



CMP 319 Penetration Test

Pen Testing a Web Application using an applied methodology.

Alex McNaughton

CMP319: Web Application Penetration Testing

BSc Ethical Hacking Year 3

2022/23

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

Abstract

Web Applications are one of the biggest targets for cybercrime, so it is vital for anyone who uses one to verify that they are not at risk of having their web application exploited. This document uses the OWASP testing guide as a model to perform a series of tests on a given webapp to determine whether it is vulnerable to being exploited, and provide countermeasures to any vulnerabilities that were found. The results of these tests concluded that the web application is extremely vulnerable to multiple exploits and should be immediately fixed using the appropriate countermeasures provided.

Contents

| | | |
|-------|--|----|
| 1 | Introduction | 1 |
| 1.1 | Background | 1 |
| 1.2 | Aims..... | 2 |
| 2 | Procedure and Results | 3 |
| | Overview of Procedure | 3 |
| 2.1 | Information Gathering | 3 |
| 2.1.1 | Fingerprint Web Server..... | 3 |
| 2.1.2 | Review Webserver Metafiles for Information Leakage | 4 |
| 2.1.3 | Enumerate Applications on Webserver | 5 |
| 2.1.4 | Review Webpage Content for Information Leakage..... | 5 |
| 2.1.5 | Identify Application Entry Points | 5 |
| 2.1.6 | Map Execution Paths Through Application..... | 5 |
| 2.1.7 | Fingerprint Web Application Framework | 6 |
| 2.1.8 | Map Application Architecture..... | 6 |
| 2.2 | Configuration and Deployment Management Testing | 8 |
| 2.2.1 | Test Network Infrastructure Configuration | 8 |
| 2.2.2 | Test Application Platform Configuration | 8 |
| 2.2.3 | Test File Extensions Handling for Sensitive Information..... | 9 |
| 2.2.4 | Review Old Backup and Unreferenced Files for Sensitive Information | 9 |
| 2.2.5 | Enumerate Infrastructure and Application Admin Interfaces | 10 |
| 2.2.6 | Test HTTP Methods..... | 11 |
| 2.2.7 | Test HTTP Strict Transport Security | 11 |
| 2.3 | Identity Management Testing..... | 11 |
| 2.3.1 | Test Role Definitions | 11 |
| 2.3.2 | Test User Registration Process..... | 11 |
| 2.3.3 | Testing for Account Enumeration and Guessable User Account..... | 12 |
| 2.3.4 | Testing for Weak or Unenforced Username Policy..... | 13 |
| 2.4 | Authentication Testing..... | 14 |
| 2.4.1 | Testing for Credentials Transported over an Encrypted Channel..... | 14 |
| 2.4.2 | Testing for Weak lock out mechanism..... | 14 |
| 2.4.3 | Testing for Bypassing Authentication Schema..... | 14 |

| | | |
|--------|---|----|
| 2.4.4 | Testing for Weak Password Policy | 15 |
| 2.4.5 | Testing for Weak Password Change or Reset Functionalities..... | 15 |
| 2.5 | Authorization Testing..... | 15 |
| 2.5.1 | Testing Directory Traversal File Include | 15 |
| 2.5.2 | Testing for Bypassing Authorization Schema..... | 16 |
| 2.5.3 | Testing for Privilege Escalation | 16 |
| 2.6 | Session Management Testing | 17 |
| 2.6.1 | Testing for Session Management Schema | 17 |
| 2.6.2 | Testing for Cookies Attributes | 18 |
| 2.6.3 | Testing for Session Fixation..... | 18 |
| 2.7 | Input Validation Testing..... | 19 |
| 2.7.1 | Testing for Stored Cross Site Scripting | 19 |
| 2.7.2 | Testing for SQL Injection | 20 |
| 2.7.3 | Testing for Local File Inclusion | 21 |
| 2.8 | Testing for Error Handling..... | 21 |
| 2.8.1 | Testing for Improper Error Handling..... | 21 |
| 2.9 | Testing for Weak Cryptography | 21 |
| 2.9.1 | Testing for Sensitive Information Sent via Unencrypted Channels | 21 |
| 2.9.2 | Testing for Weak Encryption..... | 22 |
| 2.10 | Business Logic Testing..... | 22 |
| 2.10.1 | Test Upload of Unexpected File Types..... | 22 |
| 2.11 | Client-Side Testing | 23 |
| 2.11.1 | Testing for DOM-Based Cross Site Scripting | 23 |
| 3 | Discussion..... | 24 |
| 3.1 | Overall Discussion | 24 |
| 3.2 | Countermeasures..... | 24 |
| 3.2.1 | SQL Injection | 24 |
| 3.2.2 | Using HTTPS | 25 |
| 3.2.3 | Change Encryption Methods..... | 25 |
| 3.2.4 | XSS..... | 25 |
| 3.2.5 | Username Enumeration | 26 |
| 3.2.6 | Prevent Access to Sensitive Directories | 26 |
| 3.2.7 | User Security | 27 |

| | | |
|-------|-------------------------|----|
| 3.2.8 | PHPinfo.php | 27 |
| 3.3 | Future Work | 27 |
| 4 | Bibliography | 28 |
| | Appendices part 1 | 29 |
| | Appendix A | 29 |
| | Appendix B | 48 |
| | Appendix C | 59 |

1 INTRODUCTION

1.1 BACKGROUND

Web pages have become an essential part of our daily lives, allowing businesses, organizations, and individuals to share information, connect with others, and conduct business. For so many years, the Internet has been an indispensable tool, and it's difficult to imagine a world without it. It is the foundation of modern technology and has been critical in driving innovation and growth in a diverse range of industries.

However, as the dependence on online pages grows, so do the potential security vulnerabilities connected with web page hosting. Hackers and cybercriminals are always seeking for new methods to attack web page flaws, steal important information, and disrupt online activities. According to a Cybersecurity Ventures analysis, cybercrime is expected to cost the globe \$8 trillion per year by 2023, up from \$3 trillion in 2015. Furthermore, on average, a firm is hit by a ransomware attack every 14 seconds (CyberSecurity Ventures, 2022).

This data emphasizes the necessity of website owners employing preemptive measures to safeguard and defend their websites from these potential risks. It is critical for website owners to verify that their website isn't vulnerable to the most common of attacks, and employ cybersecurity methodology to audit their systems and make sure that their web pages aren't vulnerable to, critically, the most basic types of attacks such as Cross Site Scripting or SQL Injection.

The most important part of analyzing a webpage to try and verify its safety against cyber threats is to follow a highly rigorous methodology, that tests every possible part of a webpage that could potentially be vulnerable to an attack. Following such a rigorous methodology is important to preventing a security breach, as the attacks used to gain access to sensitive information on a web server become increasingly complex as time passes, requiring web security to be extremely tight lest an attacker find the one vulnerability that went unchecked in an audit.

One of the most commonly used guidelines for testing a web page to confirm its security against hackers is the OWASP Testing Guide. The OWASP Testing Guide outlines a reliable and highly meticulous methodology for testing the security of a web page, and is used by security professionals worldwide to audit their own corporate web pages.

Web pages are a vital tool for both organizations and individuals in today's digital landscape. However, as the reliance on web sites grows, so does the possibility of security breaches. As a result, web page owners must take proactive efforts to secure their websites and protect against these possible risks. Businesses and individuals can protect themselves and their customers from the growing threat of cybercrime by taking the required steps to secure their web sites.

1.2 AIMS

The aims of this project.

- Use the OWASP Testing Guide as a framework to effectively identify the vulnerabilities present within the website provided.
- Suggest future work that could be done to help secure the web page further.
- Identify the strengths and weaknesses in following the methodology used.

2 PROCEDURE AND RESULTS

OVERVIEW OF PROCEDURE

The OWASP testing guide covers an extensive range of common vulnerabilities with web applications, and provides explanations, testing examples, and remediation processes for each step where appropriate. Because of its thoroughness, it will be used as a methodology to test the security of the given web application.

This document will follow a version of the OWASP Testing Guide that is modified to the scope of the website that is being tested (i.e. since there is no online presence of the machine being tested, the "Conduct Search Engine Discovery Reconnaissance for Information Leakage" section will be omitted, as it will be impossible to find any useful information about the machine using the methods outlined in the guide. The full testing guide can be found as part of the bibliography.

2.1 INFORMATION GATHERING

2.1.1 Fingerprint Web Server

OWASP then suggests scanning the webserver to identify the services running the web server. To complete this step, nmap will be used to find these services.

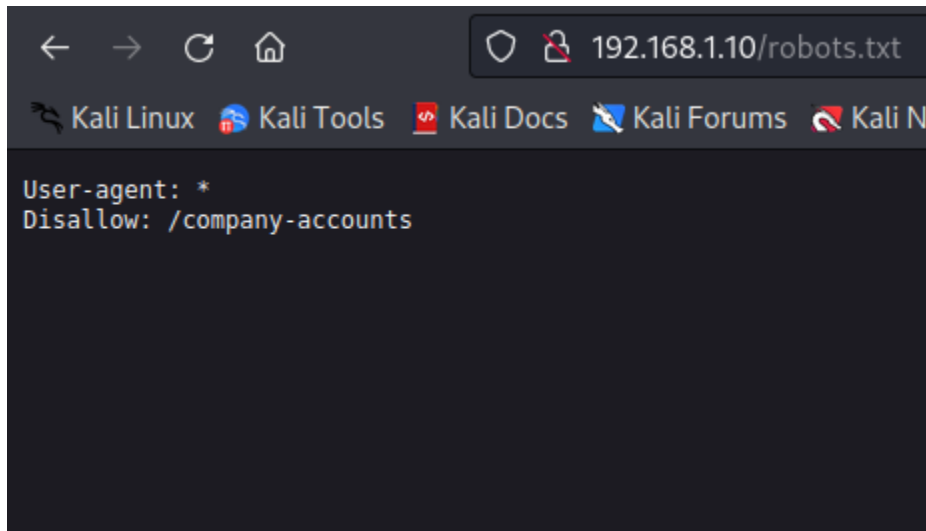
```
(kali㉿kali)-[~]
$ nmap -sV 192.168.1.10
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-14 21:05 EST
Nmap scan report for 192.168.1.10
Host is up (0.0030s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      ProFTPD 1.3.4a
80/tcp    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 16.89 seconds
```

Performing this scan revealed the server was using ProFTPD 1.3.4a for its file sharing service, Apache 2.4.3 for web server hosting, and MySQL for database handling.

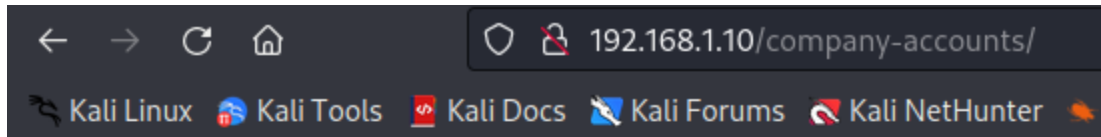
2.1.2 Review Webserver Metafiles for Information Leakage

OWASP suggests checking server metafiles, such as robots.txt, to enumerate any hidden paths on the machine, navigating to the robots.txt file gave the following results:






Above: the contents of robots.txt

This revealed the company accounts directory which, when navigated to, showed us a directory containing the accounts for the company.



Index of /company-accounts

| <u>Name</u> | <u>Last modified</u> | <u>Size</u> | <u>Description</u> |
|--|----------------------|-------------|--------------------|
|  Parent Directory | | - | |
|  finances.zip | 2022-09-20 14:09 | 293K | |
|  readme.txt | 2022-09-20 14:09 | 53 | |

2.1.3 Enumerate Applications on Webserver

Using nikto, it was possible to enumerate some of the applications running on the webserver, the most important one being PHP.

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

2.1.4 Review Webpage Content for Information Leakage

This involves manually going through every available webpage and scanning the files for comments or scripts that may contain sensitive information.

```
<link href="assets/css/bootstrap-responsive.css" rel="stylesheet">
```

The web pages index revealed some more directories, and that the webpage was most likely made using bootstrap.

```
<!--*** Denis Smith, d.smith@hacklab.com, phone number 01382 99999. Php expert.-->
<!--*** Denis Smith, d.smith@hacklab.com, phone number 01382 99999. Php expert.-->
```

user_account2.php revealed an employee's full name, phone number, and general position in the company. Knowing the full name and email of this employee could allow for email enumeration with just the name of an employee. This could also provide a reasonable target for phishing.

2.1.5 Identify Application Entry Points

Through navigating the website, it was found that there were several entry points which could be used to exploit vulnerabilities that require user input. The main entry point is the login system used for logging in users found on the home page, however others were found such as the admin login page, the announcement comments section, the user registration forum, and the products search bar.

2.1.6 Map Execution Paths Through Application

Using OWASP ZAP, it was possible to enumerate the paths more thoroughly than previous tests using the spider tool that comes with ZAP. Doing so revealed several important paths in the servers structure.

```
103 true,GET,http://192.168.1.10/assets/?C=M;O=A,
104 true,GET,http://192.168.1.10/assets/?C=S;O=A,
105 true,GET,http://192.168.1.10/assets/?C=D;O=A,
106 true,GET,http://192.168.1.10/assets/bootstrap.min.css,
107 true,GET,http://192.168.1.10/assets/bootstrap.min.js,
108 true,GET,http://192.168.1.10/assets/bootstrap/,
109 true,GET,http://192.168.1.10/assets/img/,
110 true,GET,http://192.168.1.10/assets/jquery.min.js,
111 true,GET,http://192.168.1.10/assets/js/?C=N;O=D,
112 true,GET,http://192.168.1.10/assets/offcanvas.css,
113 true,GET,http://192.168.1.10/assets/js/?C=M;O=A,
114 true,GET,http://192.168.1.10/assets/js/?C=S;O=A,
115 true,GET,http://192.168.1.10/assets/js/?C=D;O=A,
116 true,GET,http://192.168.1.10/assets/js/bootstrap.js,
117 true,GET,http://192.168.1.10/icons/unknown.gif,
118 true,GET,http://192.168.1.10/assets/js/bootstrap.min.js,
119 true,GET,http://192.168.1.10/icons/folder.gif,
120 true,GET,http://192.168.1.10/assets/js/bootstrap.min.tmp.js,
121 true,GET,http://192.168.1.10/assets/js/docs.min.js,
122 true,GET,http://192.168.1.10/assets/js/ie-emulation-modes-warning.js,
123 true,GET,http://192.168.1.10/assets/js/ie10-viewport-bug-workaround.js,
124 true,GET,http://192.168.1.10/assets/js/jquery.min.js,
```

Above: a small fraction of the paths enumerated from using the Spider tool

To further enumerate paths, dirb was also used to find any common paths that may have been missed. Doing this revealed several key paths as well.

```
--- Scanning URL: http://192.168.1.10/ ---
=> DIRECTORY: http://192.168.1.10/admin/
+ http://192.168.1.10/admin.cgi (CODE:403|SIZE:975)
+ http://192.168.1.10/admin.pl (CODE:403|SIZE:975)
=> DIRECTORY: http://192.168.1.10/assets/
+ http://192.168.1.10/AT-admin.cgi (CODE:403|SIZE:975)
+ http://192.168.1.10/cachemgr.cgi (CODE:403|SIZE:975)
+ http://192.168.1.10/cgi-bin/ (CODE:403|SIZE:989)
=> DIRECTORY: http://192.168.1.10/database/
=> DIRECTORY: http://192.168.1.10/img/
=> DIRECTORY: http://192.168.1.10/include/
+ http://192.168.1.10/index.php (CODE:200|SIZE:7443)
+ http://192.168.1.10/phpinfo.php (CODE:200|SIZE:76815)
+ http://192.168.1.10/phpmyadmin (CODE:401|SIZE:1222)
=> DIRECTORY: http://192.168.1.10/pictures/
+ http://192.168.1.10/robots.txt (CODE:200|SIZE:42)
=> DIRECTORY: http://192.168.1.10/sales/

--- Entering directory: http://192.168.1.10/admin/ ---
=> DIRECTORY: http://192.168.1.10/admin/ADMIN/
+ http://192.168.1.10/admin/admin.cgi (CODE:403|SIZE:975)
+ http://192.168.1.10/admin/admin.pl (CODE:403|SIZE:975)
=> DIRECTORY: http://192.168.1.10/admin/assets/
+ http://192.168.1.10/admin/AT-admin.cgi (CODE:403|SIZE:975)
+ http://192.168.1.10/admin/cachemgr.cgi (CODE:403|SIZE:975)
+ http://192.168.1.10/admin/error_log (CODE:200|SIZE:1320)
=> DIRECTORY: http://192.168.1.10/admin/include/
+ http://192.168.1.10/admin/index.php (CODE:200|SIZE:2654)
```

Above: an excerpt from the dirb scan, revealing the location of the admin login screen and a sales directory.

