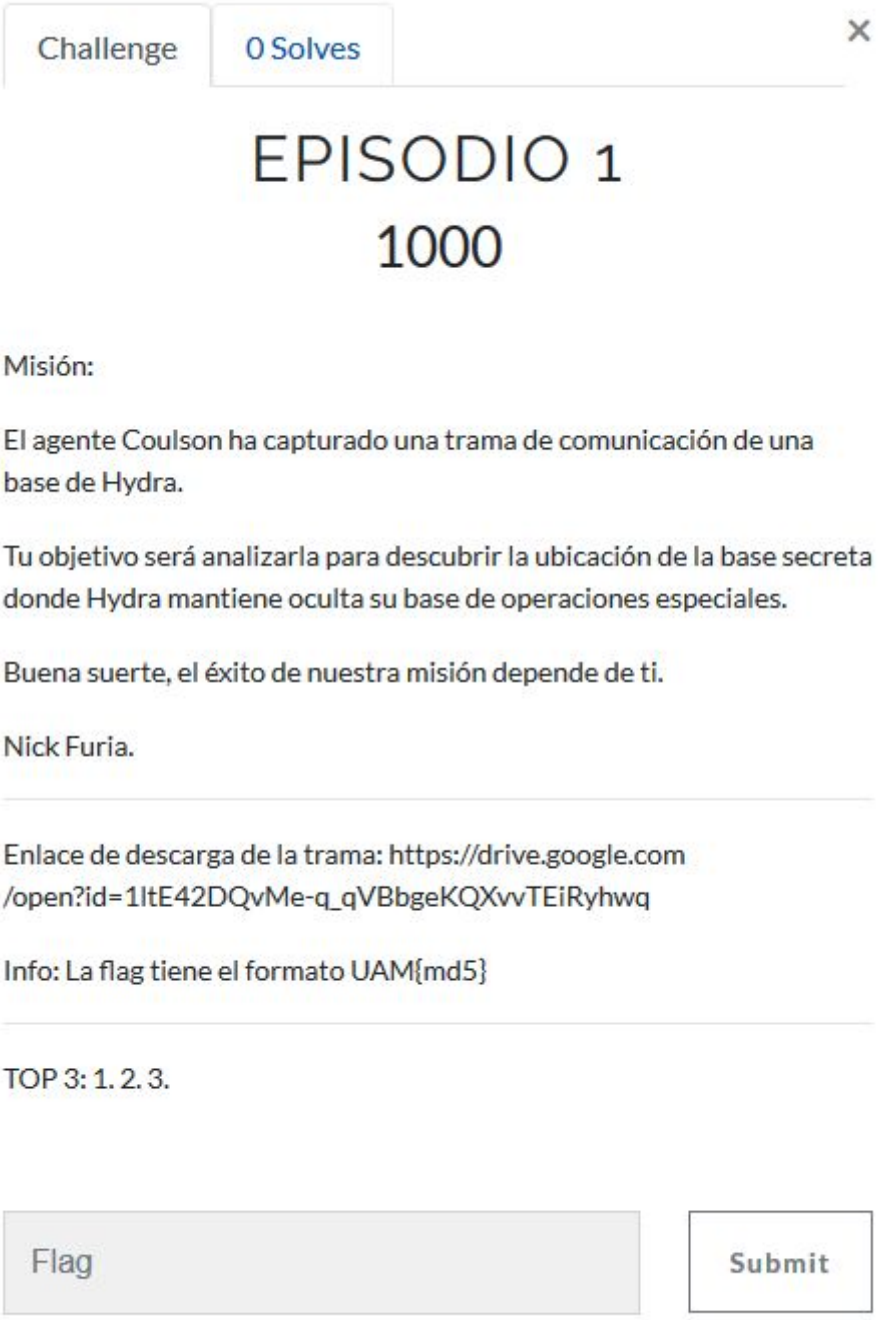
Universo Marvel - Episodio 1

UAM CTF 2018-12-15

El reto

https://unaalmes.hispasec.com/challenges#EPISODIO%201



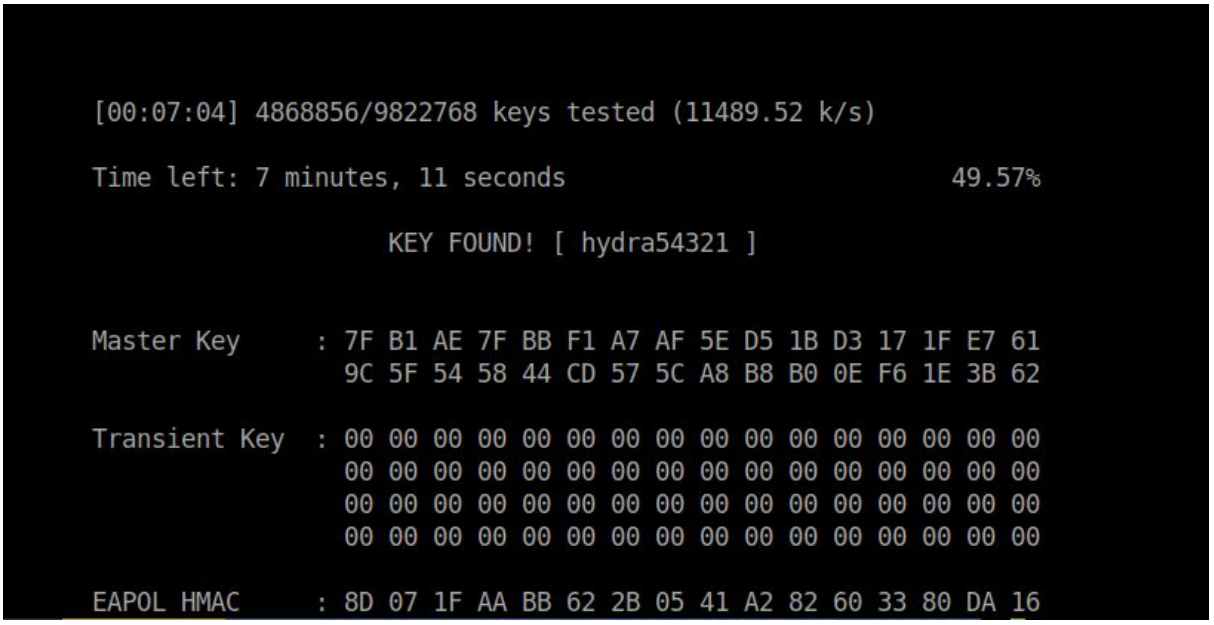
https://drive.google.com/open?id=1ltE42DQvMe-q_qVBbgeKQXvvTEiRyhwq

Descargamos el zip y contiene un cap.

Parece una captura de wifi. Vamos a tratar de encontrar la clave con aircrack-ng usando rockyou.txt

