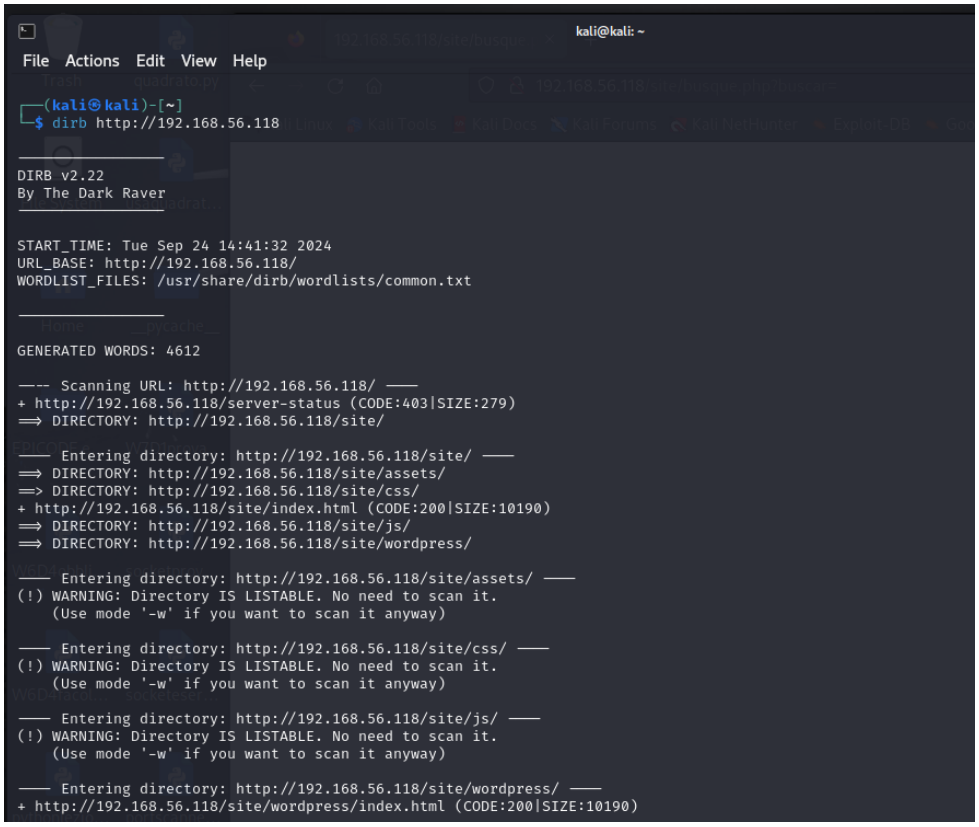
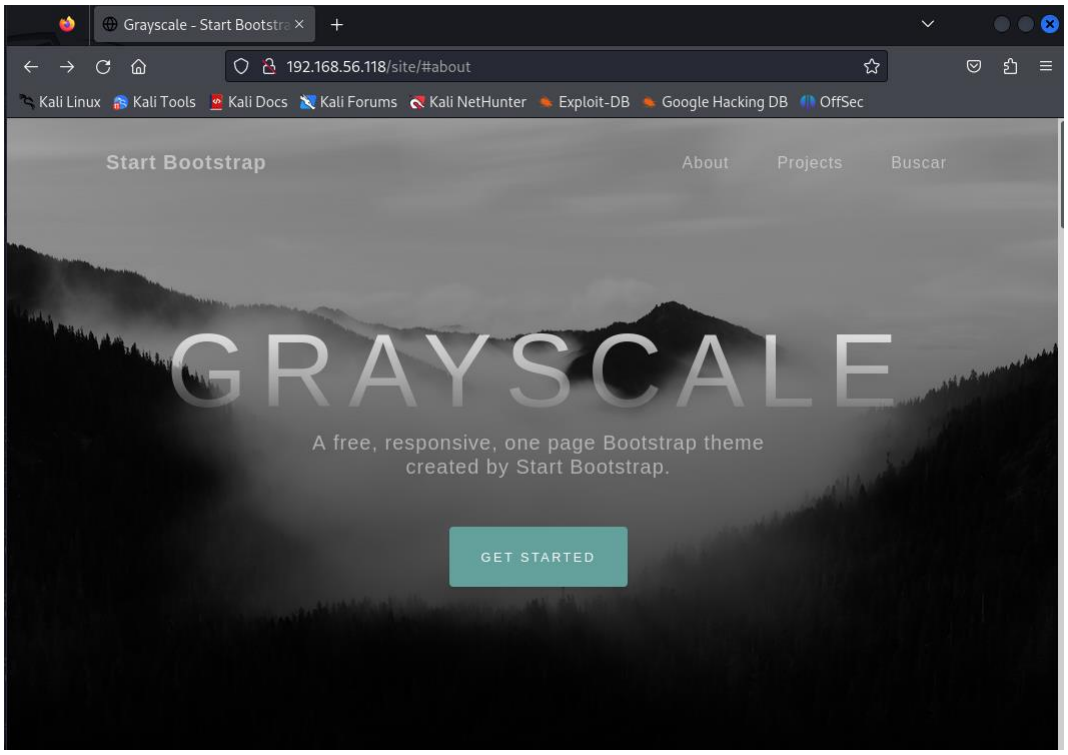
Bonus - Jangow Box