2.1.7 Fingerprint Web Application Framework

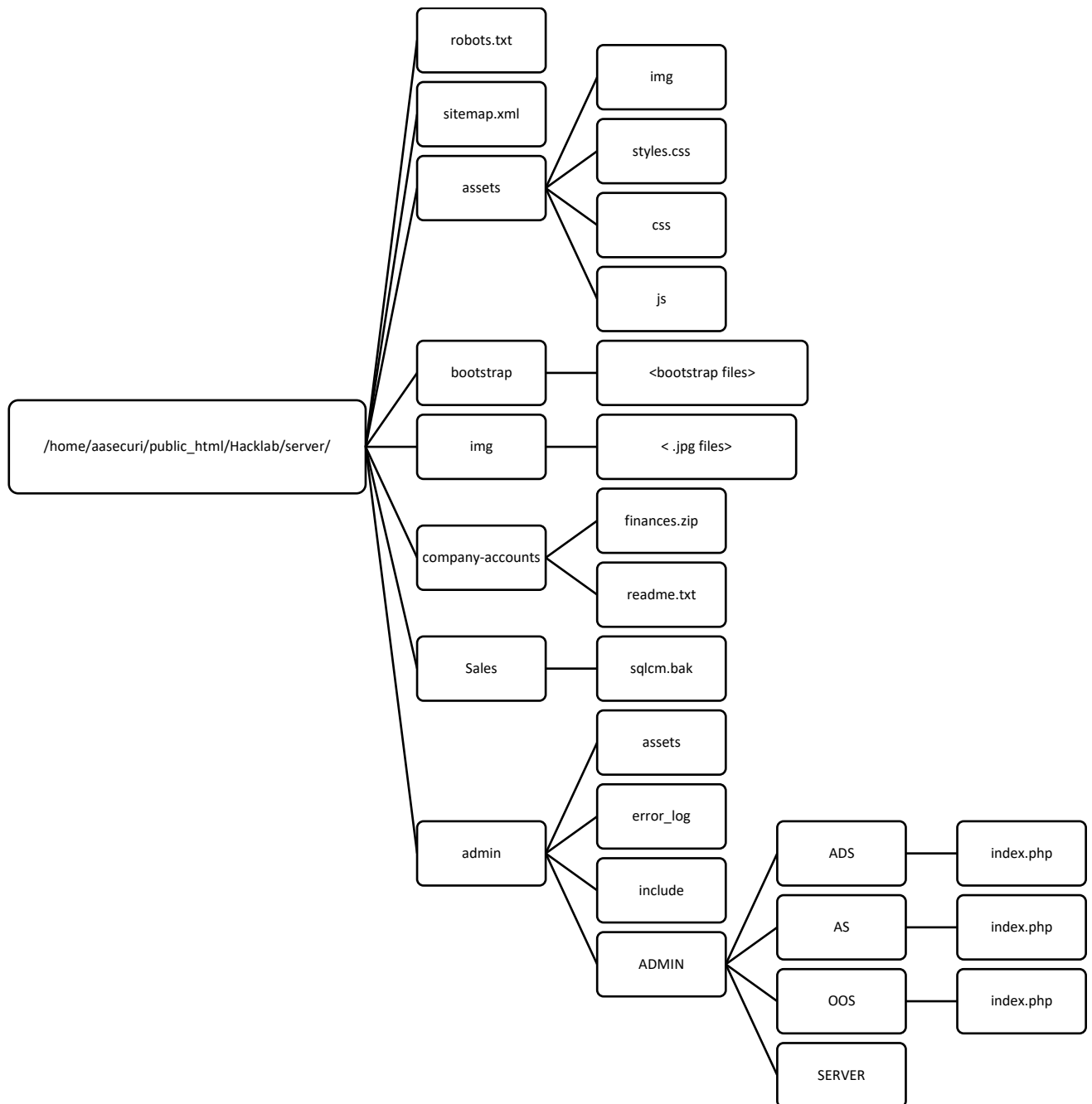
using curl, it was possible to confirm the information we knew about the framework of the server.

```
(kali㉿kali)-[~]
$ curl -I 192.168.1.10
HTTP/1.1 200 OK
Date: Mon, 16 Jan 2023 03:07:30 GMT
Server: Apache/2.4.3 (Unix) PHP/5.4.7
X-Powered-By: PHP/5.4.7
Content-Type: text/html
```

2.1.8 Map Application Architecture

Using the information already gained by spidering, the information found with dirb and a wget mirror. It was possible to estimate a map of directories and files on the server. Some sections of the server are

omitted based on their irrelevance to the security aspects of the server. The full spider scan and dirb scan logs can be viewed in Appendix B and C respectively.



2.2 CONFIGURATION AND DEPLOYMENT MANAGEMENT TESTING

2.2.1 Test Network Infrastructure Configuration

The version of Apache currently running on the server was released in 2017, around five years ago at the time of testing. In this time, many vulnerabilities have been discovered and could potentially be used on this web application to gain access to the machine.

2.2.2 Test Application Platform Configuration

As found out using a nikto scan, it is possible to see the information regarding the php version installed by navigating to phpinfo.php.



Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

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 |
| 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 |

This tells us a lot of useful information, such as the php version number and some more directories on the machine and the exact version of linux that is running the web page

| | |
|-----------------------------------|------------------------|
| Support | |
| Configuration File (php.ini) Path | /opt/lampp/etc |
| Loaded Configuration File | /opt/lampp/etc/php.ini |

2.2.3 Test File Extensions Handling for Sensitive Information

The server allows the access of file types that may serve sensitive information. In this example, the file sqlcm.bak is accessed.

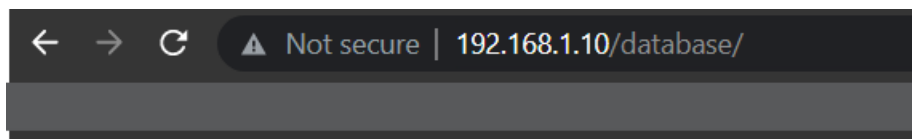
Navigating to the /sales/ directory it was possible to find a piece of sql code stored in a file named sqlcm.bak , which could reveal some information about the database.

```
(kali@kali)-[~]
$ cat sqlcm.bak
<?php $username= str_replace(array("1=1", "2=2", "Union","union","'b'='b'","'a'='a'","'b'='b'"), "", $username); ?>
```

Above: the contents of sqlcm.bak

2.2.4 Review Old Backup and Unreferenced Files for Sensitive Information

Through a previous nikto scan, a directory named databases was found a quickly accessed to discover a file named aa2000.sql. this file is not referenced by any normally accessed webpage and seems to be a database dump generated by PHPmyAdmin. This file could potentially allow a hacker to enumerate the architecture of the database currently active on the server.



Index of /database

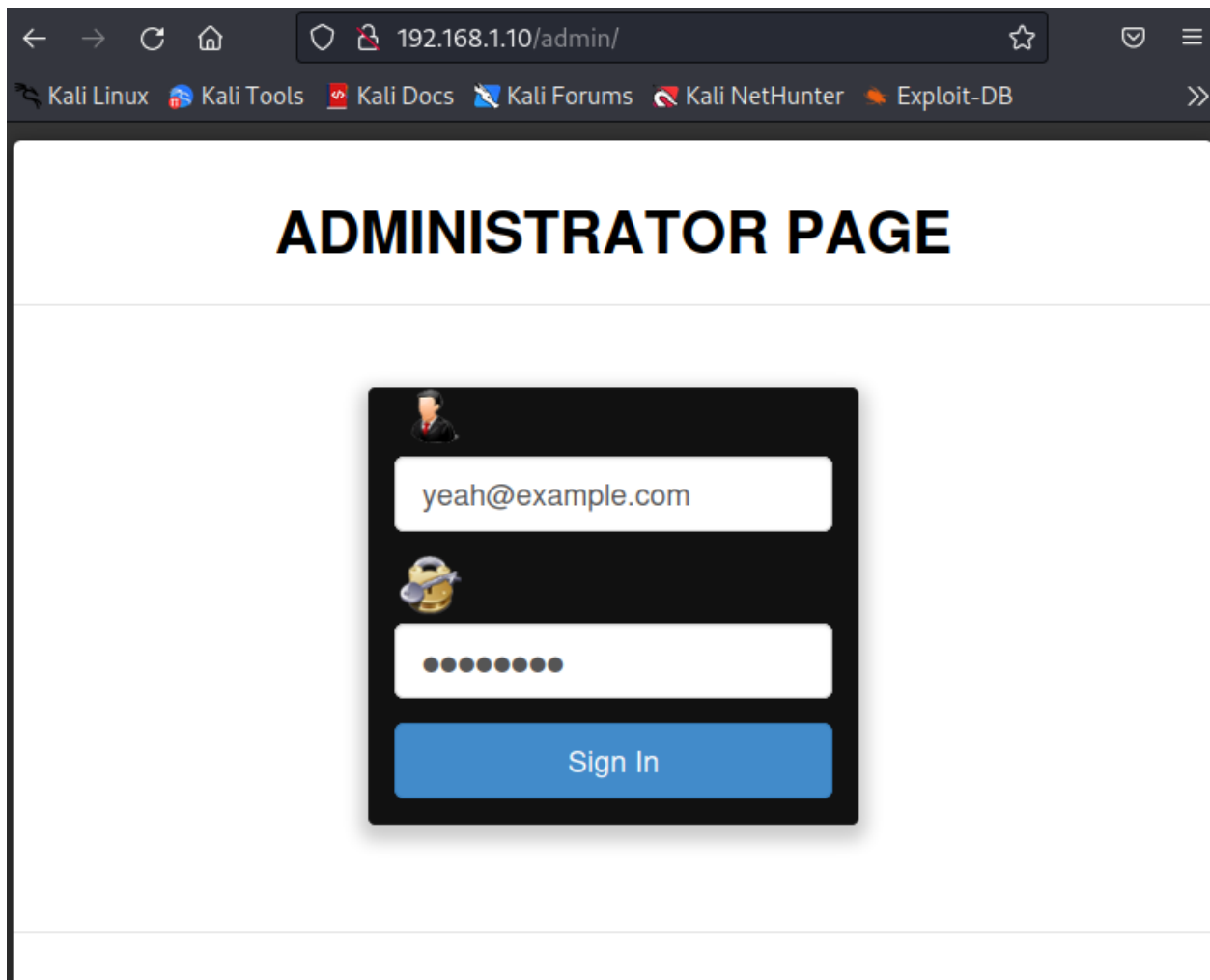
| Name | Last modified | Size | Description |
|----------------------------------|-------------------------------|----------------------|-----------------------------|
| Parent Directory | | - | |
| aa2000.sql | 2017-07-08 20:00 | 28K | |

Above: Screenshot of what happens when a user navigates to the databases directory on a browser

The contents of this file are displayed in Appendix A.

2.2.5 Enumerate Infrastructure and Application Admin Interfaces

From previous dirb scans, a directory named admin was discovered, navigating to this directory on a browser leads to an admin login page.



After discovering the error log file in the admin directory, it was possible to enumerate the path for the homepage on the filesystem.

```
[19-Aug-2015 05:09:00 UTC] PHP Warning: session_regenerate_id(): Cannot regenerate session id - headers already sent in /home/aasecure/public_html/Hacklab/server/index.php on line 75  
[19-Aug-2015 05:18:50 UTC] PHP Warning: session_start(): Cannot send session cache limiter - headers already sent (output started at /home/aasecure/public_html/Hacklab/server/index.php:49) in /home/aasecure/public_html/Hacklab/server/index.php on line 74  
[19-Aug-2015 05:18:50 UTC] PHP Warning: session_regenerate_id(): Cannot regenerate session id - headers already sent in /home/aasecure/public_html/Hacklab/server/index.php on line 75
```

Above: the location of the homepages file on the server is highlighted.

2.2.6 Test HTTP Methods

Using an nmap script called http-methods, we can test the http methods currently active on the server.

```
(kali㉿kali)-[~]
└─$ nmap -p 80 --script http-methods 192.168.1.10
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-15 23:05 EST
Nmap scan report for 192.168.1.10
Host is up (0.00090s latency).

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 0.25 seconds
```

2.2.7 Test HTTP Strict Transport Security

Following the test framework provided by OWASP indicates that the server does not support HSTS, likely due to the fact the server does not provide access through HTTPS.

2.3 IDENTITY MANAGEMENT TESTING

2.3.1 Test Role Definitions

From performed testing, it is apparent that there are at least two roles on the server: customers and admins. Customers are defined by their registered accounts, and their session cookie that identifies them. Admins are identified in the database, and aren't set using any form of onsite registration or identified by a specific cookie.

2.3.2 Test User Registration Process

Testing the user registration process in the OWASP web testing guide covers validating that the process for registration covers an appropriate amount of data required for the purposes of security and conducting the business required of the website, while also validating that the user that provides this information is submitting it truthfully.

When registering for an account on the website, a user's full name, email , date of birth, address , and a password are required. These identifiers make sense to be collected by the business, as a name and address are needed as part of delivering their product. However, the validity of the data given during the registration process is not checked outside of a length check and a date check to make sure users aren't below 18, meaning that anyone can input any information they want, and potentially pretend to be someone else using their information.

Your personal information

Gender

First name *

Middle name *

Last name *

Email *

Password *

Confirm Password *

Date of Birth *

Your address

Address *

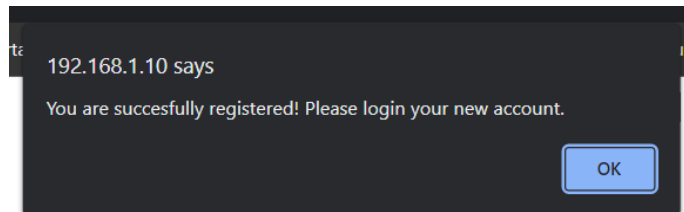
City *

Contact Number *

[Register](#)

Left: False information is inserted into the user registration form.

Below: The server accepts this information, without validating the data enough to verify that it is real or not



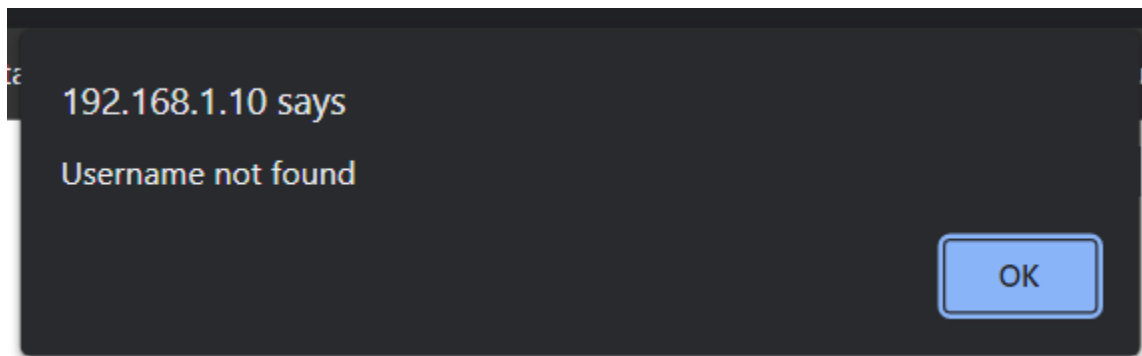
2.3.3 Testing for Account Enumeration and Guessable User Account

It may be possible to enumerate if a user is present on the database by seeing how the login system responds to different login information.

In this example, a username and password are submitted to the login system that doesn't exist on the machine.

[Sign in](#) [Sign Up](#)

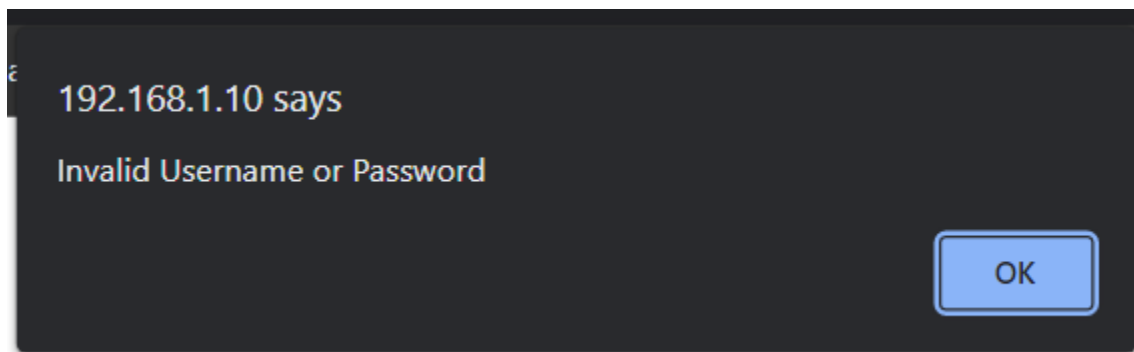
The system responds with the following message:



Then, using a username that is known to be on the machine is used, but with the wrong password.



The system responds with the following message:



This could suggest to an attacker that the username is present on the machine, but the password is incorrect.

