6.34 mod_perl/2.0.8-dev Perl/v5.16.3
+ Retrieved x-powered-by header: PHP/5.6.34
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
```

Figure 9, results of Nikto scan showing lack of crucial headers

Additionally, the tester made use of the whatweb tool, designed to identify services running for a website, this revealed the site is running JQuery 1.7.1, OpenSSL 1.0.2n, PHP 5.6.34, and Perl 5.16.3, amongst some other information. The screenshot showing this can be seen below.

```
root@kali:~/Documents/ConsoleOutputs# whatweb 192.168.1.20
http://192.168.1.20 [200 OK] Apache[2.4.29][mod_perl/2.0.8-dev], Cookies[PHPSESSID], Country[RESERVED][22], HTML5, HTTPServer[Unix][Apache/2.4.29 (Unix) OpenSSL/1.0.2n PHP/5.6.34 mod_perl/2.0.8-dev Perl/v5.16.3], IP[192.168.1.20], JQuery[1.7.1], OpenSSL[1.0.2n], PHP[5.6.34], Perl[5.16.3], Script[javascript,text/javascript], Title[RA Jewellery Online Store], X-Powered-By[PHP/5.6.34]
root@kali:~/Documents/ConsoleOutputs#
```

Figure 10, Whatweb Scan

Index of /css



<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 Parent Directory		-	
 bootstrap.css	2013-07-21 21:11	122K	
 carousel.css	2013-08-02 09:32	2.5K	
 flexslider.css	2013-08-02 09:32	3.2K	
 jquery.fancybox.css	2013-08-02 09:32	4.1K	
 slideshow.html	2013-08-09 20:57	360	
 stylesheet-1.css	2017-08-05 19:45	58K	
 stylesheet-2.css	2013-08-04 08:29	58K	
 stylesheet-3.css	2013-08-04 08:29	58K	
 stylesheet-4.css	2013-08-04 08:29	58K	
 stylesheet.css	2017-08-05 19:50	29K	

Figure 12, Index of /css/ directory

Index of /includes





<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 Parent Directory		-	
 config.php	2021-09-26 19:54	383	
 connection.php	2021-09-26 19:54	1.6K	
 mysqli_connection.php	2021-09-26 19:54	257	

Figure 13, Index of /includes/ directory

Index of /icons































Name	Last modified	Size	Description
 Parent Directory		-	
 a.gif	2004-11-20 15:16	246	
 a.png	2007-09-11 01:11	306	
 alert.black.gif	2004-11-20 15:16	242	
 alert.black.png	2007-09-11 01:11	293	
 alert.red.gif	2004-11-20 15:16	247	
 alert.red.png	2007-09-11 01:11	314	
 apache_pb.gif	2013-05-04 08:52	4.4K	
 apache_pb.png	2012-10-03 08:35	9.5K	
 apache_pb.svg	2012-10-05 10:55	260K	
 apache_pb2.gif	2013-05-04 08:52	4.1K	
 apache_pb2.png	2012-10-03 08:35	10K	
 back.gif	2004-11-20 15:16	216	
 back.png	2007-09-11 01:11	308	
 ball.gray.gif	2004-11-20 15:16	233	
 ball.gray.png	2007-09-11 01:11	298	
 ball.red.gif	2004-11-20 15:16	205	
 ball.red.png	2007-09-11 01:11	289	
 binary.gif	2004-11-20 15:16	246	
 binary.png	2007-09-11 01:11	310	
 binhex.gif	2004-11-20 15:16	246	
 binhex.png	2007-09-11 01:11	319	
 blank.gif	2004-11-20 15:16	148	
 blank.png	2007-09-11 01:11	215	
 bomb.gif	2004-11-20 15:16	308	
 bomb.png	2007-09-11 01:11	375	
 box1.gif	2004-11-20 15:16	251	
 box1.png	2007-08-28 06:53	325	
 box2.gif	2004-11-20 15:16	268	
 box2.png	2007-08-28 06:53	336	

Figure 14, Index of /icons/ directory (incomplete)

After the Nikto scan was performed, the tester made use of OWASP Zap to perform an “active scan” against the target, this was by way of confirming the vulnerabilities found in the Nikto scan and providing more context and information on each of the vulnerabilities found. A report generated by the tool outlining the output of this scan can be found in Appendix D.

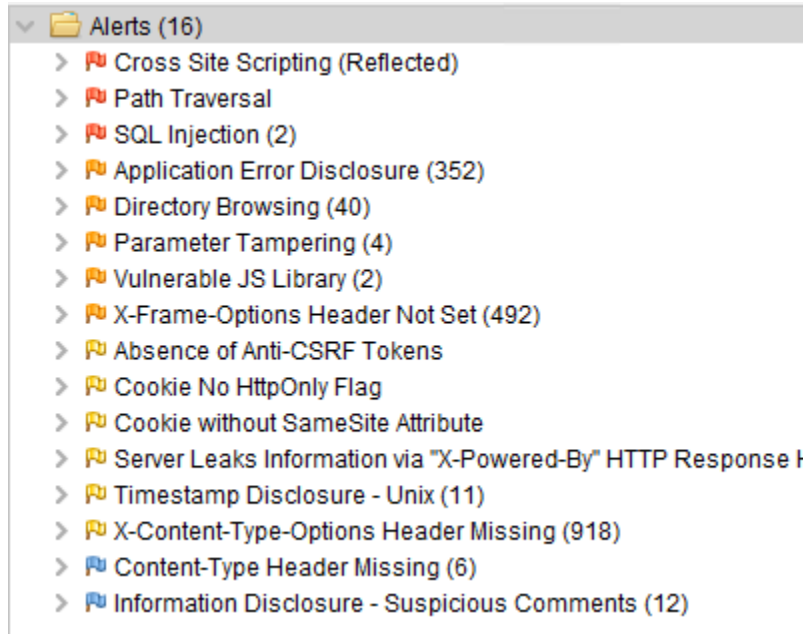


Figure 15, List of alerts generated by OWASP ZAP scan

2.2.2 Enumerate Infrastructure and Application Admin Interfaces

This section primarily concerns the presence of administrator interfaces within the web application. During this process the tester once again referenced their Dirb scan (seen in Appendix C) and discovered the presence of the /adminarea/ directory, that once navigated to displayed a full list of pages in the admin panel. In addition to this the scan also discovered a phpMyAdmin page, that is inaccessible to the tester without credentials. The tester will use this later in the exploitation stage.

The screenshot shows a web browser window displaying the 'Index of /adminarea' directory listing. The listing includes various files such as 'adminhome.php', 'adminmenu.php', 'adminstyle.css', and 'confirmcategory.php'. A terminal window in the background shows the execution of the 'dirb' command on the URL 'http://192.168.1.20'. The terminal output lists several discovered directories, including '/adminarea/', '/contact/', '/css/', and '/phpmyadmin/'. A red arrow points from the terminal output to the 'Index of /adminarea' title in the browser window.

Name	Last modified	Size	Description
Parent Directory	-	-	-
adminhome.php	2016-07-28 11:41	915	
adminmenu.php	2014-03-26 01:08	352	
adminstyle.css	2014-03-19 20:06	133	
confirmcategory.php	2014-05-18 15:38	1.3K	
confirmeditcategory.php	2016-07-28 11:41	1.3K	
confirmeditpage.php	2016-07-28 11:41	1.3K	
confirmeditprod.php	2016-07-28 11:41	1.8K	
confirmeditsubcat.php	2016-07-28 11:41	1.4K	
confirmedituser.php	2016-07-28 11:41	2.1K	
confirmprod.php	2014-05-18 16:02	1.6K	
confirmsubcat.php	2014-05-18 15:42	1.3K	
confirmuser.php	2014-05-18 15:43	1.8K	
default.php	2016-07-28 11:41	279	
delconfirm.php	2014-05-18 16:02	1.5K	
deletetcategory.php	2014-05-18 15:44	1.1K	
deletepage.php	2014-05-18 15:45	1.0K	
deleteprod.php	2014-05-18 15:45	1.1K	
deletesubcat.php	2014-05-18 15:45	1.1K	
deleteuser.php	2014-05-18 15:45	1.3K	
editcategory.php	2016-07-28 11:41	4.0K	
editpage.php	2016-07-28 11:41	3.8K	
editprod.php	2016-07-28 11:41	6.3K	
editsubcat.php	2016-07-28 11:41	4.5K	
edituser.php	2016-07-28 11:41	12K	
includes/	2021-09-26 20:02	-	
logout.php	2016-07-28 11:41	405	
newcategory.php	2016-07-28 11:41	3.3K	
newprod.php	2016-07-28 11:41	5.7K	
newsbcat.php	2016-07-28 11:41	3.8K	

```

root@kali: /usr/share/dirb/wordlists
root@kali: /usr/share/dirb/wordlists# dirb http://192.168.1.20/

DIRB v2.22
By The Dark Raver

START_TIME: Mon Nov 22 13:20:21 2021
URL_BASE: http://192.168.1.20/
WORDLIST_FILES: big.txt

GENERATED WORDS: 20458

--- Scanning URL: http://192.168.1.20/ ---
=> DIRECTORY: http://192.168.1.20/adminarea/
+ http://192.168.1.20/cgi-bin/ (CODE:403|SIZE:1038)
=> DIRECTORY: http://192.168.1.20/contact/
=> DIRECTORY: http://192.168.1.20/css/
=> DIRECTORY: http://192.168.1.20/font/
=> DIRECTORY: http://192.168.1.20/image/
=> DIRECTORY: http://192.168.1.20/includes/
=> DIRECTORY: http://192.168.1.20/js/
+ http://192.168.1.20/phpmyadmin (CODE:403|SIZE:1193)
=> DIRECTORY: http://192.168.1.20/pics/
=> DIRECTORY: http://192.168.1.20/pictures/
+ http://192.168.1.20/robots.txt (CODE:200|SIZE:36)

--- Entering directory: http://192.168.1.20/adminarea/ ---
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

--- Entering directory: http://192.168.1.20/contact/ ---
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

--- Entering directory: http://192.168.1.20/css/ ---
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    
```

Figure 16, admin panel area discovered by dirb

2.2.3 Test HTTP Strict Transport Security

HTTP Strict Transport Security, also known as HSTS, is a mechanism that prevents against man in the middle attacks (amongst other forms of attack) by specifying that a user should never be able to connect to the web server without using a secure connection (i.e., HTTPS). If this is not present on a server it is possible for an attacker to steal data from a user by monitoring unencrypted traffic to and from the client and server, this could result in a malicious actor gaining access to a user's credentials, payment info, etc.

The test for this is simple, issuing a command against the server that checks to see if the HSTS header is present, as can be seen in the screenshot below. If the command returns nothing then the server is insecure.

```
root@kali:~/Documents/ConsoleOutputs# curl -s -D- 192.168.1.20 | grep -i strict  
root@kali:~/Documents/ConsoleOutputs# █
```

Figure 17, the command issued, showing that the server is indeed insecure in this way

2.3 IDENTITY MANAGEMENT TESTING

2.3.1 Test Role Definitions

In the OWASP Methodology several user role types are defined, these are

- An Administrator
- An Auditor
- A Support Engineer
- A Customer (standard user)

Using the tool sqlmap it was possible to enumerate the presence of four separate administrator role types in addition to the standard user type which was determined to exist by virtue of the lack of access allowed by the standard user given to /adminarea/ files.

After determining the existence of an admin role on the server and subsequently gaining persistent access to admin functionality on one of the users accounts the tester has control of in a later section, the tester then proceeded to review the permissions afforded to them as an admin.

Also as mentioned previously, the passwords for each of the user accounts, including admin accounts, are stored in plaintext and viewable through a panel available to admin users. This is beyond the scope of what is reasonable for an Admin to have access to and helps a prospective attacker in being able to access all accounts on the server.

ID	First Name	Last Name	Username	Password	Email	Address	Tel	Acc Type	Status		
0001	Ian	Ferguson	ianf	12345	if@yahoo.com	Montagne Blanche	54954491	user	1	Edit	Delete
0002	Benny	Hill	admin	june	admin@hacklabmadeup.com	Montagne Blanche	54954491	Administrator	0	Edit	Delete
0003	Steve	Brown	hacklab	hacklab	hacklab@hacklab.com	1 Bell Street	59999995	Administrator	0	Edit	Delete
0005	Tom	Smith	tsmith	hacklab	tsmith@hacklab.com	1 wewer we w	12312312	user	1	Edit	Delete
0006	Isaac	Basque-Rice	IBRice101	password	1901124@uad.ac.uk	1 Bell Street	12345678	user	1	Edit	Delete
0009	a	a	a	aaaaa	a	a	11111111	user	1	Edit	Delete

Figure 18, the user database as seen in the adminarea page, with the column showing user passwords in plaintext highlighted

In addition to this, the tester is able to edit and delete content from the website at will with no Multi Factor Authentication required, this can be seen in the figure below when the tester edited the price of a diamond bangle from 1000Rs to 1Rs.

EDIT PRODUCT PAGE

| [Home](#) | [Products](#) | [Categories](#) | [Sub Categories](#) | [Users](#) | | [PAGE](#) |

ID : 0001	
Name	<input type="text" value="Diamond/Bangles/1.jpg"/>
Path	<input type="text" value="Diamond/Bangles/1.jpg"/>
Category	<input type="text" value="1"/>
Price	<input type="text" value="1.00"/>
Description	<input type="text" value="Diamond Carte:20"/>
Type	<input type="text" value="latest"/>
Views	<input type="text" value="14"/>

Figure 19, the edit product form


ID	JEWELLERY NAME	IMAGE PAGE	CATEGORY	PRICE	DESCRIPTION	TYPE	VIEWS	IMAGE		
0001	Diamond/Bangles/1.jpg	Diamond/Bangles/1.jpg	1	1.00	Diamond Carte:20	latest	14		Edit	Delete

Figure 20, the cost of the bangle after the changes

2.3.2 Test User Registration Process

The process of validating users on registration is crucial for the usability of a web application. In the case of the target, the submission of user information is validated on a purely automated basis due to the projected size of the user base, and as such is possibly open to a variety of issues to do with misconfiguration. This section primarily regards issues around proof of user identification, with issues around user input (SQL injection and cross site scripting, for example, are covered in a subsequent section).

The first test the tester undertook was to check if the same user could register multiple times with the same credentials, the credentials the tester used were as follows:

- Name: Isaac
- Surname: Basque-Rice
- Username: IBRice101

- Password: password
- Email: 1901124@uad.ac.uk
- Billing Address: 1 Bell Street, Dundee
- Telephone: 07123456

Users Registration Form

Name	Isaac
Surname	Basque-Rice
Username	IBRice101
Password	●●●●●●●●
Re-Password	●●●●●●●●
Email	1901124@uad.ac.uk
Billing Address	1 Bell Street, Dundee
Telephone	07123456

Submit

Reset Form

[Home Page](#)

Figure 21, the user registration form on the site with credentials filled out

Initial registration with these credentials was successful which was concerning for two main reasons, which are as follows.

Firstly, the password policy on this site is extremely relaxed, best practise is to make users input passwords that met certain criteria (a minimum character length, upper- and lower-case letters, numbers, symbols, etc) to ensure user security, being able to successfully use “password”, all lower case, with no extra symbols, is concerning from this perspective.

Secondly, there is no form of user identity validation present on the site, the email address the tester inputted is valid and yet there was seemingly no check to confirm this beyond whether the email was already in the database.

it is not possible through the user interface to register for different roles or permissions (I.e., Admin roles etc), which is best practise.

The tester attempted to sign up again using the exact same credentials, however this was to no avail as there is a check present on the backend to see whether users are reusing an already

existing address email address, the tester then returned to the registration page to check whether the same credentials with a different, invalid email address worked (replaced 1901124@uad.ac.uk with “saasdads”), which was successful. This hints an utter lack of form validation, which the tester will make use of in later stages of the test.

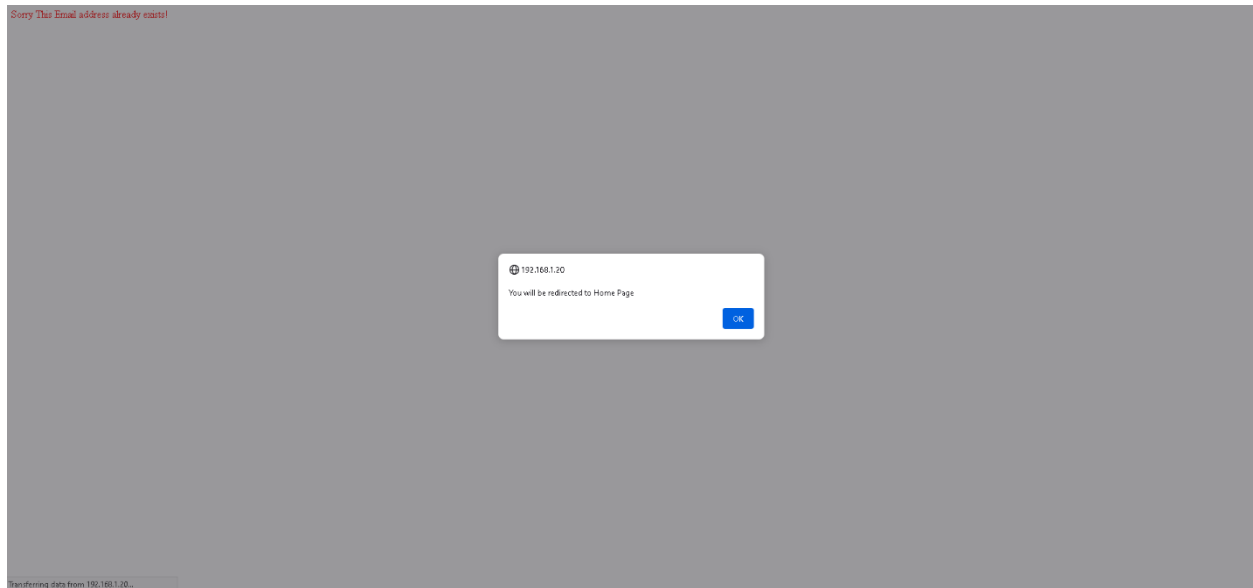


Figure 22, page that shows that an account with that email address already exists

2.3.3 Testing for Weak or Unenforced Username Policy

When creating a new user there is no visible prompt informing the user that there are restrictions on user input. As a result of this the tester decided to create a new user account with the following credentials:

Name – “a”

Surname – “a”

Username – “a”

Password – “aaaaa” (note: a popup occurs if password is shorter than 5 characters, this is covered in section 2.4.4)

Email – “a”

Billing Address – “a”

Telephone – “11111111”

As can be seen in the figure below, this account creation process was successful, as the tester was able to successfully log in to the “a” account.



Figure 23, the top right hand corner of the site when the A user is logged in

2.4 AUTHENTICATION TESTING

2.4.1 Testing for Credentials Transported over Unencrypted Channels

Sending sensitive information, such as credentials, over channels that are not encrypted is very ill-advised. A cursory glance at the website lets the tester know that this is occurring in this case, as the URL for all pages of the site are prefixed with “http” as opposed to “https”, the latter being the secure version of the former. The tester can also see this by the crossed padlock icon to the left of the URL address bar in Firefox.

At this stage, the tester thought it best to test the application to see the scale of the issue. They first made use of curl to test the login area of the site, the output of this scan can be seen below. The -kis flag allows for insecure connection, includes HTTP response headers in the output, and does not show progress or error messages.

