

# Dragon Ball - Episodio 2

UAM CTF 2019-9-15

## El reto

<https://unaalmes.hispasec.com/challenges#EPISODIO%202>

Challenge

0 Solves

×

EPISODIO 2

1000

Una sospecha tiene a Trunks bastante preocupado. Según cree, una mano negra está controlando la empresa de su familia, Capsule Corp. Jacu, el patrullero galáctico, le ha informado de que investigando este servidor podrá confirmar sus sospechas y descubrir quién mueve los hilos en Capsule Corp.

Ayuda a Trunks a desvelar el misterio que se encuentra en el siguiente servidor.

Info:

`http://34.253.120.147:5002/api/list ftp://34.253.120.147:21`

Flag

Submit

## api

Tenemos que ver averiguar qué esconden estos servers... comenzamos con la api web:

```
curl http://34.253.120.147:5002/api/list
```

```
"[{\"http://34.253.120.147:5002/api/friends\": \"True\"},  
  {\"http://34.253.120.147:5002/api/users\": \"True\"},  
  {\"http://34.253.120.147:5002/api/zabbix\": \"True\"},  
  {\"http://34.253.120.147:5002/api/zimbra\": \"True\"},  
  {\"http://34.253.120.147:5002/api/media\": \"True\"},  
  {\"http://34.253.120.147:5002/api/endpoints\": \"True\"}]\"
```

Este json mutante nos muestra unos cuantos endpoints

...que también nos retornan json:

```
19:07:45 ~/Documentos/ctf-hispasec/2019-09
curl http://34.253.120.147:5002/api/friends;\
curl http://34.253.120.147:5002/api/users;\
curl http://34.253.120.147:5002/api/zabbix;\
curl http://34.253.120.147:5002/api/zimbra;\
curl http://34.253.120.147:5002/api/media;\
curl http://34.253.120.147:5002/api/endpoints;
{"You don't have friends\": \"True\"}"
{"No users available\": \"True\"}"
{"Zabbix is not installed\": \"True\"}"
{"Zimbra is not installed\": \"True\"}"
{"Naranja\": \"True\"}"
{"This is\": \"True\"}"
```

Si cogemos la primera letra de cada endpoint construimos esto: **fuzzme**

Parece que quieren que hagamos fuzzing de nuevo... ¿se caerá el server esta vez?

Probando durante horas con dirsearch y algunas wordlists típicas como rockyou (demasiado bestia y la paré) y las de SecLists... encontramos algo usando raf-large-words.txt. Suponiendo que el endpoint está en /api/{LOQUESEA}:

```
python3 dirsearch.py -u http://34.253.120.147:5002/api/ -w
../SecList/Fuzz/Web-Content/raf-large-words.txt -e \
```

```
[21:40:38] Starting:
[21:40:39] 200 - 26B - /api/media
[21:40:41] 200 - 37B - /api/users
[21:40:43] 200 - 335B - /api/list
[21:40:48] 200 - 41B - /api/friends
[21:55:11] 200 - 26B - /api/endpoints
[21:59:50] 200 - 26B - /api/wnioski
```

...y al ~98% encontramos eso: /api/wnioski

```
curl http://34.253.120.147:5002/api/wnioski
{"TrUnK5\": \"5w0RD\"}"
```