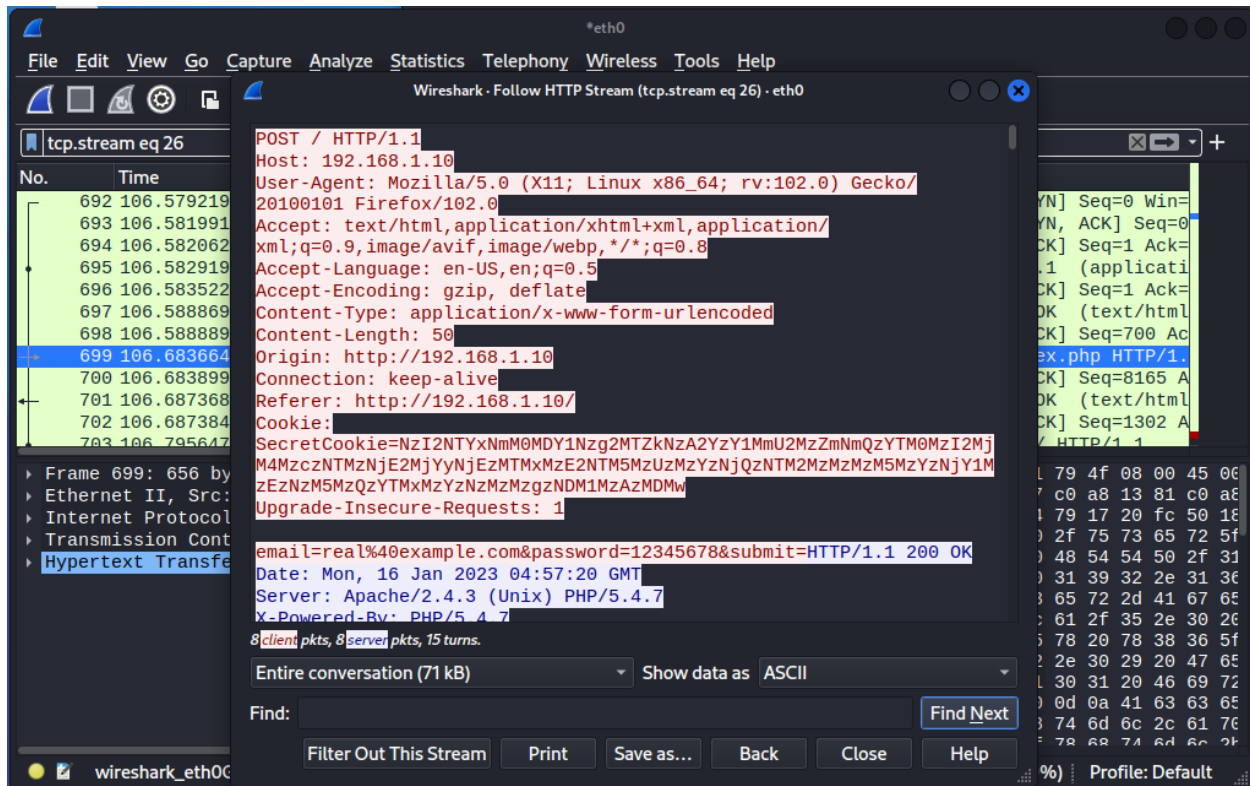
2.3.4 Testing for Weak or Unenforced Username Policy

For some systems, the username policy is highly structured i.e. usernames are generated using the first and last name of a user. This could lead to usernames being easily guessed by attackers if the structure of usernames is known. Since the username is decided by the user in the system, it is less likely that this sort of guessing would be possible.

2.4 AUTHENTICATION TESTING

2.4.1 Testing for Credentials Transported over an Encrypted Channel

Since the system only uses HTTP, it is likely that information is being sent to and from the system is unencrypted. To test this, Wireshark was used to sniff a successful login attempt on the webpage. The results show that no information is encrypted, and shows that user info is vulnerable to being intercepted and used by attackers.



2.4.2 Testing for Weak lock out mechanism

To test a weak lock out mechanism, an account was attempted to be logged into at least 20 times using the wrong password. The system did not attempt to lock out after this many attempts, implying that many more attempts would be possible after 20 attempts. This means that a brute force attack is very likely to be possible using the login form and could lead to hackers gaining access to users.

2.4.3 Testing for Bypassing Authentication Schema

To test this, an attempt to access several pages that require a user were attempted such as user_index.php, user_products.php, user_contact.php, user_aboutus.php, user_order.php, and Email.php. Trying to access any of these pages lead the client back to the homepage, confirming that the authentication schema works.

2.4.4 Testing for Weak Password Policy

The password policy as part of the registration process on users consists of checking whether the password is between 7 and 14 letters long. This policy is slightly better than none, however it still leaves room for users to be able to use some of the most common passwords (password, 12345678, and qwertyuiop are all acceptable passwords under this policy)

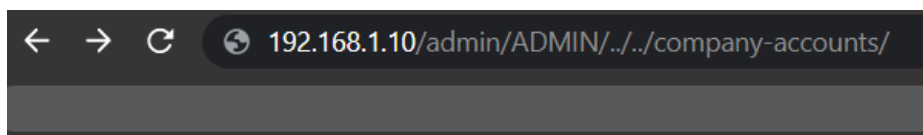
2.4.5 Testing for Weak Password Change or Reset Functionalities

Changing a user's password in their profile option requires no authentication of an old password from the user. This is highly vulnerable as if a hacker somehow gained access to a user's account without their password, they would be able to change the user's password and lock the valid user out without needing to know the old password.


2.5 AUTHORIZATION TESTING

2.5.1 Testing Directory Traversal File Include

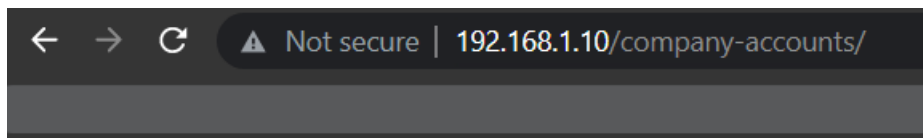
The system was found to be vulnerable to directory traversal without authentication. Using the known directories available, an attempt was made to traverse from /admin/ADMIN/ to /company-accounts/






Index of /admin/ADMIN

| <u>Name</u> | <u>Last modified</u> | <u>Size</u> | <u>Description</u> |
|--|----------------------|-------------|--------------------|
|  Parent Directory | | - | |
|  ADS/ | 2017-07-13 14:57 | - | |
|  AS/ | 2017-07-13 15:00 | - | |
|  OOS/ | 2017-07-13 15:01 | - | |
|  SERVER/ | 2017-07-08 19:53 | - | |

Above: The client is currently in the /admin/ADMIN/ directory, and will attempt to traverse the system to the directory in the URL bar.



Index of /company-accounts

| Name | Last modified | Size | Description |
|--|-------------------------------|----------------------|-----------------------------|
| <hr/> | | | |
|  Parent Directory | | - | |
|  finances.zip | 2022-09-20 14:09 | 293K | |
|  readme.txt | 2022-09-20 14:09 | 53 | |

Above: Result of testing, successful traversal.

2.5.2 Testing for Bypassing Authorization Schema

Attempting to access webpages that require authentication, such as `user_index.php` and `/admin/ADMIN/ADS/index.php` was tested. While `user_index.php` denied access, the admin panel was able to be accessed, bypassing the admin login that is usually required.

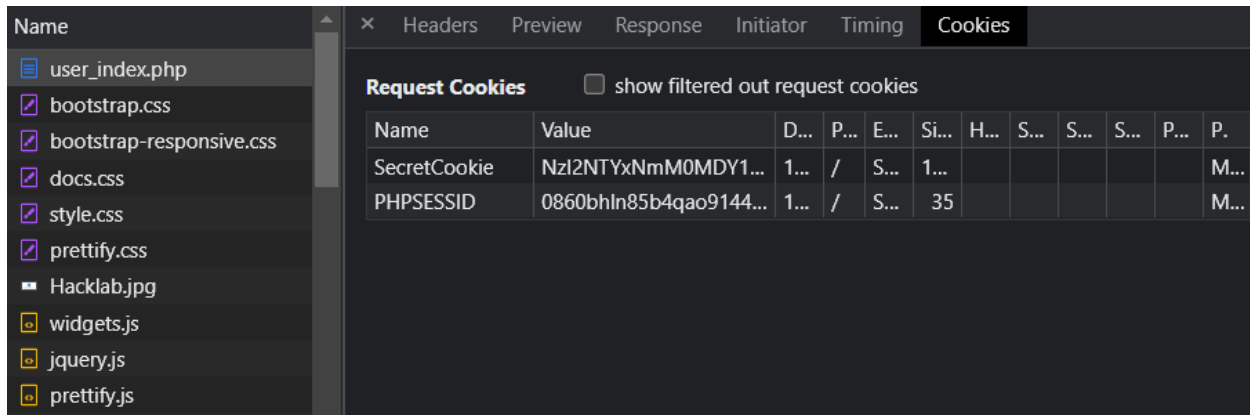
2.5.3 Testing for Privilege Escalation

Testing was performed to see if a user could elevate themselves into an admin through the web application. Since admins aren't created using any onsite systems, it isn't possible for a user to escalate their privileges from the web application itself.

2.6 SESSION MANAGEMENT TESTING

2.6.1 Testing for Session Management Schema

In order to test the session management schema, we would need to investigate the way the server kept track of sessions. This was found to be through the use of cookies, specifically through a cookie named SecretCookie



Above: Using Inspect Element revealed the session cookies

Knowing this, some tests were made to see if the session cookies found used insecure encryption methods. Using an online cipher identifier, it was found the SecretCookie was encoded by converting the cookie to hex, then to base64. Decoding the cookie by decoding the encoded cookie revealed mthat the cookie was storing the username of the user.



Above: a decoded SecretCookie

The last 10 characters appear to be a unix timestamp, given how close the number was in comparison to the unix time when the test was run.



Above: the last 10 characters of the cookie are very close to the current Unix time.

The Middle section of the cookie appears to be an MD5 encrypted string. When decoded, it reveals the middle portion of the cookie is the password of the user that is logged in.

Found : 12345678
(hash = 25d55ad283aa400af464c76d713c07ad)

This Cookie is extremely vulnerable to being decrypted by attackers if they are able to get their hands on it.

2.6.2 Testing for Cookies Attributes

To test if a user's cookies are properly managed, a cookie editor called EditThisCookie was used to observe the attributes of the user's SecretCookie, and confirm the session with the cookie ends once a user has logged out. Testing shows that the website preserves a user's cookie after a session has ended, which could potentially lead to a user's cookie being stolen ever after they have logged out of their session

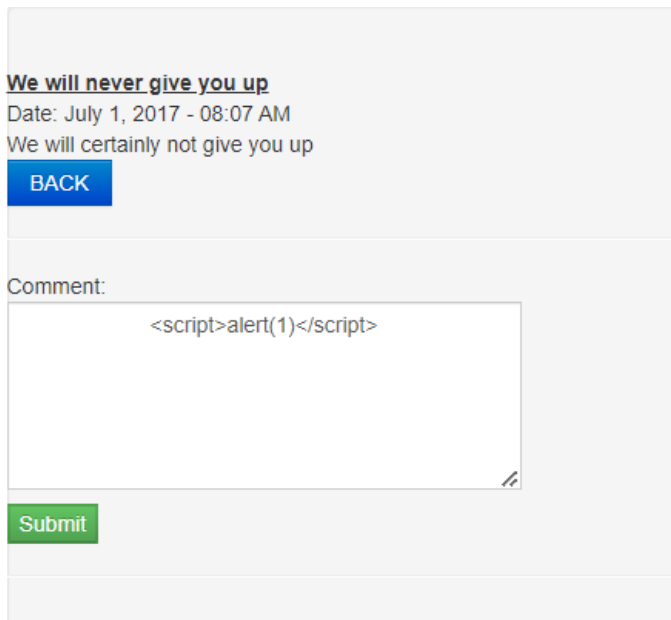
2.6.3 Testing for Session Fixation

Since a user's SecretCookie is always renewed at the start of a session, and uniquely identified by login time using the unix timestamp in the cookie, session fixation testing is not required.

2.7 INPUT VALIDATION TESTING

2.7.1 Testing for Stored Cross Site Scripting

When logged in as a user, it is possible to comment on announcements made by admins. The field for writing comments is vulnerable to having scripts written into them, as shown by the screenshots below.



The screenshot shows a web interface for submitting a comment. At the top, there is an announcement: "We will never give you up" with a date of "Date: July 1, 2017 - 08:07 AM" and the text "We will certainly not give you up". Below this is a blue "BACK" button. The main section is titled "Comment:" and contains a text input field. Inside the input field, the text "<script>alert(1)</script>" is entered. Below the input field is a green "Submit" button.

Above: the XSS payload is submitted as a comment



Above: The response from the server, indicating that the XSS attack has worked

Since the comment is stored and displayed on the page, this script will run every time a user visits the announcement page.

2.7.2 Testing for SQL Injection

Using SQLmap, it was discovered that the email and password sign in field on the homepage was vulnerable to sql injection.

```
POST parameter 'email' is vulnerable. Do you want to keep testing the others (if any)? [y/N] n
sqlmap identified the following injection point(s) with a total of 406 HTTP(s) requests:
--
Parameter: email (POST)
  Type: boolean-based blind
  Title: OR boolean-based blind - WHERE or HAVING clause (MySQL comment)
  Payload: email=-3620' OR 3571=3571#password=&submit=GJxi

  Type: error-based
  Title: MySQL >= 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (BIGINT UNSIGNED)
  Payload: email=kjli' AND (SELECT 2*(IF((SELECT * FROM (SELECT CONCAT(0x7171767a71,(SELECT (ELT(9032=9032,1))),0x717a6b6a71,0x78))s), 8446744073709551610, 8446744073709551610)))-- FXBL&password=&submit=GJxi

  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: email=kjli' AND (SELECT 1747 FROM (SELECT(SLEEP(5)))ymbI)-- Eoxg&password=&submit=GJxi
--
```

Knowing this, it was possible to enumerate the entire site's database as well as crack the usernames and passwords of known admins.

```
2029 Table: tb_user
2030 [3 entries]
2031 +-----+-----+-----+-----+-----+
2032 | userID | utype | Employee | password | username |
2033 +-----+-----+-----+-----+-----+
2034 | 1 | 3 | Benjie I. Alfanta | e10adc3949ba59abbe56e057f20f883e | BENJIE_OOS |
2035 | 2 | 2 | Leo Aranzamendez | 7052cad6b415f4272c1986aa9a50a7c3 | hacklab |
2036 | 3 | 1 | Julius Felicen | 6d44082c352def8d0b1b8a2b9ba0ce59 | admin |
2037 +-----+-----+-----+-----+-----+
```

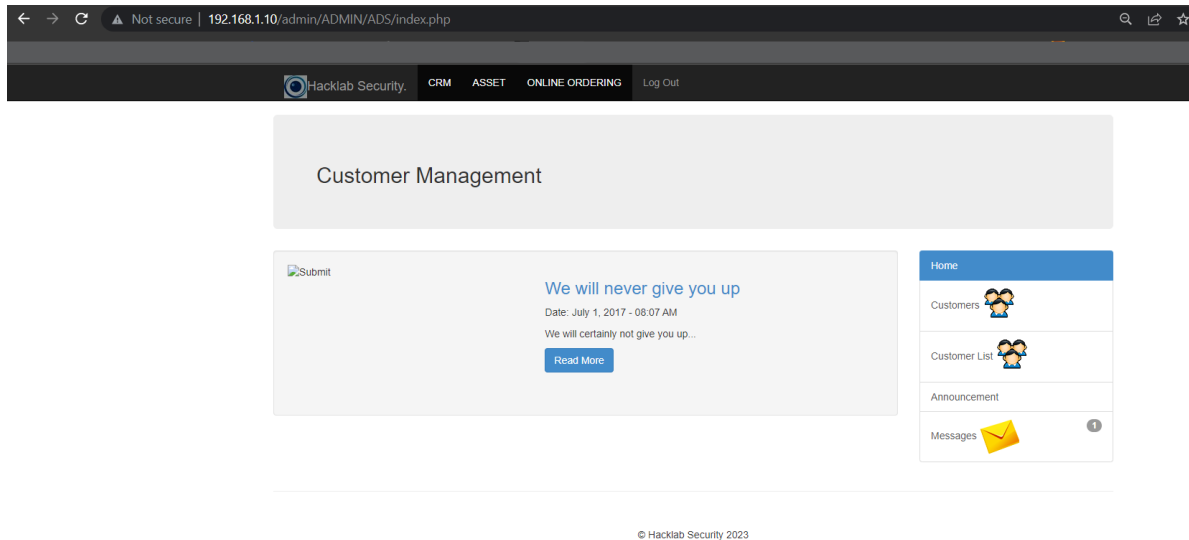
Above: List of users on the database, the password field is MD5 encrypted, which is easily decryptable.

Found : fungible

(hash = 6d44082c352def8d0b1b8a2b9ba0ce59)

Above: The password of Julius Felicen

To confirm these credentials were correct, an attempt to log into the admin panel was made using Julius Felicen's credentials. This granted successful access to the admin panel.



Above: Access to the admin panel is possible through sql injection exploitation

2.7.3 Testing for Local File Inclusion

Testing for local file inclusion was attempted on multiple pages to see if the include function was not sanitized on these pages. Results returned very little, indicating that the server was secure against local file inclusion.

2.8 TESTING FOR ERROR HANDLING

2.8.1 Testing for Improper Error Handling

Critical error handling was tested on all user inputs on the site by attempting to input unexpected inputs whenever user input is required, this includes but is not limited to:

- Leaving all fields empty
- Inputting words when numbers were required
- Editing the value of select HTML elements to be different to their expected values

Testing all of these options on every input revealed there was good error handling on the server, as none of these tests lead to a critical error.