```
root@kali:~/Documents/ConsoleOutputs# curl -kis http://192.168.1.20/login.php
HTTP/1.1 200 OK
Date: Wed, 24 Nov 2021 14:07:06 GMT
Server: Apache/2.4.29 (Unix) OpenSSL/1.0.2n PHP/5.6.34 mod_perl/2.0.8-dev Perl/v5.16.3
X-Powered-By: PHP/5.6.34
Set-Cookie: PHPSESSID=5cgnje0poi0adup0qp6mn3rop1; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Content-Length: 1222
Content-Type: text/html; charset=UTF-8
```

Figure 24, headers found on the login page

Note the presence of the unencrypted PHPSESSID, and the lack of the secure flag permitting it only to be transported over an SSL connection. This allows for users’ sessions to be hijacked and data to be stolen.

In addition to this, during the login process the tester noted in the console output pane of the F12 developer panel in Firefox a set of request cookies, the aforementioned PHPSESSID token, as well as a cookie called “SecretCookie” as can be seen in the figure below.

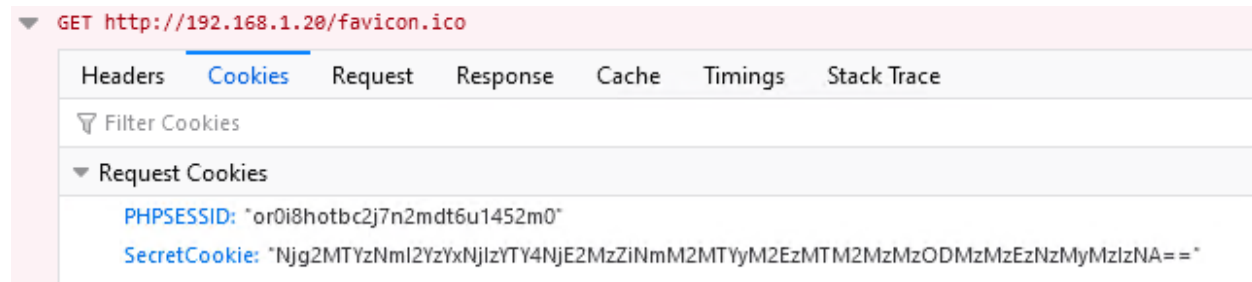


Figure 25, Cookie menu after login with hacklab/hacklab account

2.4.2 Testing for Default Credentials

In many cases when developers create a website, they create default login credentials that are trivially guessable. In his case when the tester tested for default creds they used four standard usernames with the same input in the password field, which were as follows.

- test/test
- user/user
- admin/admin
- rick/rick

Three of the inputs returned the error message “Username Not Found!”, which means that the username was not in the database on the backend, however one username, “admin”, did not return this error, instead returning “password not found”, implying the existence of an admin account with that name.



Figure 26, Username not found

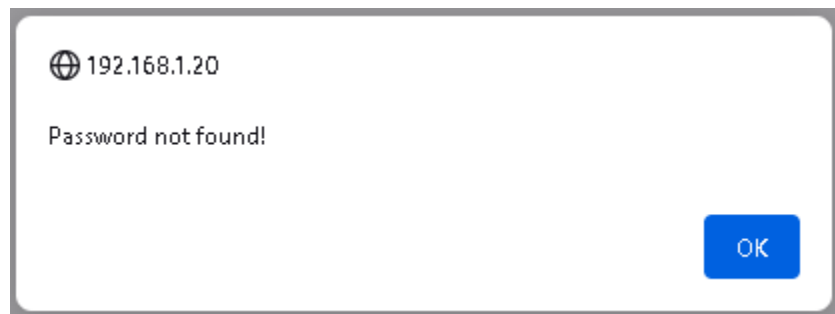


Figure 27, Password not found

In addition to the admin/admin combination, the tester attempted to input other standard default password values, these were “password”, “pass123”, “password123”, “test”, and “guest”, amongst other variants. None of these were successful however they did reveal a weakness with regards to a lack of rate limiting, which this report will go over in the next section.

2.4.3 Testing for Weak Lock Out Mechanism

Account lockout mechanisms are systems by which brute force attacks are mitigated, the concept is similar to rate limiting in other aspects of other applications whereby if a certain

number of wrong attempts to submit user info to the login form have been attempted, said user will be locked out for a certain amount of time.

The idea behind this is that if an account is being brute forced there will be multiple requests to log in in a short period of time. Typically, accounts are locked out after 3-5 unsuccessful attempts.

The tester made use of their previously created account, IBRice101 for this portion of the test. Knowing that the password was "password", the tester attempted to login to their account using a random combination of keypresses 5 times in approximately 1 minute, they were not rate limited.

After this, the tester logged in successfully with their normal credentials, thereby demonstrating that there is no lockout mechanism present.

2.4.4 Testing for Weak Password Policy

As can be seen in the screenshot below, passwords in his instance do have minimum length of 5 characters, however the password input field in the signup page has an upper limit of 10 characters available.

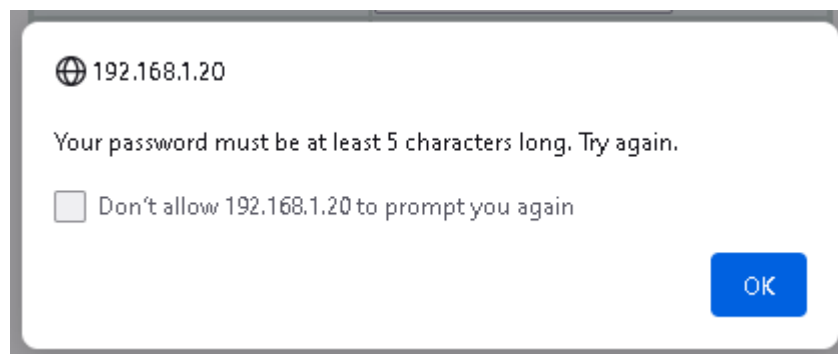


Figure 28, the minimum password length alert

In addition to this, as has been determined in a previous section (2.3.2), there are no limits to speak of with regards to required characters. From this we can determine the password policy is as follows

- Between 5-10 Characters
- Does not have to contain special characters (\$, %, !, £, etc)
- Does not have to contain uppercase characters
- Does not have to contain numbers

In mitigating a brute force attack none of these policy points are advisable for several reasons. Primarily, the presence of a maximum possible password length necessarily means the presence of a maximum possible password hash size, which results in an attacker knowing there is a finite number of hashes available for them to attempt to crack.

Isaac Basque-Rice

In addition to this, the fact that users can use a single-word password could result in even the most basic of dictionary-based attacks being successful against this target, rendering the need to crack hashes non-existent in this case.

2.5 AUTHORISATION TESTING

2.5.1 Testing Directory Traversal File Include

As previously seen, file traversal is possible in this application. By navigating to a known directory without an index page, such as /adminarea/, the tester was able to view the entire contents of that directory, including links to other directories and admin pages, as can be seen in the figure below.































Index of /adminarea		
<u>Name</u>	<u>Last modified</u>	<u>Size</u>
 Parent Directory		-
 adminhome.php	2016-07-28 11:41	915
 adminmenu.php	2014-03-26 01:08	352
 adminstyle.css	2014-03-19 20:06	133
 confirmcategory.php	2014-05-18 15:38	1.3K
 confirmitcategory.php	2016-07-28 11:41	1.3K
 confirmitpage.php	2016-07-28 11:41	1.3K
 confirmitprod.php	2016-07-28 11:41	1.8K
 confirmitsubcat.php	2016-07-28 11:41	1.4K
 confirmituser.php	2016-07-28 11:41	2.1K
 confirmprod.php	2014-05-18 16:02	1.6K
 confirmsubcat.php	2014-05-18 15:42	1.3K
 confirmuser.php	2014-05-18 15:43	1.8K
 default.php	2016-07-28 11:41	279
 delconfirm.php	2014-05-18 16:02	1.5K
 deletcategory.php	2014-05-18 15:44	1.1K
 deletpage.php	2014-05-18 15:45	1.0K
 deletprod.php	2014-05-18 15:45	1.1K
 deletesubcat.php	2014-05-18 15:45	1.1K
 deleteuser.php	2014-05-18 15:45	1.3K
 editcategory.php	2016-07-28 11:41	4.0K
 editpage.php	2016-07-28 11:41	3.8K
 editprod.php	2016-07-28 11:41	6.3K
 editsubcat.php	2016-07-28 11:41	4.5K
 edituser.php	2016-07-28 11:41	12K
 includes/	2021-09-26 20:02	-
 logout.php	2016-07-28 11:41	405
 newcategory.php	2016-07-28 11:41	3.3K
 newprod.php	2016-07-28 11:41	5.7K
 newsbcat.php	2016-07-28 11:41	3.8K

Figure 29, adminarea directory

2.6 SESSION MANAGEMENT TESTING

2.6.1 Testing for Session Management Schema

As can be seen in section 2.4.1, a secret cookie is initialised for each unique user, and due to the unencrypted channel that the website is using (HTTP), this cookie was visible to the tester using the Developer Tools menu. The tester recognised this cookie as containing a Base64 encoded value. This value was decoded into a Hex value by the CyberChef online tool (as can be seen in the below figure), which was further decoded to a plaintext value displaying the user's username, password, and third value that this paper will cover in the following section. This test was performed against another account with the same result.

The screenshot shows the CyberChef interface with the following details:

- Recipe:** From Base64, Alphabet: A-Za-z0-9+/, Remove non-alphabet chars (checked).
- From Hex:** Delimiter: Auto.
- Input:** Njg2MTYzNmI2YzYxNjIzYTU4NjE2MzZiNmM2MTYyM2EzMTM2MzZODMzEzNTMxMzAzMg==
NDk0MjUyNjIzYzY1MzEzMDMxM2E3MjYxNzIzMTMzZ3NmY3MjY0M2EzMTM2MzZODMzEzNTMzZzQzMA==
- Output:** start: 25, end: 25, length: 95, time: 2ms, lines: 1
hacklab:hacklab:1638315102IBRice101:password:1638315340
- Buttons:** STEP, BAKE!, Auto Bake.

Figure 30, CyberChef Input and Output for both registered user accounts, showing passwords in plaintext

2.6.2 Testing for Cookies Attributes

As seen in multiple previous sections, the protocol the website uses is HTTP as opposed to the more secure HTTPS. As a result of this any cookies the site uses for authentication or other miscellaneous uses are exposed and viewable in any given session.

As can be seen in the previous section, the decoded value of the SecretCookie is a triplet of values separated by a colon. The third value (after the Username and Password) is a Unix timestamp which shows the time the user logged in.

Convert epoch to human-readable date and vice versa

1638375177

Timestamp to Human date [batch convert]

Supports Unix timestamps in seconds, milliseconds, microseconds and nanoseconds.

Assuming that this timestamp is in **seconds**:

GMT : Wednesday, December 1, 2021 4:12:57 PM

Your time zone : Wednesday, December 1, 2021 4:12:57 PM GMT+00:00

Relative : A minute ago

Figure 31, third value of the triplet put through an epoch converter, showing the time the user logged in

2.6.3 Testing for Session Fixation

To test for Session Fixation, the tester the tester first authenticated using the hacklab account in a Firefox pane, they then grabbed both values and logged in to the IBRice101 account in OWASP Mantra, where they could make use of the Cookies Manager+ feature to change the cookie values they were given in the authentication process for that account to the cookies given in the hacklab authentication process. This resulted in session hijacking, where the tester was able to switch accounts without going through the proper authentication channels, this process can be seen in the screenshots below.

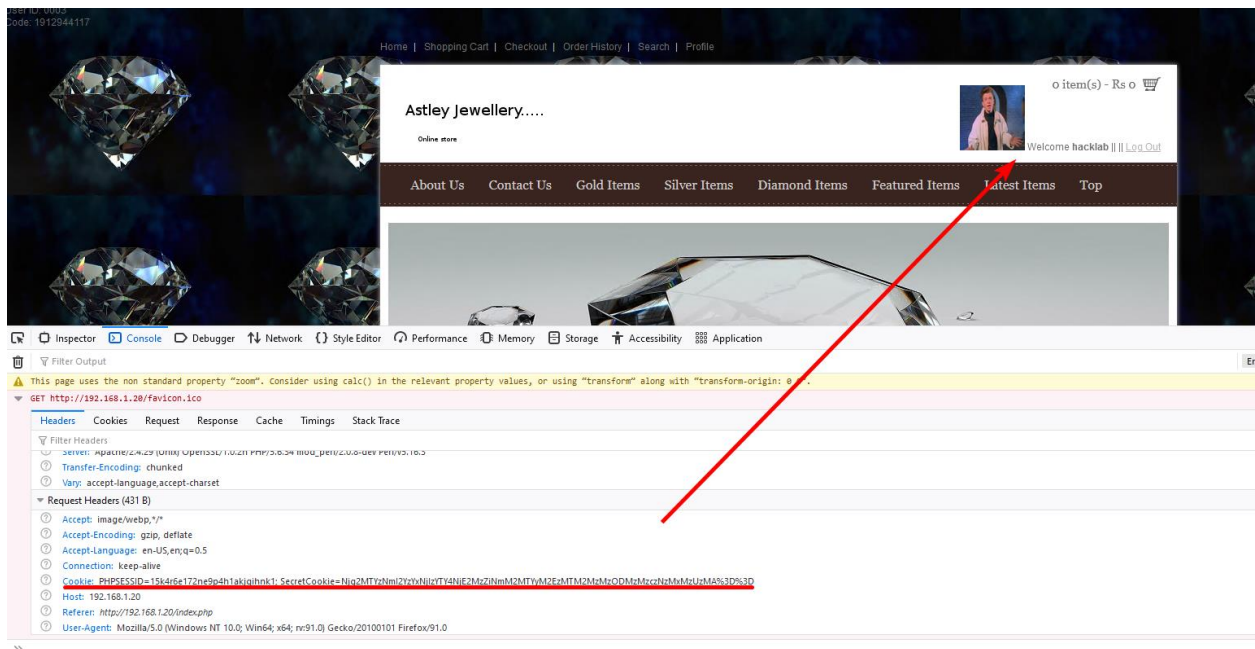


Figure 32, Step 1, grabbing cookie values for Hacklab account in Firefox

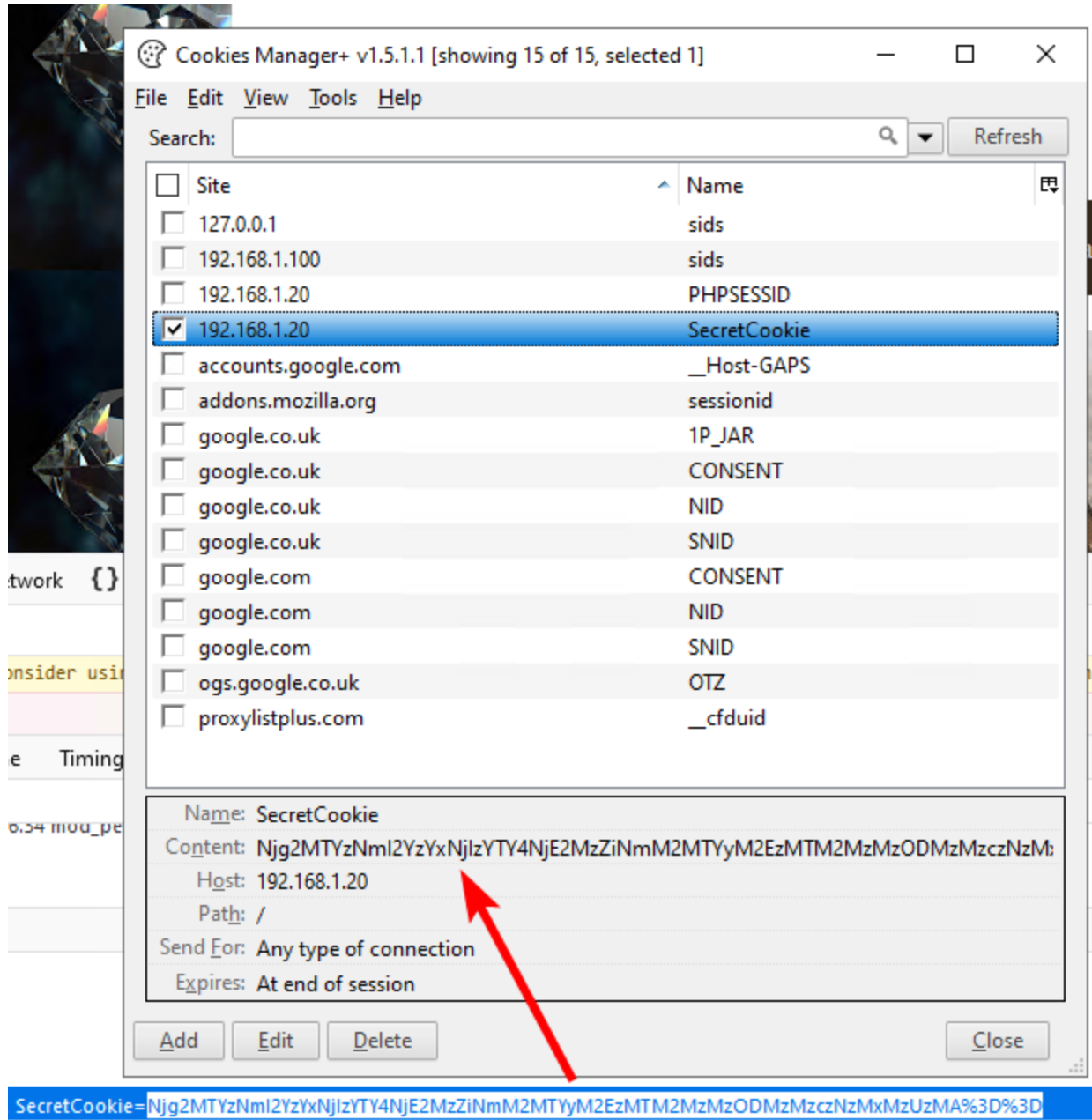


Figure 33, Step 2, copying cookie values into Cookies Manager+

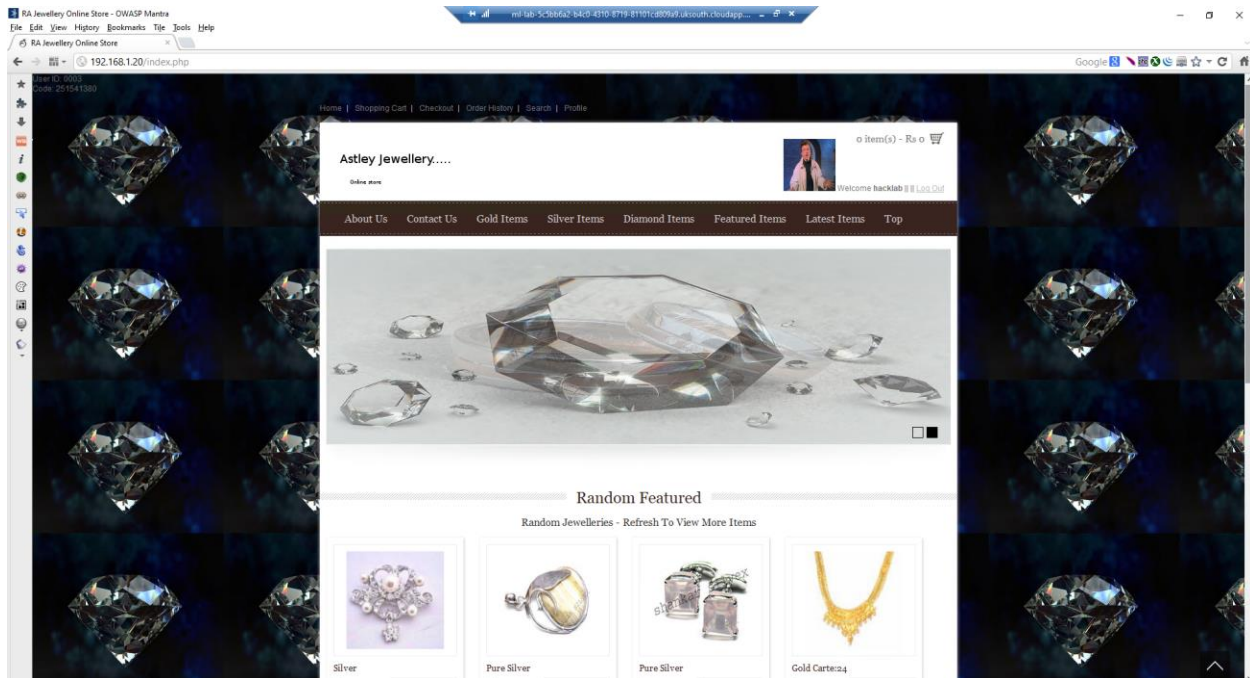


Figure 34, Step 3, Authentication as hacklab account in Mantra (after reload)

2.6.4 Testing for Logout Functionality

To test for Server-Side session termination, the tester first logged in using their “hacklab” account and then navigated to a page that they could both log out from directly and that they knew was only accessible to logged in users. The page they chose for this was an “add to cart” page for a gold necklace. As can be seen in the figure below it was possible to return to this page from a non-authenticated user’s view, meaning the login session was not adequately terminated.

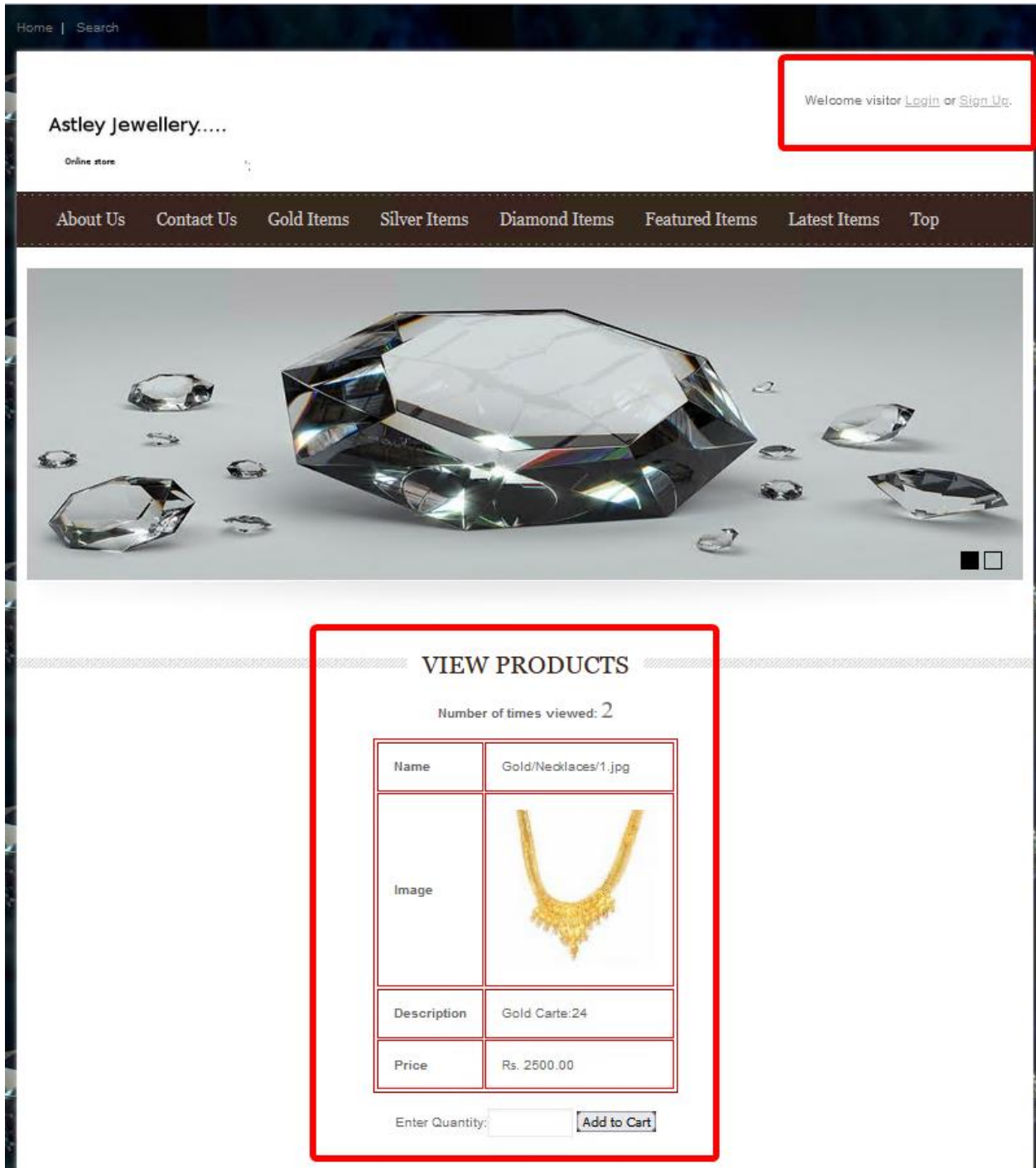


Figure 35, the user was not authenticated but managed to return to a page that required authentication.

2.7 INPUT VALIDATION TESTING

2.7.1 Testing for Reflected Cross Site Scripting

The previously conducted OWASP ZAP test had concluded that the target application was vulnerable to a cross site scripting (XSS) attack. This form of attack is a code injection attack where arbitrary browser executable code is “injected” into a user input field (or other user-accessible sections) of an application. A Reflected XSS attack, also known as a non-persistent XSS, is delivered, and executed in the same motion.

As can be seen in the figure below, a standard XSS test was performed against the target. This test is performed by placing “`<script>alert(1);</script>`” into a target text field, if an alert box containing the “1” character pops up on submission then the user input is taken literally and as such the page is vulnerable to XSS. The test was performed against multiple fields in the site, where multiple input boxes, including login and search functions, that accepted arbitrary input (i.e., not numbers only) were found to be vulnerable. The result below is from testing the search function with the input `<script>alert("XSS (Search)")</script>`.

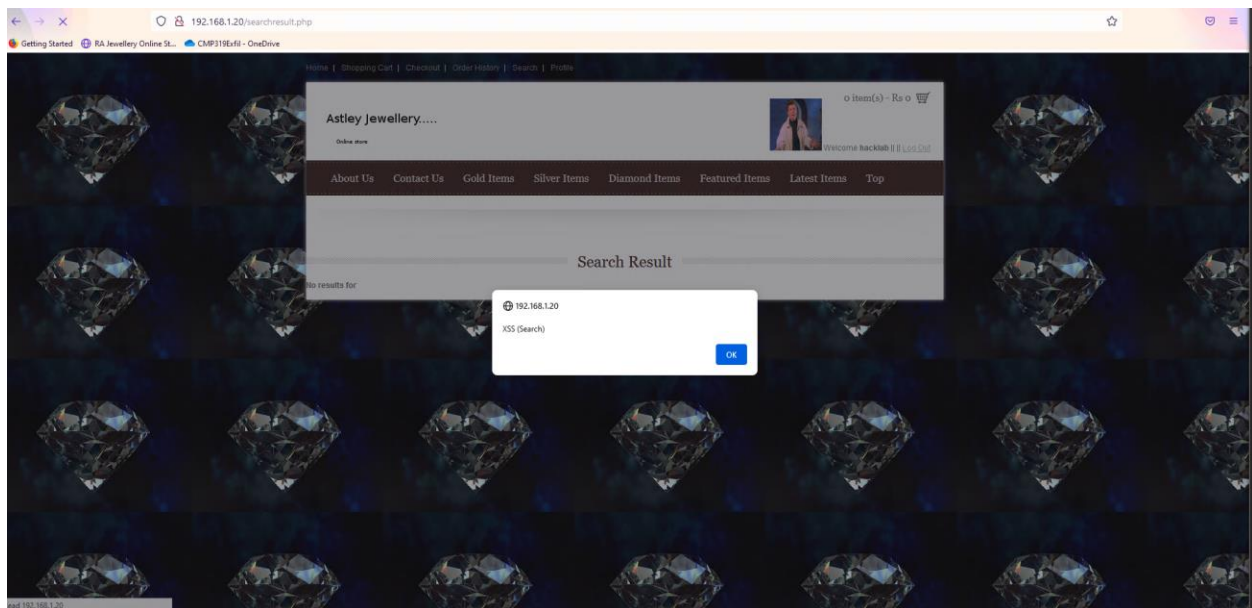


Figure 36, Successful XSS test

2.7.2 Testing for Stored Cross Site Scripting

An application is vulnerable to Stored XSS when an input field that is also vulnerable to XSS allows the user to store data that has been inputted into a database. For this target the tester created a new account whereby each field that they could enter the required text into (Name and Surname, Email, and Billing address) was filled with a payload like the ones in the previous section.

After gaining access to the admin panel (the process of which is described in the following section), the tester was able to view the list of user accounts on the system, including the XSS

exploiting account. The results, shown in the figure below, display clearly that Stored XSS is possible in this application.

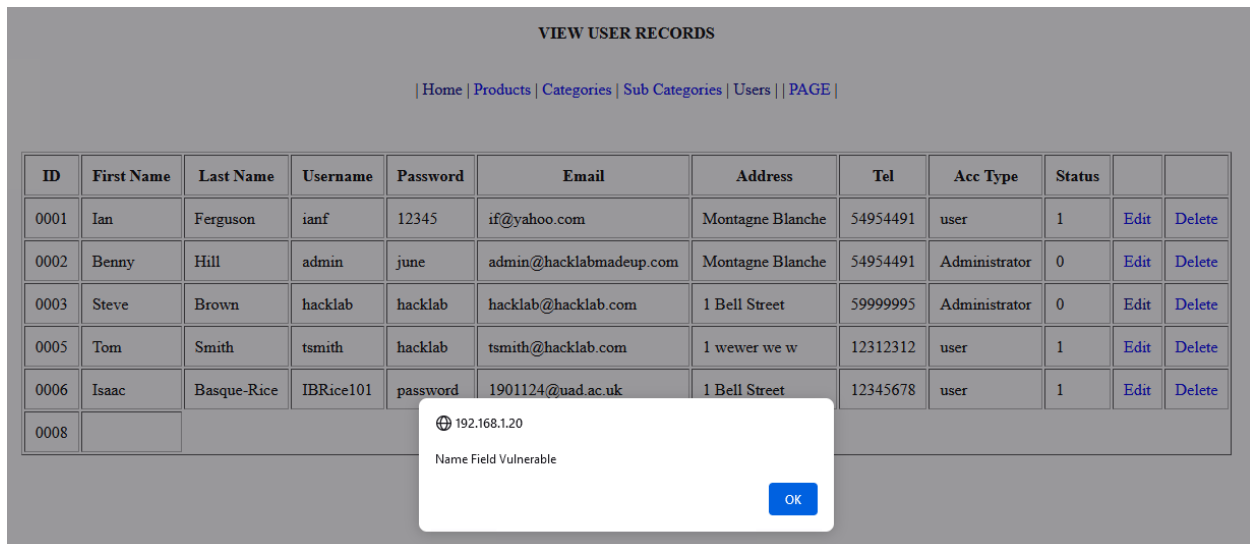


Figure 37, User Records table with a stored XSS vulnerability

2.7.3 Testing for SQL Injection

When standard SQLi input (' OR 1=1;--') is attempted against the login system, the following error is thrown:

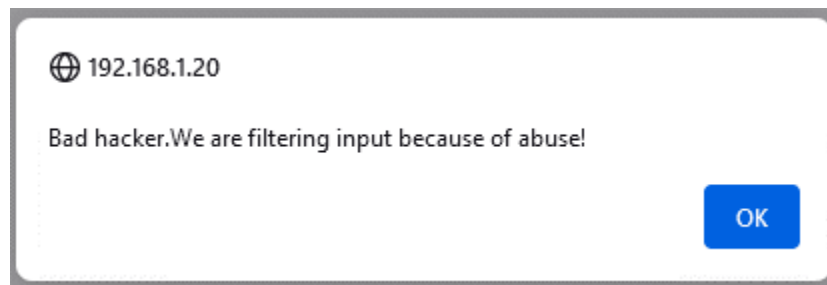


Figure 38, Error after SQLi input

From this the tester assumed due to the insecure nature of the remainder of the site, the fact the error message was non-standard and therefore likely human written, and the simple method of SQLi attempted, meant that there was most likely a SQLi filter somewhere in the backend for the site. To combat this, after trial and error, the tester crafted an SQL query designed specifically to overcome the filter.

This query, ') or 'test'='test';--, was created by first assuming the filter was a PHP statement whereby the content of the filter (1=1, amongst others) was enclosed in single quotes and parentheses,, what followed after that was a standard SQL injection attack, which granted the tester access on an admin level to the target application, as can be seen from the figures below.

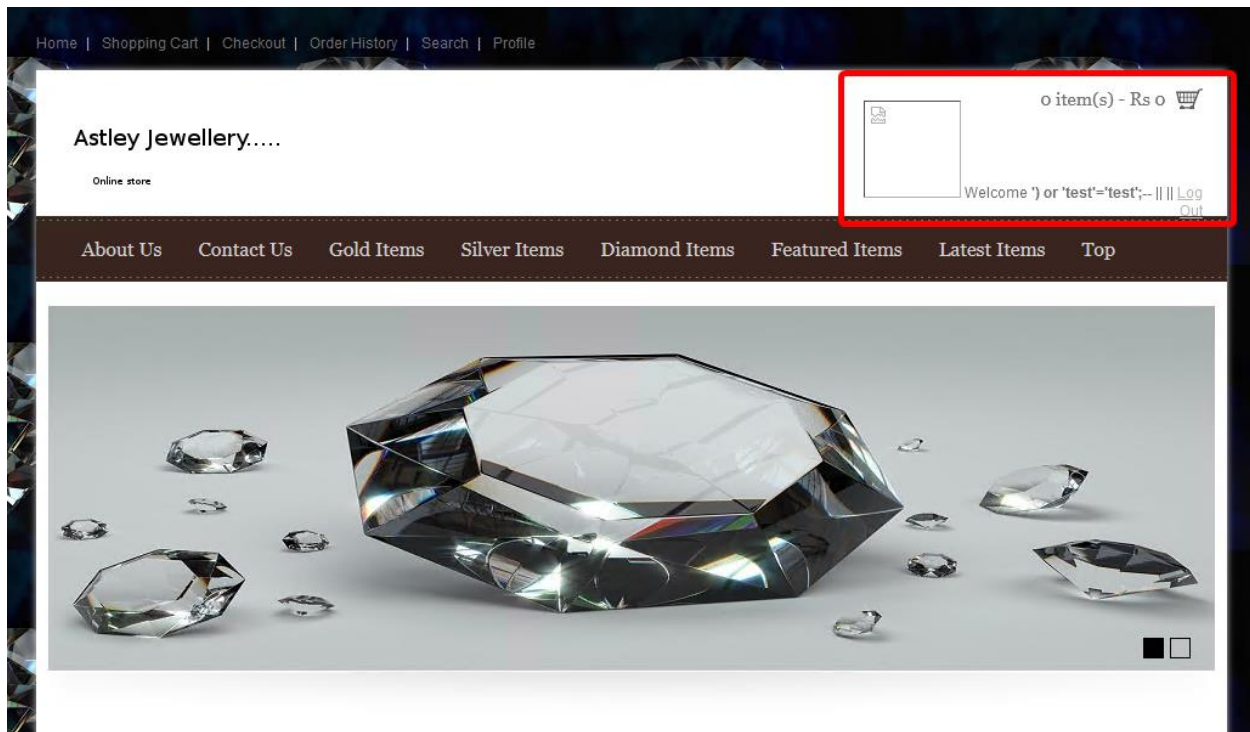


Figure 39, the tester logged in using a bogus SQL query

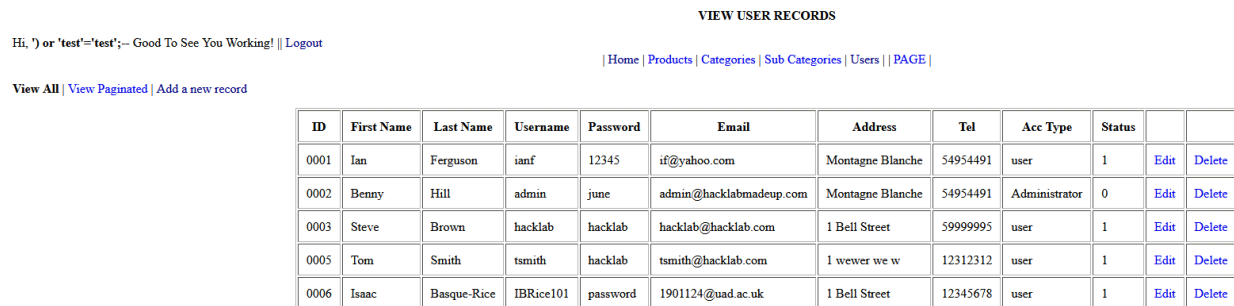


Figure 40, the tester having gained access to an admin-only page

From the admin panel for the page the tester was able to edit the hacklab account's account type and status to gain persistent administrator access to the server. In addition to this, due to the fact the passwords are stored in plaintext, the tester discovered that the admin account's credentials are admin:june.

2.7.4 Testing for Incubated Vulnerability

After determining earlier in the test that the target was vulnerable to a Stored XSS attack, the tester then progressed to testing for possibly malicious file upload. The tester created two separate files, test.txt and profile.jpg, both of these files contained the same message (the string "test") but one was saved as a standard text file and the other as an image (.jpg) file.

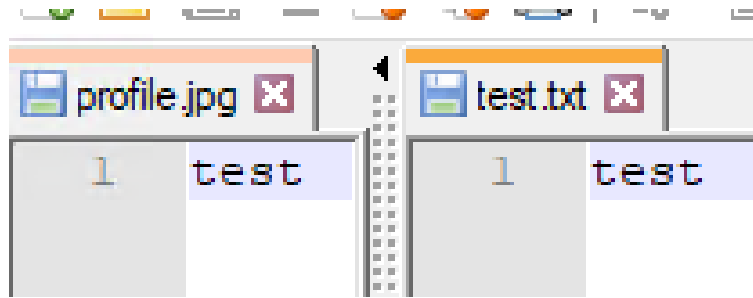


Figure 41, the two files in a text editor

The tester then attempted to submit both files as a profile picture image to the site. In the case of the .txt file, an error message appeared (see below) that indicated that the file type was not permitted as a profile picture on the site, however the .jpg file, which had the exact same contents and differed only in file extension, was permitted.

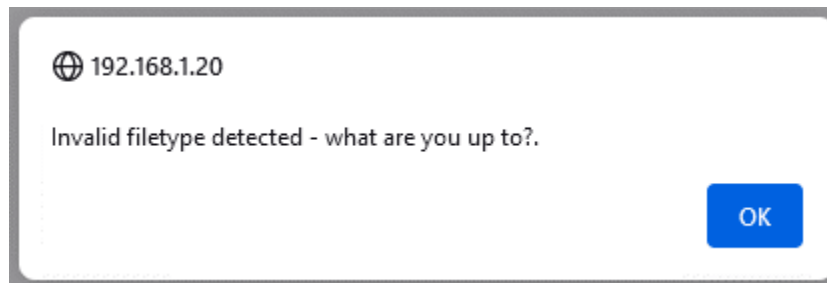


Figure 42, .txt file disallowed

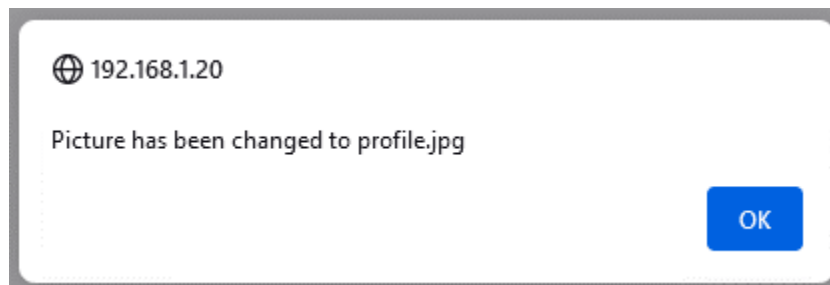


Figure 43, .jpg file allowed, despite containing text

In this instance it is not unreasonable to imagine an attacker making use of this vulnerability to inject a script into the profile picture area and have that execute when an admin navigates to the user's profile for routine work.

2.8 ERROR HANDLING

2.8.1 Testing for Improper Error Handling

When the tester navigated to a directory or page they knew not to contain content, a 404-error page is thrown up with the precise details of web-related technologies running on the server, thus confirming the accuracy of the earlier nmap testing. This can be seen in the below figure.

Object not found!

The requested URL was not found on this server. If you entered the URL manually please check your spelling and try again.

If you think this is a server error, please contact the [webmaster](#).

Error 404

192.168.1.20

Apache/2.4.29 (Unix) OpenSSL/1.0.2n PHP/5.6.34 mod_perl/2.0.8-dev Perl/v5.16.3

Figure 44, 404 error page

In addition to this, on user login and other related pages, PHP warnings display in the background.

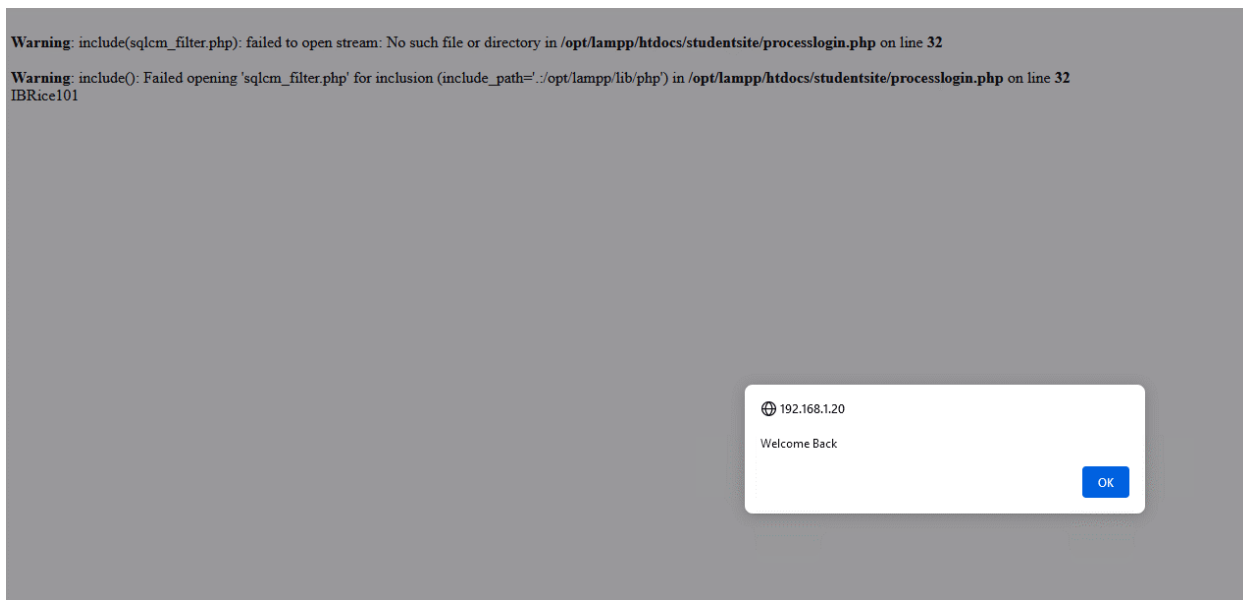


Figure 45, PHP warnings in login screen

2.9 CRYPTOGRAPHY

2.9.1 Testing for Weak Transport Layer Security

As previously mentioned, the website entirely lacks a valid SSL or TLS certificate, as demonstrated by the lack of padlock in the top right corner and the server communicating using HTTP as opposed to HTTPS. This can additionally be seen in the sslscan test conducted by the tester, shown below.