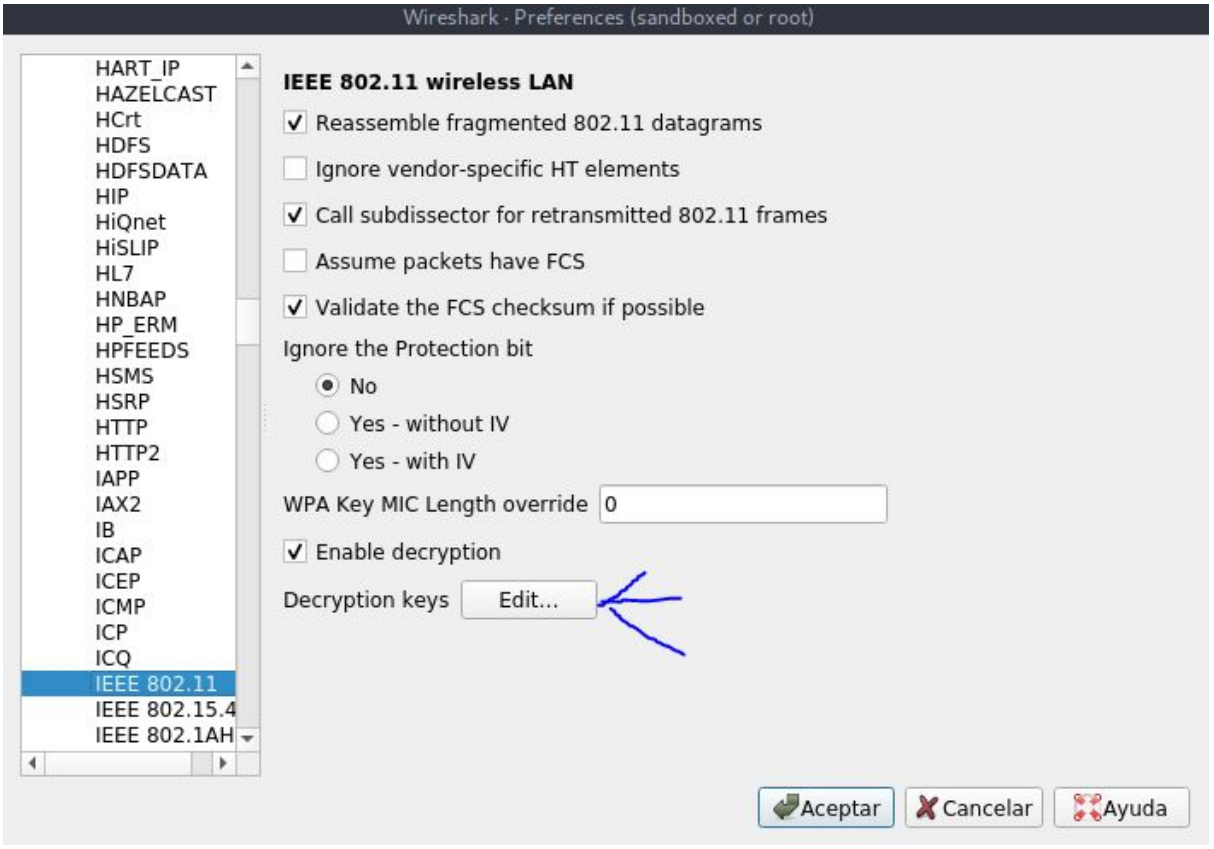
Aircrack-ng cap & rockyou.txt