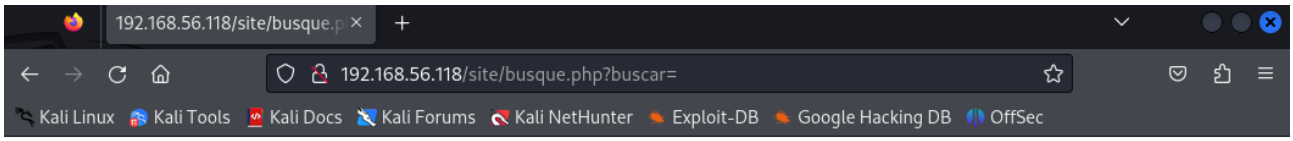
Per risolvere questa box sono partita da un directory listing usando DirBuster, per poi iniziare ad esplorare le varie directories alla ricerca di qualcosa di interessante. Non è stato necessario eseguire un arp-scan perché l'IP della macchina era già visibile all'apertura della macchina nella pagina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



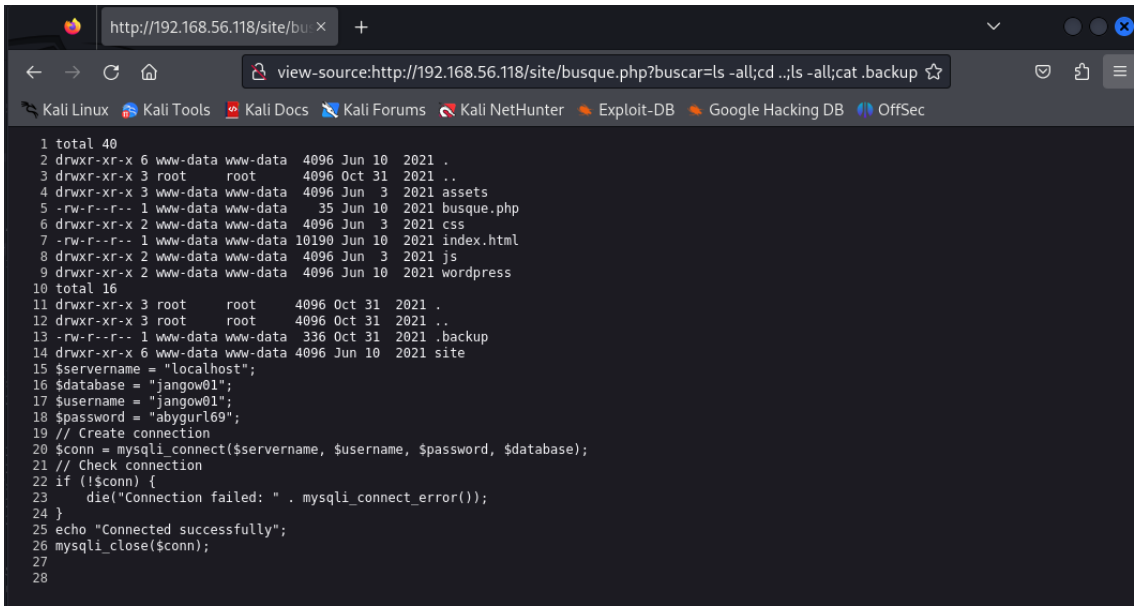
Ho esplorato le varie pagine web collegate alle directories trovate con Dirbuster e in particolare ho trovato la seguente pagina, che ho deciso di controllare meglio.