Interesante... parece que tenemos user y pass del ftp

# ftp

Accedemos al ftp con este usuario y password y descargamos un jpg

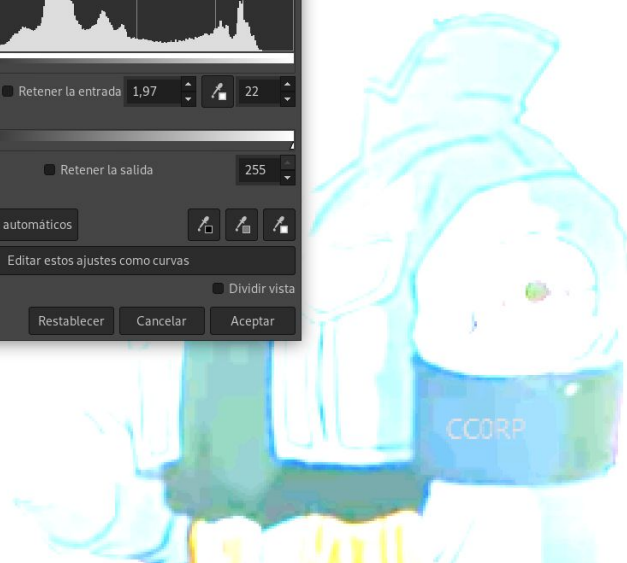
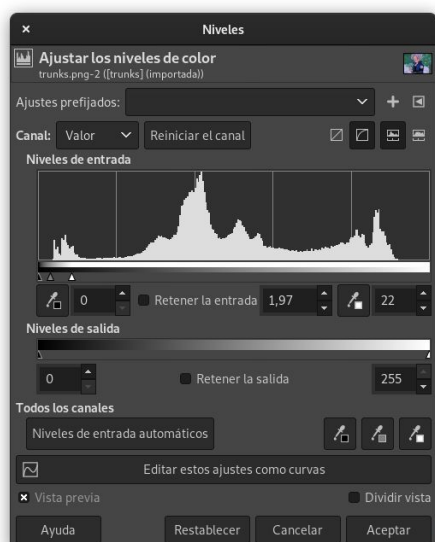
```
22:00:31 ~/src/other/dirsearch master ftp 34.253.120.147
Connected to 34.253.120.147 (34.253.120.147).
220 (vsFTPd 3.0.2)
Name (34.253.120.147:j0n3): TrUnK5
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
227 Entering Passive Mode (34,253,120,147,82,108).
150 Here comes the directory listing.
-rw-r--r-- 1 ftp ftp 243198 Sep 15 12:59 trunks.png
226 Directory send OK.
ftp> get trunks.png
local: trunks.png remote: trunks.png
227 Entering Passive Mode (34,253,120,147,82,116).
150 Opening BINARY mode data connection for trunks.png (243198 bytes).
226 Transfer complete.
243198 bytes received in 0,168 secs (1448,05 Kbytes/sec)
```

# Stego

Es una imagen en la que aparece trunks



Jugando con gimp y los niveles encontramos CCORP claramente, aunque también se distingue a simple vista... Cualquier herramienta que nos permita modificar el brillo y contraste nos valdrá.



## Metadatos

Y buscando metadatos con exiv2 veo algo interesante también:

```
22:16:05 ~/Documentos/ctf-hispasec/2019-09 exiv2 -pa trunks.png
Xmp.dc.rights LangAlt 1 lang="x-default" MM4N0N3GR4
```

MM4N0N3GR4

# ftp otra vez

probando incontables combinaciones al final di con el user:pass MM4N0N3GR4:CC0RP

```
23:28:45 ~/Documentos/ctf-hispasec/2019-09 ftp 34.253.120.147
Connected to 34.253.120.147 (34.253.120.147).
220 (vsFTPD 3.0.2)
Name (34.253.120.147:~): anonymous
331 Please specify the password.
Password:
530 Login incorrect.
Login failed.
ftp> user
(username) MM4N0N3GR4
331 Please specify the password.
Password:
230 Login successful.
ftp> ls
227 Entering Passive Mode (34,253,120,147,82,109).
150 Here comes the directory listing.
-rw-r--r-- 1 ftp ftp 101 Sep 15 13:03 flag.txt
226 Directory send OK.
ftp> get flag.txt
local: flag.txt remote: flag.txt
227 Entering Passive Mode (34,253,120,147,82,115).
150 Opening BINARY mode data connection for flag.txt (101 bytes).
WARNING: 1 bare linefeeds received in ASCII mode
File may not have transferred correctly.
226 Transfer complete.
101 bytes received in 6,6e-05 secs (1530,30 Kbytes/sec)
ftp> cat flag.txt
?Invalid command
ftp> 221 Goodbye.

23:29:19 ~/Documentos/ctf-hispasec/2019-09 cat flag.txt
RXLWMW9hV2dHVGTpcndFZUR4cU9uYU9JRzJnbkhINGtESjFqQUtPVUh6Y2lxMUFjcFJnSlowU0lj09PRjFManAwRXZDRGI9Cg==
23:29:21 ~/Documentos/ctf-hispasec/2019-09 cat flag.txt | base64 -d
EyVloaWgGtKOrwEeDxq0na0IG2gnHH4kDJlJAKOUHzcIq1AcpRgJZ0SIiw00F1Ljp0EvCdb=
```