2.9 TESTING FOR WEAK CRYPTOGRAPHY

2.9.1 Testing for Sensitive Information Sent via Unencrypted Channels

From previous pen testing, it is known that information sent to the server is unencrypted. To test if sensitive information is also sent unencrypted to the website, Wireshark was used to see if the information sent during registration was also vulnerable to being captured. The results show that potentially sensitive information such as a telephone number, a user's address and their full name could be captured by an attack during the registration process.

```
POST /register.php HTTP/1.1
Host: 192.168.1.10
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 236
Origin: http://192.168.1.10
Connection: keep-alive
Referer: http://192.168.1.10/register.php
Upgrade-Insecure-Requests: 1

gender=Male&fname=Test&middlename=Test&lastname=Test&email=test%40example.com&password=12345678&password1=12345678&bdate=1964-11-02&address=123+test+street&city=Dundee&cnumber=000000000000&email_create=1&is_new_customer=1&submit=RegisterHTTP/1.1 200 OK
```

Above: the data sent to the registration form is easy to parse and collect sensitive information from.

2.9.2 Testing for Weak Encryption

Through previous testing (See 2.8.3 and 2.7.1) testing for weak encryption has been performed. The results of the testing show that much of the sensitive information used on the website used MD5 encryption, which is incredibly easy to decrypt and can be decrypted using free online tools.

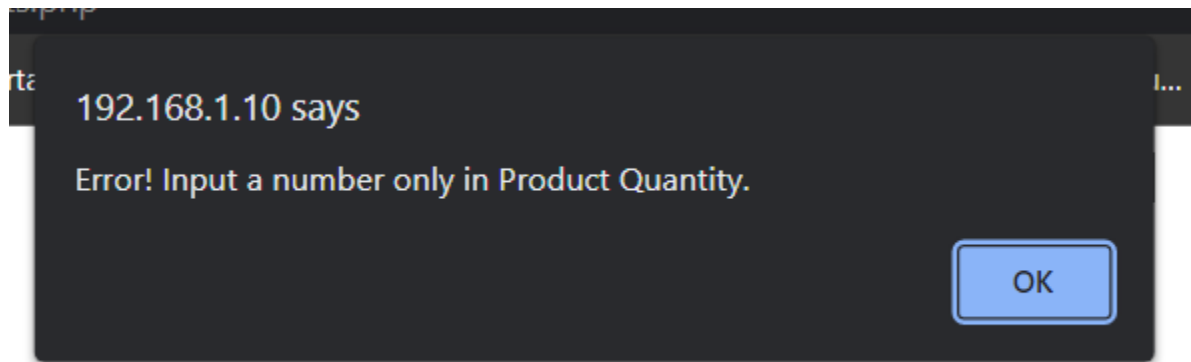
2.10 BUSINESS LOGIC TESTING

2.10.1 Test Upload of Unexpected File Types

There is one place on the web application that supports file uploading: the product image upload when creating a new product to put on the store. To test this field, a php file was attempted to be uploaded instead of an expected image file.

| | |
|---|--|
| Product Name | <input type="text" value="test"/> |
| Product Price | <input type="text" value="test"/> |
| Product Quantity | <input type="text" value="123"/> |
| Product Description | <input type="text" value="test"/> |
| Product Image | <input type="button" value="Choose File"/> example.php |
| <input type="button" value="BACK"/> <input type="button" value="Submit"/> | |

However, when uploaded, the form returns with an error:

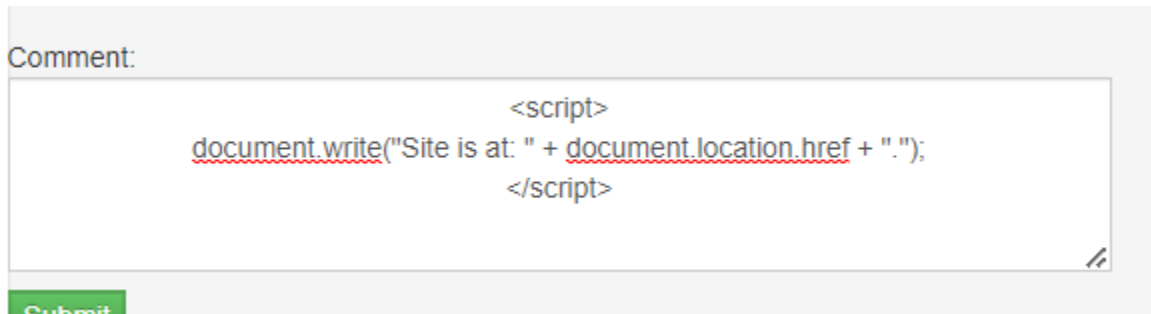


This appears to happen even when an expected input is given, indicating that the form is broken.

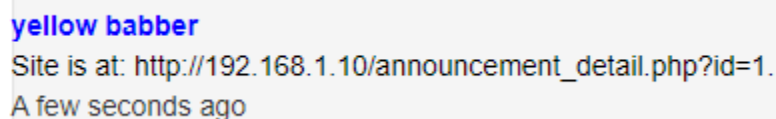
2.11 CLIENT-SIDE TESTING

2.11.1 Testing for DOM-Based Cross Site Scripting

From Previous testing, there is a known XSS vulnerability in the announcements comments section, to test how vulnerable this is, a payload is used to see if the vulnerability could be used to effectively edit the DOM.



Above: the following code is uploaded to the comments section



Above: The result, showing that DOM based XSS is possible.

3 DISCUSSION

3.1 OVERALL DISCUSSION

Using the OWASP Testing guide as a basis for testing this web application has made it clear that there are a considerable amount of vulnerabilities present within the server. Out of all of the testing stages completed, sensitive data or a potential vulnerability was discovered in almost every single test. This indicates an extreme lack of security on the web server and will very likely lead to either sensitive data being leaked in the future or to the server being shut down by malicious attackers.

Probably the most egregious vulnerability present on the server at the time of testing is the SQL injection vulnerability found in the login system for users. Through this single vulnerability, the entire web pages database was collected providing unprecedented insight into the data stored on the page. Through the collection of the database, the admin credentials were able to be found as well, leading to authorized access to the page's admin panel. This single vulnerability would most likely have the most impact on the web page if it were to be performed by an attacker, as an attacker would be able to steal all the sensitive information on the server, as well as cause significant disruption to the webpage through access to the admin panel.

3.2 COUNTERMEASURES

3.2.1 SQL Injection

The SQL Injection vulnerability makes the web application highly vulnerable to having sensitive information stolen from the database. This vulnerability is possible through the login system on the homepage as the login inputs are not properly sanitized against SQL code.

There are several ways to sanitize this input, but the easiest way would be to use MySQLi's `real_escape_string` function to sanitize the input of the fields as it is passed into the login function. This function removes any special characters from the input, making most SQL queries impossible to perform (The PHP Group, n.d.).

```
// Escape special characters, if any
$username = $mysqli -> real_escape_string($_POST['username']);
$password = $mysqli -> real_escape_string($_POST['password']);
```

Above: a hypothetical way to implement the use of the `real_escape_string` function to prevent SQL injection

3.2.2 Using HTTPS

Since the web application only uses HTTP, all of the information sent to and from the server is completely unencrypted. This could potentially lead to hackers stealing the username, password and more from anyone who wants to use the website for its intended purposes.

Using HTTPS with Apache requires obtaining a SSL certificate from either a trusted certificate authority or by generating a self-signed certificate. After the SSL certificate is installed on the machine, the configuration file should be edited to include the SSL certificate, while also configuring the server port from 80 to 443. Once this is done, the server should be restarted to confirm the changes made to the configuration file.

Since the exact specifics of the Apache configuration are not currently known, this countermeasure does not go into specifics, and further research should be performed into using HTTPS on the servers version of Apache.

3.2.3 Change Encryption Methods

In several cases, lackluster encryption has been used to attempt to obfuscate sensitive material. For example, during testing for session management schema, it was found that the current logged in user's cookie was encrypted by taking the user's username, MD5 encrypted password , and Unix timestamp and converting it to hex code, then to base64.

This encryption is easily reversible with online decryption tools and is not a secure way of generating session cookies. Even further, the MD5 encryption method used to encrypt the password in the cookie is almost 30 years old now and contains a multitude of bugs that allow it to be quickly decrypted, meaning that anyone with a user's cookie could easily enumerate their username and password.

The same encryption method was used in the database to encrypt passwords for admins, meaning that admins would be vulnerable to similar decryption methods if an attacker was able to view the database.

It is recommended that a stronger encryption method is used for both these cases , especially using encryption methods that are not reversible. A better candidate for password encryption would be to use an encryption method like SHA256, which is much harder to crack

3.2.4 XSS

The comments form on the announcements page is vulnerable to stored cross site scripting, meaning attackers could potentially inject malicious code into the page to steal users cookies or bring down the entire web application.

Since the commenting system is coded using PHP, it's possible to use the htmlspecialchars function to sanitize a comments contents before it is displayed on a webpage.

```
1 echo '<br>' .
2 '<font color="blue">
3 <b>' . $username . '</b></font>
4 <br> <font color="black">'
5 . htmlspecialchars($_POST['commentinput']) . '</font><br>' .
6 $datetime .
7 '<br>';
```

Above: a hypothetical implementation of the sanitization of user input in announcement_detail.php

3.2.5 Username Enumeration

The login system is configured in such a way that makes it possible for potential attackers to confirm if a username is used on the system (see 2.4.3: Testing for Account Enumeration and Guessable User Account). The error message for attempting to log into a user that exists, versus one that does not, should be exactly the same to prevent this kind of username enumeration.

3.2.6 Prevent Access to Sensitive Directories

There are several files and directories that are clearly not meant to be accessible by average users, including the company accounts and the admin panel (see 2.3.4 for example). Users gaining access to these types of files is a huge breach of data security and is not safe for the security of the website.

To fix this, some rules regarding user access to files through apache should be introduced. Firstly, all sensitive files should be unable to be accessed via the web application, as this poses a massive threat to data security. Secondly, the admin panel should only be viewable from a defined number of machines, so as to prevent anyone from coming across these pages randomly. Thirdly, a rule should be implemented to prevent future or unknown potentially vulnerable files from being accessed online.

These rules can be applied by editing the .htaccess file in the root directory of the apache installation to include these rules:

```
1 <Directory "/admin">
2     Require ip <insert admin machine here>
3 </Directory>
4
5 <Files "<insert affected file here">
6 Order allow,deny
7 Deny from all
8 </Files>
9
10 <FilesMatch '^.*.(asa|inc|config|zip|txt|bak|old)$'>
11 Order allow,deny
12 Deny from all
13 </FilesMatch>
14
15
```

Above: Editing .htaccess to include these lines should help prevent access to unwanted files and potentially sensitive directories.

3.2.7 User Security

The user password requirements for an account are incredibly barebones, and do not have enough rules to create a sufficiently difficult password to crack. Passwords should at least require a capital letter, a number and some kind of special character to reduce the effectiveness of attackers using brute force password guessing software.

Another vital addition that should be made to protect users from being hacked would be to implement a login lockout feature if a user fails to login to an account after a set number of attempts. Implementing this would also reduce the effectiveness of brute force attacks.

3.2.8 PHPinfo.php

The PHPinfo page makes use of the phpinfo function to display certain information about the php installation, such as the directory that the web servers contents are stored in, the variables used by php, and the current version of php installed on the machine. This information could be used by attackers to enumerate certain information about the server, and therefore this page should not be accessible to users.

Restricting access to this page can be done using the same methods in 3.2.6, however since this page isn't critical to the functioning of the server, it is recommended that the page be deleted entirely.

3.3 FUTURE WORK

From testing, there has been a wide range of vulnerabilities tested and found through the methodology provided by OWASP, however I believe that they may have been other vulnerabilities present that did not fall under the scope of the OWASP testing guide. One vulnerability that I think the server might be vulnerable to is a shellshock attack. This vulnerability was pointed out during initial scanning phases by scanning the server with nikto, which highlighted that this vulnerability may be possible.

```
+ OSVDB-112004: /cgi-bin/printenv: Site appears vulnerable to the 'shellshock' vulnerability (http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6271).  
+ OSVDB-112004: /cgi-bin/printenv: Site appears vulnerable to the 'shellshock' vulnerability (http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6278).
```

If this is true, it would be possible for an attacker to easily gain root access to the server, and with that complete control over the web application. Given more time and a broader testing scope, I would have liked to research this potential vulnerability further, and confirm if it is a potential vector for root access to the server.

The version of Apache running on the server is quite old, and is likely vulnerable to many more vulnerabilities that lie outside of the OWASP testing guides guidelines. Given more time, research into more version based vulnerabilities would have been made in order to further identify vulnerabilities that may be in the web applications configuration.

4 BIBLIOGRAPHY

Apache HTTP Server Project. (2023). *Apache HTTP Server Tutorial: .htaccess files*. Retrieved from Apache HTTP Server Project: <https://httpd.apache.org/docs/2.4/howto/htaccess.html>

CyberSecurity Ventures. (2022). Retrieved from 2022 Official Cybercrime Report: <https://www.esentire.com/resources/library/2022-official-cybercrime-report>

Infosec Scout. (n.d.). *MD5 vs SHA256: Which is Better?* Retrieved from Infosec Scout: <https://infosecscout.com/md5-vs-sha256/>

OWASP. (2023). *OWASP Web Security Testing Guide*. Retrieved from <https://owasp.org/www-project-web-security-testing-guide/>

The PHP Group. (n.d.). *PHP: htmlspecialchars*. Retrieved from <https://www.php.net/manual/en/function htmlspecialchars.php>

The PHP Group. (n.d.). *PHP: mysqli_real_escape_string*. Retrieved from PHP: <https://www.php.net/manual/en/mysqli.real-escape-string.php>

The PHP Group. (n.d.). *PHP: phpinfo.php*. Retrieved from <https://www.php.net/manual/en/function.phpinfo.php>

APPENDICES PART 1

APPENDIX A

```
-- phpMyAdmin SQL Dump
-- version 4.2.11
-- http://www.phpmyadmin.net
--
-- Host: 127.0.0.1
-- Generation Time: Sep 21, 2015 at 03:10 PM
-- Server version: 5.6.21
-- PHP Version: 5.5.19

SET SQL_MODE = "NO_AUTO_VALUE_ON_ZERO";
SET time_zone = "+00:00";

/*!40101 SET @OLD_CHARACTER_SET_CLIENT=@@CHARACTER_SET_CLIENT */;
/*!40101 SET @OLD_CHARACTER_SET_RESULTS=@@CHARACTER_SET_RESULTS */;
/*!40101 SET @OLD_COLLATION_CONNECTION=@@COLLATION_CONNECTION */;
/*!40101 SET NAMES utf8 */;

--
-- Database: `aa2000`
--

--
-- Table structure for table `asset_archive`
--

CREATE TABLE IF NOT EXISTS `asset_archive` (
  `productID` int(11) NOT NULL,
  `name` varchar(50) NOT NULL,
  `price` int(20) NOT NULL,
  `image` varchar(50) NOT NULL,
  `details` text NOT NULL,
  `quantity` int(20) NOT NULL,
  `date_created` varchar(50) NOT NULL
) ENGINE=InnoDB DEFAULT CHARSET=latin1;

--
-- Table structure for table `asset_depreciation`
--
```

```

CREATE TABLE IF NOT EXISTS `asset_depreciation` (
  `item_id` int(11) NOT NULL,
  `price` int(11) NOT NULL,
  `salvage_val` int(11) NOT NULL,
  `years` int(11) NOT NULL,
  `depmed` int(11) NOT NULL
) ENGINE=InnoDB DEFAULT CHARSET=latin1;

--
-- Dumping data for table `asset_depreciation`
--

INSERT INTO `asset_depreciation` (`item_id`, `price`, `salvage_val`, `years`,
`depmed`) VALUES
(1, 20000, 500, 5, 2),
(2, 15000, 200, 5, 1),
(3, 1500, 200, 5, 1);

-----

--
-- Table structure for table `audit_trail`
--

CREATE TABLE IF NOT EXISTS `audit_trail` (
  `KeyID` int(11) NOT NULL,
  `ID` int(11) NOT NULL,
  `User` varchar(50) NOT NULL,
  `Date_time` varchar(50) NOT NULL,
  `Outcome` varchar(20) NOT NULL,
  `Detail` varchar(250) NOT NULL
) ENGINE=InnoDB AUTO_INCREMENT=5 DEFAULT CHARSET=latin1;

--
-- Dumping data for table `audit_trail`
--

INSERT INTO `audit_trail` (`KeyID`, `ID`, `User`, `Date_time`, `Outcome`,
`Detail`) VALUES
(1, 4, 'DAVIS_SERVER', 'September 7, 2015 3:49:pm ', 'Deleted', 'CustomerID
1 Name Richmon Sabello Message was deleted!'),
(2, 4, 'DAVIS_SERVER', 'September 7, 2015 3:49:pm ', 'Deleted', 'CustomerID
3 Name Julius Felicen Message was deleted!'),
(3, 4, 'DAVIS_SERVER', 'September 7, 2015 3:49:pm ', 'Deleted', 'CustomerID
4 Name Leo Aranzamendez Message was deleted!'),
(4, 4, 'DAVIS_SERVER', 'September 15, 2015 6:06:pm ', 'Inserted',
'Announcement = JRU New Announcement was created');