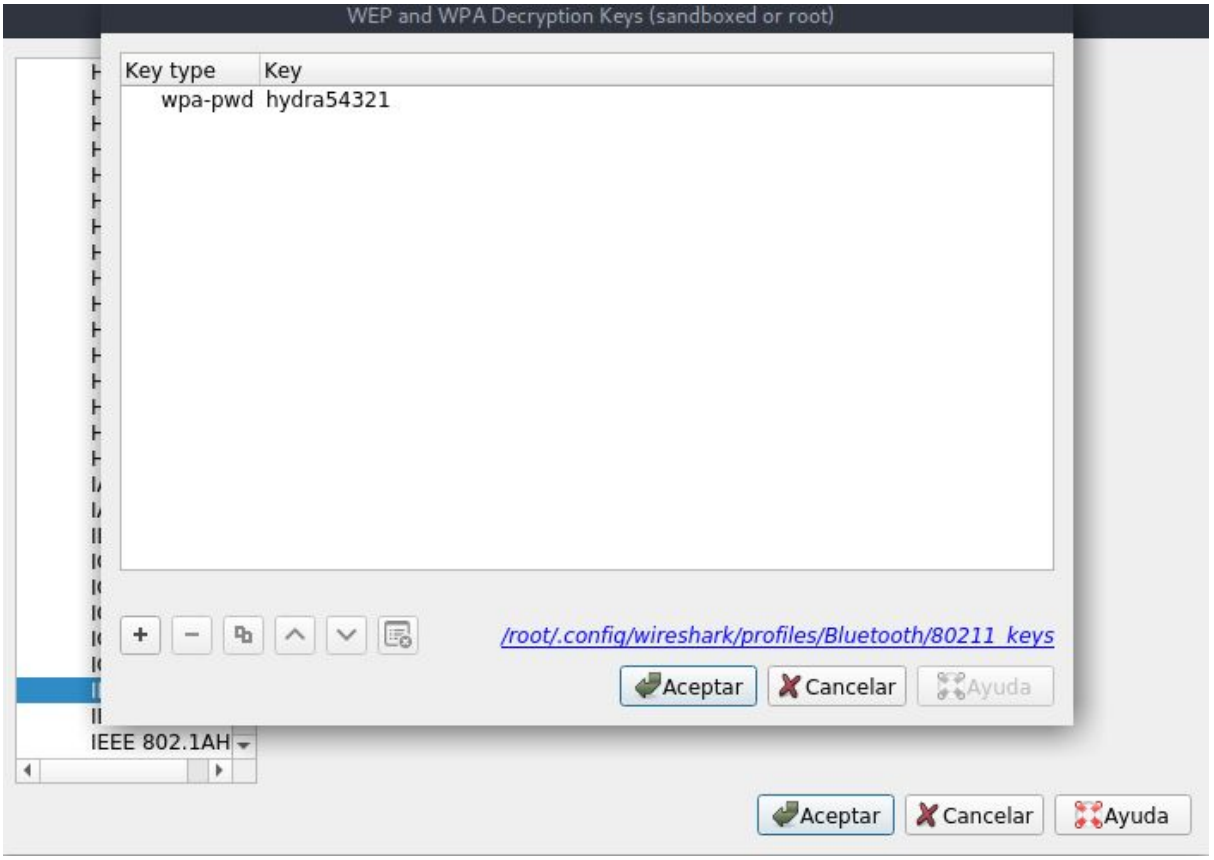
aircrack-ng -w /usr/share/wordlists/rockyou.txt capture-01.cap