bajo el fichero y parece algo codificado en base64...

Probando combinaciones en cyberchef encuentro cosas con el maravilloso plugin magic:

Operations

Magi

Magic

Detect File Type

Scan for Embedded Files

Favourites

Data format

Encryption / Encoding

Public Key

Arithmetic / Logic

Networking

Language

Recipe

Magic

Depth 3

Intensive mode

Extensive

language support

Crib (known plaintext string or regex)

Input

length: 100  
lines: 1

RXLWMW9hV2dHVGTpcndFZUR4cU9uYU9JRzJnbkhINGtESjFqQUtPVUh6Y2lxMUFjcFJnSlowU0lj09PRjFManAwRXZDRGI9Cg==

Output

time: 110ms  
length: 81569  
lines: 2928

		Entropy: 4.93
From_Base64('A-Za-z0-9+/',true)	HNZ{626n193pppq005779q10n1oqr74r45r4}.	Valid UTF8
From_Base64('N-ZA-Mn-Za-m0-9+/',true)		Entropy: 4.16
From_Base64('N-ZA-Mn-Za-m0-9+/',true)		

HNZ{626n193pppq005779q10n1oqr74r45r4} ¡Parece que está cerca!

# Flag

Tras probar algunas cosas, si hacemos un rot 13 a lo anterior...

Recipe	Input
<b>ROT13</b> <input checked="" type="checkbox"/> Rotate lower case chars <input checked="" type="checkbox"/> Rotate upper case chars Amount: 13	HNZ{626n193pppq005779q10n1oqr74r45r4}
	Output
	UAM{626a193cccd005779d10a1bde74e45e4}

UAM{626a193cccd005779d10a1bde74e45e4}

Meto la flag en la plataforma y... Gol! pero uff, julianjm ha estado a un minuto de quitarme la satisfacción de coronar xD

## Conclusión

Parece que los admins no se resignan y han hecho los deberes para crear un servicio capaz de soportar nuestro fuzzing sin pestañear, ¡bravo!. El stego no ha sido muy complicado pero me ha costado un rato encontrar la combinación de user y pass para el ftp `\_(ツ)_/`

Cyberchef ha vuelto a ser una herramienta esencial para encontrar la flag.

Rockyou.txt es una lista enorme y no contiene lo que buscábamos, pero en las wordlists de SecList aparece en varias ocasiones, así que solo era dar con la lista adecuada y tener paciencia:

```
10:09:26 ~ /src/other/SecLists master grep -R -e "^wnioski$" .
./Passwords/openwall.net-all.txt:wnioski
./Discovery/Web-Content/raft-large-words.txt:wnioski
./Discovery/Web-Content/raft-large-words-lowercase.txt:wnioski
./Discovery/Web-Content/raft-large-directories-lowercase.txt:wnioski
./Discovery/Web-Content/raft-large-directories.txt:wnioski
./Discovery/DNS/dns-Jhaddix.txt:wnioski
./Discovery/DNS/shubs-subdomains.txt:wnioski
```

José Ángel Sánchez

@j0n3

Challenge		2 Solves	X
Name		Date	
j0n3		4 minutes ago	
julianjm		3 minutes ago	