```
root@kali:~# sslscan 192.168.1.20:80
Version: 2.0.10-static
OpenSSL 1.1.1l-dev  xx XXX xxxx

Connected to 192.168.1.20

Testing SSL server 192.168.1.20 on port 80 using SNI name 192.168.1.20

SSL/TLS Protocols:
SSLv2      disabled
SSLv3      disabled
TLSv1.0    disabled
TLSv1.1    disabled
TLSv1.2    disabled
TLSv1.3    disabled

TLS Fallback SCSV:
Connection failed - unable to determine TLS Fallback SCSV support

TLS renegotiation:
Session renegotiation not supported

TLS Compression:
Compression disabled

Heartbleed:

Supported Server Cipher(s):
Certificate information cannot be retrieved.
```

Figure 46, SSLScan test conducted by the tester showing no valid security system in place

2.10 BUSINESS LOGIC TESTING

2.10.1 Test Ability to Forge Requests

As seen previously in this report in multiple sections, the target application contains a multitude of vulnerabilities such as Cross Site Scripting, SQL Injection, and possibly session hijacking. Through these vulnerabilities the tester managed to gain unauthorised access to critical information such as user data and the entirety of the admin functionality of the application.

2.10.2 Test Number of Times a Function Can Be Used Limits

As can be seen in section 2.4.3, the application does not have any lock out method, which is used in many other applications as a defence against brute force attacks. This issue can result in unauthorised users gaining access to a user account by repeatedly and systematically trying different credentials against the login page until one works.

2.10.3 Test Upload of Unexpected File Types

As can be seen in section 2.7.4, very little validation is applied to the files that can be uploaded by the user. The user can upload a profile picture to the application which only checks the file extension of the image as opposed to the content, because of this a malicious user could successfully upload a script with the aim of gaining sensitive information or remote code execution against the target as an image file.

3 DISCUSSION

3.1 SOURCE CODE ANALYSIS

3.1.1 Analysis

The process of static source code analysis was, in this case, handled manually by the tester. This was due to the considerable number of drawbacks automatic code analysis tools offer in relation to their strengths. These drawbacks include a high false positive rate, difficulty finding many kinds of vulnerabilities, failure to find configuration issues, and possible difficulties non-compiled code (OWASP Foundation n.d.). All these issues may at once necessitate manual code review anyway, and as such this process was not deemed to be beneficial to the tester. Analysis was therefore conducted manually.

3.1.2 Results

3.1.2.1 General Grep

For this stage, Mike McCabe's GitHub Gist describing a list of dangerous functions in PHP (McCabe n.d.) was used. An initial grep of the code base discovered 191 possible instances of vulnerability, the vast majority of which are includes (As can be seen in Appendix A - Grep Results), with several write, preg_replace, and open functions included therein. The command used here was a one liner that made use of regular expressions to whittle down the results returned to PHP files.

In total, according to the grep results, there were:

- 163 uses of include()
 - Can be used for RCE in the event of a misconfigured server by allowing an attacker to include a remotely hosted file (Radware n.d.)
- 10 uses of header()
 - In earlier versions of PHP this can be used for a header injection attack where an attacker can use multiple headers using a param that includes a newline (Anders 2016)
- 4 uses of preg_replace()
 - Not an issue in this instance as the /e parameter needs to be set for this to be vulnerable, this param performs an eval() search which can allow for code execution
- 3 uses of mail()
 - In the third parameter of this function there's a possible CLRF injection issue where an attacker can write contents to the screen after a carriage return line feed character (\r\n) (OWASP Foundation n.d.)

- 1 use of Phpinfo()
 - Outputs a significant amount of information about a PHP system's state and configuration including versions, server info, headers, compilation options, and so on. This function should not be in production servers (Acunetix n.d.) (and there is a comment telling the developer to remove it that has gone unheeded)
- 1 use of move_uploaded_file()
 - This function can be used by bad actors to force the creation of a malicious file through the usage of the null character (%00), especially in user uploaded files. An example of this could be pic.jpg%00.sh, a shell script file, being interpreted as pic.jpg by PHP and being uploaded as an image (Vigil@nce 2015).
- 1 use of chmod()
 - Allows files on the PHP server's local filesystem to be viewed and/or modified, a bad actor could inject a maliciously crafted request and, in the site's usage, have it globally readable, writable, and executable on the target server.

3.1.2.2 SQL Injection

The project was found to contain SQL commands that are vulnerable to a SQL injection attack. Because the command is bundled in with user submitted data it is possible for an attacker to gain unauthorised access to the website and database by submitting a specially crafted string in certain text fields that interfaces with the database in an unintended way. Further information on this can be found in section 3.2.13.

An example of a vulnerable query can be found in "processlogin.php" on line 37, however similar issues can be found across the site's codebase. A solution to this is to escape the user's input thereby making whatever value is submitted to the database explicitly part of a string, reducing ambiguity.

3.1.2.3 Finding Hardcoded Values

Searching in the project for hardcoded credentials revealed the database password used in the database is "Thisisverysecret21", this is an issue as if a malicious actor gained access to the codebase of the site then they could also gain access to the database storing all users' credentials.

This can be prevented by placing a ".env" (pronounced dotenv) file one level up outside of the site root directory, this allows php to access it through the "../" file path. Inside this file it is important to place an encrypted version of the password so if an attacker can perform a directory traversal attack and access the .env file they still wouldn't gain access to the password itself (Cornutt 2018).

3.1.2.4 Code Comment Issues

This section concerns issues caused by the developer leaving a comment with sensitive information in the code base. The clearest example of this is in the comments within the source code, particularly on line 1 in viewpurchase.php, which says the following:

```
<!-- *** Remember that phpinfo.php should be deleted in the real version -->
```

This comment shows both an awareness of the presence of the phpinfo function (elaborated on further in section 3.2.12) on the developer's part, and also if this file was accessed by a malicious actor, they could use this information to determine the presence of this function if they hadn't already.

A similar issue can be found on line 1 of hidden.php. This file contains a single comment that reads as follows:

```
<!-- ***Note to self: Door entry number is 1846 -->
```

If an attacker has access to information around the physical location of the organisation, this information can lead to a physical penetration of the organisation's security.

3.1.2.5 *Weak Cryptography*

In several cases in the application the md5 hashing algorithm is used to encrypt data. MD5 has unfortunately been cryptographically broken, meaning it is now a fundamentally insecure format for encryption and any data that has been hashed using this algorithm can be considered compromised if a malicious actor manages to acquire it (Manley 2020).

The recommended course of action is to switch from using MD5 to a more secure hashing algorithm, such as SHA-256, which has not been cryptographically broken.

3.2 VULNERABILITIES DISCOVERED AND COUNTERMEASURES

3.2.1 Robots.txt vulnerability

3.2.1.1 *Vulnerability*

This file is not in and of itself a vulnerability, however it is responsible for providing information for web crawlers, spiders, or robots regarding what files and directories on the target site should and should not be indexed, usually by search engines such as Google and DuckDuckGo. If these files are visible to malicious actors they may be able to more successfully enumerate a target site by being aware of what areas of the site the developer explicitly does not want anyone to see (AlSuwailem 2015).

There are, of course, many valid reasons for using this file, search engine optimisation being one such reason, however in this case the file is being used to hide the sql schema, a private internal file that should not be publicly available.

3.2.1.2 *Mitigation*

Robots.txt should not ever be used for sensitive information as it is always a publicly available file if it is being employed. The simplest fix for this issue is to remove the schema.sql file from the robots.txt file entirely, simply disallowing prospective hackers from learning about that file in the first place.

Another mitigation for attackers could be the creation of a honeypot. Add an interestingly named file or directory not present in the genuine application (such as /administration, for example), and set up a script to add all IP addresses that visit it to a blacklist (Hackerbinhminh 2011).

3.2.2 Local File Inclusion vulnerability

3.2.2.1 Vulnerability

Local File Inclusion (LFI) is a command injection vulnerability whereby an attacker can “trick a web application into either running or exposing files on a web server” (Kovacic 2021). In vulnerable applications an attacker can redirect to another page by replacing a called page with an arbitrary file, provided the location is valid.

In this case the page is vulnerable in the attachment.php file, where a call “?type=xyz.php” can be replaced with arbitrary file locations (e.g. ?type=/etc/passwd) provided the necessary knowledge of the system (or brute force) regarding directory traversal.

3.2.2.2 Mitigation

Some rudimentary mitigation is present in this application, a filter that excludes certain values from being accepted, however this filter is unsuitable as it only works in specific circumstances (when the values “..” and “../” are inputted, exclusively). The filter is as follows:

```
$pagetype = str_replace( array( "../", ".." ), "", $pagetype);
```

A much more suitable mitigation strategy would be to modify this filter to be more exclusionary, i.e. restricting input to a whitelist of acceptable parameters and rejecting input that does not meet this criteria (Chandel 2020).

3.2.3 Hidden source code vulnerability

3.2.3.1 Vulnerability

In several points in the application the developer has left comments pertaining to information that could be used by a malicious actor to carry out their attack. Comments like “remember that Phpinfo.php should be deleted in the real version” can be used by an attacker to know that a file with that name exists or has existed at some point, and to look for it.

3.2.3.2 Mitigation

Before publication to a version controlling or live system, multiple reviews by separate individuals or groups should take place within the code base for comments that may be sensitive.

3.2.4 Reversible cookie vulnerability

3.2.4.1 Vulnerability

As seen in section 2.7.1-3, the secret cookie value can be reverse engineered to display the logged in user's username, password in plain text, and Unix timestamp when logged on. This can be used in some applications to login to another user's session in an unauthorised manner.

The method of encoding the cookie is expressed in PHP as follows:

```
$str=$username.':'.$password.':'.strtotime("now");$str =  
base64_encode(bin2hex($str)); setcookie("SecretCookie", $str);
```

concatenating the username, password, and current time strings using the colon character as a delineator, and then encoding the result into Hexadecimal and Binary allowed for trivial reversing using the CyberChef tool.

3.2.4.2 Mitigation

A potential mitigation for this vulnerability is to prevent browser caching or end user cookie access by keeping the cookie on the server side of the application. This can be achieved by adding the HttpOnly tag in the Set-Cookie section of the HTTP response header. This results in the browser being unable to access the cookie through methods such as JavaScript or Cross-Site Scripting, instead returning an empty string when an attacker attempts this. This occurs even if such a flaw is present in the application (CookiePro 2021).

3.2.5 Cookie attributes vulnerability

3.2.5.1 Vulnerability

The developer of the site has not set attributes for the cookies used within the site, attributes describe a series of rules the cookie can follow, such as the "secure" attribute which ensures the cookie is only transported over HTTPS, or the "expires" attribute that describes how long a cookie should be active for (Venkatasubramanian 2010).

Of particular interest is the HttpOnly attribute. This attribute serves to prevent any client-side scripts from accessing data (as mentioned in section 3.2.4.2) and in this case the attribute is not set, resulting in the site being vulnerable to cross-site scripting, as an attacker can gain access to a cookie's value by calling the document.cookie value in a JavaScript terminal in-browser.

3.2.5.2 Mitigation

The only real mitigation in this case is to set the HttpOnly attribute on the website. This can be achieved in PHP by using the setcookie function like so:

```
setcookie("sessionid", "IAmACookieValue", ['httponly' => true]);
```

where the value "IAmACookieValue" is a string of text and the value surrounded by square braces is the attribute being set to "true" (Nidecki 2020).

3.2.6 Directory browsing vulnerability

3.2.6.1 Vulnerability

Directory browsing is the process of navigating to a URL within a website associated with a valid directory on that site. Expected behaviour in the case of the directory not having an associated index page is the user not being able to access the page, however in certain circumstances it is possible to see the entire contents of the directory in a list format, and for an attacker to navigate the directory at will. This is an issue as attackers can use information found in the directory listing to create other attacks, or as background knowledge about an organisation's inner workings. For example, it could be used for enumeration of the site or, in particularly bad cases, sensitive data such as database connection strings can be pulled from cached files on the server (Banach 2019).

3.2.6.2 Mitigation

Directory Listing can be trivially mitigated. A quick fix could be to create a blank index file in each directory; however, this is not a fool proof system as doing this can often be forgotten about on the creation of new directories, server migration, etc. A more permanent solution is disabling directory listing on a server level, which can be done in Apache by either inputting the following command on the webserver:

```
a2dismod --force autoindex
```

To disable directory listing entirely, or edit a configuration file located at `/etc/apache2/sites-enabled/000-default.conf` and add the following lines to the config file:

```
<Directory /path/to/add>  
    Options -Indexes  
</Directory>
```

Which disables file listing on specified directories (CISSP et al. 2021).

3.2.7 User enumeration vulnerability.

3.2.7.1 Vulnerability

When an invalid username is entered into the site, the message "user not found" is returned by the application. This can allow an attacker to enumerate a set of valid usernames through brute force, (the presence of the "admin" account can be determined through this method) which may lead to a more easily conducted password brute forcing test.

3.2.7.2 Mitigation

Remove the distinction between an incorrect username and incorrect password, replace "user not found" with "incorrect credentials", for example, and have that message display both if the username does not exist in the database and if it does but the password is incorrect. This will prevent an attacker from enumerating existing usernames.

3.2.8 Unlimited login attempts.

3.2.8.1 Vulnerability

A user can attempt to login to the website an infinite number of times with no lockout mechanism preventing them from doing so and no password throttling in place, this can result in an attacker sending a large volume of login attempts in a brute force attack.

3.2.8.2 Mitigation

There are two mitigations that can be employed in this instance, the first is password throttling. This is the practise of introducing a set delay of a certain amount of time on each failed attempt, or after a set number of failed attempts. For example, a single failed attempt could incur no delay, 2 could result in a 2 second delay, 3 in a 4 second delay, 4 in 8 seconds, and so on (Willeke 2018). Attempting to go through even a 25-word dictionary attack would result in over two years of wait time.

The other mitigation is account lockout, which is where, after a certain number of attempts, the user in question's account is inaccessible for either a predetermined amount of time or until an administrator or other authorised person can manually unlock it.

Throttling is preferred as account locking could prevent a legitimate user who has mistakenly entered their password a certain number of times from accessing their account, as well as the fact that lockout can allow an attacker to pivot to a Denial of Service attack (NCSC 2018).

3.2.9 No HTTPS vulnerability.

3.2.9.1 Vulnerability

The site uses the HTTP protocol over HTTPS, this results in packets being transmitted over the internet unencrypted meaning sensitive information such as credentials, addresses, and payment information are vulnerable to packet sniffing attacks.

3.2.9.2 Mitigation

Assuming the site has an SSL/TLS certificate already, force redirecting HTTP to HTTPS is trivial, and can be done in two ways.

The first is the Virtual Hosts method, this is done by editing the virtual hosts configuration file (located in Debian based systems at `/etc/apache2/sites-available/`) and ensuring it appears like so:

```
<VirtualHost *:80>
    ServerName 192.168.1.20
    Redirect permanent / https://192.168.1.20/
</VirtualHost>

<VirtualHost _default_:443>
    ServerName 192.168.1.20
    DocumentRoot /usr/local/apache2/htdocs
    SSLEngine On
```

```
# Configuration Continues...  
</VirtualHost>
```

This forces any user who attempts to access the site on port 80 (HTTP) to be redirected to https/port 443 (SSL Support Team 2020).

The other method of force redirecting is using the .htaccess file, which is a per-directory config file in Apache which can be placed in the root to affect the project globally. This method requires the mod_rewrite module which should be enabled by default.

To force redirect, add the following lines to the .htaccess file:

```
RewriteEngine On  
RewriteCond %{HTTPS} off  
RewriteRule ^(.*)$ https://example.com/$1 [L,R=301]
```

This checks if HTTPS is off, and if so redirects HTTP to HTTPS permanently with status code 301 (Linuxize 2020).

3.2.10 File upload vulnerability.

3.2.10.1 Vulnerability

The site has facility for a user uploaded profile picture, to this end the developer is attempting to use a filter to remove what they deem to be invalid files upon user upload (i.e., anything that is not an image file).

The filter in question declares a variable \$validtypes as an array containing the values “image/jpeg”, “.../jpg”, and “.../png”, and then if the file that has been uploaded is not named in a way that conforms to this format, the upload is disallowed. However, due to the nature of this check, it is possible to upload a file that ends in, for example, “.jpg”, but the contents of said file are a shell script or other executable piece of code.

3.2.10.2 Mitigation

It is possible to alter the filter to allow for the checking of a genuine image file by using PHP’s pathinfo filesystem function. One of the flags of this function is “PATHINFO_EXTENSION”, which returns the final extension of any files uploaded (The PHP Group n.d.).

This can be used as a first line of defence alongside other mitigations, such as saving the image file in a database if possible (as opposed to saving on the server’s filesystem), or isolating the images from the main server, and otherwise ensuring that files with double extensions cannot be executed. This can be done by changing the execution permissions of any files that match a regular expression for two file extensions (OWASP Foundation n.d.).

3.2.11 Cross Site Request Forgery (CSRF) vulnerability.

3.2.11.1 Vulnerability

Cross Site Request Forgery is a vulnerability that allows for an attacker to target a user by getting them to send a request by visiting a page or performing an action outwith the scope of the target application (Computerphile 2013).

In this instance the field that is vulnerable to CSRF exists in the password update function and could result in a user's password being changed to another arbitrary value, hence locking out the true user from the account and likely allowing the attacker access to personal information and payment details.

3.2.11.2 Mitigation

CSRF Attacks can be launched against a target if the attacker is aware of the parameters and values that are used in a form. As a result of this if an additional, unknown parameter is used then CSRF can be successfully mitigated against (Banach 2020). This can be done in multiple ways.

An anti-CSRF token can be generated between the client and the server-side application, this token is a pseudo-randomised, and crucially, secret value known only to the user's browser and the server. This token can be used to validate requests by only allowing the request to be processed if the correct token is present with said request. CSRF tokens can be generated with a pseudorandom number generator seeded with the generation time Unix timestamp and a static secret, and sent to the client within a hidden field in a form that's submitted using a POST request, with type "hidden" (PortSwigger n.d.).

Another method of mitigation could be the use of the SameSite flag in cookies sent to and from the host and client. This cookie, if the "strict" attribute is used, ensures that requests sent within the site are not sent elsewhere, thus restricting access to the same site. This can be used for all requests to do with user authentication (Merewood 2019).

3.2.12 PHP information disclosure vulnerability.

3.2.12.1 Vulnerability

Phpinfo is a function in PHP that outputs PHP's configuration on the system. This includes data like compilation options, extensions, OS information, license, and much more information (Acunetix n.d.).

The function can and is frequently used as a debugging tool, however it is inadvisable to push the code with this function present into production as an attacker knowing information about the configuration of the stack in such detail could theoretically make planning an attack trivial.

Other impacts of Phpinfo being present include directory traversal (due to the fact the attacker knows the full layout of the application), remote code execution on the web server, access to the Ips on the internal network, and of course SQLi and XSS (Beagle Security 2018).

3.2.12.2 Mitigation

Simply remove instances of the Phpinfo function within the codebase.

3.2.13 SQL Injection vulnerability.

3.2.13.1 Vulnerability

SQL Injection, or SQLi, is a vulnerability whereby an attacker creates a specially crafted SQL query and submits that to the database via a user input field like a username or password input box. The query is designed in this case to always return true, so by way of a simple example an attacker could enter the following in both username and password fields:

```
a' OR 1=1;--
```

And if the target was vulnerable to SQLi, this string would allow for login, as the query would return true since 1=1 is true. The query in question would appear something like this:

```
SELECT * FROM users WHERE username = 'a' OR 1=1;--
```

Meaning login to the service if 1=1, the – characters at the end denote the beginning of a comment, so if there's any SQL after this it will be commented out.

The target site is indeed vulnerable to this form of attack. The SQL query used to interface with the database looks something like the following:

```
$sql = "SELECT user_id, username, password, ac_type, user_status, thumbnail FROM `users` WHERE username = ('$username') AND password = '$password'";
```

This is vulnerable because input is taken literally with no sanitation, meaning characters such as ', =, -, and ,, are all taken and submitted to the query as their literal values.

In the code base for the site, the developer is attempting to detect attacks by employing the following check:

```
if(preg_match("[1=1|2=2|select|Union|2 =2|3=3|1 =1]", $username)){ echo ' '; die(); }
```

Which is an issue as any true statements outwith the ones outlined in the parentheses, in a well-formed SQLi attack, would succeed (for example a') OR 10=10;--).

3.2.13.2 Mitigation

The best mitigation for this vulnerability is to separate user defined input from the SQL query. Writing a SQL query in the way the developer has done in this case allows user submitted data to be embedded directly into crucial server-side code, the best way to prevent this happening is with the use of prepared statements.

Prepared statements work by sending the SQL query and data separately using the “?” character as a placeholder and using the bind_param function to fill the placeholders with data (HackedU Team n.d.). The SELECT statement above would be replaced as so:

```
$stmt = $db->prepare("SELECT user_id, username, password, ac_type, user_status, thumbnail FROM `users` WHERE username = ? AND password = ?");  
$stmt->bind_param('ss', $username, $password);
```

```
$stmt->execute();
```

'ss' means that both parameters were strings, if one was a string and one was an int this would be replaced accordingly with 'si'.

3.2.14 Hidden guessable folder vulnerability.

3.2.14.1 Vulnerability

A hidden folder containing a backup of the SQL injection query is in /pics/sqlcm.bak, this file could be discovered using a directory enumeration tool like dirbuster and may allow for an attacker to view files and folders they were explicitly not meant to see.

3.2.14.2 Mitigation

Place backups of files, and other files that are not meant to be seen, outside the scope of the website, ideally in a location on the webserver that is inaccessible to an attacker or even off the webserver in a backup storage drive.

3.2.15 Brute-forceable Admin password.

3.2.15.1 Vulnerability

The admin password in this instance is especially weak, "june", 4 lowercase letters, any number of dictionary attacks could crack this in an especially short amount of time, especially if the admin username, which is particularly common in sites such as this, has already been enumerated (possibly via another vulnerability such as the User enumeration vulnerability.)

3.2.15.2 Mitigation

Employ a stronger password, ideally one that contains a mix of upper- and lower-case letters, numbers, and special characters or symbols. In addition to this, the usage of a password manager, whereby strong passwords can be automatically generated and stored in a single application with an ideally strong master password, is highly recommended.

3.2.16 Generic issues

Alongside the other vulnerabilities that have been covered previously, several smaller vulnerabilities exist within the project that require addressing. These vulnerabilities are as follows:

- x-powered-by header: gives PHP/5.4.7 reported.

The x-powered-by header reveals what version of PHP is running, this can be used by an attacker to employ vulnerabilities discovered in specific PHP versions. This can be mitigated by removing the header.

- The anti-clickjacking X-Frame-Options header is not present.

This header ensures that the application cannot be rendered as an embed in another separate, possibly malicious application. If an attacker were to do this they could trick a user into clicking

an object that could steal credentials or install malware (Netsparker n.d.). The mitigation for this is to set the X-Frame-Options header in the server's Apache settings.

- The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS.

This header prevents pages from loading when it detects a reflected XSS attack. The mitigation for this issue is, once again, to set the header with relevant flags (Mozilla n.d.).

- X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type.

This header being missing allows for a malicious user to execute unauthorised code on the server through a MIME sniffing attack leading into an XSS exploit in a similar way to what is described in section 3.2.10 (Scan Repeat n.d.). Mitigate this by setting the header in Apache.

- GET Apache mod_negotiation is enabled with MultiViews

This issue can allow for attackers to easily brute force file names by sending a crafted request to the server for an arbitrary file name (such as index) without specifying an extension, this would return all files that have that filename irrespective of extension. This vulnerability in tandem with a dictionary of common filenames can result in an effective enumeration strategy for an attacker (Di Paola 2007). This issue can be remediated by disabling the multiviews directive in apache using a .htaccess file (Acunetix n.d.).

- OSVDB-112004: GET /cgi-bin/printenv: Site appears vulnerable to the 'shellshock' vulnerability (CVE-2014-6271) and (CVE-2014-6278)

The shellshock vulnerability is present within the /cgi-bin/printenv directory. This is a vulnerability within the Bash shell and scripting language that allows for remote code execution through crafted environment variables declared after function definitions in the bash scripting language (Miller 2014). Remediation for this vulnerability is as simple as updating the version of bash in the directory. This can be done using the following command:

```
sudo apt-get update && sudo apt-get upgrade --only-upgrade bash
```

- TRACE HTTP TRACE method is active, suggesting the host is vulnerable to XST

This method, much like phpinfo, is a diagnostic tool that echoes requests to the server after they have been made. This is an issue as it allows a user to see potentially sensitive information pertaining to the configuration of the server in an attack known as cross-site tracing. The mitigation for this is to disable the method in Apache.

- The management package Phypmyadmin is visible to the outside world (192.168.1.20/PHPmyadmin).

Having this administration page viewable to the outside world is an issue as, if an attacker can obtain the credentials for the admin account (through brute force or other means) they would be able to access the SQL database and other administrative tools in an unauthorised manner. The mitigation for this vulnerability is to remove access to this page by hiding it outside of the scope of the webpage.

3.3 OVERALL DISCUSSION

Throughout the course of the investigation a number of vulnerabilities have been discovered in the web application. Many of these vulnerabilities have been discovered by the tester through the use of the OWASP Web Application Penetration Testing Methodology, with the tester employing a number of techniques and tools therein.

The majority of vulnerabilities discovered by the tester fall into one of two camps, a lack of input sanitation, and misconfiguration of certain services and tools on the developer's side that result in weak or no security in parts of the application.

This report outlines the vulnerabilities and other miscellaneous security concerns present in the application, why they are of issue, and methods of mitigation for these issues.

4 FUTURE WORK

The contents of this report in its entirety outline the issues present currently in the client's web application, alongside countermeasures that can be taken to mitigate any vulnerabilities present, this has been done with the expectation that these fixes would be implemented by the client at some point in the hopefully near future.

To this end, after the mitigations have been implemented, a second investigation in a similar vein to this one should be conducted against the web application to determine if the fixes implemented by the developer have either worked to fix the issues present currently, or if any fixes the developer did implement have introduced new vulnerabilities to the system that need addressing themselves,.

In addition to this, a second test against the organisation holistically may be beneficial. A genuine malicious actor would not necessarily stop at attacking the web application itself, they may in fact attempt unauthorised access through an employee, a server, or physically.

A second test in this manner include the site (such as has been presented in this document) as well as organisation members (i.e., employees) submitting to social engineering attacks such as email phishing attempts or impersonation of a contractor or jewellery supplier. A holistic test may also test the web application server, bolstering the security of said server from attack.

REFERENCES PART 1

Lallie, HS, Shepherd, LA, Nurse, JRC, Erola, A, Epiphaniou, G, Maple, C and Bellekens, X 2021, Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic, Computers & Security, 105, p. 102248.

OWASP n.d., WSTG - Stable | OWASP, viewed 7 November, 2021, <https://owasp.org/www-project-web-security-testing-guide/stable/4-Web_Application_Security_Testing/>.

REFERENCES PART 2

Acunetix (no date a) Apache mod_negotiation filename bruteforcing - Vulnerabilities, Acunetix. Available at: https://www.acunetix.com/vulnerabilities/web/apache-mod_negotiation-filename-bruteforcing/ (Accessed: 18 January 2022).

Acunetix (no date b) PHPinfo page - Vulnerabilities, Acunetix. Available at: <https://www.acunetix.com/vulnerabilities/web/phpinfo-page/> (Accessed: 15 January 2022).

AlSuwailem, A. (2015) Robots.txt security risk review and mitigation | Synopsys, Software Integrity Blog. Available at: <https://www.synopsys.com/blogs/software-security/robots-txt/> (Accessed: 3 January 2022).

Anders (2016) web application - Is header('Location: ../page.php?param='.\$param); vulnerable to unvalidated redirects?, Information Security Stack Exchange. Available at: <https://security.stackexchange.com/a/124197> (Accessed: 15 January 2022).

Banach, Z. (2019) How you can disable directory listing on your web server – and why you should. Available at: <https://www.netsparker.com/blog/web-security/disable-directory-listing-web-servers/> (Accessed: 13 January 2022).

Banach, Z. (2020) Cross-Site Request Forgery Attacks. Available at: <https://www.netsparker.com/blog/web-security/csrf-cross-site-request-forgery/> (Accessed: 16 January 2022).

Beagle Security (2018) Revealing phpinfo(), Revealing phpinfo(). Available at: <https://beaglesecurity.com/blog/vulnerability/revealing-phpinfo.html> (Accessed: 16 January 2022).

Chandel, R. (2020) 'Comprehensive Guide on Local File Inclusion (LFI)', Hacking Articles, 3 July. Available at: <https://www.hackingarticles.in/comprehensive-guide-to-local-file-inclusion/> (Accessed: 3 January 2022).

CISSP, V. et al. (2021) 'Tutorial Apache - Disable directory listing [step by step]', TechExpert, 14 January. Available at: <https://techexpert.tips/apache/apache-disable-directory-listing/> (Accessed: 13 January 2022).

Computerphile (2013) Cross Site Request Forgery - Computerphile. Available at: <https://www.youtube.com/watch?v=vRBihr41JTo> (Accessed: 16 January 2022).

CookiePro (2021) What is an HttpOnly Cookie?, CookiePro. Available at: <https://www.cookiepro.com/knowledge/httponly-cookie/> (Accessed: 3 January 2022).

Cornutt, C. (2018) *Keeping Credentials Secure in PHP* | Codementor. Available at: <https://www.codementor.io/@ccornutt/keeping-credentials-secure-in-php-kvcbrk55z> (Accessed: 17 January 2022).

Di Paola, F. (2007) *Wisec - The Wise SECURITY*. Available at: <http://www.wisec.it/sectou.php?id=4698ebdc59d15> (Accessed: 18 January 2022).

HackEDU Team (no date) *How to prevent SQL Injection vulnerabilities: How Prepared Statements Work*. Available at: <https://www.hackedu.com/blog/how-to-prevent-sql-injection-vulnerabilities-how-prepared-statements-work> (Accessed: 16 January 2022).

Hackerbinhminh (2011) 'Creating a Robots.txt Honeypot', 23 February. Available at: <http://hackupshell.blogspot.com/2011/02/creating-robotstxt-honeypot.html> (Accessed: 3 January 2022).

Kovacic, D. (2021) 'Local File Inclusion: Understanding and Preventing Attacks', *NeuraLegion*, 13 December. Available at: <https://www.neuralegion.com/blog/local-file-inclusion-lfi/> (Accessed: 3 January 2022).

Linuxize (2020) *Redirect HTTP to HTTPS in Apache*. Available at: <https://linuxize.com/post/redirect-http-to-https-in-apache/> (Accessed: 15 January 2022).

Manley, G. (2020) *What Is MD5 and Why Is It Considered Insecure?*, *Engineering Education (EngEd) Program* | Section. Available at: <https://www.section.io/engineering-education/what-is-md5/> (Accessed: 17 January 2022).

McCabe, M. (no date) *Dangerous PHP Functions*, *Gist*. Available at: <https://gist.github.com/mccabe615/b0907514d34b2de088c4996933ea1720> (Accessed: 14 January 2022).

Merewood, R. (2019) *SameSite cookies explained*, *web.dev*. Available at: <https://web.dev/samesite-cookies-explained/> (Accessed: 16 January 2022).

Miller, M. (2014) *Shellshock: How does it actually work?*, *Fedora Magazine*. Available at: <https://fedoramagazine.org/shellshock-how-does-it-actually-work/> (Accessed: 18 January 2022).

Mozilla (no date) *X-XSS-Protection - HTTP* | MDN. Available at: <https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-XSS-Protection> (Accessed: 18 January 2022).

NCSC (2018) *Password policy: updating your approach*. Available at: <https://www.ncsc.gov.uk/collection/passwords/updating-your-approach> (Accessed: 15 January 2022).

Netsparker (no date) Missing X-Frame-Options Header | Netsparker. Available at: <https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-x-frame-options-header/> (Accessed: 18 January 2022).

Nidecki, T.A. (2020) The HttpOnly Flag – Protecting Cookies against XSS, Acunetix. Available at: <https://www.acunetix.com/blog/web-security-zone/httponly-flag-protecting-cookies/> (Accessed: 13 January 2022).

OWASP Foundation (no date a) CRLF Injection | OWASP Foundation. Available at: https://owasp.org/www-community/vulnerabilities/CRLF_Injection (Accessed: 15 January 2022).

OWASP Foundation (no date b) Static Code Analysis Control | OWASP Foundation. Available at: https://owasp.org/www-community/controls/Static_Code_Analysis (Accessed: 3 January 2022).

OWASP Foundation (no date c) Unrestricted File Upload | OWASP Foundation. Available at: https://owasp.org/www-community/vulnerabilities/Unrestricted_File_Upload (Accessed: 16 January 2022).

'OWASP_Code_Review_Guide_v2.pdf' (no date). Available at: https://owasp.org/www-project-code-review-guide/assets/OWASP_Code_Review_Guide_v2.pdf (Accessed: 16 January 2022).

PortSwigger (no date) CSRF tokens | Web Security Academy. Available at: <https://portswigger.net/web-security/csrf/tokens> (Accessed: 16 January 2022).

Radware (no date) RFI - LFI. Available at: <https://www.radware.com/security/ddos-knowledge-center/ddospedia/rfi-lfi/> (Accessed: 15 January 2022).

Scan Repeat (no date) X-Content-Type-Options Header Missing, ScanRepeat. Available at: <https://scanrepeat.com/web-security-knowledge-base/x-content-type-options-header-missing> (Accessed: 18 January 2022).

SSL Support Team (2020) 'Redirect HTTP to HTTPS with Apache', SSL.com, 2 December. Available at: <https://www.ssl.com/how-to/redirect-http-to-https-with-apache/> (Accessed: 15 January 2022).

The PHP Group (no date) PHP: pathinfo - Manual. Available at: <https://www.php.net/manual/en/function.pathinfo.php> (Accessed: 16 January 2022).

Venkatasubramanian, B. (2010) Cookie Attributes and their Importance. Available at: <https://www.paladion.net/blogs/cookie-attributes-and-their-importance> (Accessed: 13 January 2022).

Vigil@nce (2015) Vulnerability about PHP: file creation via move_uploaded_file, Vigil@nce. Available at: <https://vigilance.fr/vulnerability/PHP-file-creation-via-move-uploaded-file-16495> (Accessed: 15 January 2022).

Isaac Basque-Rice

Willeke, J. (2018) Ldapwiki: Server-Side Login throttling schemes. Available at: <https://ldapwiki.com/wiki/Server-Side%20Login%20throttling%20schemes> (Accessed: 15 January 2022).

1 APPENDICES PART 1

4.1 APPENDIX A – OMITTED METHODOLOGY

As mentioned in the Overview of Procedure section and can be inferred throughout the remainder of this section, there is several OWASP Web Application Penetration Testing Methodology sections that had to be omitted due to the fact they were out of scope for this project. The OWASP methodology is an extremely thorough one, and therefore covers many areas of web application testing that isn't relevant to our case, or may be explicitly out of scope, in the cases of sections that require the tester to test the server. In addition, they may be simply irrelevant, with certain sections only having relevance to certain aspects of the website which do not apply in this case. In addition to these reasons, some areas of testing are covered in other subsections, and some areas were tested but revealed no unusual or wrong activity. The following is a list of areas omitted because of these reasons

- *Information Gathering*
 - *Conduct Search Engine Discovery Reconnaissance for Information Leakage*
 - *Fingerprint Web Application (Merged into Fingerprint Web Application Framework)*
 - *Map Application Architecture*
- *Configuration and Deployment Management Testing*
 - *Test Network Infrastructure Configuration*
 - *Review Old Backup and Unreferenced Files for Sensitive Information*
 - *Test File Extensions Handling for Sensitive Information*
 - *Test HTTP Methods*
 - *Test RIA Cross Domain Policy*
 - *Test File Permission*
 - *Test for Subdomain Takeover*
 - *Test Cloud Storage*
- *Identity Management Testing*
 - *Test Account Provisioning Process*
 - *Testing for Account Enumeration and Guessable User Account*
 - *Testing for Weak or Unenforced Username Policy*
- *Authentication Testing*
 - *Testing for Bypassing Authentication Schema*
 - *Testing for Browser Cache Weaknesses*
 - *Testing for Weak Security Question Answer*
 - *Testing for Weaker Authentication in Alternative Channel*
 - *Testing for Weak Password Change or Reset Functionalities*

- *Authorisation Testing*
 - *Testing for Insecure Direct Object References*
 - *Testing for Bypassing Authorization Schema*
 - *Testing for Privilege Escalation*
- *Session Management Testing*
 - *Testing for Exposed Session Variables*
 - *Testing for Cross Site Request Forgery*
 - *Testing Session Timeout*
 - *Testing for Session Puzzling*
 - *Testing for Session Hijacking*
- *Input Validation Testing*
 - *Testing for HTTP Verb Tampering (merged into Test HTTP Methods)*
 - *Testing for HTTP Parameter Pollution*
 - *Testing for LDAP Injection*
 - *Testing for XML Injection*
 - *Testing for SSI Injection*
 - *Testing for XPath Injection*
 - *Testing for IMAP SMTP Injection*
 - *Testing for Code Injection*
 - *Testing for Command Injection*
 - *Testing for HTTP Splitting Smuggling*
 - *Testing for HTTP Incoming Requests*
 - *Testing for Host Header Injection*
 - *Testing for Server-side Template Injection*
 - *Testing for Server-Side Request Forgery*
- *Testing for Error Handling*
 - *Testing for Stack Traces (merged into improper error handling)*
- *Testing for Weak Cryptography*
 - *Testing for Padding Oracle*
 - *Testing for Sensitive Information Sent via Unencrypted Channels*
- *Business Logic Testing*
 - *Test Business Logic Data Validation*
 - *Test Integrity Checks*
 - *Test for Process Timing*
 - *Testing for the Circumvention of Workflows*
 - *Test Defences Against Application Misuse*
 - *Test Upload of Malicious Files*
- *Client-Side Testing (all)*

4.2 APPENDIX B – SITE FILES AND DATA

4.2.1 Section 1 – Site URLs

<http://192.168.1.20/>
<http://192.168.1.20/Photos>
<http://192.168.1.20/Photos/>
<http://192.168.1.20/Photos/Diamond>
<http://192.168.1.20/Photos/Diamond/>
<http://192.168.1.20/Photos/Diamond/Bangles>
<http://192.168.1.20/Photos/Diamond/Bangles/>
<http://192.168.1.20/Photos/Diamond/Bangles/1.jpg>
<http://192.168.1.20/Photos/Diamond/Bangles/10.jpg>
<http://192.168.1.20/Photos/Diamond/Bangles/11.jpg>
<http://192.168.1.20/Photos/Diamond/Bangles/2.jpg>
<http://192.168.1.20/Photos/Diamond/Bangles/3.jpg>
<http://192.168.1.20/Photos/Diamond/Bangles/4.jpg>
<http://192.168.1.20/Photos/Diamond/Bangles/5.jpg>
<http://192.168.1.20/Photos/Diamond/Bangles/6.jpg>
<http://192.168.1.20/Photos/Diamond/Bangles/7.jpg>
<http://192.168.1.20/Photos/Diamond/Bangles/8.jpg>
<http://192.168.1.20/Photos/Diamond/Bangles/9.jpg>
<http://192.168.1.20/Photos/Diamond/EarRings>
<http://192.168.1.20/Photos/Diamond/EarRings/>
<http://192.168.1.20/Photos/Diamond/EarRings/1.jpg>
<http://192.168.1.20/Photos/Diamond/EarRings/2.jpg>
<http://192.168.1.20/Photos/Diamond/EarRings/3.jpg>
<http://192.168.1.20/Photos/Diamond/EarRings/4.jpg>
<http://192.168.1.20/Photos/Diamond/EarRings/5.jpg>
<http://192.168.1.20/Photos/Diamond/EarRings/6.jpg>
<http://192.168.1.20/Photos/Diamond/EarRings/7.jpg>
<http://192.168.1.20/Photos/Diamond/EarRings/8.jpg>
<http://192.168.1.20/Photos/Diamond/EarRings/9.jpg>
<http://192.168.1.20/Photos/Diamond/Lady%20Ring>

<http://192.168.1.20/Photos/Diamond/Lady%20Ring/>
<http://192.168.1.20/Photos/Diamond/Lady%20Ring/1.jpg>
<http://192.168.1.20/Photos/Diamond/Lady%20Ring/10.jpg>
<http://192.168.1.20/Photos/Diamond/Lady%20Ring/2.jpg>
<http://192.168.1.20/Photos/Diamond/Lady%20Ring/3.jpg>
<http://192.168.1.20/Photos/Diamond/Lady%20Ring/4.jpg>
<http://192.168.1.20/Photos/Diamond/Lady%20Ring/5.jpg>
<http://192.168.1.20/Photos/Diamond/Lady%20Ring/6.jpg>
<http://192.168.1.20/Photos/Diamond/Lady%20Ring/7.jpg>
<http://192.168.1.20/Photos/Diamond/Lady%20Ring/8.jpg>
<http://192.168.1.20/Photos/Diamond/Lady%20Ring/9.jpg>
<http://192.168.1.20/Photos/Diamond/NeckLaces>
<http://192.168.1.20/Photos/Diamond/NeckLaces/>
<http://192.168.1.20/Photos/Diamond/NeckLaces/1.jpg>
<http://192.168.1.20/Photos/Diamond/NeckLaces/2.jpg>
<http://192.168.1.20/Photos/Diamond/NeckLaces/3.jpg>
<http://192.168.1.20/Photos/Diamond/NeckLaces/4.jpg>
<http://192.168.1.20/Photos/Diamond/NeckLaces/5.jpg>
<http://192.168.1.20/Photos/Diamond/NeckLaces/6.jpg>
<http://192.168.1.20/Photos/Diamond/NeckLaces/7.jpg>
<http://192.168.1.20/Photos/Diamond/Nose%20Pin>
<http://192.168.1.20/Photos/Diamond/Nose%20Pin/>
<http://192.168.1.20/Photos/Diamond/Nose%20Pin/1.jpg>
<http://192.168.1.20/Photos/Diamond/Nose%20Pin/10.jpg>
<http://192.168.1.20/Photos/Diamond/Nose%20Pin/2.jpg>
<http://192.168.1.20/Photos/Diamond/Nose%20Pin/3.jpg>
<http://192.168.1.20/Photos/Diamond/Nose%20Pin/4.jpg>
<http://192.168.1.20/Photos/Diamond/Nose%20Pin/5.jpg>
<http://192.168.1.20/Photos/Diamond/Nose%20Pin/6.jpg>
<http://192.168.1.20/Photos/Diamond/Nose%20Pin/7.jpg>
<http://192.168.1.20/Photos/Diamond/Nose%20Pin/8.jpg>
<http://192.168.1.20/Photos/Diamond/Nose%20Pin/9.jpg>
<http://192.168.1.20/Photos/Diamond/Pendant%20Set>

<http://192.168.1.20/Photos/Diamond/Pendant%20Set/>
<http://192.168.1.20/Photos/Diamond/Pendant%20Set/1.jpg>
<http://192.168.1.20/Photos/Diamond/Pendant%20Set/10.jpg>
<http://192.168.1.20/Photos/Diamond/Pendant%20Set/2.jpg>
<http://192.168.1.20/Photos/Diamond/Pendant%20Set/3.jpg>
<http://192.168.1.20/Photos/Diamond/Pendant%20Set/4.jpg>
<http://192.168.1.20/Photos/Diamond/Pendant%20Set/5.jpg>
<http://192.168.1.20/Photos/Diamond/Pendant%20Set/6.jpg>
<http://192.168.1.20/Photos/Diamond/Pendant%20Set/7.jpg>
<http://192.168.1.20/Photos/Diamond/Pendant%20Set/8.jpg>
<http://192.168.1.20/Photos/Diamond/Pendant%20Set/9.jpg>
<http://192.168.1.20/Photos/Diamond/Pendants>
<http://192.168.1.20/Photos/Diamond/Pendants/>
<http://192.168.1.20/Photos/Diamond/Pendants/1.jpg>
<http://192.168.1.20/Photos/Diamond/Pendants/10.jpg>
<http://192.168.1.20/Photos/Diamond/Pendants/2.jpg>
<http://192.168.1.20/Photos/Diamond/Pendants/3.jpg>
<http://192.168.1.20/Photos/Diamond/Pendants/4.jpg>
<http://192.168.1.20/Photos/Diamond/Pendants/5.jpg>
<http://192.168.1.20/Photos/Diamond/Pendants/6.jpg>
<http://192.168.1.20/Photos/Diamond/Pendants/7.jpg>
<http://192.168.1.20/Photos/Diamond/Pendants/8.jpg>
<http://192.168.1.20/Photos/Diamond/Pendants/9.jpg>
<http://192.168.1.20/Photos/Gold>
<http://192.168.1.20/Photos/Gold/>
<http://192.168.1.20/Photos/Gold/BangLes>
<http://192.168.1.20/Photos/Gold/BangLes/>
<http://192.168.1.20/Photos/Gold/BangLes/1.jpg>
<http://192.168.1.20/Photos/Gold/BangLes/10.jpg>
<http://192.168.1.20/Photos/Gold/BangLes/2.jpg>
<http://192.168.1.20/Photos/Gold/BangLes/3.jpg>
<http://192.168.1.20/Photos/Gold/BangLes/4.jpg>
<http://192.168.1.20/Photos/Gold/BangLes/5.jpg>

<http://192.168.1.20/Photos/Gold/BangLes/6.jpg>

<http://192.168.1.20/Photos/Gold/BangLes/7.jpg>

<http://192.168.1.20/Photos/Gold/BangLes/8.jpg>

<http://192.168.1.20/Photos/Gold/BangLes/9.jpg>

<http://192.168.1.20/Photos/Gold/Ear%20Rings>

<http://192.168.1.20/Photos/Gold/Ear%20Rings/>

<http://192.168.1.20/Photos/Gold/Ear%20Rings/1.jpg>

<http://192.168.1.20/Photos/Gold/Ear%20Rings/10.jpg>

<http://192.168.1.20/Photos/Gold/Ear%20Rings/2.jpg>

<http://192.168.1.20/Photos/Gold/Ear%20Rings/3.jpg>

<http://192.168.1.20/Photos/Gold/Ear%20Rings/4.jpg>

<http://192.168.1.20/Photos/Gold/Ear%20Rings/5.jpg>

<http://192.168.1.20/Photos/Gold/Ear%20Rings/6.jpg>

<http://192.168.1.20/Photos/Gold/Ear%20Rings/7.jpg>

<http://192.168.1.20/Photos/Gold/Ear%20Rings/8.jpg>

<http://192.168.1.20/Photos/Gold/Ear%20Rings/9.jpg>

<http://192.168.1.20/Photos/Gold/Lady%20Rings>

<http://192.168.1.20/Photos/Gold/Lady%20Rings/>

<http://192.168.1.20/Photos/Gold/Lady%20Rings/1.jpg>

<http://192.168.1.20/Photos/Gold/Lady%20Rings/10.jpg>

<http://192.168.1.20/Photos/Gold/Lady%20Rings/2.jpg>

<http://192.168.1.20/Photos/Gold/Lady%20Rings/3.jpg>

<http://192.168.1.20/Photos/Gold/Lady%20Rings/4.jpg>

<http://192.168.1.20/Photos/Gold/Lady%20Rings/5.jpg>

<http://192.168.1.20/Photos/Gold/Lady%20Rings/6.jpg>

<http://192.168.1.20/Photos/Gold/Lady%20Rings/7.jpg>

<http://192.168.1.20/Photos/Gold/Lady%20Rings/8.jpg>

<http://192.168.1.20/Photos/Gold/Lady%20Rings/9.jpg>

<http://192.168.1.20/Photos/Gold/Man%20Rings>

<http://192.168.1.20/Photos/Gold/Man%20Rings/>

<http://192.168.1.20/Photos/Gold/Man%20Rings/1.jpg>

<http://192.168.1.20/Photos/Gold/Man%20Rings/2.jpg>

<http://192.168.1.20/Photos/Gold/Man%20Rings/3.jpg>

<http://192.168.1.20/Photos/Gold/Man%20Rings/4.jpg>

<http://192.168.1.20/Photos/Gold/Man%20Rings/5.jpg>

<http://192.168.1.20/Photos/Gold/Man%20Rings/6.jpg>

<http://192.168.1.20/Photos/Gold/Man%20Rings/7.jpg>

<http://192.168.1.20/Photos/Gold/Man%20Rings/8.jpg>

<http://192.168.1.20/Photos/Gold/Man%20Rings/9.jpg>

<http://192.168.1.20/Photos/Gold/Mang%20Tika>

<http://192.168.1.20/Photos/Gold/Mang%20Tika/>

<http://192.168.1.20/Photos/Gold/Mang%20Tika/1.jpg>

<http://192.168.1.20/Photos/Gold/Mang%20Tika/10.jpg>

<http://192.168.1.20/Photos/Gold/Mang%20Tika/2.jpg>

<http://192.168.1.20/Photos/Gold/Mang%20Tika/3.jpg>

<http://192.168.1.20/Photos/Gold/Mang%20Tika/4.jpg>

<http://192.168.1.20/Photos/Gold/Mang%20Tika/5.jpg>

<http://192.168.1.20/Photos/Gold/Mang%20Tika/6.jpg>

<http://192.168.1.20/Photos/Gold/Mang%20Tika/7.jpg>

<http://192.168.1.20/Photos/Gold/Mang%20Tika/9.jpg>

<http://192.168.1.20/Photos/Gold/MangalSutra>

<http://192.168.1.20/Photos/Gold/MangalSutra/>

<http://192.168.1.20/Photos/Gold/MangalSutra/1.jpg>

<http://192.168.1.20/Photos/Gold/MangalSutra/10.jpg>

<http://192.168.1.20/Photos/Gold/MangalSutra/2.jpg>

<http://192.168.1.20/Photos/Gold/MangalSutra/3.jpg>

<http://192.168.1.20/Photos/Gold/MangalSutra/4.jpg>

<http://192.168.1.20/Photos/Gold/MangalSutra/5.jpg>

<http://192.168.1.20/Photos/Gold/MangalSutra/6.jpg>

<http://192.168.1.20/Photos/Gold/MangalSutra/7.jpg>

<http://192.168.1.20/Photos/Gold/MangalSutra/8.jpg>

<http://192.168.1.20/Photos/Gold/MangalSutra/9.jpg>

<http://192.168.1.20/Photos/Gold/NeckLaces>

<http://192.168.1.20/Photos/Gold/NeckLaces/>

<http://192.168.1.20/Photos/Gold/NeckLaces/1.jpg>

<http://192.168.1.20/Photos/Gold/NeckLaces/10.jpg>

<http://192.168.1.20/Photos/Gold/NeckLaces/2.jpg>
<http://192.168.1.20/Photos/Gold/NeckLaces/3.jpg>
<http://192.168.1.20/Photos/Gold/NeckLaces/4.jpg>
<http://192.168.1.20/Photos/Gold/NeckLaces/5.jpg>
<http://192.168.1.20/Photos/Gold/NeckLaces/6.jpg>
<http://192.168.1.20/Photos/Gold/NeckLaces/7.jpg>
<http://192.168.1.20/Photos/Gold/NeckLaces/8.jpg>
<http://192.168.1.20/Photos/Gold/NeckLaces/9.jpg>
<http://192.168.1.20/Photos/Gold/Nose%20Rings/>
<http://192.168.1.20/Photos/Gold/Nose%20Rings/1.jpg>
<http://192.168.1.20/Photos/Gold/Nose%20Rings/2.jpg>
<http://192.168.1.20/Photos/Gold/Nose%20Rings/3.jpg>
<http://192.168.1.20/Photos/Gold/Nose%20Rings/4.jpg>
<http://192.168.1.20/Photos/Gold/Nose%20Rings/5.jpg>
<http://192.168.1.20/Photos/Gold/Nose%20Rings/6.jpg>
<http://192.168.1.20/Photos/Gold/Nose%20Rings/7.jpg>
<http://192.168.1.20/Photos/Gold/Nose%20Rings/8.jpg>
<http://192.168.1.20/Photos/Gold/Pendant%20Set/>
<http://192.168.1.20/Photos/Gold/Pendant%20Set/1.jpg>
<http://192.168.1.20/Photos/Gold/Pendant%20Set/10.jpg>
<http://192.168.1.20/Photos/Gold/Pendant%20Set/2.jpg>
<http://192.168.1.20/Photos/Gold/Pendant%20Set/3.jpg>
<http://192.168.1.20/Photos/Gold/Pendant%20Set/4.jpg>
<http://192.168.1.20/Photos/Gold/Pendant%20Set/5.jpg>
<http://192.168.1.20/Photos/Gold/Pendant%20Set/6.jpg>
<http://192.168.1.20/Photos/Gold/Pendant%20Set/7.jpg>
<http://192.168.1.20/Photos/Gold/Pendant%20Set/8.jpg>
<http://192.168.1.20/Photos/Gold/Pendant%20Set/9.jpg>
<http://192.168.1.20/Photos/Gold/Pendants/>
<http://192.168.1.20/Photos/Gold/Pendants/1.jpg>

<http://192.168.1.20/Photos/Gold/Pendants/10.jpg>

<http://192.168.1.20/Photos/Gold/Pendants/2.jpg>

<http://192.168.1.20/Photos/Gold/Pendants/3.jpg>

<http://192.168.1.20/Photos/Gold/Pendants/4.jpg>

<http://192.168.1.20/Photos/Gold/Pendants/5.jpg>

<http://192.168.1.20/Photos/Gold/Pendants/6.jpg>

<http://192.168.1.20/Photos/Gold/Pendants/7.jpg>

<http://192.168.1.20/Photos/Gold/Pendants/8.jpg>

<http://192.168.1.20/Photos/Gold/Pendants/9.jpg>

<http://192.168.1.20/Photos/Silver>

<http://192.168.1.20/Photos/Silver/>

<http://192.168.1.20/Photos/Silver/Anklets>

<http://192.168.1.20/Photos/Silver/Anklets/>

<http://192.168.1.20/Photos/Silver/Anklets/1.jpg>

<http://192.168.1.20/Photos/Silver/Anklets/10.jpg>

<http://192.168.1.20/Photos/Silver/Anklets/2.jpg>

<http://192.168.1.20/Photos/Silver/Anklets/3.jpg>

<http://192.168.1.20/Photos/Silver/Anklets/4.jpg>

<http://192.168.1.20/Photos/Silver/Anklets/5.jpg>

<http://192.168.1.20/Photos/Silver/Anklets/6.jpg>

<http://192.168.1.20/Photos/Silver/Anklets/7.jpg>

<http://192.168.1.20/Photos/Silver/Anklets/8.jpg>

<http://192.168.1.20/Photos/Silver/Anklets/9.jpg>

<http://192.168.1.20/Photos/Silver/Armllets>

<http://192.168.1.20/Photos/Silver/Armllets/>

<http://192.168.1.20/Photos/Silver/Armllets/1.jpg>

<http://192.168.1.20/Photos/Silver/Armllets/10.jpg>

<http://192.168.1.20/Photos/Silver/Armllets/2.jpg>

<http://192.168.1.20/Photos/Silver/Armllets/3.jpg>

<http://192.168.1.20/Photos/Silver/Armllets/4.jpg>

<http://192.168.1.20/Photos/Silver/Armllets/5.jpg>

<http://192.168.1.20/Photos/Silver/Armllets/6.jpg>

<http://192.168.1.20/Photos/Silver/Armllets/7.jpg>

<http://192.168.1.20/Photos/Silver/Armlets/8.jpg>
<http://192.168.1.20/Photos/Silver/Armlets/9.jpg>
<http://192.168.1.20/Photos/Silver/Bracelet>
<http://192.168.1.20/Photos/Silver/Bracelet/>
<http://192.168.1.20/Photos/Silver/Bracelet/1.jpg>
<http://192.168.1.20/Photos/Silver/Bracelet/10.jpg>
<http://192.168.1.20/Photos/Silver/Bracelet/2.jpg>
<http://192.168.1.20/Photos/Silver/Bracelet/3.jpg>
<http://192.168.1.20/Photos/Silver/Bracelet/4.jpg>
<http://192.168.1.20/Photos/Silver/Bracelet/5.jpg>
<http://192.168.1.20/Photos/Silver/Bracelet/6.jpg>
<http://192.168.1.20/Photos/Silver/Bracelet/7.jpg>
<http://192.168.1.20/Photos/Silver/Bracelet/8.jpg>
<http://192.168.1.20/Photos/Silver/Bracelet/9.jpg>
<http://192.168.1.20/Photos/Silver/Brooches>
<http://192.168.1.20/Photos/Silver/Brooches/>
<http://192.168.1.20/Photos/Silver/Brooches/1.jpg>
<http://192.168.1.20/Photos/Silver/Brooches/10.jpg>
<http://192.168.1.20/Photos/Silver/Brooches/2.jpg>
<http://192.168.1.20/Photos/Silver/Brooches/3.jpg>
<http://192.168.1.20/Photos/Silver/Brooches/4.jpg>
<http://192.168.1.20/Photos/Silver/Brooches/5.jpg>
<http://192.168.1.20/Photos/Silver/Brooches/6.jpg>
<http://192.168.1.20/Photos/Silver/Brooches/7.jpg>
<http://192.168.1.20/Photos/Silver/Brooches/8.jpg>
<http://192.168.1.20/Photos/Silver/Brooches/9.jpg>
<http://192.168.1.20/Photos/Silver/Chain>
<http://192.168.1.20/Photos/Silver/Chain/>
<http://192.168.1.20/Photos/Silver/Chain/1.jpg>
<http://192.168.1.20/Photos/Silver/Chain/10.jpg>
<http://192.168.1.20/Photos/Silver/Chain/2.jpg>
<http://192.168.1.20/Photos/Silver/Chain/3.jpg>
<http://192.168.1.20/Photos/Silver/Chain/4.jpg>

<http://192.168.1.20/Photos/Silver/Chain/5.jpg>
<http://192.168.1.20/Photos/Silver/Chain/6.jpg>
<http://192.168.1.20/Photos/Silver/Chain/7.jpg>
<http://192.168.1.20/Photos/Silver/Chain/8.jpg>
<http://192.168.1.20/Photos/Silver/Chain/9.jpg>
<http://192.168.1.20/Photos/Silver/Cufflinks>
<http://192.168.1.20/Photos/Silver/Cufflinks/>
<http://192.168.1.20/Photos/Silver/Cufflinks/1.jpg>
<http://192.168.1.20/Photos/Silver/Cufflinks/10.jpg>
<http://192.168.1.20/Photos/Silver/Cufflinks/2.jpg>
<http://192.168.1.20/Photos/Silver/Cufflinks/3.jpg>
<http://192.168.1.20/Photos/Silver/Cufflinks/4.jpg>
<http://192.168.1.20/Photos/Silver/Cufflinks/5.jpg>
<http://192.168.1.20/Photos/Silver/Cufflinks/6.jpg>
<http://192.168.1.20/Photos/Silver/Cufflinks/7.jpg>
<http://192.168.1.20/Photos/Silver/Cufflinks/8.jpg>
<http://192.168.1.20/Photos/Silver/Cufflinks/9.jpg>
<http://192.168.1.20/Photos/Silver/Earrings>
<http://192.168.1.20/Photos/Silver/Earrings/>
<http://192.168.1.20/Photos/Silver/Earrings/1.jpg>
<http://192.168.1.20/Photos/Silver/Earrings/10.jpg>
<http://192.168.1.20/Photos/Silver/Earrings/2.jpg>
<http://192.168.1.20/Photos/Silver/Earrings/3.jpg>
<http://192.168.1.20/Photos/Silver/Earrings/4.jpg>
<http://192.168.1.20/Photos/Silver/Earrings/5.jpg>
<http://192.168.1.20/Photos/Silver/Earrings/6.jpg>
<http://192.168.1.20/Photos/Silver/Earrings/7.jpg>
<http://192.168.1.20/Photos/Silver/Earrings/8.jpg>
<http://192.168.1.20/Photos/Silver/Earrings/9.jpg>
<http://192.168.1.20/Photos/Silver/Hair%20Pin>
<http://192.168.1.20/Photos/Silver/Hair%20Pin/>
<http://192.168.1.20/Photos/Silver/Hair%20Pin/1.jpg>
<http://192.168.1.20/Photos/Silver/Hair%20Pin/10.jpg>

<http://192.168.1.20/Photos/SilVer/Hair%20Pin/2.jpg>

<http://192.168.1.20/Photos/SilVer/Hair%20Pin/4.jpg>

<http://192.168.1.20/Photos/SilVer/Hair%20Pin/6.jpg>

<http://192.168.1.20/Photos/SilVer/Hair%20Pin/7.jpg>

<http://192.168.1.20/Photos/SilVer/Hair%20Pin/8.jpg>

<http://192.168.1.20/Photos/SilVer/Hair%20Pin/9.jpg>

<http://192.168.1.20/Photos/SilVer/Lady%20Rings>

<http://192.168.1.20/Photos/SilVer/Lady%20Rings/>

<http://192.168.1.20/Photos/SilVer/Lady%20Rings/1.jpg>

<http://192.168.1.20/Photos/SilVer/Lady%20Rings/10.jpg>

<http://192.168.1.20/Photos/SilVer/Lady%20Rings/3.jpg>

<http://192.168.1.20/Photos/SilVer/Lady%20Rings/4.jpg>

<http://192.168.1.20/Photos/SilVer/Lady%20Rings/5.jpg>

<http://192.168.1.20/Photos/SilVer/Lady%20Rings/6.jpg>

<http://192.168.1.20/Photos/SilVer/Lady%20Rings/7.jpg>

<http://192.168.1.20/Photos/SilVer/Lady%20Rings/8.jpg>

<http://192.168.1.20/Photos/SilVer/Lady%20Rings/9.jpg>

<http://192.168.1.20/Photos/SilVer/Man%20Ring>

<http://192.168.1.20/Photos/SilVer/Man%20Ring/>

<http://192.168.1.20/Photos/SilVer/Man%20Ring/1.jpg>

<http://192.168.1.20/Photos/SilVer/Man%20Ring/10.jpg>

<http://192.168.1.20/Photos/SilVer/Man%20Ring/2.jpg>

<http://192.168.1.20/Photos/SilVer/Man%20Ring/3.jpg>

<http://192.168.1.20/Photos/SilVer/Man%20Ring/4.jpg>

<http://192.168.1.20/Photos/SilVer/Man%20Ring/5.jpg>

<http://192.168.1.20/Photos/SilVer/Man%20Ring/6.jpg>

<http://192.168.1.20/Photos/SilVer/Man%20Ring/8.jpg>

<http://192.168.1.20/Photos/SilVer/Man%20Ring/9.jpg>

<http://192.168.1.20/Photos/SilVer/Pendants>

<http://192.168.1.20/Photos/SilVer/Pendants%20Sets>

<http://192.168.1.20/Photos/SilVer/Pendants%20Sets/>

<http://192.168.1.20/Photos/SilVer/Pendants%20Sets/1.jpg>

<http://192.168.1.20/Photos/SilVer/Pendants%20Sets/10.jpg>

<http://192.168.1.20/Photos/SilVer/Pendants%20Sets/2.jpg>

<http://192.168.1.20/Photos/SilVer/Pendants%20Sets/3.jpg>

<http://192.168.1.20/Photos/SilVer/Pendants%20Sets/4.jpg>

<http://192.168.1.20/Photos/SilVer/Pendants%20Sets/5.jpg>

<http://192.168.1.20/Photos/SilVer/Pendants%20Sets/6.jpg>

<http://192.168.1.20/Photos/SilVer/Pendants%20Sets/7.jpg>

<http://192.168.1.20/Photos/SilVer/Pendants%20Sets/8.jpg>

<http://192.168.1.20/Photos/SilVer/Pendants%20Sets/9.jpg>

<http://192.168.1.20/Photos/SilVer/Pendants/>

<http://192.168.1.20/Photos/SilVer/Pendants/1.jpg>

<http://192.168.1.20/Photos/SilVer/Pendants/10.jpg>

<http://192.168.1.20/Photos/SilVer/Pendants/3.jpg>

<http://192.168.1.20/Photos/SilVer/Pendants/4.jpg>

<http://192.168.1.20/Photos/SilVer/Pendants/5.jpg>

<http://192.168.1.20/Photos/SilVer/Pendants/6.jpg>

<http://192.168.1.20/Photos/SilVer/Pendants/7.jpg>

<http://192.168.1.20/Photos/SilVer/Pendants/8.jpg>

<http://192.168.1.20/Photos/SilVer/Pendants/9.jpg>

<http://192.168.1.20/Photos/SilVer/Toe%20Ring>

<http://192.168.1.20/Photos/SilVer/Toe%20Ring/>

<http://192.168.1.20/Photos/SilVer/Toe%20Ring/1.jpg>

<http://192.168.1.20/Photos/SilVer/Toe%20Ring/2.jpg>

<http://192.168.1.20/Photos/SilVer/Toe%20Ring/3.jpg>

<http://192.168.1.20/Photos/SilVer/Toe%20Ring/4.jpg>

<http://192.168.1.20/Photos/SilVer/Toe%20Ring/5.jpg>

<http://192.168.1.20/Photos/SilVer/Toe%20Ring/6.jpg>

<http://192.168.1.20/Photos/SilVer/Toe%20Ring/7.jpg>

<http://192.168.1.20/Photos/SilVer/Toe%20Ring/8.jpg>

<http://192.168.1.20/Photos/SilVer/Toe%20Ring/9.jpg>

<http://192.168.1.20/about.php>

<http://192.168.1.20/adminstyle.css>

[http://192.168.1.20/attachment.php?="](http://192.168.1.20/attachment.php?=)

<http://192.168.1.20/attachment.php?type=terms.php>

Isaac Basque-Rice

<http://192.168.1.20/contact.php>
<http://192.168.1.20/css>
<http://192.168.1.20/css/>
<http://192.168.1.20/css/carousel.css>
<http://192.168.1.20/css/flexslider.css>
<http://192.168.1.20/css/stylesheet.css>
<http://192.168.1.20/default.php>
<http://192.168.1.20/featured.php>
<http://192.168.1.20/featured.php?pn=24>
<http://192.168.1.20/image>
<http://192.168.1.20/image/>
<http://192.168.1.20/image/addBanner-940x145.jpg>
<http://192.168.1.20/image/banner1-960x300.jpg>
<http://192.168.1.20/image/banner2-960x300.jpg>
<http://192.168.1.20/image/favicon.png>
<http://192.168.1.20/image/logo.png>
<http://192.168.1.20/image/mail.png>
<http://192.168.1.20/image/phone.png>
<http://192.168.1.20/index.php>
<http://192.168.1.20/js>
<http://192.168.1.20/js/>
<http://192.168.1.20/js/custom.js>
<http://192.168.1.20/js/html5.js>
<http://192.168.1.20/js/jquery-1.7.1.min.js>
<http://192.168.1.20/js/jquery.fancybox.pack.js>
<http://192.168.1.20/js/jquery.flexslider-min.js>
<http://192.168.1.20/js/jquery.jcarousel.min.js>
<http://192.168.1.20/js/tabs.js>
<http://192.168.1.20/latest.php>
<http://192.168.1.20/latest.php?pn=1>
<http://192.168.1.20/register.html>
<http://192.168.1.20/robots.txt>
<http://192.168.1.20/schema.sql>

<http://192.168.1.20/sitemap.xml>
<http://192.168.1.20/topsell.php?Items=0032&MenuCat=8&Subname=Sellings>
<http://192.168.1.20/topviewed.php?Items=0031&MenuCat=8&Subname=Views>
<http://192.168.1.20/viewproduct.php?=&MenuCat=5&Subname=Pendants>
<http://192.168.1.20/viewproduct.php?=&pn=>
<http://192.168.1.20/viewproduct.php?Items=0006&MenuCat=5&=>
<http://192.168.1.20/viewproduct.php?Items=0006&MenuCat=5&Subname=Pendants>
<http://192.168.1.20/viewproduct.php?Items=0006&pn>
<http://192.168.1.20/viewpurchase.php>

4.3 APPENDIX C – CONSOLE OUTPUT

4.3.1 Section 1 – Dirb Output

```
-----  
DIRB v2.22  
By The Dark Raver  
-----  
  
OUTPUT_FILE: dirb.txt  
START_TIME: Tue Nov 16 10:12:48 2021  
URL_BASE: http://192.168.1.20/  
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt  
  
-----  
  
GENERATED WORDS: 4612  
  
---- Scanning URL: http://192.168.1.20/ ----  
==> DIRECTORY: http://192.168.1.20/adminarea/  
+ http://192.168.1.20/cgi-bin/ (CODE:403|SIZE:1038)  
==> DIRECTORY: http://192.168.1.20/contact/  
==> DIRECTORY: http://192.168.1.20/css/  
==> DIRECTORY: http://192.168.1.20/font/
```

```
==> DIRECTORY: http://192.168.1.20/image/
==> DIRECTORY: http://192.168.1.20/includes/
+ http://192.168.1.20/index.php (CODE:200|SIZE:16657)
==> DIRECTORY: http://192.168.1.20/js/
+ http://192.168.1.20/phpinfo.php (CODE:200|SIZE:98420)
+ http://192.168.1.20/phpmyadmin (CODE:403|SIZE:1193)
==> DIRECTORY: http://192.168.1.20/pics/
==> DIRECTORY: http://192.168.1.20/pictures/
+ http://192.168.1.20/robots.txt (CODE:200|SIZE:36)

---- Entering directory: http://192.168.1.20/adminarea/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.1.20/contact/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.1.20/css/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.1.20/font/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.1.20/image/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.1.20/includes/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)
```

```
---- Entering directory: http://192.168.1.20/js/ ----  
(!) WARNING: Directory IS LISTABLE. No need to scan it.  
      (Use mode '-w' if you want to scan it anyway)  
  
---- Entering directory: http://192.168.1.20/pics/ ----  
(!) WARNING: Directory IS LISTABLE. No need to scan it.  
      (Use mode '-w' if you want to scan it anyway)  
  
---- Entering directory: http://192.168.1.20/pictures/ ----  
(!) WARNING: Directory IS LISTABLE. No need to scan it.  
      (Use mode '-w' if you want to scan it anyway)
```

```
-----  
END_TIME: Tue Nov 16 10:12:53 2021
```

```
DOWNLOADED: 4612 - FOUND: 5
```

4.3.2 Section 2 – Nikto Output

- Nikto v2.1.6

```
-----  
+ Target IP:          192.168.1.20  
+ Target Hostname:    192.168.1.20  
+ Target Port:        80  
+ Start Time:         2021-11-16 10:00:24 (GMT-5)  
  