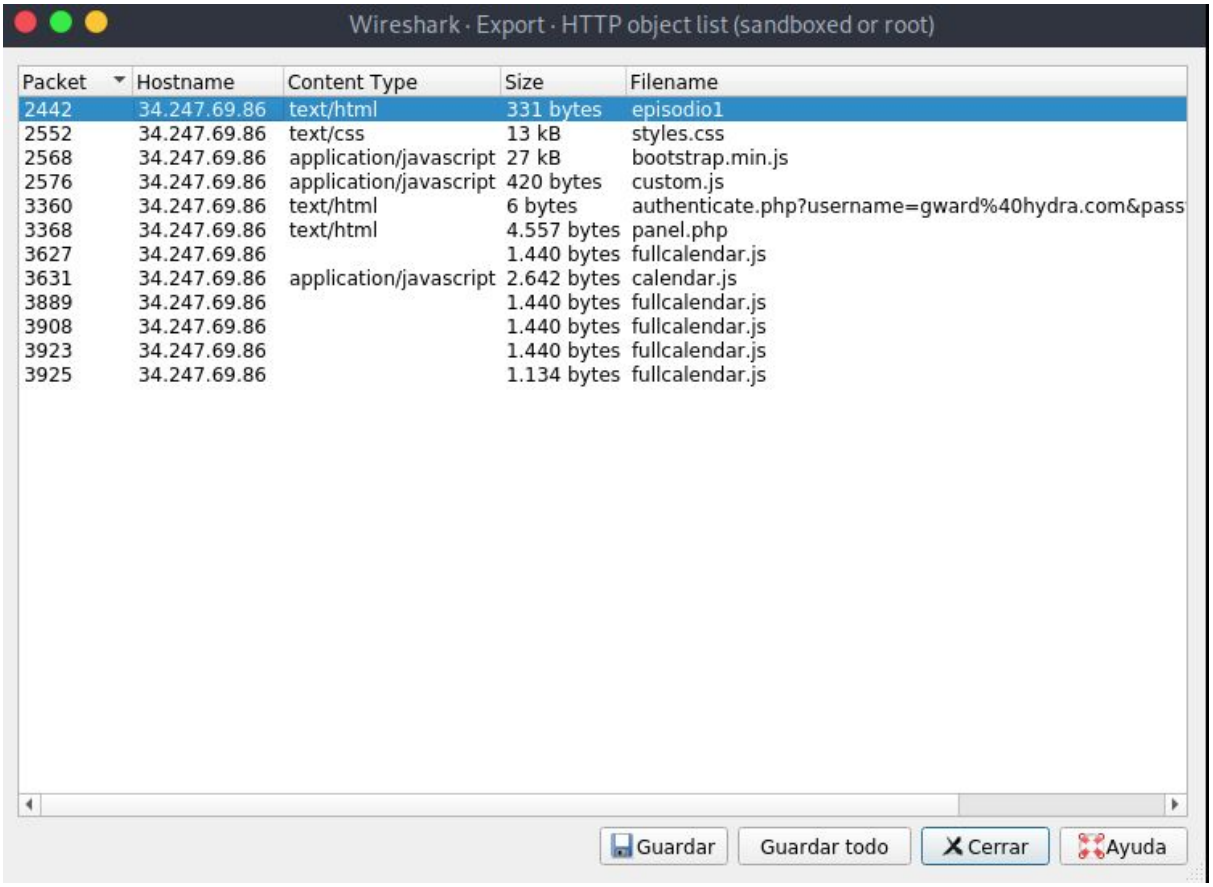


Después de un rato, tenemos la clave: hydra54321

Configuramos la key en wireshark y exportamos los objetos que encontramos.