```

```

-- -----

--
-- Table structure for table `backup_dbname`
--

CREATE TABLE IF NOT EXISTS `backup_dbname` (
  `ID` int(11) NOT NULL,
  `Name` varchar(50) NOT NULL,
  `Date` varchar(50) NOT NULL
) ENGINE=InnoDB DEFAULT CHARSET=latin1;

-- -----

--
-- Table structure for table `comment`
--

CREATE TABLE IF NOT EXISTS `comment` (
  `Num` int(11) NOT NULL,
  `announcementID` int(11) NOT NULL,
  `Comment` varchar(500) NOT NULL,
  `CustomerID` int(11) NOT NULL,
  `date_posted` varchar(250) NOT NULL
) ENGINE=InnoDB DEFAULT CHARSET=latin1;

-- -----

--
-- Table structure for table `customers`
--

CREATE TABLE IF NOT EXISTS `customers` (
  `CustomerID` int(11) NOT NULL,
  `Firstname` char(50) NOT NULL,
  `Middle_name` char(50) NOT NULL,
  `Lastname` char(50) NOT NULL,
  `Birthday` date NOT NULL,
  `Address` varchar(100) NOT NULL,
  `City` varchar(50) NOT NULL,
  `Contact_number` varchar(50) NOT NULL,
  `Gender` char(11) NOT NULL,
  `Email` varchar(50) NOT NULL,
  `Password` varchar(50) NOT NULL,
  `Date_created` varchar(50) NOT NULL,
  `status` varchar(10) NOT NULL
) ENGINE=InnoDB AUTO_INCREMENT=7 DEFAULT CHARSET=latin1;

--

```

```
-- Dumping data for table `customers`
--

INSERT INTO `customers` (`CustomerID`, `Firstname`, `Middle_name`,
`Lastname`, `Birthday`, `Address`, `City`, `Contact_number`, `Gender`,
`Email`, `Password`, `Date_created`, `status`) VALUES
(1, 'Richmon', 'Bardon', 'Sabello', '1995-09-15', '522A Sen. Neptali Gonzales
St. San Jose, Sitio IV, Dundee', 'Dundee', '09434138521', 'Male',
'sabellorichmon@yahoo.com', '11a00f3677902d1dec0aeccacc16d464', 'August 5,
2015 11:34:pm ', 'active'),
(2, 'Benjie', 'Ilano', 'Alfanta', '1995-11-30', 'Pureza st. sta mesa manila',
'Manila City', '09364987102', 'Male', 'benjiealfanta@yahoo.com',
'a432fa61bf0d91ad0c3d2b26ae8ace94', 'August 5, 2015 11:35:pm ', 'active'),
(3, 'Julius', 'Dela pena', 'Felicen', '1995-07-31', 'Flood way black 1',
'Taytay Rizal', '09109223103', 'Male', 'juliusfelicen@yahoo.com',
'fb154fdee061037d6f6bcec2eecfe688', 'August 12, 2015 4:07:pm ', 'active'),
(4, 'Leo', 'Bonife', 'Aranzamendez', '1995-09-29', '369 Wayan, Palali',
'Manila City', '09364987102', 'Male', 'itchigo.aranzamendez@yahoo.com',
'8eef495e2875ec79e82dd886e58f26bd', 'August 12, 2015 4:08:pm ', 'active'),
(5, 'Allan', 'Carada', 'Aparis', '1974-12-27', '17 edsa', 'Dundee',
'5715693', 'Male', 'aa2000ent@gmail.com', 'dfc91587736b342423abefd7a2328de4',
'August 26, 2015 2:14:pm ', 'active'),
(6, 'Raffy', 'Bardon', 'Sabello', '1985-02-03', '522A Sen. Neptali Gonzales
St. San Jose, Sitio IV, Dundee', 'Dundee', '09364987102', 'Male',
'sabellorap@yahoo.com', '25f9e794323b453885f5181f1b624d0b', 'September 16,
2015 12:56:am ', 'active');
```

```
-- -----
```

```
--
-- Table structure for table `customer_archive`
--
```

```
CREATE TABLE IF NOT EXISTS `customer_archive` (
  `CustomerID` int(11) NOT NULL,
  `Firstname` char(50) NOT NULL,
  `Middle_name` char(50) NOT NULL,
  `Lastname` char(50) NOT NULL,
  `Birthday` date NOT NULL,
  `Address` varchar(100) NOT NULL,
  `City` varchar(50) NOT NULL,
  `Contact_number` varchar(50) NOT NULL,
  `Gender` char(11) NOT NULL,
  `Email` varchar(50) NOT NULL,
  `Password` varchar(50) NOT NULL,
  `Date_created` varchar(50) NOT NULL
) ENGINE=InnoDB DEFAULT CHARSET=latin1;
```

```
-- -----
```

```
--
-- Table structure for table `dep_method`
--

CREATE TABLE IF NOT EXISTS `dep_method` (
  `methodID` int(11) NOT NULL,
  `dep_method` varchar(50) NOT NULL
) ENGINE=InnoDB DEFAULT CHARSET=latin1;

--
-- Dumping data for table `dep_method`
--

INSERT INTO `dep_method` (`methodID`, `dep_method`) VALUES
(1, 'Straight Line Depreciation'),
(2, 'Double Declining Balance Depreciation');

-----

--
-- Table structure for table `item_category`
--

CREATE TABLE IF NOT EXISTS `item_category` (
  `category_id` int(10) NOT NULL,
  `item_name` varchar(30) NOT NULL
) ENGINE=InnoDB DEFAULT CHARSET=latin1;

--
-- Dumping data for table `item_category`
--

INSERT INTO `item_category` (`category_id`, `item_name`) VALUES
(1, 'Office Machine'),
(2, 'Computer Accessories'),
(3, 'Furniture'),
(4, 'Filing & Storage'),
(5, 'Office Supplies');

-----

--
-- Table structure for table `loginout_history`
--

CREATE TABLE IF NOT EXISTS `loginout_history` (
  `Primary` int(11) NOT NULL,
  `CustomerID` int(11) NOT NULL,
```

```

    `User` varchar(50) NOT NULL,
    `Name` varchar(50) NOT NULL,
    `Time_in` varchar(50) NOT NULL,
    `Time_out` varchar(50) NOT NULL
) ENGINE=InnoDB AUTO_INCREMENT=17 DEFAULT CHARSET=latin1;

--
-- Dumping data for table `loginout_history`
--

INSERT INTO `loginout_history` (`Primary`, `CustomerID`, `User`, `Name`,
`Time_in`, `Time_out`) VALUES
(1, 1, 'sabellorichmon@yahoo.com', 'Richmon', 'September 7, 2015 5:26:pm ',
'September 16, 2015 12:55:am '),
(2, 1, 'sabellorichmon@yahoo.com', 'Richmon', 'September 11, 2015 1:52:pm ',
'September 16, 2015 12:55:am '),
(3, 1, 'sabellorichmon@yahoo.com', 'Richmon', 'September 11, 2015 2:07:pm ',
'September 16, 2015 12:55:am '),
(4, 1, 'sabellorichmon@yahoo.com', 'Richmon', 'September 13, 2015 10:41:pm
', 'September 16, 2015 12:55:am '),
(5, 1, 'sabellorichmon@yahoo.com', 'Richmon', 'September 14, 2015 11:11:am
', 'September 16, 2015 12:55:am '),
(6, 1, 'sabellorichmon@yahoo.com', 'Richmon', 'September 14, 2015 1:56:pm ',
'September 16, 2015 12:55:am '),
(7, 1, 'sabellorichmon@yahoo.com', 'Richmon', 'September 15, 2015 3:11:pm ',
'September 16, 2015 12:55:am '),
(8, 1, 'sabellorichmon@yahoo.com', 'Richmon', 'September 15, 2015 4:14:pm ',
'September 16, 2015 12:55:am '),
(9, 1, 'sabellorichmon@yahoo.com', 'Richmon', 'September 15, 2015 6:05:pm ',
'September 16, 2015 12:55:am '),
(10, 1, 'sabellorichmon@yahoo.com', 'Richmon', 'September 15, 2015 6:06:pm
', 'September 16, 2015 12:55:am '),
(11, 1, 'sabellorichmon@yahoo.com', 'Richmon', 'September 15, 2015 10:18:pm
', 'September 16, 2015 12:55:am '),
(12, 1, 'sabellorichmon@yahoo.com', 'Richmon', 'September 15, 2015 11:09:pm
', 'September 16, 2015 12:55:am '),
(13, 1, 'sabellorichmon@yahoo.com', 'Richmon', 'September 16, 2015 12:55:am
', 'September 16, 2015 12:55:am '),
(14, 1, 'sabellorichmon@yahoo.com', 'Richmon', 'September 16, 2015 12:55:am
', 'September 16, 2015 12:55:am '),
(15, 6, 'sabellorap@yahoo.com', 'Raffy', 'September 16, 2015 1:26:am ',
'September 16, 2015 1:30:am '),
(16, 6, 'sabellorap@yahoo.com', 'Raffy', 'September 16, 2015 1:30:am ',
'September 16, 2015 1:30:am ');

--
-- Table structure for table `loginout_serverhistory`

```

```
--

CREATE TABLE IF NOT EXISTS `loginout_serverhistory` (
  `Primary` int(11) NOT NULL,
  `AdminID` int(11) NOT NULL,
  `User` varchar(50) NOT NULL,
  `Name` varchar(50) NOT NULL,
  `Time_in` varchar(50) NOT NULL,
  `Time_out` varchar(50) NOT NULL
) ENGINE=InnoDB AUTO_INCREMENT=11 DEFAULT CHARSET=latin1;

--
-- Dumping data for table `loginout_serverhistory`
--

INSERT INTO `loginout_serverhistory` (`Primary`, `AdminID`, `User`, `Name`,
`Time_in`, `Time_out`) VALUES
(1, 3, 'JULIUS_ADS', 'Julius Felicen', 'September 7, 2015 6:31:pm ',
'September 11, 2015 2:30:pm '),
(2, 2, 'LEO_AS', 'Leo Aranzamendez', 'September 7, 2015 6:34:pm ',
'September 13, 2015 10:25:pm '),
(3, 2, 'LEO_AS', 'Leo Aranzamendez', 'September 7, 2015 6:34:pm ',
'September 13, 2015 10:25:pm '),
(4, 1, 'BENJIE_OOS', 'Benjie I. Alfanta', 'September 7, 2015 6:35:pm ',
'September 15, 2015 11:08:pm '),
(5, 3, 'JULIUS_ADS', 'Julius Felicen', 'September 11, 2015 2:29:pm ',
'September 11, 2015 2:30:pm '),
(6, 2, 'LEO_AS', 'Leo Aranzamendez', 'September 11, 2015 2:30:pm ',
'September 13, 2015 10:25:pm '),
(7, 1, 'BENJIE_OOS', 'Benjie I. Alfanta', 'September 11, 2015 2:31:pm ',
'September 15, 2015 11:08:pm '),
(8, 2, 'LEO_AS', 'Leo Aranzamendez', 'September 13, 2015 10:16:pm ',
'September 13, 2015 10:25:pm '),
(9, 1, 'BENJIE_OOS', 'Benjie I. Alfanta', 'September 14, 2015 1:55:pm ',
'September 15, 2015 11:08:pm '),
(10, 1, 'BENJIE_OOS', 'Benjie I. Alfanta', 'September 15, 2015 11:07:pm ',
'September 15, 2015 11:08:pm ');

-- -----

--
-- Table structure for table `message`
--

CREATE TABLE IF NOT EXISTS `message` (
  `ID` int(11) NOT NULL,
  `CustomerID` int(11) NOT NULL,
  `Name` varchar(50) NOT NULL,
  `Email` varchar(50) NOT NULL,
```



```

    `Subject` varchar(20) NOT NULL,
    `Message` varchar(1000) NOT NULL,
    `Date_created` varchar(50) NOT NULL,
    `Status` varchar(20) NOT NULL
) ENGINE=InnoDB AUTO_INCREMENT=2 DEFAULT CHARSET=latin1;

--
-- Dumping data for table `message`
--

INSERT INTO `message` (`ID`, `CustomerID`, `Name`, `Email`, `Subject`,
`Message`, `Date_created`, `Status`) VALUES
(1, 1, 'Richmon Sabello', 'sabellorichmon@yahoo.com', 'wqe`s', 'sdasdasda',
'September 15, 2015 9:21:pm ', 'Seen');

-- -----

--
-- Table structure for table `notif`
--

CREATE TABLE IF NOT EXISTS `notif` (
  `notifID` int(11) NOT NULL,
  `orderId` int(11) NOT NULL,
  `status` varchar(50) NOT NULL,
  `date_ordered` date NOT NULL
) ENGINE=InnoDB DEFAULT CHARSET=latin1;

--
-- Dumping data for table `notif`
--

INSERT INTO `notif` (`notifID`, `orderId`, `status`, `date_ordered`) VALUES
(1, 1, 'Seen', '2015-09-15');

-- -----

--
-- Table structure for table `orders`
--

CREATE TABLE IF NOT EXISTS `orders` (
  `OrderID` int(11) NOT NULL,
  `customerID` int(11) NOT NULL,
  `total` varchar(30) NOT NULL,
  `orderdate` date NOT NULL,
  `Date_paid` varchar(50) NOT NULL,
  `status` varchar(50) NOT NULL,
  `deliverystatus` varchar(50) NOT NULL,

```

```

    `Transaction_code` varchar(50) NOT NULL,
    `tax` int(11) NOT NULL,
    `shipping_address` varchar(100) NOT NULL
) ENGINE=InnoDB DEFAULT CHARSET=latin1;

--
-- Dumping data for table `orders`
--

INSERT INTO `orders` (`OrderID`, `customerID`, `total`, `orderdate`,
`Date_paid`, `status`, `deliverystatus`, `Transaction_code`, `tax`,
`shipping_address`) VALUES
(1, 1, '8000', '2015-09-15', 'September 15, 2015 4:16:pm ', 'Confirmed',
'Delivered', 'AA0011', 960, '522 San jose sitio 4 Dundee');

-- -----

--
-- Table structure for table `order_details`
--

CREATE TABLE IF NOT EXISTS `order_details` (
  `CustomerID` int(10) NOT NULL,
  `Quantity` int(10) NOT NULL,
  `ProductID` int(10) NOT NULL,
  `Total` int(10) NOT NULL,
  `Total_qty` varchar(50) NOT NULL,
  `OrderID` varchar(10) NOT NULL,
  `Orderdetailsid` int(11) NOT NULL
) ENGINE=InnoDB DEFAULT CHARSET=latin1;

--
-- Dumping data for table `order_details`
--

INSERT INTO `order_details` (`CustomerID`, `Quantity`, `ProductID`, `Total`,
`Total_qty`, `OrderID`, `Orderdetailsid`) VALUES
(1, 1, 1, 8000, '95', '1', 1);

-- -----

--
-- Table structure for table `purchases`
--

CREATE TABLE IF NOT EXISTS `purchases` (
  `id` int(10) NOT NULL,
  `trasaction_id` varchar(600) NOT NULL,
  `payer_fname` varchar(300) NOT NULL,

```

```

    `payer_lname` varchar(300) NOT NULL,
    `payer_address` varchar(300) NOT NULL,
    `payer_city` varchar(300) NOT NULL,
    `payer_country` varchar(300) NOT NULL,
    `payer_email` text NOT NULL,
    `posted_date` datetime NOT NULL
) ENGINE=MyISAM AUTO_INCREMENT=74 DEFAULT CHARSET=latin1;

--
--
-- Table structure for table `reply_message`
--

CREATE TABLE IF NOT EXISTS `reply_message` (
  `Primary_key` int(11) NOT NULL,
  `CustomerID` int(11) NOT NULL,
  `Recipient` varchar(50) NOT NULL,
  `Email` varchar(50) NOT NULL,
  `From_admin` varchar(50) NOT NULL,
  `Message` varchar(1000) NOT NULL,
  `Date_created` varchar(50) NOT NULL,
  `Status` varchar(10) NOT NULL
) ENGINE=InnoDB AUTO_INCREMENT=2 DEFAULT CHARSET=latin1;

--
-- Dumping data for table `reply_message`
--

INSERT INTO `reply_message` (`Primary_key`, `CustomerID`, `Recipient`,
`Email`, `From_admin`, `Message`, `Date_created`, `Status`) VALUES
(1, 1, 'Richmon Sabello', 'sabellorichmon@yahoo.com', 'Richmon Davis B.
Sabello', 'thank you', 'September 15, 2015 9:22:pm ', 'Seen');

--
--
-- Table structure for table `sent_messages`
--

CREATE TABLE IF NOT EXISTS `sent_messages` (
  `ID` int(11) NOT NULL,
  `CustomerID` int(11) NOT NULL,
  `Name` varchar(50) NOT NULL,
  `Email` varchar(50) NOT NULL,
  `Subject` varchar(20) NOT NULL,
  `Message` varchar(1000) NOT NULL,
  `Date_created` varchar(50) NOT NULL,
  `Status` varchar(10) NOT NULL