-----  
+ Server: Apache/2.4.29 (Unix) OpenSSL/1.0.2n PHP/5.6.34 mod_perl/2.0.8-dev  
Perl/v5.16.3  
+ Retrieved x-powered-by header: PHP/5.6.34  
+ The anti-clickjacking X-Frame-Options header is not present.  
+ The X-XSS-Protection header is not defined. This header can hint to the user agent  
to protect against some forms of XSS  
+ The X-Content-Type-Options header is not set. This could allow the user agent to  
render the content of the site in a different fashion to the MIME type  
+ Cookie PHPSESSID created without the httponly flag  
+ Entry '/schema.sql' in robots.txt returned a non-forbidden or redirect HTTP code  
(200)
```


+ Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. See <http://www.wisec.it/sectou.php?id=4698ebdc59d15>. The following alternatives for 'index' were found: HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var

+ Apache/2.4.29 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.

+ PHP/5.6.34 appears to be outdated (current is at least 7.2.12). PHP 5.6.33, 7.0.27, 7.1.13, 7.2.1 may also current release for each branch.

+ OpenSSL/1.0.2n appears to be outdated (current is at least 1.1.1). OpenSSL 1.0.0o and 0.9.8zc are also current.

+ Perl/v5.16.3 appears to be outdated (current is at least v5.20.0)

+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.

+ DEBUG HTTP verb may show server debugging information. See <http://msdn.microsoft.com/en-us/library/e8z01xdh%28VS.80%29.aspx> for details.

+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST

+ /phpinfo.php: Output from the phpinfo() function was found.

+ OSVDB-3268: /css/: Directory indexing found.

+ OSVDB-3092: /css/: This might be interesting...

+ OSVDB-3268: /includes/: Directory indexing found.

+ OSVDB-3092: /includes/: This might be interesting...

+ OSVDB-3268: /pics/: Directory indexing found.

+ OSVDB-3092: /pics/: This might be interesting...

+ OSVDB-3233: /phpinfo.php: PHP is installed, and a test script which runs phpinfo() was found. This gives a lot of system information.

+ OSVDB-3268: /icons/: Directory indexing found.

+ OSVDB-3268: /image/: Directory indexing found.

+ OSVDB-3233: /icons/README: Apache default file found.

+ /login.php: Admin Login page/section found.

+ 8725 requests: 0 error(s) and 26 item(s) reported on remote host

+ End Time: 2021-11-16 10:01:20 (GMT-5) (56 seconds)

+ 1 host(s) tested

4.4 APPENDIX D - GUI TOOL OUTPUT

4.4.1 OWASP Zap Scan Report Output

ZAP Scanning Report

Generated with The ZAP LogoZAP on Tue 23 Nov 2021, at 14:37:47

Contents

[About this report](#)

[Report parameters](#)

Summaries

[Alert counts by risk and confidence](#)

[Alert counts by site and risk](#)

[Alert counts by alert type](#)

Alerts

[Risk=High, Confidence=Medium \(4\)](#)

[Risk=Medium, Confidence=Medium \(179\)](#)

[Risk=Medium, Confidence=Low \(4\)](#)

[Risk=Low, Confidence=Medium \(589\)](#)

[Risk=Low, Confidence=Low \(6\)](#)

[Risk=Informational, Confidence=Medium \(1\)](#)

[Risk=Informational, Confidence=Low \(5\)](#)

Appendix

[Alert types](#)

[About this report](#)

[Report parameters](#)

Contexts

No contexts were selected, so all contexts were included by default.

Sites

The following sites were included:

http://192.168.1.20

(If no sites were selected, all sites were included by default.)

Isaac Basque-Rice

An included site must also be within one of the included contexts for its data to be included in the report.

Risk Levels

Included: High, Medium, Low, Informational

Excluded: None

Confidence Levels

Included: User Confirmed, High, Medium, Low

Excluded: User Confirmed, High, Medium, Low, False Positive

Summaries

Alert counts by risk and confidence

This table shows the number of alerts for each level of risk and confidence included in the report.

(The percentages in brackets represent the count as a percentage of the total number of alerts included in the report, rounded to one decimal place.)

Confidence

User Confirmed High Medium Low Total

Risk High 0

(0.0%) 0

(0.0%) 4

(0.5%) 0

(0.0%) 4

(0.5%)

Medium 0

(0.0%) 0

(0.0%) 179

(22.7%) 4

Isaac Basque-Rice

(0.5%) 183
(23.2%)
Low 0
(0.0%) 0
(0.0%) 589
(74.7%) 6
(0.8%) 595
(75.5%)
Informational 0
(0.0%) 0
(0.0%) 1
(0.1%) 5
(0.6%) 6
(0.8%)
Total 0
(0.0%) 0
(0.0%) 773
(98.1%) 15
(1.9%) 788
(100%)

Alert counts by site and risk

This table shows, for each site for which one or more alerts were raised, the number of alerts raised at each risk level.

Alerts with a confidence level of "False Positive" have been excluded from these counts.

(The numbers in brackets are the number of alerts raised for the site at or above that risk level.)

Risk

High

(= High) Medium

(>= Medium) Low

Isaac Basque-Rice

(>= Low) Informational

(>= Informational)

Site <http://192.168.1.20> 4

(4) 183

(187) 595

(782) 6

(788)

Alert counts by alert type

This table shows the number of alerts of each alert type, together with the alert type's risk level.

(The percentages in brackets represent each count as a percentage, rounded to one decimal place, of the total number of alerts included in this report.)

Alert type	Risk	Count
Cross Site Scripting (Reflected)	High	1 (0.1%)
Path Traversal	High	1 (0.1%)
SQL Injection	High	2 (0.3%)
Application Error Disclosure	Medium	1 (0.1%)
Directory Browsing	Medium	37 (4.7%)
Parameter Tampering	Medium	4 (0.5%)
Vulnerable JS Library	Medium	1 (0.1%)
X-Frame-Options Header Not Set	Medium	140 (17.8%)
Absence of Anti-CSRF Tokens	Low	1 (0.1%)
Cookie No HttpOnly Flag	Low	1

Isaac Basque-Rice

(0.1%)

Cookie without SameSite Attribute Low 1

(0.1%)

Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s) Low
140

(17.8%)

Timestamp Disclosure - Unix Low 6

(0.8%)

X-Content-Type-Options Header Missing Low 446

(56.6%)

Content-Type Header Missing Informational1

(0.1%)

Information Disclosure - Suspicious Comments Informational5

(0.6%)

Total 788

Alerts

Risk=High, Confidence=Medium (4)

<http://192.168.1.20> (4)

Cross Site Scripting (Reflected) (1)

GET

<http://192.168.1.20/viewproduct.php?Items=0006&MenuCat=5&Subname=%3C%2Fh2%3E%3Cscript%3Ealert%281%29%3B%3C%2Fscript%3E%3Ch2%3E>

Path Traversal (1)

GET <http://192.168.1.20/attachment.php?type=%2Fetc%2Fpasswd>

SQL Injection (2)

GET <http://192.168.1.20/viewproduct.php?Items=8-2&MenuCat=5&Subname=Pendants>

GET <http://192.168.1.20/viewproduct.php?Items=8-2&pn=1>

Risk=Medium, Confidence=Medium (179)

<http://192.168.1.20> (179)

Application Error Disclosure (1)

GET <http://192.168.1.20/viewpurchase.php>

Directory Browsing (37)

GET <http://192.168.1.20/css/>

GET <http://192.168.1.20/image/>

GET <http://192.168.1.20/js/>
GET <http://192.168.1.20/Photos/>
GET <http://192.168.1.20/Photos/Diamond/>
GET <http://192.168.1.20/Photos/Diamond/Bangles/>
GET <http://192.168.1.20/Photos/Diamond/Earrings/>
GET <http://192.168.1.20/Photos/Diamond/Lady%20Ring/>
GET <http://192.168.1.20/Photos/Diamond/Necklaces/>
GET <http://192.168.1.20/Photos/Diamond/Nose%20Pin/>
GET <http://192.168.1.20/Photos/Diamond/Pendant%20Set/>
GET <http://192.168.1.20/Photos/Diamond/Pendants/>
GET <http://192.168.1.20/Photos/Gold/>
GET <http://192.168.1.20/Photos/Gold/Bangles/>
GET <http://192.168.1.20/Photos/Gold/Ear%20Rings/>
GET <http://192.168.1.20/Photos/Gold/Lady%20Rings/>
GET <http://192.168.1.20/Photos/Gold/Man%20Rings/>
GET <http://192.168.1.20/Photos/Gold/Mang%20Tika/>
GET <http://192.168.1.20/Photos/Gold/Mangalsutra/>
GET <http://192.168.1.20/Photos/Gold/Necklaces/>
GET <http://192.168.1.20/Photos/Gold/Nose%20Rings/>
GET <http://192.168.1.20/Photos/Gold/Pendant%20Set/>
GET <http://192.168.1.20/Photos/Gold/Pendants/>
GET <http://192.168.1.20/Photos/Silver/>
GET <http://192.168.1.20/Photos/Silver/Anklets/>
GET <http://192.168.1.20/Photos/Silver/Armllets/>
GET <http://192.168.1.20/Photos/Silver/Bracelet/>
GET <http://192.168.1.20/Photos/Silver/Brooches/>
GET <http://192.168.1.20/Photos/Silver/Chain/>
GET <http://192.168.1.20/Photos/Silver/Cufflinks/>
GET <http://192.168.1.20/Photos/Silver/Earrings/>
GET <http://192.168.1.20/Photos/Silver/Hair%20Pin/>
GET <http://192.168.1.20/Photos/Silver/Lady%20Rings/>
GET <http://192.168.1.20/Photos/Silver/Man%20Ring/>
GET <http://192.168.1.20/Photos/Silver/Pendants%20Sets/>

GET http://192.168.1.20/Photos/Silver/Pendants/
GET http://192.168.1.20/Photos/Silver/Toe%20Ring/
Vulnerable JS Library (1)
GET http://192.168.1.20/js/jquery-1.7.1.min.js
X-Frame-Options Header Not Set (140)
GET http://192.168.1.20
GET http://192.168.1.20/
GET http://192.168.1.20/about.php
GET http://192.168.1.20/attachment.php?type=delivery.php
GET http://192.168.1.20/attachment.php?type=terms.php
GET http://192.168.1.20/contact.php
GET http://192.168.1.20/featured.php
GET http://192.168.1.20/featured.php?pn=1
GET http://192.168.1.20/featured.php?pn=10
GET http://192.168.1.20/featured.php?pn=11
GET http://192.168.1.20/featured.php?pn=12
GET http://192.168.1.20/featured.php?pn=13
GET http://192.168.1.20/featured.php?pn=14
GET http://192.168.1.20/featured.php?pn=15
GET http://192.168.1.20/featured.php?pn=16
GET http://192.168.1.20/featured.php?pn=17
GET http://192.168.1.20/featured.php?pn=18
GET http://192.168.1.20/featured.php?pn=19
GET http://192.168.1.20/featured.php?pn=2
GET http://192.168.1.20/featured.php?pn=20
GET http://192.168.1.20/featured.php?pn=21
GET http://192.168.1.20/featured.php?pn=22
GET http://192.168.1.20/featured.php?pn=23
GET http://192.168.1.20/featured.php?pn=24
GET http://192.168.1.20/featured.php?pn=25
GET http://192.168.1.20/featured.php?pn=26
GET http://192.168.1.20/featured.php?pn=27
GET http://192.168.1.20/featured.php?pn=28

GET <http://192.168.1.20/featured.php?pn=29>
GET <http://192.168.1.20/featured.php?pn=3>
GET <http://192.168.1.20/featured.php?pn=30>
GET <http://192.168.1.20/featured.php?pn=31>
GET <http://192.168.1.20/featured.php?pn=32>
GET <http://192.168.1.20/featured.php?pn=33>
GET <http://192.168.1.20/featured.php?pn=34>
GET <http://192.168.1.20/featured.php?pn=35>
GET <http://192.168.1.20/featured.php?pn=4>
GET <http://192.168.1.20/featured.php?pn=5>
GET <http://192.168.1.20/featured.php?pn=6>
GET <http://192.168.1.20/featured.php?pn=7>
GET <http://192.168.1.20/featured.php?pn=8>
GET <http://192.168.1.20/featured.php?pn=9>
GET <http://192.168.1.20/index.php>
GET <http://192.168.1.20/latest.php>
GET <http://192.168.1.20/latest.php?pn=1>
GET <http://192.168.1.20/latest.php?pn=2>
GET <http://192.168.1.20/register.html>
GET <http://192.168.1.20/topsell.php?Items=0032&MenuCat=8&Subname=Sellings>
GET <http://192.168.1.20/topviewed.php?Items=0031&MenuCat=8&Subname=Views>
GET <http://192.168.1.20/viewproduct.php?Items=0001&MenuCat=5&Subname=Bangles>
GET <http://192.168.1.20/viewproduct.php?Items=0001&pn>
GET <http://192.168.1.20/viewproduct.php?Items=0001&pn=1>
GET <http://192.168.1.20/viewproduct.php?Items=0001&pn=2>
GET <http://192.168.1.20/viewproduct.php?Items=0002&MenuCat=5&Subname=EarRings>
GET <http://192.168.1.20/viewproduct.php?Items=0002&pn>
GET <http://192.168.1.20/viewproduct.php?Items=0002&pn=1>
GET <http://192.168.1.20/viewproduct.php?Items=0002&pn=2>
GET <http://192.168.1.20/viewproduct.php?Items=0003&MenuCat=5&Subname=Necklaces>
GET <http://192.168.1.20/viewproduct.php?Items=0004&MenuCat=5&Subname=Nose%20Pin>
GET <http://192.168.1.20/viewproduct.php?Items=0004&pn>
GET <http://192.168.1.20/viewproduct.php?Items=0004&pn=1>

GET <http://192.168.1.20/viewproduct.php?Items=0004&pn=2>
GET <http://192.168.1.20/viewproduct.php?Items=0005&MenuCat=5&Subname=Pendant%20Set>
GET <http://192.168.1.20/viewproduct.php?Items=0006&MenuCat=5&Subname=Pendants>
GET <http://192.168.1.20/viewproduct.php?Items=0006&pn>
GET <http://192.168.1.20/viewproduct.php?Items=0006&pn=1>
GET <http://192.168.1.20/viewproduct.php?Items=0006&pn=2>
GET <http://192.168.1.20/viewproduct.php?Items=0007&MenuCat=5&Subname=LadyRings>
GET <http://192.168.1.20/viewproduct.php?Items=0007&pn>
GET <http://192.168.1.20/viewproduct.php?Items=0007&pn=1>
GET <http://192.168.1.20/viewproduct.php?Items=0007&pn=2>
GET <http://192.168.1.20/viewproduct.php?Items=0008&MenuCat=3&Subname=Bangles>
GET <http://192.168.1.20/viewproduct.php?Items=0008&pn>
GET <http://192.168.1.20/viewproduct.php?Items=0008&pn=1>
GET <http://192.168.1.20/viewproduct.php?Items=0008&pn=2>
GET <http://192.168.1.20/viewproduct.php?Items=0009&MenuCat=3&Subname=Ear%20Rings>
GET <http://192.168.1.20/viewproduct.php?Items=0009&pn>
GET <http://192.168.1.20/viewproduct.php?Items=0009&pn=1>
GET <http://192.168.1.20/viewproduct.php?Items=0009&pn=2>
GET <http://192.168.1.20/viewproduct.php?Items=0010&MenuCat=3&Subname=Mang%20Tika>
GET <http://192.168.1.20/viewproduct.php?Items=0010&pn>
GET <http://192.168.1.20/viewproduct.php?Items=0010&pn=1>
GET <http://192.168.1.20/viewproduct.php?Items=0010&pn=2>
GET <http://192.168.1.20/viewproduct.php?Items=0011&MenuCat=3&Subname=Mangalsutra>
GET <http://192.168.1.20/viewproduct.php?Items=0011&pn>
GET <http://192.168.1.20/viewproduct.php?Items=0011&pn=1>
GET <http://192.168.1.20/viewproduct.php?Items=0011&pn=2>
GET <http://192.168.1.20/viewproduct.php?Items=0012&MenuCat=3&Subname=NeckLaces>
GET <http://192.168.1.20/viewproduct.php?Items=0012&pn>
GET <http://192.168.1.20/viewproduct.php?Items=0012&pn=1>
GET <http://192.168.1.20/viewproduct.php?Items=0012&pn=2>
GET <http://192.168.1.20/viewproduct.php?Items=0013&MenuCat=3&Subname=Nose%20Rings>
GET <http://192.168.1.20/viewproduct.php?Items=0013&pn>
GET <http://192.168.1.20/viewproduct.php?Items=0013&pn=1>

GET <http://192.168.1.20/viewproduct.php?Items=0013&pn=2>
GET <http://192.168.1.20/viewproduct.php?Items=0014&MenuCat=3&Subname=Pendant%20Set>
GET <http://192.168.1.20/viewproduct.php?Items=0015&MenuCat=3&Subname=Pendants>
GET <http://192.168.1.20/viewproduct.php?Items=0015&pn>
GET <http://192.168.1.20/viewproduct.php?Items=0015&pn=1>
GET <http://192.168.1.20/viewproduct.php?Items=0015&pn=2>
GET <http://192.168.1.20/viewproduct.php?Items=0016&MenuCat=4&Subname=AnkLets>
GET <http://192.168.1.20/viewproduct.php?Items=0016&pn>
GET <http://192.168.1.20/viewproduct.php?Items=0016&pn=1>
GET <http://192.168.1.20/viewproduct.php?Items=0016&pn=2>
GET <http://192.168.1.20/viewproduct.php?Items=0017&MenuCat=4&Subname=ArmLets>
GET <http://192.168.1.20/viewproduct.php?Items=0018&MenuCat=4&Subname=BraceLet>
GET <http://192.168.1.20/viewproduct.php?Items=0019&MenuCat=4&Subname=Brooches>
GET <http://192.168.1.20/viewproduct.php?Items=0020&MenuCat=4&Subname=Hair%20Pin>
GET <http://192.168.1.20/viewproduct.php?Items=0021&MenuCat=4&Subname=EarRings>
GET <http://192.168.1.20/viewproduct.php?Items=0021&pn>
GET <http://192.168.1.20/viewproduct.php?Items=0021&pn=1>
GET <http://192.168.1.20/viewproduct.php?Items=0021&pn=2>
GET <http://192.168.1.20/viewproduct.php?Items=0022&MenuCat=4&Subname=Cuffilinks>
GET <http://192.168.1.20/viewproduct.php?Items=0022&pn>
GET <http://192.168.1.20/viewproduct.php?Items=0022&pn=1>
GET <http://192.168.1.20/viewproduct.php?Items=0022&pn=2>
GET <http://192.168.1.20/viewproduct.php?Items=0023&MenuCat=4&Subname=Chain>
GET <http://192.168.1.20/viewproduct.php?Items=0023&pn>
GET <http://192.168.1.20/viewproduct.php?Items=0023&pn=1>
GET <http://192.168.1.20/viewproduct.php?Items=0023&pn=2>
GET <http://192.168.1.20/viewproduct.php?Items=0024&MenuCat=4&Subname=ManRings>
GET <http://192.168.1.20/viewproduct.php?Items=0024&pn>
GET <http://192.168.1.20/viewproduct.php?Items=0024&pn=1>
GET <http://192.168.1.20/viewproduct.php?Items=0024&pn=2>
GET <http://192.168.1.20/viewproduct.php?Items=0025&MenuCat=4&Subname=Pendants>
GET <http://192.168.1.20/viewproduct.php?Items=0026&MenuCat=4&Subname=Pendants%20Sets>
GET <http://192.168.1.20/viewproduct.php?Items=0026&pn>

GET <http://192.168.1.20/viewproduct.php?Items=0026&pn=1>
GET <http://192.168.1.20/viewproduct.php?Items=0026&pn=2>
GET <http://192.168.1.20/viewproduct.php?Items=0027&MenuCat=4&Subname=Lady%20Rings>
GET <http://192.168.1.20/viewproduct.php?Items=0028&MenuCat=3&Subname=LadyRings>
GET <http://192.168.1.20/viewproduct.php?Items=0028&pn>
GET <http://192.168.1.20/viewproduct.php?Items=0028&pn=1>
GET <http://192.168.1.20/viewproduct.php?Items=0028&pn=2>
GET <http://192.168.1.20/viewproduct.php?Items=0029&MenuCat=3&Subname=ManRings>
GET <http://192.168.1.20/viewproduct.php?Items=0030&MenuCat=4&Subname=ToeRings>
GET <http://192.168.1.20/viewproduct.php?Items=0030&pn>
GET <http://192.168.1.20/viewproduct.php?Items=0030&pn=1>
GET <http://192.168.1.20/viewproduct.php?Items=0030&pn=2>
GET <http://192.168.1.20/viewpurchase.php>
Risk=Medium, Confidence=Low (4)
<http://192.168.1.20> (4)
Parameter Tampering (4)
GET [http://192.168.1.20/attachment.php?="](http://192.168.1.20/attachment.php?=)
GET <http://192.168.1.20/viewproduct.php?=&MenuCat=5&Subname=Pendants>
GET <http://192.168.1.20/viewproduct.php?=&pn=1>
GET [http://192.168.1.20/viewproduct.php?Items=0006&MenuCat=5&="](http://192.168.1.20/viewproduct.php?Items=0006&MenuCat=5&=)
Risk=Low, Confidence=Medium (589)
<http://192.168.1.20> (589)
Absence of Anti-CSRF Tokens (1)
GET <http://192.168.1.20/viewpurchase.php>
Cookie No HttpOnly Flag (1)
GET <http://192.168.1.20>
Cookie without SameSite Attribute (1)
GET <http://192.168.1.20>
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s) (140)
GET <http://192.168.1.20>
GET <http://192.168.1.20/>
GET <http://192.168.1.20/about.php>
GET <http://192.168.1.20/attachment.php?type=delivery.php>

GET <http://192.168.1.20/attachment.php?type=terms.php>
GET <http://192.168.1.20/contact.php>
GET <http://192.168.1.20/default.php>
GET <http://192.168.1.20/featured.php>
GET <http://192.168.1.20/featured.php?pn=1>
GET <http://192.168.1.20/featured.php?pn=10>
GET <http://192.168.1.20/featured.php?pn=11>
GET <http://192.168.1.20/featured.php?pn=12>
GET <http://192.168.1.20/featured.php?pn=13>
GET <http://192.168.1.20/featured.php?pn=14>
GET <http://192.168.1.20/featured.php?pn=15>
GET <http://192.168.1.20/featured.php?pn=16>
GET <http://192.168.1.20/featured.php?pn=17>
GET <http://192.168.1.20/featured.php?pn=18>
GET <http://192.168.1.20/featured.php?pn=19>
GET <http://192.168.1.20/featured.php?pn=2>
GET <http://192.168.1.20/featured.php?pn=20>
GET <http://192.168.1.20/featured.php?pn=21>
GET <http://192.168.1.20/featured.php?pn=22>
GET <http://192.168.1.20/featured.php?pn=23>
GET <http://192.168.1.20/featured.php?pn=24>
GET <http://192.168.1.20/featured.php?pn=25>
GET <http://192.168.1.20/featured.php?pn=26>
GET <http://192.168.1.20/featured.php?pn=27>
GET <http://192.168.1.20/featured.php?pn=28>
GET <http://192.168.1.20/featured.php?pn=29>
GET <http://192.168.1.20/featured.php?pn=3>
GET <http://192.168.1.20/featured.php?pn=30>
GET <http://192.168.1.20/featured.php?pn=31>
GET <http://192.168.1.20/featured.php?pn=32>
GET <http://192.168.1.20/featured.php?pn=33>
GET <http://192.168.1.20/featured.php?pn=34>
GET <http://192.168.1.20/featured.php?pn=35>

GET <http://192.168.1.20/featured.php?pn=4>
GET <http://192.168.1.20/featured.php?pn=5>
GET <http://192.168.1.20/featured.php?pn=6>
GET <http://192.168.1.20/featured.php?pn=7>
GET <http://192.168.1.20/featured.php?pn=8>
GET <http://192.168.1.20/featured.php?pn=9>
GET <http://192.168.1.20/index.php>
GET <http://192.168.1.20/latest.php>
GET <http://192.168.1.20/latest.php?pn=1>
GET <http://192.168.1.20/latest.php?pn=2>
GET <http://192.168.1.20/topsell.php?Items=0032&MenuCat=8&Subname=Sellings>
GET <http://192.168.1.20/topviewed.php?Items=0031&MenuCat=8&Subname=Views>
GET <http://192.168.1.20/viewproduct.php?Items=0001&MenuCat=5&Subname=Bangles>
GET <http://192.168.1.20/viewproduct.php?Items=0001&pn>
GET <http://192.168.1.20/viewproduct.php?Items=0001&pn=1>
GET <http://192.168.1.20/viewproduct.php?Items=0001&pn=2>
GET <http://192.168.1.20/viewproduct.php?Items=0002&MenuCat=5&Subname=EarRings>
GET <http://192.168.1.20/viewproduct.php?Items=0002&pn>
GET <http://192.168.1.20/viewproduct.php?Items=0002&pn=1>
GET <http://192.168.1.20/viewproduct.php?Items=0002&pn=2>
GET <http://192.168.1.20/viewproduct.php?Items=0003&MenuCat=5&Subname=NeckLaces>
GET <http://192.168.1.20/viewproduct.php?Items=0004&MenuCat=5&Subname=Nose%20Pin>
GET <http://192.168.1.20/viewproduct.php?Items=0004&pn>
GET <http://192.168.1.20/viewproduct.php?Items=0004&pn=1>
GET <http://192.168.1.20/viewproduct.php?Items=0004&pn=2>
GET <http://192.168.1.20/viewproduct.php?Items=0005&MenuCat=5&Subname=Pendant%20Set>
GET <http://192.168.1.20/viewproduct.php?Items=0006&MenuCat=5&Subname=Pendants>
GET <http://192.168.1.20/viewproduct.php?Items=0006&pn>
GET <http://192.168.1.20/viewproduct.php?Items=0006&pn=1>
GET <http://192.168.1.20/viewproduct.php?Items=0006&pn=2>
GET <http://192.168.1.20/viewproduct.php?Items=0007&MenuCat=5&Subname=LadyRings>
GET <http://192.168.1.20/viewproduct.php?Items=0007&pn>
GET <http://192.168.1.20/viewproduct.php?Items=0007&pn=1>

GET <http://192.168.1.20/viewproduct.php?Items=0007&pn=2>
GET <http://192.168.1.20/viewproduct.php?Items=0008&MenuCat=3&Subname=Bangles>
GET <http://192.168.1.20/viewproduct.php?Items=0008&pn>
GET <http://192.168.1.20/viewproduct.php?Items=0008&pn=1>
GET <http://192.168.1.20/viewproduct.php?Items=0008&pn=2>
GET <http://192.168.1.20/viewproduct.php?Items=0009&MenuCat=3&Subname=Ear%20Rings>
GET <http://192.168.1.20/viewproduct.php?Items=0009&pn>
GET <http://192.168.1.20/viewproduct.php?Items=0009&pn=1>
GET <http://192.168.1.20/viewproduct.php?Items=0009&pn=2>
GET <http://192.168.1.20/viewproduct.php?Items=0010&MenuCat=3&Subname=Mang%20Tika>
GET <http://192.168.1.20/viewproduct.php?Items=0010&pn>
GET <http://192.168.1.20/viewproduct.php?Items=0010&pn=1>
GET <http://192.168.1.20/viewproduct.php?Items=0010&pn=2>
GET <http://192.168.1.20/viewproduct.php?Items=0011&MenuCat=3&Subname=Mangalsutra>
GET <http://192.168.1.20/viewproduct.php?Items=0011&pn>
GET <http://192.168.1.20/viewproduct.php?Items=0011&pn=1>
GET <http://192.168.1.20/viewproduct.php?Items=0011&pn=2>
GET <http://192.168.1.20/viewproduct.php?Items=0012&MenuCat=3&Subname=NeckLaces>
GET <http://192.168.1.20/viewproduct.php?Items=0012&pn>
GET <http://192.168.1.20/viewproduct.php?Items=0012&pn=1>
GET <http://192.168.1.20/viewproduct.php?Items=0012&pn=2>
GET <http://192.168.1.20/viewproduct.php?Items=0013&MenuCat=3&Subname=Nose%20Rings>
GET <http://192.168.1.20/viewproduct.php?Items=0013&pn>
GET <http://192.168.1.20/viewproduct.php?Items=0013&pn=1>
GET <http://192.168.1.20/viewproduct.php?Items=0013&pn=2>
GET <http://192.168.1.20/viewproduct.php?Items=0014&MenuCat=3&Subname=Pendant%20Set>
GET <http://192.168.1.20/viewproduct.php?Items=0015&MenuCat=3&Subname=Pendants>
GET <http://192.168.1.20/viewproduct.php?Items=0015&pn>
GET <http://192.168.1.20/viewproduct.php?Items=0015&pn=1>
GET <http://192.168.1.20/viewproduct.php?Items=0015&pn=2>
GET <http://192.168.1.20/viewproduct.php?Items=0016&MenuCat=4&Subname=AnkLets>
GET <http://192.168.1.20/viewproduct.php?Items=0016&pn>
GET <http://192.168.1.20/viewproduct.php?Items=0016&pn=1>

GET <http://192.168.1.20/viewproduct.php?Items=0016&pn=2>
GET <http://192.168.1.20/viewproduct.php?Items=0017&MenuCat=4&Subname=ArmLets>
GET <http://192.168.1.20/viewproduct.php?Items=0018&MenuCat=4&Subname=BraceLet>
GET <http://192.168.1.20/viewproduct.php?Items=0019&MenuCat=4&Subname=Brooches>
GET <http://192.168.1.20/viewproduct.php?Items=0020&MenuCat=4&Subname=Hair%20Pin>
GET <http://192.168.1.20/viewproduct.php?Items=0021&MenuCat=4&Subname=EarRings>
GET <http://192.168.1.20/viewproduct.php?Items=0021&pn>
GET <http://192.168.1.20/viewproduct.php?Items=0021&pn=1>
GET <http://192.168.1.20/viewproduct.php?Items=0021&pn=2>
GET <http://192.168.1.20/viewproduct.php?Items=0022&MenuCat=4&Subname=Cuffilinks>
GET <http://192.168.1.20/viewproduct.php?Items=0022&pn>
GET <http://192.168.1.20/viewproduct.php?Items=0022&pn=1>
GET <http://192.168.1.20/viewproduct.php?Items=0022&pn=2>
GET <http://192.168.1.20/viewproduct.php?Items=0023&MenuCat=4&Subname=Chain>
GET <http://192.168.1.20/viewproduct.php?Items=0023&pn>
GET <http://192.168.1.20/viewproduct.php?Items=0023&pn=1>
GET <http://192.168.1.20/viewproduct.php?Items=0023&pn=2>
GET <http://192.168.1.20/viewproduct.php?Items=0024&MenuCat=4&Subname=ManRings>
GET <http://192.168.1.20/viewproduct.php?Items=0024&pn>
GET <http://192.168.1.20/viewproduct.php?Items=0024&pn=1>
GET <http://192.168.1.20/viewproduct.php?Items=0024&pn=2>
GET <http://192.168.1.20/viewproduct.php?Items=0025&MenuCat=4&Subname=Pendants>
GET <http://192.168.1.20/viewproduct.php?Items=0026&MenuCat=4&Subname=Pendants%20Sets>
GET <http://192.168.1.20/viewproduct.php?Items=0026&pn>
GET <http://192.168.1.20/viewproduct.php?Items=0026&pn=1>
GET <http://192.168.1.20/viewproduct.php?Items=0026&pn=2>
GET <http://192.168.1.20/viewproduct.php?Items=0027&MenuCat=4&Subname=Lady%20Rings>
GET <http://192.168.1.20/viewproduct.php?Items=0028&MenuCat=3&Subname=LadyRings>
GET <http://192.168.1.20/viewproduct.php?Items=0028&pn>
GET <http://192.168.1.20/viewproduct.php?Items=0028&pn=1>
GET <http://192.168.1.20/viewproduct.php?Items=0028&pn=2>
GET <http://192.168.1.20/viewproduct.php?Items=0029&MenuCat=3&Subname=ManRings>
GET <http://192.168.1.20/viewproduct.php?Items=0030&MenuCat=4&Subname=ToeRings>

GET <http://192.168.1.20/viewproduct.php?Items=0030&pn>
GET <http://192.168.1.20/viewproduct.php?Items=0030&pn=1>
GET <http://192.168.1.20/viewproduct.php?Items=0030&pn=2>
GET <http://192.168.1.20/viewpurchase.php>
X-Content-Type-Options Header Missing (446)
GET <http://192.168.1.20/>
GET <http://192.168.1.20/>
GET <http://192.168.1.20/about.php>
GET <http://192.168.1.20/attachment.php?type=delivery.php>
GET <http://192.168.1.20/attachment.php?type=terms.php>
GET <http://192.168.1.20/contact.php>
GET <http://192.168.1.20/css/carousel.css>
GET <http://192.168.1.20/css/flexslider.css>
GET <http://192.168.1.20/css/stylesheet.css>
GET <http://192.168.1.20/featured.php>
GET <http://192.168.1.20/featured.php?pn=1>
GET <http://192.168.1.20/featured.php?pn=10>
GET <http://192.168.1.20/featured.php?pn=11>
GET <http://192.168.1.20/featured.php?pn=12>
GET <http://192.168.1.20/featured.php?pn=13>
GET <http://192.168.1.20/featured.php?pn=14>
GET <http://192.168.1.20/featured.php?pn=15>
GET <http://192.168.1.20/featured.php?pn=16>
GET <http://192.168.1.20/featured.php?pn=17>
GET <http://192.168.1.20/featured.php?pn=18>
GET <http://192.168.1.20/featured.php?pn=19>
GET <http://192.168.1.20/featured.php?pn=2>
GET <http://192.168.1.20/featured.php?pn=20>
GET <http://192.168.1.20/featured.php?pn=21>
GET <http://192.168.1.20/featured.php?pn=22>
GET <http://192.168.1.20/featured.php?pn=23>
GET <http://192.168.1.20/featured.php?pn=24>
GET <http://192.168.1.20/featured.php?pn=25>

GET <http://192.168.1.20/featured.php?pn=26>
GET <http://192.168.1.20/featured.php?pn=27>
GET <http://192.168.1.20/featured.php?pn=28>
GET <http://192.168.1.20/featured.php?pn=29>
GET <http://192.168.1.20/featured.php?pn=3>
GET <http://192.168.1.20/featured.php?pn=30>
GET <http://192.168.1.20/featured.php?pn=31>
GET <http://192.168.1.20/featured.php?pn=32>
GET <http://192.168.1.20/featured.php?pn=33>
GET <http://192.168.1.20/featured.php?pn=34>
GET <http://192.168.1.20/featured.php?pn=35>
GET <http://192.168.1.20/featured.php?pn=4>
GET <http://192.168.1.20/featured.php?pn=5>
GET <http://192.168.1.20/featured.php?pn=6>
GET <http://192.168.1.20/featured.php?pn=7>
GET <http://192.168.1.20/featured.php?pn=8>
GET <http://192.168.1.20/featured.php?pn=9>
GET <http://192.168.1.20/image/addBanner-940x145.jpg>
GET <http://192.168.1.20/image/banner1-960x300.jpg>
GET <http://192.168.1.20/image/banner2-960x300.jpg>
GET <http://192.168.1.20/image/favicon.png>
GET <http://192.168.1.20/image/Logo.png>
GET <http://192.168.1.20/image/mail.png>
GET <http://192.168.1.20/image/phone.png>
GET <http://192.168.1.20/index.php>
GET <http://192.168.1.20/js/custom.js>
GET <http://192.168.1.20/js/html5.js>
GET <http://192.168.1.20/js/jquery-1.7.1.min.js>
GET <http://192.168.1.20/js/jquery.fancybox.pack.js>
GET <http://192.168.1.20/js/jquery.flexslider-min.js>
GET <http://192.168.1.20/js/jquery.jcarousel.min.js>
GET <http://192.168.1.20/js/tabs.js>
GET <http://192.168.1.20/latest.php>

GET <http://192.168.1.20/latest.php?pn=1>
GET <http://192.168.1.20/latest.php?pn=2>
GET <http://192.168.1.20/Photos/Diamond/Bangles/1.jpg>
GET <http://192.168.1.20/Photos/Diamond/Bangles/10.jpg>
GET <http://192.168.1.20/Photos/Diamond/Bangles/11.jpg>
GET <http://192.168.1.20/Photos/Diamond/Bangles/2.jpg>
GET <http://192.168.1.20/Photos/Diamond/Bangles/3.jpg>
GET <http://192.168.1.20/Photos/Diamond/Bangles/4.jpg>
GET <http://192.168.1.20/Photos/Diamond/Bangles/5.jpg>
GET <http://192.168.1.20/Photos/Diamond/Bangles/6.jpg>
GET <http://192.168.1.20/Photos/Diamond/Bangles/7.jpg>
GET <http://192.168.1.20/Photos/Diamond/Bangles/8.jpg>
GET <http://192.168.1.20/Photos/Diamond/Bangles/9.jpg>
GET <http://192.168.1.20/Photos/Diamond/EarRings/1.jpg>
GET <http://192.168.1.20/Photos/Diamond/EarRings/2.jpg>
GET <http://192.168.1.20/Photos/Diamond/EarRings/3.jpg>
GET <http://192.168.1.20/Photos/Diamond/EarRings/4.jpg>
GET <http://192.168.1.20/Photos/Diamond/EarRings/5.jpg>
GET <http://192.168.1.20/Photos/Diamond/EarRings/6.jpg>
GET <http://192.168.1.20/Photos/Diamond/EarRings/7.jpg>
GET <http://192.168.1.20/Photos/Diamond/EarRings/8.jpg>
GET <http://192.168.1.20/Photos/Diamond/EarRings/9.jpg>
GET <http://192.168.1.20/Photos/Diamond/Lady%20Ring/1.jpg>
GET <http://192.168.1.20/Photos/Diamond/Lady%20Ring/10.jpg>
GET <http://192.168.1.20/Photos/Diamond/Lady%20Ring/2.jpg>
GET <http://192.168.1.20/Photos/Diamond/Lady%20Ring/3.jpg>
GET <http://192.168.1.20/Photos/Diamond/Lady%20Ring/4.jpg>
GET <http://192.168.1.20/Photos/Diamond/Lady%20Ring/5.jpg>
GET <http://192.168.1.20/Photos/Diamond/Lady%20Ring/6.jpg>
GET <http://192.168.1.20/Photos/Diamond/Lady%20Ring/7.jpg>
GET <http://192.168.1.20/Photos/Diamond/Lady%20Ring/8.jpg>
GET <http://192.168.1.20/Photos/Diamond/Lady%20Ring/9.jpg>
GET <http://192.168.1.20/Photos/Diamond/Necklaces/1.jpg>

GET <http://192.168.1.20/Photos/Diamond/Necklaces/2.jpg>
GET <http://192.168.1.20/Photos/Diamond/Necklaces/3.jpg>
GET <http://192.168.1.20/Photos/Diamond/Necklaces/4.jpg>
GET <http://192.168.1.20/Photos/Diamond/Necklaces/5.jpg>
GET <http://192.168.1.20/Photos/Diamond/Necklaces/6.jpg>
GET <http://192.168.1.20/Photos/Diamond/Necklaces/7.jpg>
GET <http://192.168.1.20/Photos/Diamond/Nose%20Pin/1.jpg>
GET <http://192.168.1.20/Photos/Diamond/Nose%20Pin/10.jpg>
GET <http://192.168.1.20/Photos/Diamond/Nose%20Pin/2.jpg>
GET <http://192.168.1.20/Photos/Diamond/Nose%20Pin/3.jpg>
GET <http://192.168.1.20/Photos/Diamond/Nose%20Pin/4.jpg>
GET <http://192.168.1.20/Photos/Diamond/Nose%20Pin/5.jpg>
GET <http://192.168.1.20/Photos/Diamond/Nose%20Pin/6.jpg>
GET <http://192.168.1.20/Photos/Diamond/Nose%20Pin/7.jpg>
GET <http://192.168.1.20/Photos/Diamond/Nose%20Pin/8.jpg>
GET <http://192.168.1.20/Photos/Diamond/Nose%20Pin/9.jpg>
GET <http://192.168.1.20/Photos/Diamond/Pendant%20Set/1.jpg>
GET <http://192.168.1.20/Photos/Diamond/Pendant%20Set/10.jpg>
GET <http://192.168.1.20/Photos/Diamond/Pendant%20Set/2.jpg>
GET <http://192.168.1.20/Photos/Diamond/Pendant%20Set/3.jpg>
GET <http://192.168.1.20/Photos/Diamond/Pendant%20Set/4.jpg>
GET <http://192.168.1.20/Photos/Diamond/Pendant%20Set/5.jpg>
GET <http://192.168.1.20/Photos/Diamond/Pendant%20Set/6.jpg>
GET <http://192.168.1.20/Photos/Diamond/Pendant%20Set/7.jpg>
GET <http://192.168.1.20/Photos/Diamond/Pendant%20Set/8.jpg>
GET <http://192.168.1.20/Photos/Diamond/Pendant%20Set/9.jpg>
GET <http://192.168.1.20/Photos/Diamond/Pendants/1.jpg>
GET <http://192.168.1.20/Photos/Diamond/Pendants/10.jpg>
GET <http://192.168.1.20/Photos/Diamond/Pendants/2.jpg>
GET <http://192.168.1.20/Photos/Diamond/Pendants/3.jpg>
GET <http://192.168.1.20/Photos/Diamond/Pendants/4.jpg>
GET <http://192.168.1.20/Photos/Diamond/Pendants/5.jpg>
GET <http://192.168.1.20/Photos/Diamond/Pendants/6.jpg>

GET <http://192.168.1.20/Photos/Diamond/Pendants/7.jpg>
GET <http://192.168.1.20/Photos/Diamond/Pendants/8.jpg>
GET <http://192.168.1.20/Photos/Diamond/Pendants/9.jpg>
GET <http://192.168.1.20/Photos/Gold/Bangles/1.jpg>
GET <http://192.168.1.20/Photos/Gold/Bangles/10.jpg>
GET <http://192.168.1.20/Photos/Gold/Bangles/2.jpg>
GET <http://192.168.1.20/Photos/Gold/Bangles/3.jpg>
GET <http://192.168.1.20/Photos/Gold/Bangles/4.jpg>
GET <http://192.168.1.20/Photos/Gold/Bangles/5.jpg>
GET <http://192.168.1.20/Photos/Gold/Bangles/6.jpg>
GET <http://192.168.1.20/Photos/Gold/Bangles/7.jpg>
GET <http://192.168.1.20/Photos/Gold/Bangles/8.jpg>
GET <http://192.168.1.20/Photos/Gold/Bangles/9.jpg>
GET <http://192.168.1.20/Photos/Gold/Ear%20Rings/1.jpg>
GET <http://192.168.1.20/Photos/Gold/Ear%20Rings/10.jpg>
GET <http://192.168.1.20/Photos/Gold/Ear%20Rings/2.jpg>
GET <http://192.168.1.20/Photos/Gold/Ear%20Rings/3.jpg>
GET <http://192.168.1.20/Photos/Gold/Ear%20Rings/4.jpg>
GET <http://192.168.1.20/Photos/Gold/Ear%20Rings/5.jpg>
GET <http://192.168.1.20/Photos/Gold/Ear%20Rings/6.jpg>
GET <http://192.168.1.20/Photos/Gold/Ear%20Rings/7.jpg>
GET <http://192.168.1.20/Photos/Gold/Ear%20Rings/8.jpg>
GET <http://192.168.1.20/Photos/Gold/Ear%20Rings/9.jpg>
GET <http://192.168.1.20/Photos/Gold/Lady%20Rings/1.jpg>
GET <http://192.168.1.20/Photos/Gold/Lady%20Rings/10.jpg>
GET <http://192.168.1.20/Photos/Gold/Lady%20Rings/2.jpg>
GET <http://192.168.1.20/Photos/Gold/Lady%20Rings/3.jpg>
GET <http://192.168.1.20/Photos/Gold/Lady%20Rings/4.jpg>
GET <http://192.168.1.20/Photos/Gold/Lady%20Rings/5.jpg>
GET <http://192.168.1.20/Photos/Gold/Lady%20Rings/6.jpg>
GET <http://192.168.1.20/Photos/Gold/Lady%20Rings/7.jpg>
GET <http://192.168.1.20/Photos/Gold/Lady%20Rings/8.jpg>
GET <http://192.168.1.20/Photos/Gold/Lady%20Rings/9.jpg>

GET <http://192.168.1.20/Photos/Gold/Man%20Rings/1.jpg>
GET <http://192.168.1.20/Photos/Gold/Man%20Rings/2.jpg>
GET <http://192.168.1.20/Photos/Gold/Man%20Rings/3.jpg>
GET <http://192.168.1.20/Photos/Gold/Man%20Rings/4.jpg>
GET <http://192.168.1.20/Photos/Gold/Man%20Rings/5.jpg>
GET <http://192.168.1.20/Photos/Gold/Man%20Rings/6.jpg>
GET <http://192.168.1.20/Photos/Gold/Man%20Rings/7.jpg>
GET <http://192.168.1.20/Photos/Gold/Man%20Rings/8.jpg>
GET <http://192.168.1.20/Photos/Gold/Man%20Rings/9.jpg>
GET <http://192.168.1.20/Photos/Gold/Mang%20Tika/1.jpg>
GET <http://192.168.1.20/Photos/Gold/Mang%20Tika/10.jpg>
GET <http://192.168.1.20/Photos/Gold/Mang%20Tika/2.jpg>
GET <http://192.168.1.20/Photos/Gold/Mang%20Tika/3.jpg>
GET <http://192.168.1.20/Photos/Gold/Mang%20Tika/4.jpg>
GET <http://192.168.1.20/Photos/Gold/Mang%20Tika/5.jpg>
GET <http://192.168.1.20/Photos/Gold/Mang%20Tika/6.jpg>
GET <http://192.168.1.20/Photos/Gold/Mang%20Tika/7.jpg>
GET <http://192.168.1.20/Photos/Gold/Mang%20Tika/9.jpg>
GET <http://192.168.1.20/Photos/Gold/Mangalsutra/1.jpg>
GET <http://192.168.1.20/Photos/Gold/Mangalsutra/10.jpg>
GET <http://192.168.1.20/Photos/Gold/Mangalsutra/2.jpg>
GET <http://192.168.1.20/Photos/Gold/Mangalsutra/3.jpg>
GET <http://192.168.1.20/Photos/Gold/Mangalsutra/4.jpg>
GET <http://192.168.1.20/Photos/Gold/Mangalsutra/5.jpg>
GET <http://192.168.1.20/Photos/Gold/Mangalsutra/6.jpg>
GET <http://192.168.1.20/Photos/Gold/Mangalsutra/7.jpg>
GET <http://192.168.1.20/Photos/Gold/Mangalsutra/8.jpg>
GET <http://192.168.1.20/Photos/Gold/Mangalsutra/9.jpg>
GET <http://192.168.1.20/Photos/Gold/Necklaces/1.jpg>
GET <http://192.168.1.20/Photos/Gold/Necklaces/10.jpg>
GET <http://192.168.1.20/Photos/Gold/Necklaces/2.jpg>
GET <http://192.168.1.20/Photos/Gold/Necklaces/3.jpg>
GET <http://192.168.1.20/Photos/Gold/Necklaces/4.jpg>

GET <http://192.168.1.20/Photos/GoLd/NeckLaces/5.jpg>
GET <http://192.168.1.20/Photos/GoLd/NeckLaces/6.jpg>
GET <http://192.168.1.20/Photos/GoLd/NeckLaces/7.jpg>
GET <http://192.168.1.20/Photos/GoLd/NeckLaces/8.jpg>
GET <http://192.168.1.20/Photos/GoLd/NeckLaces/9.jpg>
GET <http://192.168.1.20/Photos/GoLd/Nose%20Rings/1.jpg>
GET <http://192.168.1.20/Photos/GoLd/Nose%20Rings/2.jpg>
GET <http://192.168.1.20/Photos/GoLd/Nose%20Rings/3.jpg>
GET <http://192.168.1.20/Photos/GoLd/Nose%20Rings/4.jpg>
GET <http://192.168.1.20/Photos/GoLd/Nose%20Rings/5.jpg>
GET <http://192.168.1.20/Photos/GoLd/Nose%20Rings/6.jpg>
GET <http://192.168.1.20/Photos/GoLd/Nose%20Rings/7.jpg>
GET <http://192.168.1.20/Photos/GoLd/Nose%20Rings/8.jpg>
GET <http://192.168.1.20/Photos/GoLd/Pendant%20Set/1.jpg>
GET <http://192.168.1.20/Photos/GoLd/Pendant%20Set/10.jpg>
GET <http://192.168.1.20/Photos/GoLd/Pendant%20Set/2.jpg>
GET <http://192.168.1.20/Photos/GoLd/Pendant%20Set/3.jpg>
GET <http://192.168.1.20/Photos/GoLd/Pendant%20Set/4.jpg>
GET <http://192.168.1.20/Photos/GoLd/Pendant%20Set/5.jpg>
GET <http://192.168.1.20/Photos/GoLd/Pendant%20Set/6.jpg>
GET <http://192.168.1.20/Photos/GoLd/Pendant%20Set/7.jpg>
GET <http://192.168.1.20/Photos/GoLd/Pendant%20Set/8.jpg>
GET <http://192.168.1.20/Photos/GoLd/Pendant%20Set/9.jpg>
GET <http://192.168.1.20/Photos/GoLd/Pendants/1.jpg>
GET <http://192.168.1.20/Photos/GoLd/Pendants/10.jpg>
GET <http://192.168.1.20/Photos/GoLd/Pendants/2.jpg>
GET <http://192.168.1.20/Photos/GoLd/Pendants/3.jpg>
GET <http://192.168.1.20/Photos/GoLd/Pendants/4.jpg>
GET <http://192.168.1.20/Photos/GoLd/Pendants/5.jpg>
GET <http://192.168.1.20/Photos/GoLd/Pendants/6.jpg>
GET <http://192.168.1.20/Photos/GoLd/Pendants/7.jpg>
GET <http://192.168.1.20/Photos/GoLd/Pendants/8.jpg>
GET <http://192.168.1.20/Photos/GoLd/Pendants/9.jpg>

GET <http://192.168.1.20/Photos/Silver/Anklets/1.jpg>
GET <http://192.168.1.20/Photos/Silver/Anklets/10.jpg>
GET <http://192.168.1.20/Photos/Silver/Anklets/2.jpg>
GET <http://192.168.1.20/Photos/Silver/Anklets/3.jpg>
GET <http://192.168.1.20/Photos/Silver/Anklets/4.jpg>
GET <http://192.168.1.20/Photos/Silver/Anklets/5.jpg>
GET <http://192.168.1.20/Photos/Silver/Anklets/6.jpg>
GET <http://192.168.1.20/Photos/Silver/Anklets/7.jpg>
GET <http://192.168.1.20/Photos/Silver/Anklets/8.jpg>
GET <http://192.168.1.20/Photos/Silver/Anklets/9.jpg>
GET <http://192.168.1.20/Photos/Silver/Armllets/1.jpg>
GET <http://192.168.1.20/Photos/Silver/Armllets/10.jpg>
GET <http://192.168.1.20/Photos/Silver/Armllets/2.jpg>
GET <http://192.168.1.20/Photos/Silver/Armllets/3.jpg>
GET <http://192.168.1.20/Photos/Silver/Armllets/4.jpg>
GET <http://192.168.1.20/Photos/Silver/Armllets/5.jpg>
GET <http://192.168.1.20/Photos/Silver/Armllets/6.jpg>
GET <http://192.168.1.20/Photos/Silver/Armllets/7.jpg>
GET <http://192.168.1.20/Photos/Silver/Armllets/8.jpg>
GET <http://192.168.1.20/Photos/Silver/Armllets/9.jpg>
GET <http://192.168.1.20/Photos/Silver/Bracelet/1.jpg>
GET <http://192.168.1.20/Photos/Silver/Bracelet/10.jpg>
GET <http://192.168.1.20/Photos/Silver/Bracelet/2.jpg>
GET <http://192.168.1.20/Photos/Silver/Bracelet/3.jpg>
GET <http://192.168.1.20/Photos/Silver/Bracelet/4.jpg>
GET <http://192.168.1.20/Photos/Silver/Bracelet/5.jpg>
GET <http://192.168.1.20/Photos/Silver/Bracelet/6.jpg>
GET <http://192.168.1.20/Photos/Silver/Bracelet/7.jpg>
GET <http://192.168.1.20/Photos/Silver/Bracelet/8.jpg>
GET <http://192.168.1.20/Photos/Silver/Bracelet/9.jpg>
GET <http://192.168.1.20/Photos/Silver/Brooches/1.jpg>
GET <http://192.168.1.20/Photos/Silver/Brooches/10.jpg>
GET <http://192.168.1.20/Photos/Silver/Brooches/2.jpg>

GET <http://192.168.1.20/Photos/Silver/Brooches/3.jpg>
GET <http://192.168.1.20/Photos/Silver/Brooches/4.jpg>
GET <http://192.168.1.20/Photos/Silver/Brooches/5.jpg>
GET <http://192.168.1.20/Photos/Silver/Brooches/6.jpg>
GET <http://192.168.1.20/Photos/Silver/Brooches/7.jpg>
GET <http://192.168.1.20/Photos/Silver/Brooches/8.jpg>
GET <http://192.168.1.20/Photos/Silver/Brooches/9.jpg>
GET <http://192.168.1.20/Photos/Silver/Chain/1.jpg>
GET <http://192.168.1.20/Photos/Silver/Chain/10.jpg>
GET <http://192.168.1.20/Photos/Silver/Chain/2.jpg>
GET <http://192.168.1.20/Photos/Silver/Chain/3.jpg>
GET <http://192.168.1.20/Photos/Silver/Chain/4.jpg>
GET <http://192.168.1.20/Photos/Silver/Chain/5.jpg>
GET <http://192.168.1.20/Photos/Silver/Chain/6.jpg>
GET <http://192.168.1.20/Photos/Silver/Chain/7.jpg>
GET <http://192.168.1.20/Photos/Silver/Chain/8.jpg>
GET <http://192.168.1.20/Photos/Silver/Chain/9.jpg>
GET <http://192.168.1.20/Photos/Silver/Cufflinks/1.jpg>
GET <http://192.168.1.20/Photos/Silver/Cufflinks/10.jpg>
GET <http://192.168.1.20/Photos/Silver/Cufflinks/2.jpg>
GET <http://192.168.1.20/Photos/Silver/Cufflinks/3.jpg>
GET <http://192.168.1.20/Photos/Silver/Cufflinks/4.jpg>
GET <http://192.168.1.20/Photos/Silver/Cufflinks/5.jpg>
GET <http://192.168.1.20/Photos/Silver/Cufflinks/6.jpg>
GET <http://192.168.1.20/Photos/Silver/Cufflinks/7.jpg>
GET <http://192.168.1.20/Photos/Silver/Cufflinks/8.jpg>
GET <http://192.168.1.20/Photos/Silver/Cufflinks/9.jpg>
GET <http://192.168.1.20/Photos/Silver/Earrings/1.jpg>
GET <http://192.168.1.20/Photos/Silver/Earrings/10.jpg>
GET <http://192.168.1.20/Photos/Silver/Earrings/2.jpg>
GET <http://192.168.1.20/Photos/Silver/Earrings/3.jpg>
GET <http://192.168.1.20/Photos/Silver/Earrings/4.jpg>
GET <http://192.168.1.20/Photos/Silver/Earrings/5.jpg>

GET <http://192.168.1.20/Photos/Silver/EarRings/6.jpg>
GET <http://192.168.1.20/Photos/Silver/EarRings/7.jpg>
GET <http://192.168.1.20/Photos/Silver/EarRings/8.jpg>
GET <http://192.168.1.20/Photos/Silver/EarRings/9.jpg>
GET <http://192.168.1.20/Photos/Silver/Hair%20Pin/1.jpg>
GET <http://192.168.1.20/Photos/Silver/Hair%20Pin/10.jpg>
GET <http://192.168.1.20/Photos/Silver/Hair%20Pin/2.jpg>
GET <http://192.168.1.20/Photos/Silver/Hair%20Pin/4.jpg>
GET <http://192.168.1.20/Photos/Silver/Hair%20Pin/6.jpg>
GET <http://192.168.1.20/Photos/Silver/Hair%20Pin/7.jpg>
GET <http://192.168.1.20/Photos/Silver/Hair%20Pin/8.jpg>
GET <http://192.168.1.20/Photos/Silver/Hair%20Pin/9.jpg>
GET <http://192.168.1.20/Photos/Silver/Lady%20Rings/1.jpg>
GET <http://192.168.1.20/Photos/Silver/Lady%20Rings/10.jpg>
GET <http://192.168.1.20/Photos/Silver/Lady%20Rings/3.jpg>
GET <http://192.168.1.20/Photos/Silver/Lady%20Rings/4.jpg>
GET <http://192.168.1.20/Photos/Silver/Lady%20Rings/5.jpg>
GET <http://192.168.1.20/Photos/Silver/Lady%20Rings/6.jpg>
GET <http://192.168.1.20/Photos/Silver/Lady%20Rings/7.jpg>
GET <http://192.168.1.20/Photos/Silver/Lady%20Rings/8.jpg>
GET <http://192.168.1.20/Photos/Silver/Lady%20Rings/9.jpg>
GET <http://192.168.1.20/Photos/Silver/Man%20Ring/1.jpg>
GET <http://192.168.1.20/Photos/Silver/Man%20Ring/10.jpg>
GET <http://192.168.1.20/Photos/Silver/Man%20Ring/2.jpg>
GET <http://192.168.1.20/Photos/Silver/Man%20Ring/3.jpg>
GET <http://192.168.1.20/Photos/Silver/Man%20Ring/4.jpg>
GET <http://192.168.1.20/Photos/Silver/Man%20Ring/5.jpg>
GET <http://192.168.1.20/Photos/Silver/Man%20Ring/6.jpg>
GET <http://192.168.1.20/Photos/Silver/Man%20Ring/8.jpg>
GET <http://192.168.1.20/Photos/Silver/Man%20Ring/9.jpg>
GET <http://192.168.1.20/Photos/Silver/Pendants%20Sets/1.jpg>
GET <http://192.168.1.20/Photos/Silver/Pendants%20Sets/10.jpg>
GET <http://192.168.1.20/Photos/Silver/Pendants%20Sets/2.jpg>

GET <http://192.168.1.20/Photos/Silver/Pendants%20Sets/3.jpg>
GET <http://192.168.1.20/Photos/Silver/Pendants%20Sets/4.jpg>
GET <http://192.168.1.20/Photos/Silver/Pendants%20Sets/5.jpg>
GET <http://192.168.1.20/Photos/Silver/Pendants%20Sets/6.jpg>
GET <http://192.168.1.20/Photos/Silver/Pendants%20Sets/7.jpg>
GET <http://192.168.1.20/Photos/Silver/Pendants%20Sets/8.jpg>
GET <http://192.168.1.20/Photos/Silver/Pendants%20Sets/9.jpg>
GET <http://192.168.1.20/Photos/Silver/Pendants/1.jpg>
GET <http://192.168.1.20/Photos/Silver/Pendants/10.jpg>
GET <http://192.168.1.20/Photos/Silver/Pendants/3.jpg>
GET <http://192.168.1.20/Photos/Silver/Pendants/4.jpg>
GET <http://192.168.1.20/Photos/Silver/Pendants/5.jpg>
GET <http://192.168.1.20/Photos/Silver/Pendants/6.jpg>
GET <http://192.168.1.20/Photos/Silver/Pendants/7.jpg>
GET <http://192.168.1.20/Photos/Silver/Pendants/8.jpg>
GET <http://192.168.1.20/Photos/Silver/Pendants/9.jpg>
GET <http://192.168.1.20/Photos/Silver/Toe%20Ring/1.jpg>
GET <http://192.168.1.20/Photos/Silver/Toe%20Ring/2.jpg>
GET <http://192.168.1.20/Photos/Silver/Toe%20Ring/3.jpg>
GET <http://192.168.1.20/Photos/Silver/Toe%20Ring/4.jpg>
GET <http://192.168.1.20/Photos/Silver/Toe%20Ring/5.jpg>
GET <http://192.168.1.20/Photos/Silver/Toe%20Ring/6.jpg>
GET <http://192.168.1.20/Photos/Silver/Toe%20Ring/7.jpg>
GET <http://192.168.1.20/Photos/Silver/Toe%20Ring/8.jpg>
GET <http://192.168.1.20/Photos/Silver/Toe%20Ring/9.jpg>
GET <http://192.168.1.20/register.html>
GET <http://192.168.1.20/robots.txt>
GET <http://192.168.1.20/schema.sql>
GET <http://192.168.1.20/topsell.php?Items=0032&MenuCat=8&Subname=Sellings>
GET <http://192.168.1.20/topviewed.php?Items=0031&MenuCat=8&Subname=Views>
GET <http://192.168.1.20/viewproduct.php?Items=0001&MenuCat=5&Subname=Bangles>
GET <http://192.168.1.20/viewproduct.php?Items=0001&pn>
GET <http://192.168.1.20/viewproduct.php?Items=0001&pn=1>

GET <http://192.168.1.20/viewproduct.php?Items=0001&pn=2>
GET <http://192.168.1.20/viewproduct.php?Items=0002&MenuCat=5&Subname=EarRings>
GET <http://192.168.1.20/viewproduct.php?Items=0002&pn>
GET <http://192.168.1.20/viewproduct.php?Items=0002&pn=1>
GET <http://192.168.1.20/viewproduct.php?Items=0002&pn=2>
GET <http://192.168.1.20/viewproduct.php?Items=0003&MenuCat=5&Subname=NeckLaces>
GET <http://192.168.1.20/viewproduct.php?Items=0004&MenuCat=5&Subname=Nose%20Pin>
GET <http://192.168.1.20/viewproduct.php?Items=0004&pn>
GET <http://192.168.1.20/viewproduct.php?Items=0004&pn=1>
GET <http://192.168.1.20/viewproduct.php?Items=0004&pn=2>
GET <http://192.168.1.20/viewproduct.php?Items=0005&MenuCat=5&Subname=Pendant%20Set>
GET <http://192.168.1.20/viewproduct.php?Items=0006&MenuCat=5&Subname=Pendants>
GET <http://192.168.1.20/viewproduct.php?Items=0006&pn>
GET <http://192.168.1.20/viewproduct.php?Items=0006&pn=1>
GET <http://192.168.1.20/viewproduct.php?Items=0006&pn=2>
GET <http://192.168.1.20/viewproduct.php?Items=0007&MenuCat=5&Subname=LadyRings>
GET <http://192.168.1.20/viewproduct.php?Items=0007&pn>
GET <http://192.168.1.20/viewproduct.php?Items=0007&pn=1>
GET <http://192.168.1.20/viewproduct.php?Items=0007&pn=2>
GET <http://192.168.1.20/viewproduct.php?Items=0008&MenuCat=3&Subname=Bangles>
GET <http://192.168.1.20/viewproduct.php?Items=0008&pn>
GET <http://192.168.1.20/viewproduct.php?Items=0008&pn=1>
GET <http://192.168.1.20/viewproduct.php?Items=0008&pn=2>
GET <http://192.168.1.20/viewproduct.php?Items=0009&MenuCat=3&Subname=Ear%20Rings>
GET <http://192.168.1.20/viewproduct.php?Items=0009&pn>
GET <http://192.168.1.20/viewproduct.php?Items=0009&pn=1>
GET <http://192.168.1.20/viewproduct.php?Items=0009&pn=2>
GET <http://192.168.1.20/viewproduct.php?Items=0010&MenuCat=3&Subname=Mang%20Tika>
GET <http://192.168.1.20/viewproduct.php?Items=0010&pn>
GET <http://192.168.1.20/viewproduct.php?Items=0010&pn=1>
GET <http://192.168.1.20/viewproduct.php?Items=0010&pn=2>
GET <http://192.168.1.20/viewproduct.php?Items=0011&MenuCat=3&Subname=MangalSutra>
GET <http://192.168.1.20/viewproduct.php?Items=0011&pn>

GET <http://192.168.1.20/viewproduct.php?Items=0011&pn=1>
GET <http://192.168.1.20/viewproduct.php?Items=0011&pn=2>
GET <http://192.168.1.20/viewproduct.php?Items=0012&MenuCat=3&Subname=NeckLaces>
GET <http://192.168.1.20/viewproduct.php?Items=0012&pn>
GET <http://192.168.1.20/viewproduct.php?Items=0012&pn=1>
GET <http://192.168.1.20/viewproduct.php?Items=0012&pn=2>
GET <http://192.168.1.20/viewproduct.php?Items=0013&MenuCat=3&Subname=Nose%20Rings>
GET <http://192.168.1.20/viewproduct.php?Items=0013&pn>
GET <http://192.168.1.20/viewproduct.php?Items=0013&pn=1>
GET <http://192.168.1.20/viewproduct.php?Items=0013&pn=2>
GET <http://192.168.1.20/viewproduct.php?Items=0014&MenuCat=3&Subname=Pendant%20Set>
GET <http://192.168.1.20/viewproduct.php?Items=0015&MenuCat=3&Subname=Pendants>
GET <http://192.168.1.20/viewproduct.php?Items=0015&pn>
GET <http://192.168.1.20/viewproduct.php?Items=0015&pn=1>
GET <http://192.168.1.20/viewproduct.php?Items=0015&pn=2>
GET <http://192.168.1.20/viewproduct.php?Items=0016&MenuCat=4&Subname=Anklets>
GET <http://192.168.1.20/viewproduct.php?Items=0016&pn>
GET <http://192.168.1.20/viewproduct.php?Items=0016&pn=1>
GET <http://192.168.1.20/viewproduct.php?Items=0016&pn=2>
GET <http://192.168.1.20/viewproduct.php?Items=0017&MenuCat=4&Subname=ArmLets>
GET <http://192.168.1.20/viewproduct.php?Items=0018&MenuCat=4&Subname=BraceLet>
GET <http://192.168.1.20/viewproduct.php?Items=0019&MenuCat=4&Subname=Brooches>
GET <http://192.168.1.20/viewproduct.php?Items=0020&MenuCat=4&Subname=Hair%20Pin>
GET <http://192.168.1.20/viewproduct.php?Items=0021&MenuCat=4&Subname=EarRings>
GET <http://192.168.1.20/viewproduct.php?Items=0021&pn>
GET <http://192.168.1.20/viewproduct.php?Items=0021&pn=1>
GET <http://192.168.1.20/viewproduct.php?Items=0021&pn=2>
GET <http://192.168.1.20/viewproduct.php?Items=0022&MenuCat=4&Subname=Cuffilinks>
GET <http://192.168.1.20/viewproduct.php?Items=0022&pn>
GET <http://192.168.1.20/viewproduct.php?Items=0022&pn=1>
GET <http://192.168.1.20/viewproduct.php?Items=0022&pn=2>
GET <http://192.168.1.20/viewproduct.php?Items=0023&MenuCat=4&Subname=Chain>
GET <http://192.168.1.20/viewproduct.php?Items=0023&pn>

Isaac Basque-Rice

GET <http://192.168.1.20/viewproduct.php?Items=0023&pn=1>
GET <http://192.168.1.20/viewproduct.php?Items=0023&pn=2>
GET <http://192.168.1.20/viewproduct.php?Items=0024&MenuCat=4&Subname=ManRings>
GET <http://192.168.1.20/viewproduct.php?Items=0024&pn>
GET <http://192.168.1.20/viewproduct.php?Items=0024&pn=1>
GET <http://192.168.1.20/viewproduct.php?Items=0024&pn=2>
GET <http://192.168.1.20/viewproduct.php?Items=0025&MenuCat=4&Subname=Pendants>
GET <http://192.168.1.20/viewproduct.php?Items=0026&MenuCat=4&Subname=Pendants%20Sets>
GET <http://192.168.1.20/viewproduct.php?Items=0026&pn>
GET <http://192.168.1.20/viewproduct.php?Items=0026&pn=1>
GET <http://192.168.1.20/viewproduct.php?Items=0026&pn=2>
GET <http://192.168.1.20/viewproduct.php?Items=0027&MenuCat=4&Subname=Lady%20Rings>
GET <http://192.168.1.20/viewproduct.php?Items=0028&MenuCat=3&Subname=LadyRings>
GET <http://192.168.1.20/viewproduct.php?Items=0028&pn>
GET <http://192.168.1.20/viewproduct.php?Items=0028&pn=1>
GET <http://192.168.1.20/viewproduct.php?Items=0028&pn=2>
GET <http://192.168.1.20/viewproduct.php?Items=0029&MenuCat=3&Subname=ManRings>
GET <http://192.168.1.20/viewproduct.php?Items=0030&MenuCat=4&Subname=ToeRings>
GET <http://192.168.1.20/viewproduct.php?Items=0030&pn>
GET <http://192.168.1.20/viewproduct.php?Items=0030&pn=1>
GET <http://192.168.1.20/viewproduct.php?Items=0030&pn=2>
GET <http://192.168.1.20/viewpurchase.php>
Risk=Low, Confidence=Low (6)
<http://192.168.1.20> (6)
Timestamp Disclosure - Unix (6)
GET <http://192.168.1.20>
GET <http://192.168.1.20>
GET <http://192.168.1.20/>
GET <http://192.168.1.20/index.php>
GET <http://192.168.1.20/Photos/Silver/Armlets/2.jpg>
GET <http://192.168.1.20/Photos/Silver/Armlets/5.jpg>
Risk=Informational, Confidence=Medium (1)
<http://192.168.1.20> (1)

Content-Type Header Missing (1)

GET http://192.168.1.20/schema.sql

Risk=Informational, Confidence=Low (5)

http://192.168.1.20 (5)

Information Disclosure - Suspicious Comments (5)

GET http://192.168.1.20/js/html5.js

GET http://192.168.1.20/js/jquery-1.7.1.min.js

GET http://192.168.1.20/js/jquery-1.7.1.min.js

GET http://192.168.1.20/js/jquery.fancybox.pack.js

GET http://192.168.1.20/register.html

Appendix

Alert types

This section contains additional information on the types of alerts in the report.

Cross Site Scripting (Reflected)

Source raised by an active scanner (plugin ID: 40012)

CWE ID 79

WASC ID 8

Reference

<http://projects.webappsec.org/Cross-Site-Scripting>

<http://cwe.mitre.org/data/definitions/79.html>

Path Traversal

Source raised by an active scanner (plugin ID: 6)

CWE ID 22

WASC ID 33

Reference

<http://projects.webappsec.org/Path-Traversal>

<http://cwe.mitre.org/data/definitions/22.html>

SQL Injection

Source raised by an active scanner (plugin ID: 40018)

CWE ID 89

WASC ID 19

Reference

https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html

Application Error Disclosure

Source raised by a passive scanner (Application Error Disclosure)

CWE ID 200

WASC ID 13

Directory Browsing

Source raised by an active scanner (plugin ID: 0)

CWE ID 548

WASC ID 48

Reference

<http://httpd.apache.org/docs/mod/core.html#options>

<http://alamo.satlug.org/pipermail/satLug/2002-February/000053.html>

Parameter Tampering

Source raised by an active scanner (plugin ID: 40008)

CWE ID 472

WASC ID 20

Vulnerable JS Library

Source raised by a passive scanner (Vulnerable JS Library)

CWE ID 829

Reference

<https://nvd.nist.gov/vuln/detail/CVE-2012-6708>

<https://github.com/jquery/jquery/issues/2432>

<http://research.insecurelabs.org/jquery/test/>

<http://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/>

<http://bugs.jquery.com/ticket/11290>

<https://blog.jquery.com/2019/04/10/jquery-3-4-0-released/>

<https://nvd.nist.gov/vuln/detail/CVE-2019-11358>

<https://nvd.nist.gov/vuln/detail/CVE-2015-9251>

<https://github.com/jquery/jquery/commit/753d591aea698e57d6db58c9f722cd0808619b1b>

<https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/>

X-Frame-Options Header Not Set

Source raised by a passive scanner (X-Frame-Options Header)

CWE ID 1021

WASC ID 15

Reference

<https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options>

Absence of Anti-CSRF Tokens

Source raised by a passive scanner (Absence of Anti-CSRF Tokens)

CWE ID 352

WASC ID 9

Reference

<http://projects.webappsec.org/Cross-Site-Request-Forgery>

<http://cwe.mitre.org/data/definitions/352.html>

Cookie No HttpOnly Flag

Source raised by a passive scanner (Cookie No HttpOnly Flag)

CWE ID 1004

WASC ID 13

Reference

<https://owasp.org/www-community/HttpOnly>

Cookie without SameSite Attribute

Source raised by a passive scanner (Cookie without SameSite Attribute)

CWE ID 1275

WASC ID 13

Reference

<https://tools.ietf.org/html/draft-ietf-httpbis-cookie-same-site>

Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)

Source raised by a passive scanner (Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s))

CWE ID 200

WASC ID 13

Reference

<http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx>

<http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html>

Timestamp Disclosure - Unix

Source raised by a passive scanner (Timestamp Disclosure)

CWE ID 200

WASC ID 13

Reference

<http://projects.webappsec.org/w/page/13246936/Information%20Leakage>

X-Content-Type-Options Header Missing

Source raised by a passive scanner (X-Content-Type-Options Header Missing)

CWE ID 693

WASC ID 15

Reference

<http://msdn.microsoft.com/en-us/Library/ie/gg622941%28v=vs.85%29.aspx>

<https://owasp.org/www-community/Security-Headers>

Content-Type Header Missing

Source raised by a passive scanner (Content-Type Header Missing)

CWE ID 345

WASC ID 12

Reference

<http://msdn.microsoft.com/en-us/Library/ie/gg622941%28v=vs.85%29.aspx>

Information Disclosure - Suspicious Comments

Source raised by a passive scanner (Information Disclosure - Suspicious Comments)

CWE ID 200

WASC ID 13

4.5 APPENDIX A - GREP RESULTS