Wireshark · Preferences (sandboxed or root)
HART_IP
HAZELCAST
HCrt
HDFS
HDFSDATA
HIP
HiQnet
HiSLIP
HL7
HNBAP
HP_ERM
HPFEEDS
HSMS
HSRP
HTTP
HTTP2
IAPP
IAX2
IB
ICAP
ICEP
ICMP
ICP
ICQ
IEEE 802.11
IEEE 802.15.4
IEEE 802.1AH
IEEE 802.11 wireless LAN
Reassemble fragmented 802.11 datagrams
Ignore vendor-specific HT elements
Call subdissector for retransmitted 802.11 frames
Assume packets have FCS
Validate the FCS checksum if possible
Ignore the Protection bit
No
Yes - without IV
Yes - with IV
WPA Key MIC Length override
0
Enable decryption
Decryption keys
Edit...
Aceptar
Cancelar
Ayuda


WEP and WPA Decryption Keys (sandboxed or root)
Key type
Key
wpa-pwd
hydra54321
/root/.config/wireshark/profiles/Bluetooth/80211_keys
Aceptar
Cancelar
Ayuda
IEEE 802.1AH
Aceptar
Cancelar
Ayuda




```
total 20M
drwxr-xr-x 2 j0n3 j0n3 4,0K dic 15 15:57  .
drwxr-xr-x 3 j0n3 j0n3 4,0K dic 15 15:15  ..
-rw-r--r-- 1 j0n3 j0n3  18M dic 15 15:15  asd
-rw-r--r-- 1 root root    6 dic 15 15:54 'authenticate.php%3fusername=gward%40hydra.com&password=rUHp6e7FVds2nRPZ'
-rw-r--r-- 1 root root  28K dic 15 15:54  bootstrap.min.js
-rw-r--r-- 1 root root 2,6K dic 15 15:54  calendar.js
-rw-r--r-- 1 root root 1,7M dic 15 15:39  capture-01.cap
-rw-r--r-- 1 root root  420 dic 15 15:54  custom.js
-rw-r--r-- 1 root root  331 dic 15 15:54  episodio1
-rw-r--r-- 1 root root 1,5K dic 15 15:54 'fullcalendar(1).js'
-rw-r--r-- 1 root root 1,5K dic 15 15:54 'fullcalendar(2).js'
-rw-r--r-- 1 root root 1,5K dic 15 15:54 'fullcalendar(3).js'
-rw-r--r-- 1 root root 1,2K dic 15 15:54 'fullcalendar(4).js'
-rw-r--r-- 1 root root 1,5K dic 15 15:54  fullcalendar.js
-rw-r--r-- 1 root root 4,5K dic 15 15:54  panel.php
-rw-r--r-- 1 root root  14K dic 15 15:54  styles.css
```