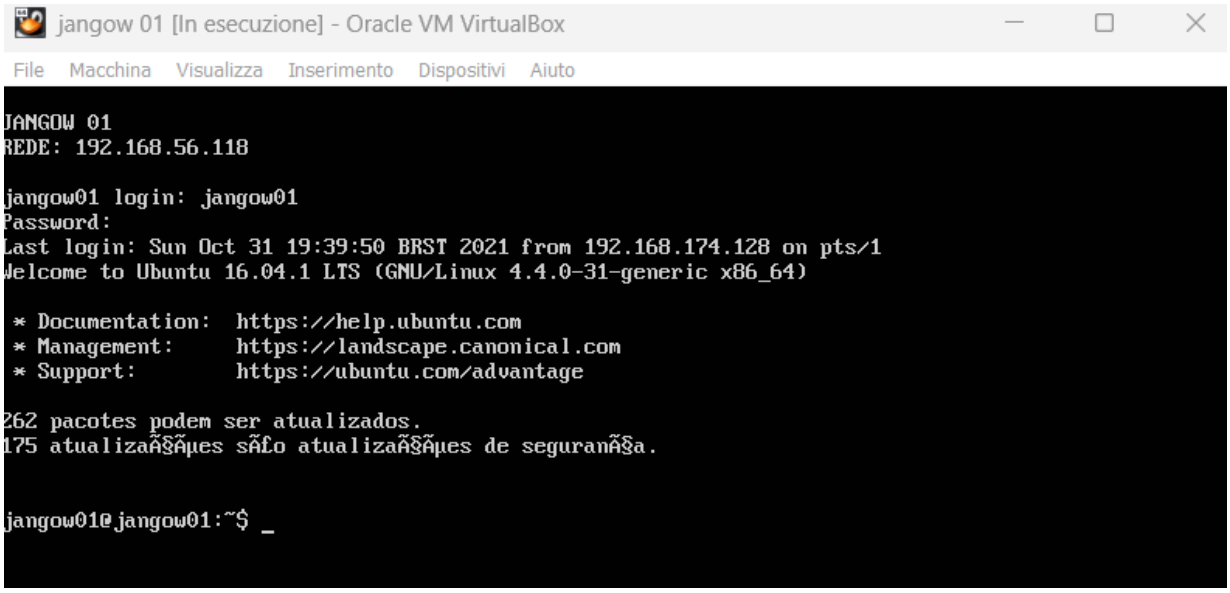
Dalle ricerche, è emerso che la pagina busque.php potrebbe essere vulnerabile ad una SQL injection, come si nota dal = alla fine dell'URL, che sembra indicare la possibilità di inserire dei comandi. Il parametro buscar è quindi vulnerabile.