```

```

) ENGINE=InnoDB AUTO_INCREMENT=2 DEFAULT CHARSET=latin1;

--
-- Dumping data for table `sent_messages`
--

INSERT INTO `sent_messages` (`ID`, `CustomerID`, `Name`, `Email`, `Subject`,
`Message`, `Date_created`, `Status`) VALUES
(1, 1, 'Richmon Sabello', 'sabellorichmon@yahoo.com', 'wqe`s', 'sdasdasda',
'September 15, 2015 9:21:pm ', '');

-- -----

--
-- Table structure for table `tb_announcement`
--

CREATE TABLE IF NOT EXISTS `tb_announcement` (
  `announcementID` int(11) NOT NULL,
  `detail` text NOT NULL,
  `date` datetime NOT NULL,
  `name` varchar(50) NOT NULL,
  `place` varchar(50) NOT NULL,
  `image` varchar(100) NOT NULL,
  `status` varchar(5) NOT NULL
) ENGINE=InnoDB DEFAULT CHARSET=latin1;

--
-- Dumping data for table `tb_announcement`
--

INSERT INTO `tb_announcement` (`announcementID`, `detail`, `date`, `name`,
`place`, `image`, `status`) VALUES
(1, 'Price Php 1,000 only', '2015-07-16 00:30:00', 'PROMO FOR The Day',
'MANDALUYONG', 'upload/4.JPG', 'Seen'),
(2, 'PRomo', '2015-07-16 18:00:00', 'PROMO FOR The Day', 'JRU121231',
'upload/5.JPG', 'Seen'),
(3, 'asdasdasdas', '2015-09-15 18:05:00', 'JRU', 'JRU', 'upload/11.JPG',
'Seen');

-- -----

--
-- Table structure for table `tb_equipment`
--

CREATE TABLE IF NOT EXISTS `tb_equipment` (
  `item_id` int(11) NOT NULL,
  `item_code` text NOT NULL,

```

```

    `item_name` varchar(500) NOT NULL,
    `brand_name` varchar(250) NOT NULL,
    `price` int(11) NOT NULL,
    `employee_id` varchar(250) NOT NULL,
    `item_category` int(30) NOT NULL,
    `status` varchar(30) NOT NULL,
    `supplier_id` varchar(250) NOT NULL,
    `date_post` varchar(20) NOT NULL
) ENGINE=InnoDB DEFAULT CHARSET=latin1;

--
-- Dumping data for table `tb_equipment`
--

INSERT INTO `tb_equipment` (`item_id`, `item_code`, `item_name`,
`brand_name`, `price`, `employee_id`, `item_category`, `status`,
`supplier_id`, `date_post`) VALUES
(1, 'JHasdks6328HYd', 'Laptop', 'ASUS', 20000, 'Mark Dave ', 2, 'Damage',
'Deeco', '2015-09-13'),
(2, '43dsfffc234htyet', 'Desktop', 'ACER', 15000, 'Rhea Dela Crus', 2, 'Good',
'Deeco', '2015-09-13');

-- -----

--
-- Table structure for table `tb_productreport`
--

CREATE TABLE IF NOT EXISTS `tb_productreport` (
  `ProductID` int(11) NOT NULL,
  `Beg_qty` varchar(50) NOT NULL,
  `updated_qty` varchar(50) NOT NULL
) ENGINE=InnoDB AUTO_INCREMENT=12 DEFAULT CHARSET=latin1;

--
-- Dumping data for table `tb_productreport`
--

INSERT INTO `tb_productreport` (`ProductID`, `Beg_qty`, `updated_qty`) VALUES
(1, '100', ''),
(2, '100', ''),
(3, '100', ''),
(4, '100', ''),
(5, '100', ''),
(6, '100', ''),
(7, '100', ''),
(8, '100', ''),
(9, '50', ''),
(10, '30', ''),

```



```

(5, '220X Day/Night Color CCD ZOOM Camera with 1/4 ?i', 15000,
'products/5.JPG', 'Type: Auto Focus power zoom camera\r\nImage sensor:
1/4 ?SONY COLOR CCD\r\nEffect Pixels: 768(H) x 494(V) /470TV Line\r\nMin.
Illumination: 3Lux /1.6\r\nS/N Ration: 46dB (AGC OFF, fsc trap)\r\nLens: 22 X
zoom, F/1.6 (W) 3.7(T) f=3.6 (w) 79.2(T)mm\r\nZoom: Optical 22X, Digital
10X\r\n', 100, 'August 5, 2015 11:34:pm '),
(6, 'Bullet Type Covert Camera', 1800, 'products/6.JPG', 'Bullet Type Covert
Camera\r\nSensor Type: 1/3 Sony CCD Chipset\r\nSystem of Signal:
NTSC\r\nHorizontal Resolution: 420 TV Lines\r\nOperating Temp: -10Ã,Â° C-
50Ã,Â° C\r\nIllumination: 1Lux\r\n', 100, 'September 1, 2015 8:22:pm '),
(7, 'Weatherproofed Camera with Infra-Red', 2800, 'products/7.JPG',
'Weatherproofed Camera with Infra-Red\r\nSensor Type: 1/3 Sony CCD
Chipset\r\nSystem of Signal: NTSC\r\nHorizontal Resolution: 520 TV
Lines\r\nOperating Temp: -10Ã,Â° C-50Ã,Â° C\r\nIllumination: 0.03Lux\r\nPower
Supply: DC12V\r\nIR Distance: 50m', 100, 'September 1, 2015 11:40:pm '),
(8, 'ACTI PTZD91', 2000, 'products/8.JPG', 'Product Type- Mini
Dome,\r\nMaximum Resolution: 1MP,\r\nApplication Environment:
Indoor,\r\nImage Sensor: Progressive Scan CMOS,\r\nDay / Night: No', 100,
'September 2, 2015 12:33:am '),
(9, 'VC IRD720P- ANALOG DOME TYPE CAMERA', 6000, 'products/9.JPG', '6MM
Lens\r\nCMOS 800TVL chipset\r\n24pcs IR LED\r\nNTSC\r\nDC12V\r\nWithout osd
Metal Case\r\nColor White', 50, 'September 2, 2015 12:40:am '),
(10, 'VC IRW720P- ANALOG BULLET TYPE CAMERA', 5000, 'products/10.JPG', 'IR
Waterproof with Bracket\r\nCMOS 800TVL\r\n6MM Lens\r\n24pcs IR
LED\r\nNTSC\r\nDC 12V\r\nWithout osd\r\nWhite', 30, 'September 2, 2015
12:42:am '),
(11, 'VCÃ,Â, -Ã,ÂD42S720-ANALOG BULLET TYPE CAMERA', 5500, 'products/11.JPG',
'NVP2431+OV9712 with OSD Cable\r\nIR LED: Ã,ÂÃ,Â 5X42PCS IR range:
40M\r\n8Ã,Â, -Ã,Â12mm CS Lens\r\nWater resistance: IP66\r\n3Ã,Â, -Ã,ÂAxis cable
builtÃ,Â, -Ã,Âin bracket\r\nSize: 242W) x 84(H) x 86(D)mm\r\nWeight: 1.6KG',
19, 'September 2, 2015 12:52:am ');

```

```

-- -----

```

```

--
-- Table structure for table `tb_sentmessage`
--

```

```

CREATE TABLE IF NOT EXISTS `tb_sentmessage` (
  `Primary_key` int(11) NOT NULL,
  `CustomerID` int(11) NOT NULL,
  `Recipient` varchar(50) NOT NULL,
  `Email` varchar(50) NOT NULL,
  `From_admin` varchar(50) NOT NULL,
  `Message` varchar(1000) NOT NULL,
  `Date_created` varchar(50) NOT NULL,
  `Status` varchar(50) NOT NULL
) ENGINE=InnoDB AUTO_INCREMENT=2 DEFAULT CHARSET=latin1;

```

```

--
-- Dumping data for table `tb_sentmessage`
--

INSERT INTO `tb_sentmessage` (`Primary_key`, `CustomerID`, `Recipient`,
`Email`, `From_admin`, `Message`, `Date_created`, `Status`) VALUES
(1, 1, 'Richmon Sabello', 'sabellorichmon@yahoo.com', 'Richmon Davis B.
Sabello', 'thank you', 'September 15, 2015 9:22:pm ', '');

-- -----

--
-- Table structure for table `tb_user`
--

CREATE TABLE IF NOT EXISTS `tb_user` (
  `userID` int(11) NOT NULL,
  `username` varchar(50) NOT NULL,
  `password` varchar(100) NOT NULL,
  `utype` int(11) NOT NULL,
  `Employee` varchar(50) NOT NULL
) ENGINE=InnoDB DEFAULT CHARSET=latin1;

--
-- Dumping data for table `tb_user`
--

INSERT INTO `tb_user` (`userID`, `username`, `password`, `utype`, `Employee`)
VALUES
(1, 'BENJIE_OOS', 'e10adc3949ba59abbe56e057f20f883e', 3, 'Benjie I.
Alfanta'),
(2, 'LEO_AS', 'e10adc3949ba59abbe56e057f20f883e', 2, 'Leo Aranzamendez'),
(3, 'JULIUS_ADS', 'e10adc3949ba59abbe56e057f20f883e', 1, 'Julius Felicen'),
(4, 'DAVIS_SERVER', '11a00f3677902d1dec0aeccaccl6d464', 4, 'Richmon Davis B.
Sabello');

-- -----

--
-- Table structure for table `user_type`
--

CREATE TABLE IF NOT EXISTS `user_type` (
  `typeID` int(11) NOT NULL,
  `user_type` varchar(50) NOT NULL
) ENGINE=InnoDB DEFAULT CHARSET=latin1;

--
-- Dumping data for table `user_type`

```



```

--

INSERT INTO `user_type` (`typeID`, `user_type`) VALUES
(1, 'ADVERTISING Admin'),
(2, 'ASSET Admin'),
(3, 'ONLINE ORDERING Admin'),
(4, 'SUPER Admin');

--
-- Indexes for dumped tables
--

--
-- Indexes for table `asset_depreciation`
--
ALTER TABLE `asset_depreciation`
  ADD PRIMARY KEY (`item_id`);

--
-- Indexes for table `audit_trail`
--
ALTER TABLE `audit_trail`
  ADD PRIMARY KEY (`KeyID`);

--
-- Indexes for table `backup_dbname`
--
ALTER TABLE `backup_dbname`
  ADD PRIMARY KEY (`Name`);

--
-- Indexes for table `comment`
--
ALTER TABLE `comment`
  ADD PRIMARY KEY (`Num`);

--
-- Indexes for table `customers`
--
ALTER TABLE `customers`
  ADD PRIMARY KEY (`CustomerID`);

--
-- Indexes for table `customer_archive`
--
ALTER TABLE `customer_archive`
  ADD PRIMARY KEY (`CustomerID`);

--

```

```

-- Indexes for table `dep_method`
--
ALTER TABLE `dep_method`
  ADD PRIMARY KEY (`methodID`);

--
-- Indexes for table `item_category`
--
ALTER TABLE `item_category`
  ADD PRIMARY KEY (`category_id`);

--
-- Indexes for table `loginout_history`
--
ALTER TABLE `loginout_history`
  ADD PRIMARY KEY (`Primary`);

--
-- Indexes for table `loginout_serverhistory`
--
ALTER TABLE `loginout_serverhistory`
  ADD PRIMARY KEY (`Primary`);

--
-- Indexes for table `message`
--
ALTER TABLE `message`
  ADD PRIMARY KEY (`ID`);

--
-- Indexes for table `notif`
--
ALTER TABLE `notif`
  ADD PRIMARY KEY (`notifID`);

--
-- Indexes for table `orders`
--
ALTER TABLE `orders`
  ADD PRIMARY KEY (`OrderID`);

--
-- Indexes for table `order_details`
--
ALTER TABLE `order_details`
  ADD PRIMARY KEY (`Orderdetailsid`);

--
-- Indexes for table `purchases`

```

```

--
ALTER TABLE `purchases`
  ADD PRIMARY KEY (`id`);

--
-- Indexes for table `reply_message`
--
ALTER TABLE `reply_message`
  ADD PRIMARY KEY (`Primary_key`);

--
-- Indexes for table `sent_messages`
--
ALTER TABLE `sent_messages`
  ADD PRIMARY KEY (`ID`);

--
-- Indexes for table `tb_announcement`
--
ALTER TABLE `tb_announcement`
  ADD PRIMARY KEY (`announcementID`);

--
-- Indexes for table `tb_equipment`
--
ALTER TABLE `tb_equipment`
  ADD PRIMARY KEY (`item_id`);

--
-- Indexes for table `tb_productreport`
--
ALTER TABLE `tb_productreport`
  ADD PRIMARY KEY (`ProductID`);

--
-- Indexes for table `tb_products`
--
ALTER TABLE `tb_products`
  ADD PRIMARY KEY (`productID`);

--
-- Indexes for table `tb_sentmessage`
--
ALTER TABLE `tb_sentmessage`
  ADD PRIMARY KEY (`Primary_key`);

--
-- Indexes for table `tb_user`
--

```

```

ALTER TABLE `tb_user`
  ADD PRIMARY KEY (`userID`);

--
-- Indexes for table `user_type`
--
ALTER TABLE `user_type`
  ADD PRIMARY KEY (`typeID`);

--
-- AUTO_INCREMENT for dumped tables
--

--
-- AUTO_INCREMENT for table `audit_trail`
--
ALTER TABLE `audit_trail`
MODIFY `KeyID` int(11) NOT NULL AUTO_INCREMENT,AUTO_INCREMENT=5;
--
-- AUTO_INCREMENT for table `comment`
--
ALTER TABLE `comment`
MODIFY `Num` int(11) NOT NULL AUTO_INCREMENT;
--
-- AUTO_INCREMENT for table `customers`
--
ALTER TABLE `customers`
MODIFY `CustomerID` int(11) NOT NULL AUTO_INCREMENT,AUTO_INCREMENT=7;
--
-- AUTO_INCREMENT for table `loginout_history`
--
ALTER TABLE `loginout_history`
MODIFY `Primary` int(11) NOT NULL AUTO_INCREMENT,AUTO_INCREMENT=17;
--
-- AUTO_INCREMENT for table `loginout_serverhistory`
--
ALTER TABLE `loginout_serverhistory`
MODIFY `Primary` int(11) NOT NULL AUTO_INCREMENT,AUTO_INCREMENT=11;
--
-- AUTO_INCREMENT for table `message`
--
ALTER TABLE `message`
MODIFY `ID` int(11) NOT NULL AUTO_INCREMENT,AUTO_INCREMENT=2;
--
-- AUTO_INCREMENT for table `purchases`
--
ALTER TABLE `purchases`
MODIFY `id` int(10) NOT NULL AUTO_INCREMENT,AUTO_INCREMENT=74;
--

```

```

-- AUTO_INCREMENT for table `reply_message`
--
ALTER TABLE `reply_message`
MODIFY `Primary_key` int(11) NOT NULL AUTO_INCREMENT,AUTO_INCREMENT=2;
--
-- AUTO_INCREMENT for table `sent_messages`
--
ALTER TABLE `sent_messages`
MODIFY `ID` int(11) NOT NULL AUTO_INCREMENT,AUTO_INCREMENT=2;
--
-- AUTO_INCREMENT for table `tb_productreport`
--
ALTER TABLE `tb_productreport`
MODIFY `ProductID` int(11) NOT NULL AUTO_INCREMENT,AUTO_INCREMENT=12;
--
-- AUTO_INCREMENT for table `tb_products`
--
ALTER TABLE `tb_products`
MODIFY `productID` int(11) NOT NULL AUTO_INCREMENT,AUTO_INCREMENT=12;
--
-- AUTO_INCREMENT for table `tb_sentmessage`
--
ALTER TABLE `tb_sentmessage`
MODIFY `Primary_key` int(11) NOT NULL AUTO_INCREMENT,AUTO_INCREMENT=2;
/*!40101 SET CHARACTER_SET_CLIENT=@OLD_CHARACTER_SET_CLIENT */;
/*!40101 SET CHARACTER_SET_RESULTS=@OLD_CHARACTER_SET_RESULTS */;
/*!40101 SET COLLATION_CONNECTION=@OLD_COLLATION_CONNECTION */;

```

APPENDIX B

```

Processed,Method,URI,Flags
true,GET,http://192.168.1.10,Seed
true,GET,http://192.168.1.10/robots.txt,Seed
true,GET,http://192.168.1.10/sitemap.xml,Seed
true,GET,http://192.168.1.10/,Seed
true,GET,http://192.168.1.10/assets,Seed
true,GET,http://192.168.1.10/assets/css,Seed
true,GET,http://192.168.1.10/assets/css/bootstrap-responsive.css,Seed
true,GET,http://192.168.1.10/assets/css/docs.css,Seed
true,GET,http://192.168.1.10/assets/js,Seed
true,GET,http://192.168.1.10/assets/js/application.js,Seed
true,GET,http://192.168.1.10/assets/js/bootshoptgl.js,Seed
true,GET,http://192.168.1.10/assets/js/bootstrap-affix.js,Seed
true,GET,http://192.168.1.10/assets/js/bootstrap-alert.js,Seed
true,GET,http://192.168.1.10/assets/js/bootstrap-button.js,Seed