```
1901124/about.php:19:include("head1.html")
1901124/about.php:26:include("top_links2.php")
1901124/about.php:30:include("top_links.php")
1901124/about.php:44:include("header2.php")
1901124/about.php:48:include("header.php")
1901124/about.php:55:include("section.html")
1901124/about.php:65:include("includes/mysqli_connection.php")
1901124/about.php:109:include("footer.php")
1901124/about.php:115:include("flexslider.php")
1901124/attachment.php:19:include("head1.html")
1901124/attachment.php:26:include("top_links2.php")
1901124/attachment.php:30:include("top_links.php")
1901124/attachment.php:44:include("header2.php")
1901124/attachment.php:48:include("header.php")
1901124/attachment.php:55:include("section.html")
1901124/attachment.php:68:include('lfilter.php')
1901124/attachment.php:86:include("footer.php")
1901124/attachment.php:92:include("flexslider.php")
1901124/cart.php:38:include("head1.html")
1901124/cart.php:45:include("top_links2.php")
1901124/cart.php:49:include("top_links.php")
1901124/cart.php:63:include("header2.php")
1901124/cart.php:67:include("header.php")
1901124/cart.php:74:include("section.html")
1901124/cart.php:85:include("includes/mysqli_connection.php")
1901124/cart.php:263:include("comingsoon.php")
1901124/cart.php:273:include("footer.php")
1901124/cart.php:279:include("flexslider.php")
1901124/Changepassword.php:15:include("head1.html")
1901124/Changepassword.php:19:include("top_links2.php")
1901124/Changepassword.php:23:include("top_links.php")
1901124/Changepassword.php:32:include("section.html")
1901124/Changepassword.php:38:include("conection.php")
1901124/Changepassword.php:54:include("updatepassword.php")
1901124/Changepassword.php:71:include("studentsidebar.php")
1901124/Changepassword.php:107:include("footer.php")
1901124/Changepassword.php:113:include("flexslider.php")
1901124/changepicture.php:4:include('fileuploadtype.php')
1901124/changepicture.php:58:move_uploaded_file($_FILES['uploadedfile']['tmp_name'],
$target_path)
1901124/changepicture.php:59:chmod($target_path,0777)
1901124/checkout.php:37:include("head1.html")
1901124/checkout.php:44:include("top_links2.php")
1901124/checkout.php:48:include("top_links.php")
1901124/checkout.php:62:include("header2.php")
1901124/checkout.php:66:include("header.php")
1901124/checkout.php:73:include("section.html")
1901124/checkout.php:84:include("includes/mysqli_connection.php")
1901124/checkout.php:364:include("comingsoon.php")
1901124/checkout.php:374:include("footer.php")
```