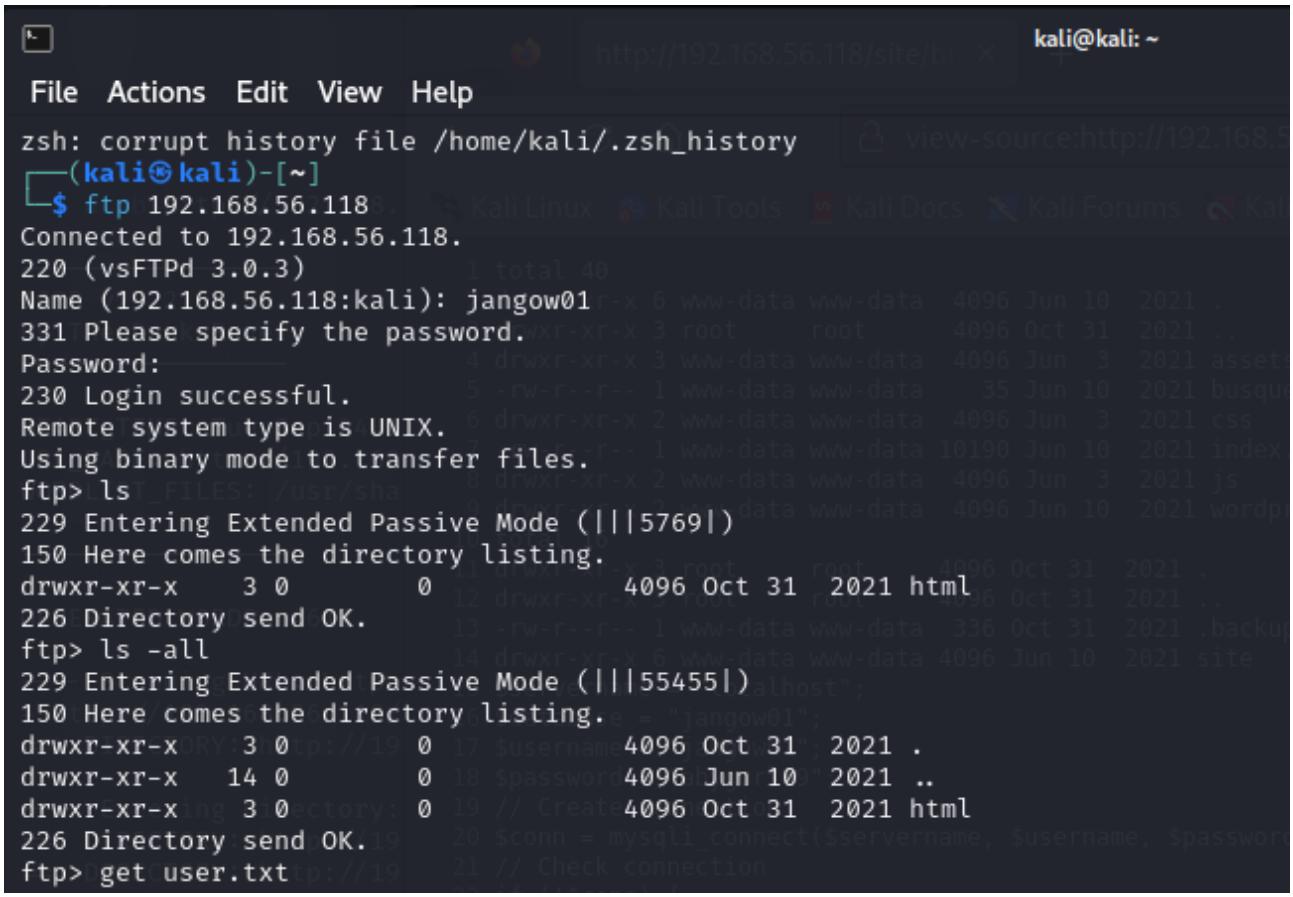
Ho ispezionato la pagina cercando il suo codice sorgente ed ho trovato proprio lo username e la password per il login su Jangow in un file di backup.



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



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.


kali@kali: ~
File Actions Edit View Help
zsh: corrupt history file /home/kali/.zsh_history
┌──(kali㉿kali)-[~]
└─$ ftp 192.168.56.118
Connected to 192.168.56.118.
220 (vsFTPd 3.0.3)
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