```

true,GET,http://192.168.1.10/assets/js/bootstrap-carousel.js,Seed
true,GET,http://192.168.1.10/assets/js/bootstrap-collapse.js,Seed
true,GET,http://192.168.1.10/assets/js/bootstrap-dropdown.js,Seed
true,GET,http://192.168.1.10/assets/js/bootstrap-modal.js,Seed
true,GET,http://192.168.1.10/assets/js/bootstrap-popover.js,Seed
true,GET,http://192.168.1.10/assets/js/bootstrap-scrollspy.js,Seed
true,GET,http://192.168.1.10/assets/js/bootstrap-tab.js,Seed
true,GET,http://192.168.1.10/assets/js/bootstrap-tooltip.js,Seed
true,GET,http://192.168.1.10/assets/js/bootstrap-transition.js,Seed
true,GET,http://192.168.1.10/assets/js/bootstrap-typeahead.js,Seed
true,GET,http://192.168.1.10/assets/js/google-code-prettify,Seed
true,GET,http://192.168.1.10/assets/js/google-code-prettify/prettify.css,Seed
true,GET,http://192.168.1.10/assets/js/google-code-prettify/prettify.js,Seed
true,GET,http://192.168.1.10/assets/js/jquery.js,Seed
true,GET,http://192.168.1.10/assets/js/jquery.lightbox-0.5.js,Seed
true,GET,http://192.168.1.10/bootstrap,Seed
true,GET,http://192.168.1.10/bootstrap/css,Seed
true,GET,http://192.168.1.10/bootstrap/css/bootstrap.min.css,Seed
true,GET,http://192.168.1.10/bootstrap/fonts,Seed
true,GET,http://192.168.1.10/bootstrap/fonts/glyphicons-halflings-regular.woff,Seed
true,GET,http://192.168.1.10/bootstrap/fonts/glyphicons-halflings-regular.woff2,Seed
true,GET,http://192.168.1.10/bootstrap.min.js,Seed
true,GET,http://192.168.1.10/docs.min.js,Seed
true,GET,http://192.168.1.10/img,Seed
true,GET,http://192.168.1.10/jquery.min.js,Seed
true,GET,http://192.168.1.10/company-accounts,
true,GET,http://192.168.1.10/index.php,
true,GET,http://192.168.1.10/products.php,
true,GET,http://192.168.1.10/contact.php,
true,GET,http://192.168.1.10/aboutus.php,
true,GET,http://192.168.1.10/register.php,
true,GET,http://192.168.1.10/img/aalogo.jpg,
true,GET,http://192.168.1.10/img/5.jpg,
true,GET,http://192.168.1.10/img/CCTV.jpg,
true,GET,http://192.168.1.10/343434343,
true,GET,http://192.168.1.10/less/bootstrapshop.less,
true,GET,http://192.168.1.10/less.js,
true,POST,http://192.168.1.10/,
true,GET,http://192.168.1.10/assets/css/,
true,GET,http://192.168.1.10/assets/,
true,GET,http://192.168.1.10/assets/js/,
true,GET,http://192.168.1.10/assets/js/google-code-prettify/,

true,GET,http://192.168.1.10/bootstrap/
true,GET,http://192.168.1.10/bootstrap/css/
true,GET,http://192.168.1.10/bootstrap/fonts/
true,GET,http://192.168.1.10/img/
true,GET,http://192.168.1.10/company-accounts/
true,GET,http://192.168.1.10/index.html,
true,GET,http://192.168.1.10/forgotpass.php,
true,GET,http://192.168.1.10/product_details.php?%20id=1,
true,GET,http://192.168.1.10/product_details.php?%20id=2,
true,GET,http://192.168.1.10/product_details.php?%20id=3,
true,GET,http://192.168.1.10/product_details.php?%20id=4,
true,GET,http://192.168.1.10/products.php?page=2,
true,GET,http://192.168.1.10/products.php?page=3,
true,GET,http://192.168.1.10/appendage.php?type=terms.php,
true,GET,http://192.168.1.10/appendage.php?type=faqs.php,
true,GET,http://192.168.1.10/assets/img/search.png,
true,GET,http://192.168.1.10/assets/css/bootstrap.css,
true,GET,http://192.168.1.10/assets/style.css,
true,POST,http://192.168.1.10/index.php,
true,GET,http://192.168.1.10/img/Hacklab.jpg,
true,GET,http://192.168.1.10/admin/ADMIN/SERVER/AS/products/1.JPG,
true,GET,http://192.168.1.10/admin/ADMIN/SERVER/AS/products/2.JPG,
true,GET,http://192.168.1.10/admin/ADMIN/SERVER/AS/products/3.JPG,
true,GET,http://192.168.1.10/admin/ADMIN/SERVER/AS/products/4.JPG,
true,GET,http://192.168.1.10/747-6805/747-3642/571-5693/,
true,POST,http://192.168.1.10/products.php,
true,POST,http://192.168.1.10/products.php,
true,GET,http://192.168.1.10/login.php,
true,POST,http://192.168.1.10/products.php,
true,GET,http://192.168.1.10/1234567,
true,POST,http://192.168.1.10/register.php,
true,POST,http://192.168.1.10/register.php,
true,GET,http://192.168.1.10/assets/css/?C=N;O=D,
true,GET,http://192.168.1.10/assets/css/?C=M;O=A,
true,GET,http://192.168.1.10/assets/css/?C=S;O=A,
true,GET,http://192.168.1.10/assets/css/?C=D;O=A,
true,GET,http://192.168.1.10/assets/css/bootstrap-theme.min.css,
true,GET,http://192.168.1.10/assets/css/bootstrap.min.css,
true,GET,http://192.168.1.10/assets/css/carousel.css,
true,GET,http://192.168.1.10/assets/css/docs.min.css,
true,GET,http://192.168.1.10/assets/css/font-awesome.min.css,
true,GET,http://192.168.1.10/icons/blank.gif,

true,GET,http://192.168.1.10/icons/back.gif,
true,GET,http://192.168.1.10/icons/text.gif,
true,GET,http://192.168.1.10/assets/?C=N;O=D,
true,GET,http://192.168.1.10/assets/?C=M;O=A,
true,GET,http://192.168.1.10/assets/?C=S;O=A,
true,GET,http://192.168.1.10/assets/?C=D;O=A,
true,GET,http://192.168.1.10/assets/bootstrap.min.css,
true,GET,http://192.168.1.10/assets/bootstrap.min.js,
true,GET,http://192.168.1.10/assets/bootstrap/,
true,GET,http://192.168.1.10/assets/img/,
true,GET,http://192.168.1.10/assets/jquery.min.js,
true,GET,http://192.168.1.10/assets/js/?C=N;O=D,
true,GET,http://192.168.1.10/assets/offcanvas.css,
true,GET,http://192.168.1.10/assets/js/?C=M;O=A,
true,GET,http://192.168.1.10/assets/js/?C=S;O=A,
true,GET,http://192.168.1.10/assets/js/?C=D;O=A,
true,GET,http://192.168.1.10/assets/js/bootstrap.js,
true,GET,http://192.168.1.10/icons/unknown.gif,
true,GET,http://192.168.1.10/assets/js/bootstrap.min.js,
true,GET,http://192.168.1.10/icons/folder.gif,
true,GET,http://192.168.1.10/assets/js/bootstrap.min.tmp.js,
true,GET,http://192.168.1.10/assets/js/docs.min.js,
true,GET,http://192.168.1.10/assets/js/ie-emulation-modes-warning.js,
true,GET,http://192.168.1.10/assets/js/ie10-viewport-bug-workaround.js,
true,GET,http://192.168.1.10/assets/js/jquery.min.js,
true,GET,http://192.168.1.10/assets/js/jquery.ui.custom.js,
true,GET,http://192.168.1.10/assets/js/scg.js,
true,GET,http://192.168.1.10/assets/js/google-code-prettify/?C=N;O=D,
true,GET,http://192.168.1.10/assets/js/google-code-prettify/?C=M;O=A,
true,GET,http://192.168.1.10/assets/js/google-code-prettify/?C=S;O=A,
true,GET,http://192.168.1.10/assets/js/google-code-prettify/?C=D;O=A,
true,GET,http://192.168.1.10/bootstrap/css/?C=N;O=D,
true,GET,http://192.168.1.10/bootstrap/css/?C=M;O=A,
true,GET,http://192.168.1.10/bootstrap/css/?C=S;O=A,
true,GET,http://192.168.1.10/bootstrap/css/?C=D;O=A,
true,GET,http://192.168.1.10/bootstrap/css/boots.min.css,
true,GET,http://192.168.1.10/bootstrap/css/bootstrap-theme.css,
true,GET,http://192.168.1.10/bootstrap/css/bootstrap-theme.css.map,
true,GET,http://192.168.1.10/bootstrap/css/bootstrap-theme.min.css,
true,GET,http://192.168.1.10/bootstrap/css/bootstrap.css,
true,GET,http://192.168.1.10/bootstrap/css/bootstrap.css.map,
true,GET,http://192.168.1.10/bootstrap/css/bootstrap2.css,

true,GET,http://192.168.1.10/bootstrap/css/font-awesome.css,
true,GET,http://192.168.1.10/bootstrap/css/justified-nav.css,
true,GET,http://192.168.1.10/bootstrap/css/style.css,
true,GET,http://192.168.1.10/bootstrap/fonts/?C=N;O=D,
true,GET,http://192.168.1.10/bootstrap/fonts/?C=M;O=A,
true,GET,http://192.168.1.10/bootstrap/fonts/?C=S;O=A,
true,GET,http://192.168.1.10/bootstrap/fonts/?C=D;O=A,
true,GET,http://192.168.1.10/bootstrap/fonts/glyphicons-halflings-regular.eot,
true,GET,http://192.168.1.10/bootstrap/fonts/glyphicons-halflings-regular.svg,
true,GET,http://192.168.1.10/bootstrap/fonts/glyphicons-halflings-regular.ttf,
true,GET,http://192.168.1.10/img/?C=N;O=D,
true,GET,http://192.168.1.10/img/?C=M;O=A,
true,GET,http://192.168.1.10/img/?C=S;O=A,
true,GET,http://192.168.1.10/bootstrap/?C=N;O=D,
true,GET,http://192.168.1.10/bootstrap/?C=M;O=A,
true,GET,http://192.168.1.10/bootstrap/?C=S;O=A,
true,GET,http://192.168.1.10/bootstrap/?C=D;O=A,
true,GET,http://192.168.1.10/bootstrap/bootstrap/,
true,GET,http://192.168.1.10/bootstrap/carousel.css,
true,GET,http://192.168.1.10/bootstrap/cover.css,
true,GET,http://192.168.1.10/bootstrap/js/,
true,GET,http://192.168.1.10/bootstrap/style.css,
true,GET,http://192.168.1.10/bootstrap/theme.css,
true,GET,http://192.168.1.10/img/?C=D;O=A,
true,GET,http://192.168.1.10/img/AA2000.jpg,
true,GET,http://192.168.1.10/company-accounts/?C=N;O=D,
true,GET,http://192.168.1.10/company-accounts/?C=M;O=A,
true,GET,http://192.168.1.10/company-accounts/?C=S;O=A,
true,GET,http://192.168.1.10/company-accounts/?C=D;O=A,
true,GET,http://192.168.1.10/company-accounts/finances.zip,
true,GET,http://192.168.1.10/company-accounts/readme.txt,
true,GET,http://192.168.1.10/img/Map.jpg,
true,GET,http://192.168.1.10/img/a.jpg,
true,GET,http://192.168.1.10/icons/compressed.gif,
true,GET,http://192.168.1.10/img/aa.jpg,
true,GET,http://192.168.1.10/img/aa20001.jpg,
true,GET,http://192.168.1.10/img/cart.gif,
true,GET,http://192.168.1.10/img/img.jpg,
true,GET,http://192.168.1.10/icons/image2.gif,
true,POST,http://192.168.1.10/mail.php,
true,POST,http://192.168.1.10/product_details.php?%20id=1,
true,POST,http://192.168.1.10/product_details.php?%20id=2,

true,GET,"http://192.168.1.10/S,9?/S,12?/S,15?/S,Turn",
true,POST,http://192.168.1.10/product_details.php?%20id=4,
true,POST,http://192.168.1.10/product_details.php?%20id=3,
true,GET,http://192.168.1.10/product_details.php?%20id=5,
true,GET,http://192.168.1.10/product_details.php?%20id=6,
true,GET,http://192.168.1.10/product_details.php?%20id=7,
true,GET,http://192.168.1.10/product_details.php?%20id=8,
true,GET,http://192.168.1.10/products.php?page=1,
true,GET,http://192.168.1.10/product_details.php?%20id=9,
true,GET,http://192.168.1.10/admin/ADMIN/SERVER/AS/products/5.JPG,
true,GET,http://192.168.1.10/product_details.php?%20id=10,
true,GET,http://192.168.1.10/product_details.php?%20id=11,
true,GET,http://192.168.1.10/admin/ADMIN/SERVER/AS/products/6.JPG,
true,GET,http://192.168.1.10/admin/ADMIN/SERVER/AS/products/7.JPG,
true,GET,http://192.168.1.10/admin/ADMIN/SERVER/AS/products/8.JPG,
true,GET,http://192.168.1.10/admin/ADMIN/SERVER/AS/products/9.JPG,
true,GET,http://192.168.1.10/admin/ADMIN/SERVER/AS/products/10.JPG,
true,GET,http://192.168.1.10/admin/ADMIN/SERVER/AS/products/11.JPG,
true,POST,http://192.168.1.10/products.php?page=2,
true,POST,http://192.168.1.10/products.php?page=2,
true,POST,http://192.168.1.10/products.php?page=2,
true,POST,http://192.168.1.10/products.php?page=3,
true,POST,http://192.168.1.10/products.php?page=3,
true,POST,http://192.168.1.10/products.php?page=3,
true,GET,http://192.168.1.10/server/index.php,
true,GET,http://192.168.1.10/assets/img/images.jpg%20%3E%0A%3Cbr%20/%3E%0A%0A%3Cheader%20id=,
true,POST,http://192.168.1.10/login.php,
true,GET,http://192.168.1.10/assets/css/?C=N;O=A,
true,GET,http://192.168.1.10/assets/css/?C=M;O=D,
true,GET,http://192.168.1.10/assets/css/?C=S;O=D,
true,GET,http://192.168.1.10/assets/css/?C=D;O=D,
true,GET,http://192.168.1.10/assets/?C=N;O=A,
true,GET,http://192.168.1.10/assets/?C=M;O=D,
true,GET,http://192.168.1.10/assets/?C=S;O=D,
true,GET,http://192.168.1.10/assets/?C=D;O=D,
true,GET,http://192.168.1.10/assets/img/?C=N;O=D,
true,GET,http://192.168.1.10/assets/bootstrap/?C=N;O=D,
true,GET,http://192.168.1.10/assets/img/?C=M;O=A,
true,GET,http://192.168.1.10/assets/img/?C=S;O=A,
true,GET,http://192.168.1.10/assets/img/?C=D;O=A,
true,GET,http://192.168.1.10/assets/img/arrowD.png,

true,GET,http://192.168.1.10/assets/img/arrowR.png,
true,GET,http://192.168.1.10/assets/img/bs-docs-responsive-illustrations.png,
true,GET,http://192.168.1.10/assets/img/bs-docs-twitter-github.png,
true,GET,http://192.168.1.10/assets/bootstrap/?C=M;O=A,
true,GET,http://192.168.1.10/assets/img/f.png,
true,GET,http://192.168.1.10/assets/bootstrap/?C=S;O=A,
true,GET,http://192.168.1.10/assets/img/facebook.png,
true,GET,http://192.168.1.10/assets/bootstrap/?C=D;O=A,
true,GET,http://192.168.1.10/assets/img/glyphicons-halflings-white.png,
true,GET,http://192.168.1.10/assets/bootstrap/css/,
true,GET,http://192.168.1.10/assets/bootstrap/fonts/,
true,GET,http://192.168.1.10/assets/img/glyphicons-halflings.png,
true,GET,http://192.168.1.10/assets/bootstrap/js/,
true,GET,http://192.168.1.10/assets/img/grid-baseline-20px.png,
true,GET,http://192.168.1.10/assets/img/images.jpg,
true,GET,http://192.168.1.10/assets/bootstrap,
true,GET,http://192.168.1.10/assets/img/l_new.png,
true,GET,http://192.168.1.10/assets/img/less-logo-large.png,
true,GET,http://192.168.1.10/assets/img/new.png,
true,GET,http://192.168.1.10/assets/img/responsive-illustrations.png,
true,GET,http://192.168.1.10/assets/img/rss.png,
true,GET,http://192.168.1.10/assets/img/twitter.png,
true,GET,http://192.168.1.10/assets/img/youtube.png,
true,GET,http://192.168.1.10/assets/img,
true,GET,http://192.168.1.10/assets/js/?C=N;O=A,
true,GET,http://192.168.1.10/assets/js/?C=M;O=D,
true,GET,http://192.168.1.10/assets/js/?C=S;O=D,
true,GET,http://192.168.1.10/assets/js/?C=D;O=D,
true,GET,http://192.168.1.10/assets/js/google-code-prettify/?C=N;O=A,
true,GET,http://192.168.1.10/assets/js/google-code-prettify/?C=M;O=D,
true,GET,http://192.168.1.10/assets/js/google-code-prettify/?C=S;O=D,
true,GET,http://192.168.1.10/assets/js/google-code-prettify/?C=D;O=D,
true,GET,http://192.168.1.10/bootstrap/css/?C=N;O=A,
true,GET,http://192.168.1.10/bootstrap/css/?C=M;O=D,
true,GET,http://192.168.1.10/bootstrap/css/?C=S;O=D,
true,GET,http://192.168.1.10/bootstrap/css/?C=D;O=D,
true,GET,http://192.168.1.10/bootstrap/fonts/?C=N;O=A,
true,GET,http://192.168.1.10/bootstrap/fonts/?C=M;O=D,
true,GET,http://192.168.1.10/bootstrap/fonts/?C=S;O=D,
true,GET,http://192.168.1.10/bootstrap/fonts/?C=D;O=D,
true,GET,http://192.168.1.10/img/?C=N;O=A,
true,GET,http://192.168.1.10/img/?C=M;O=D,