```
1901124/checkout.php:380:include("flexslider.php")
1901124/comingsoon.php:2:include("includes/mysqli_connection.php")
1901124/comingsoon.php:27:preg_replace('#[^\0-9]#', '', $_GET['pn'])
1901124/confirmcheckout.php:28:include("includes/mysqli_connection.php")
1901124/copy of Changepassword.php:3:include("head1.html")
1901124/copy of Changepassword.php:6:include("top_links2.php")
1901124/copy of Changepassword.php:10:include("top_links.php")
1901124/copy of Changepassword.php:13:include("conection.php")
1901124/copy of Changepassword.php:45:include("studentsidebar.php")
1901124/copy of Changepassword.php:81:include("footer.php")
1901124/default.php:3:header("location:index.php")
1901124/extras.php:19:include("head1.html")
1901124/extras.php:26:include("top_links2.php")
1901124/extras.php:30:include("top_links.php")
1901124/extras.php:44:include("header2.php")
1901124/extras.php:48:include("header.php")
1901124/extras.php:55:include("section.html")
1901124/extras.php:72:file_exists($filename)
1901124/extras.php:94:include("footer.php")
1901124/extras.php:100:include("flexslider.php")
1901124/featured.php:19:include("head1.html")
1901124/featured.php:26:include("top_links2.php")
1901124/featured.php:30:include("top_links.php")
1901124/featured.php:44:include("header2.php")
1901124/featured.php:48:include("header.php")
1901124/featured.php:55:include("section.html")
1901124/featured.php:65:include("includes/mysqli_connection.php")
1901124/featured.php:90:preg_replace('#[^\0-9]#', '', $_GET['pn'])
1901124/featured.php:254:include("footer.php")
1901124/featured.php:260:include("flexslider.php")
1901124/flexslider.php:11:function()
1901124/header2.php:23:include("includes/mysqli_connection.php")
1901124/header2.php:108:include("navigation.php")
1901124/header.php:7:in()
1901124/header.php:15:include("navigation.php")
1901124/index.php:36:include("head1.html")
1901124/index.php:43:include("top_links2.php")
1901124/index.php:47:include("top_links.php")
1901124/index.php:61:include("header2.php")
1901124/index.php:65:include("header.php")
1901124/index.php:72:include("section.html")
1901124/index.php:83:include("randomfeatured.php")
1901124/index.php:109:include("comingsoon.php")
1901124/index.php:118:include("footer.php")
1901124/index.php:124:include("flexslider.php")
1901124/latest.php:19:include("head1.html")
1901124/latest.php:26:include("top_links2.php")
1901124/latest.php:30:include("top_links.php")
1901124/latest.php:44:include("header2.php")
1901124/latest.php:48:include("header.php")
1901124/latest.php:55:include("section.html")
1901124/latest.php:65:include("includes/mysqli_connection.php")
1901124/latest.php:90:preg_replace('#[^\0-9]#', '', $_GET['pn'])
1901124/latest.php:254:include("footer.php")
1901124/latest.php:260:include("flexslider.php")
1901124/login.php:10:function(e)
1901124/navigation.php:10:include("includes/config.php")
1901124/Phpinfo.php:4:Phpinfo()
```

```
1901124/processcheckout.php:41:include("includes/mysqli_connection.php")
1901124/processcheckout.php:64:header(location='cart.php')
1901124/processcheckout.php:70:header(location='index.php')
1901124/processcheckout.php:100:header(location='cart.php')
1901124/processcheckout.php:102:header("refresh:5; url=cart.php")
1901124/processcheckout.php:107:header(location='index.php')
1901124/processlogin.php:36:open()
1901124/processlogin.php:54:open()
1901124/profile.php:30:include("head1.html")
1901124/profile.php:37:include("top_links2.php")
1901124/profile.php:41:include("top_links.php")
1901124/profile.php:52:include("section.html")
1901124/profile.php:216:mail()
1901124/profile.php:419:include("footer.php")
1901124/profile.php:425:include("flexslider.php")
1901124/randomfeatured.php:2:include("includes/mysqli_connection.php")
1901124/receipt.php:52:include("includes/mysqli_connection.php")
1901124/receipt.php:110:include("includes/mysqli_connection.php")
1901124/receipt.php:142:header(location='index.php')
1901124/receipt.php:285:write('<form> <input type=button value="Print this Page"
name="Print" onClick="printit()"> </form>')
1901124/register.php:25:include("head1.html")
1901124/register.php:32:include("top_links2.php")
1901124/register.php:36:include("top_links.php")
1901124/register.php:47:include("section.html")
1901124/register.php:118:mail() && isAddress() && isTel()
1901124/register.php:212:mail()
1901124/register.php:396:include("footer.php")
1901124/register.php:402:include("flexslider.php")
1901124/remove.php:24:include("includes/mysqli_connection.php")
1901124/removeqty.php:24:include("includes/mysqli_connection.php")
1901124/removeqty.php:54:header(location='cart.php')
1901124/removeqty.php:55:header("location:cart.php")
1901124/search.php:10:function(e)
1901124/searchresult.php:17:include("head1.html")
1901124/searchresult.php:24:include("top_links2.php")
1901124/searchresult.php:28:include("top_links.php")
1901124/searchresult.php:42:include("header2.php")
1901124/searchresult.php:46:include("header.php")
1901124/searchresult.php:53:include("section.html")
1901124/searchresult.php:63:include("includes/config.php")
1901124/searchresult.php:209:include("footer.php")
1901124/searchresult.php:215:include("flexslider.php")
1901124/topsell.php:17:include("head1.html")
1901124/topsell.php:24:include("top_links2.php")
1901124/topsell.php:28:include("top_links.php")
1901124/topsell.php:42:include("header2.php")
1901124/topsell.php:46:include("header.php")
1901124/topsell.php:53:include("section.html")
1901124/topsell.php:63:include("includes/mysqli_connection.php")
1901124/topsell.php:186:include("footer.php")
1901124/topsell.php:192:include("flexslider.php")
1901124/topviewed.php:17:include("head1.html")
1901124/topviewed.php:24:include("top_links2.php")
1901124/topviewed.php:28:include("top_links.php")
1901124/topviewed.php:42:include("header2.php")
1901124/topviewed.php:46:include("header.php")
1901124/topviewed.php:53:include("section.html")
```

```
1901124/topviewed.php:63:include("includes/mysqli_connection.php")
1901124/topviewed.php:186:include("footer.php")
1901124/topviewed.php:192:include("flexslider.php")
1901124/updateqty.php:27:include("includes/mysqli_connection.php")
1901124/updateqty.php:56:header("location:cart.php")
1901124/view.php:36:include("head1.html")
1901124/view.php:43:include("top_links2.php")
1901124/view.php:47:include("top_links.php")
1901124/view.php:61:include("header2.php")
1901124/view.php:65:include("header.php")
1901124/view.php:72:include("section.html")
1901124/view.php:84:include("includes/mysqli_connection.php")
1901124/view.php:241:include("comingsoon.php")
1901124/view.php:251:include("footer.php")
1901124/view.php:257:include("flexslider.php")
1901124/viewproduct.php:2:include("includes/mysqli_connection.php")
1901124/viewproduct.php:22:include("head1.html")
1901124/viewproduct.php:29:include("top_links2.php")
1901124/viewproduct.php:33:include("top_links.php")
1901124/viewproduct.php:46:include("header2.php")
1901124/viewproduct.php:50:include("header.php")
1901124/viewproduct.php:58:include("section.html")
1901124/viewproduct.php:91:preg_replace('#[^\0-9]#', '', $_GET['pn'])
1901124/viewproduct.php:258:include("footer.php")
1901124/viewproduct.php:264:include("flexslider.php")
1901124/viewpurchase.php:63:write('<form> <input type=button value="Print this Page"
name="Print" onClick="printit()"> </form>')
1901124/viewpurchase.php:78:include("includes/mysqli_connection.php")
1901124/viewpurchase.php:134:include("includes/mysqli_connection.php")
```