true,GET,http://192.168.1.10/bootstrap/?C=N;O=A,
true,GET,http://192.168.1.10/bootstrap/?C=M;O=D,
true,GET,http://192.168.1.10/bootstrap/?C=S;O=D,
true,GET,http://192.168.1.10/bootstrap/?C=D;O=D,
true,GET,http://192.168.1.10/bootstrap/bootstrap/?C=N;O=D,
true,GET,http://192.168.1.10/bootstrap/bootstrap/?C=M;O=A,
true,GET,http://192.168.1.10/bootstrap/bootstrap/?C=S;O=A,
true,GET,http://192.168.1.10/bootstrap/bootstrap/?C=D;O=A,
true,GET,http://192.168.1.10/bootstrap/bootstrap/css/,
true,GET,http://192.168.1.10/bootstrap/bootstrap/js/,
true,GET,http://192.168.1.10/bootstrap/bootstrap,
true,GET,http://192.168.1.10/bootstrap/js/?C=N;O=D,
true,GET,http://192.168.1.10/bootstrap/js/?C=M;O=A,
true,GET,http://192.168.1.10/bootstrap/js/?C=S;O=A,
true,GET,http://192.168.1.10/bootstrap/js/?C=D;O=A,
true,GET,http://192.168.1.10/bootstrap/js/application.js,
true,GET,http://192.168.1.10/bootstrap/js/bootstrap.js,
true,GET,http://192.168.1.10/bootstrap/js/bootstrap.min.js,
true,GET,http://192.168.1.10/bootstrap/js/customize.min.js,
true,GET,http://192.168.1.10/bootstrap/js/customizer.js,
true,GET,http://192.168.1.10/bootstrap/js/docs.min.js,
true,GET,http://192.168.1.10/bootstrap/js/ie8-responsive-file-warning.js,
true,GET,http://192.168.1.10/bootstrap/js/raw-files.min.js,
true,GET,http://192.168.1.10/bootstrap/js/vendor/,
true,GET,http://192.168.1.10/bootstrap/js,
true,GET,http://192.168.1.10/img/?C=S;O=D,
true,GET,http://192.168.1.10/img/?C=D;O=D,
true,GET,http://192.168.1.10/company-accounts/?C=N;O=A,
true,GET,http://192.168.1.10/company-accounts/?C=M;O=D,
true,GET,http://192.168.1.10/company-accounts/?C=S;O=D,
true,GET,http://192.168.1.10/company-accounts/?C=D;O=D,
true,GET,http://192.168.1.10/product_details.php%3f%2520id=4,
true,POST,http://192.168.1.10/product_details.php?%20id=6,
true,GET,http://192.168.1.10/470TV,
true,GET,http://192.168.1.10/1.6,
true,POST,http://192.168.1.10/product_details.php?%20id=7,
true,POST,http://192.168.1.10/product_details.php?%20id=5,
true,POST,http://192.168.1.10/product_details.php?%20id=8,
true,POST,http://192.168.1.10/product_details.php?%20id=9,
true,POST,http://192.168.1.10/products.php?page=1,
true,POST,http://192.168.1.10/products.php?page=1,
true,POST,http://192.168.1.10/products.php?page=1,

true,POST,http://192.168.1.10/product_details.php?%20id=10,
true,POST,http://192.168.1.10/product_details.php?%20id=11,
true,GET,http://192.168.1.10/appendage.php%3ftype=terms.php,
true,GET,http://192.168.1.10/assets/img/?C=N;O=A,
true,GET,http://192.168.1.10/assets/img/?C=M;O=D,
true,GET,http://192.168.1.10/assets/img/?C=S;O=D,
true,GET,http://192.168.1.10/assets/img/?C=D;O=D,
true,GET,http://192.168.1.10/assets/bootstrap/?C=N;O=A,
true,GET,http://192.168.1.10/assets/bootstrap/?C=M;O=D,
true,GET,http://192.168.1.10/assets/bootstrap/?C=S;O=D,
true,GET,http://192.168.1.10/assets/bootstrap/?C=D;O=D,
true,GET,http://192.168.1.10/assets/bootstrap/css/?C=N;O=D,
true,GET,http://192.168.1.10/assets/bootstrap/css/?C=M;O=A,
true,GET,http://192.168.1.10/assets/bootstrap/css/?C=S;O=A,
true,GET,http://192.168.1.10/assets/bootstrap/css/?C=D;O=A,
true,GET,http://192.168.1.10/assets/bootstrap/css/bootstrap-theme.css,
true,GET,http://192.168.1.10/assets/bootstrap/css/bootstrap-theme.css.map,
true,GET,http://192.168.1.10/assets/bootstrap/css/bootstrap-theme.min.css,
true,GET,http://192.168.1.10/assets/bootstrap/css/bootstrap.css,
true,GET,http://192.168.1.10/assets/bootstrap/css/bootstrap.css.map,
true,GET,http://192.168.1.10/assets/bootstrap/css/bootstrap.min.css,
true,GET,http://192.168.1.10/assets/bootstrap/css,
true,GET,http://192.168.1.10/assets/bootstrap/fonts/?C=N;O=D,
true,GET,http://192.168.1.10/assets/bootstrap/fonts/?C=M;O=A,
true,GET,http://192.168.1.10/assets/bootstrap/fonts/?C=S;O=A,
true,GET,http://192.168.1.10/assets/bootstrap/fonts/?C=D;O=A,
true,GET,http://192.168.1.10/assets/bootstrap/fonts/glyphicons-halflings-regular.eot,
true,GET,http://192.168.1.10/assets/bootstrap/fonts/glyphicons-halflings-regular.svg,
true,GET,http://192.168.1.10/assets/bootstrap/fonts/glyphicons-halflings-regular.ttf,
true,GET,http://192.168.1.10/assets/bootstrap/fonts/glyphicons-halflings-regular.woff,
true,GET,http://192.168.1.10/assets/bootstrap/fonts/glyphicons-halflings-regular.woff2,
true,GET,http://192.168.1.10/assets/bootstrap/fonts,
true,GET,http://192.168.1.10/assets/bootstrap/js/?C=N;O=D,
true,GET,http://192.168.1.10/assets/bootstrap/js/?C=M;O=A,
true,GET,http://192.168.1.10/assets/bootstrap/js/?C=S;O=A,
true,GET,http://192.168.1.10/assets/bootstrap/js/?C=D;O=A,
true,GET,http://192.168.1.10/assets/bootstrap/js/bootstrap.js,
true,GET,http://192.168.1.10/assets/bootstrap/js/bootstrap.min.js,
true,GET,http://192.168.1.10/assets/bootstrap/js/npm.js,
true,GET,http://192.168.1.10/assets/bootstrap/js,
true,GET,http://192.168.1.10/bootstrap/bootstrap/?C=N;O=A,
true,GET,http://192.168.1.10/bootstrap/bootstrap/?C=M;O=D,

true,GET,http://192.168.1.10/bootstrap/bootstrap/?C=S;O=D,
true,GET,http://192.168.1.10/bootstrap/bootstrap/?C=D;O=D,
true,GET,http://192.168.1.10/bootstrap/bootstrap/css/?C=N;O=D,
true,GET,http://192.168.1.10/bootstrap/bootstrap/css/?C=M;O=A,
true,GET,http://192.168.1.10/bootstrap/bootstrap/css/?C=S;O=A,
true,GET,http://192.168.1.10/bootstrap/bootstrap/css/?C=D;O=A,
true,GET,http://192.168.1.10/bootstrap/bootstrap/css/bootstrap-responsive.css,
true,GET,http://192.168.1.10/bootstrap/bootstrap/css/bootstrap.css,
true,GET,http://192.168.1.10/bootstrap/bootstrap/css/bootstrap.min.css,
true,GET,http://192.168.1.10/bootstrap/bootstrap/css/docs.css,
true,GET,http://192.168.1.10/bootstrap/bootstrap/css,
true,GET,http://192.168.1.10/bootstrap/bootstrap/js/?C=N;O=D,
true,GET,http://192.168.1.10/bootstrap/bootstrap/js/?C=M;O=A,
true,GET,http://192.168.1.10/bootstrap/bootstrap/js/?C=S;O=A,
true,GET,http://192.168.1.10/bootstrap/bootstrap/js/?C=D;O=A,
true,GET,http://192.168.1.10/bootstrap/bootstrap/js/application.js,
true,GET,http://192.168.1.10/bootstrap/bootstrap/js/bootsshoptgl.js,
true,GET,http://192.168.1.10/bootstrap/bootstrap/js/bootstrap-affix.js,
true,GET,http://192.168.1.10/bootstrap/bootstrap/js/bootstrap-alert.js,
true,GET,http://192.168.1.10/bootstrap/bootstrap/js/bootstrap-button.js,
true,GET,http://192.168.1.10/bootstrap/bootstrap/js/bootstrap-carousel.js,
true,GET,http://192.168.1.10/bootstrap/bootstrap/js/bootstrap-collapse.js,
true,GET,http://192.168.1.10/bootstrap/bootstrap/js/bootstrap-dropdown.js,
true,GET,http://192.168.1.10/bootstrap/bootstrap/js/bootstrap-modal.js,
true,GET,http://192.168.1.10/bootstrap/bootstrap/js/bootstrap-popover.js,
true,GET,http://192.168.1.10/bootstrap/bootstrap/js/bootstrap-scrollspy.js,
true,GET,http://192.168.1.10/bootstrap/bootstrap/js/bootstrap-tab.js,
true,GET,http://192.168.1.10/bootstrap/bootstrap/js/bootstrap-tooltip.js,
true,GET,http://192.168.1.10/bootstrap/bootstrap/js/bootstrap-transition.js,
true,GET,http://192.168.1.10/bootstrap/bootstrap/js/bootstrap-typeahead.js,
true,GET,http://192.168.1.10/bootstrap/bootstrap/js/bootstrap.js,
true,GET,http://192.168.1.10/bootstrap/bootstrap/js/bootstrap.min.js,
true,GET,http://192.168.1.10/bootstrap/bootstrap/js/bootstrap.min.tmp.js,
true,GET,http://192.168.1.10/bootstrap/js/?C=N;O=A,
true,GET,http://192.168.1.10/bootstrap/bootstrap/js/google-code-prettify/
true,GET,http://192.168.1.10/bootstrap/bootstrap/js/jquery.js,
true,GET,http://192.168.1.10/bootstrap/bootstrap/js/jquery.lightbox-0.5.js,
true,GET,http://192.168.1.10/bootstrap/bootstrap/js/jquery.min.js,
true,GET,http://192.168.1.10/bootstrap/bootstrap/js/jquery.ui.custom.js,
true,GET,http://192.168.1.10/bootstrap/bootstrap/js,
true,GET,http://192.168.1.10/bootstrap/js/?C=M;O=D,
true,GET,http://192.168.1.10/bootstrap/js/?C=S;O=D,

true,GET,http://192.168.1.10/bootstrap/js/?C=D;O=D,
true,GET,http://192.168.1.10/bootstrap/js/vendor/?C=N;O=D,
true,GET,http://192.168.1.10/bootstrap/js/vendor/?C=M;O=A,
true,GET,http://192.168.1.10/bootstrap/js/vendor/?C=S;O=A,
true,GET,http://192.168.1.10/bootstrap/js/vendor/?C=D;O=A,
true,GET,http://192.168.1.10/bootstrap/js/vendor/blob.js,
true,GET,http://192.168.1.10/bootstrap/js/vendor/filesaver.js,
true,GET,http://192.168.1.10/bootstrap/js/vendor/holder.js,
true,GET,http://192.168.1.10/bootstrap/js/vendor/jszip.min.js,
true,GET,http://192.168.1.10/bootstrap/js/vendor/less.min.js,
true,GET,http://192.168.1.10/bootstrap/js/vendor/uglify.min.js,
true,GET,http://192.168.1.10/bootstrap/js/vendor,
true,GET,"http://192.168.1.10/S,9%3f/S,12%3f/S,15%3f/S,Turn",
true,GET,http://192.168.1.10/product_details.php%3f%2520id=5,
true,GET,http://192.168.1.10/assets/bootstrap/css/?C=N;O=A,
true,GET,http://192.168.1.10/assets/bootstrap/css/?C=M;O=D,
true,GET,http://192.168.1.10/assets/bootstrap/css/?C=S;O=D,
true,GET,http://192.168.1.10/assets/bootstrap/css/?C=D;O=D,
true,GET,http://192.168.1.10/assets/bootstrap/fonts/?C=N;O=A,
true,GET,http://192.168.1.10/assets/bootstrap/fonts/?C=M;O=D,
true,GET,http://192.168.1.10/assets/bootstrap/fonts/?C=D;O=D,
true,GET,http://192.168.1.10/assets/bootstrap/fonts/?C=S;O=D,
true,GET,http://192.168.1.10/assets/bootstrap/js/?C=N;O=A,
true,GET,http://192.168.1.10/assets/bootstrap/js/?C=M;O=D,
true,GET,http://192.168.1.10/assets/bootstrap/js/?C=S;O=D,
true,GET,http://192.168.1.10/assets/bootstrap/js/?C=D;O=D,
true,GET,http://192.168.1.10/bootstrap/bootstrap/css/?C=N;O=A,
true,GET,http://192.168.1.10/bootstrap/bootstrap/css/?C=M;O=D,
true,GET,http://192.168.1.10/bootstrap/bootstrap/css/?C=S;O=D,
true,GET,http://192.168.1.10/bootstrap/bootstrap/css/?C=D;O=D,
true,GET,http://192.168.1.10/bootstrap/bootstrap/js/?C=N;O=A,
true,GET,http://192.168.1.10/bootstrap/bootstrap/js/?C=M;O=D,
true,GET,http://192.168.1.10/bootstrap/bootstrap/js/?C=D;O=D,
true,GET,http://192.168.1.10/bootstrap/bootstrap/js/?C=S;O=D,
true,GET,http://192.168.1.10/bootstrap/bootstrap/js/google-code-prettify/?C=N;O=D,
true,GET,http://192.168.1.10/bootstrap/bootstrap/js/google-code-prettify/?C=M;O=A,
true,GET,http://192.168.1.10/bootstrap/bootstrap/js/google-code-prettify/?C=S;O=A,
true,GET,http://192.168.1.10/bootstrap/bootstrap/js/google-code-prettify/?C=D;O=A,
true,GET,http://192.168.1.10/bootstrap/bootstrap/js/google-code-prettify/prettify.css,
true,GET,http://192.168.1.10/bootstrap/bootstrap/js/google-code-prettify/prettify.js,
true,GET,http://192.168.1.10/bootstrap/bootstrap/js/google-code-prettify,
true,GET,http://192.168.1.10/bootstrap/js/vendor/?C=N;O=A,

true,GET,http://192.168.1.10/bootstrap/js/vendor/?C=M;O=D,
true,GET,http://192.168.1.10/bootstrap/js/vendor/?C=S;O=D,
true,GET,http://192.168.1.10/bootstrap/js/vendor/?C=D;O=D,

APPENDIX C

DIRB v2.22
By The Dark Raver

START_TIME: Tue Jan 17 18:05:30 2023
URL_BASE: http://192.168.1.10/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.1.10/ ----
==> DIRECTORY: http://192.168.1.10/admin/
+ http://192.168.1.10/admin.cgi (CODE:403|SIZE:975)
+ http://192.168.1.10/admin.pl (CODE:403|SIZE:975)
==> DIRECTORY: http://192.168.1.10/assets/
+ http://192.168.1.10/AT-admin.cgi (CODE:403|SIZE:975)
+ http://192.168.1.10/cachemgr.cgi (CODE:403|SIZE:975)
+ http://192.168.1.10/cgi-bin/ (CODE:403|SIZE:989)
==> DIRECTORY: http://192.168.1.10/database/
==> DIRECTORY: http://192.168.1.10/img/
==> DIRECTORY: http://192.168.1.10/include/
+ http://192.168.1.10/index.php (CODE:200|SIZE:7443)
+ http://192.168.1.10/phpinfo.php (CODE:200|SIZE:76766)
+ http://192.168.1.10/phpmyadmin (CODE:401|SIZE:1222)
==> DIRECTORY: http://192.168.1.10/pictures/
+ http://192.168.1.10/robots.txt (CODE:200|SIZE:42)
==> DIRECTORY: http://192.168.1.10/sales/

---- Entering directory: http://192.168.1.10/admin/ ----
==> DIRECTORY: http://192.168.1.10/admin/ADMIN/
+ http://192.168.1.10/admin/admin.cgi (CODE:403|SIZE:975)
+ http://192.168.1.10/admin/admin.pl (CODE:403|SIZE:975)

==> DIRECTORY: http://192.168.1.10/admin/assets/
+ http://192.168.1.10/admin/AT-admin.cgi (CODE:403|SIZE:975)
+ http://192.168.1.10/admin/cachemgr.cgi (CODE:403|SIZE:975)
+ http://192.168.1.10/admin/error_log (CODE:200|SIZE:1320)
==> DIRECTORY: http://192.168.1.10/admin/include/
+ http://192.168.1.10/admin/index.php (CODE:200|SIZE:2654)

---- Entering directory: http://192.168.1.10/assets/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.1.10/database/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.1.10/img/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.1.10/include/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.1.10/pictures/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.1.10/sales/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.1.10/admin/ADMIN/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.1.10/admin/assets/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.1.10/admin/include/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

END_TIME: Tue Jan 17 18:06:18 2023

DOWNLOADED: 9224 - FOUND: 15