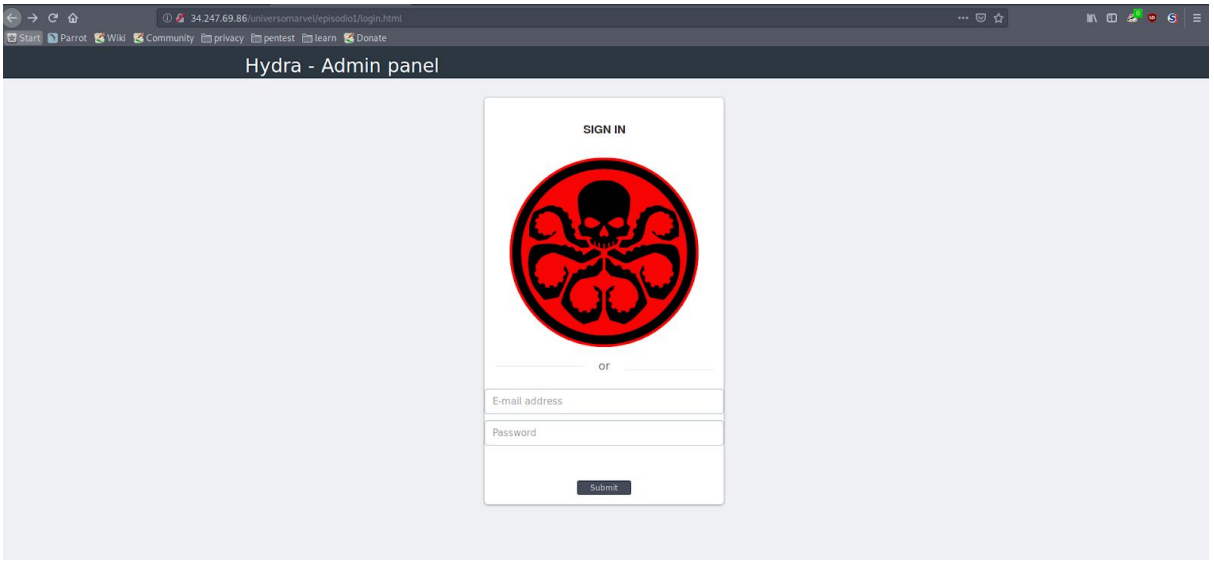
Episodio1

cat episodio1

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>301 Moved Permanently</title>
</head><body>
<h1>Moved Permanently</h1>
<p>The document has moved <a href="http://34.247.69.86/universomarvel/episodio1/">here</a>.</p>
<hr>
<address>Apache/2.4.25 (Debian) Server at 34.247.69.86 Port 80</address>
</body></html>
```

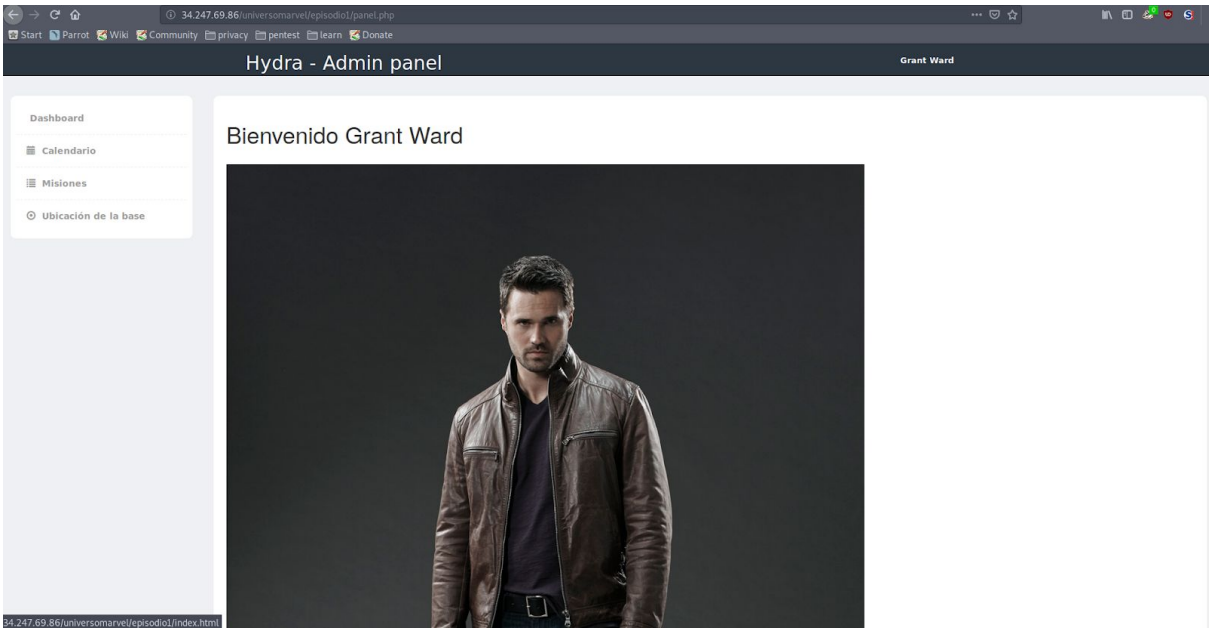
Hydra Admin panel

Vamos a ve qué hay en esa url: http://34.247.69.86/universomarvel/episodio1/

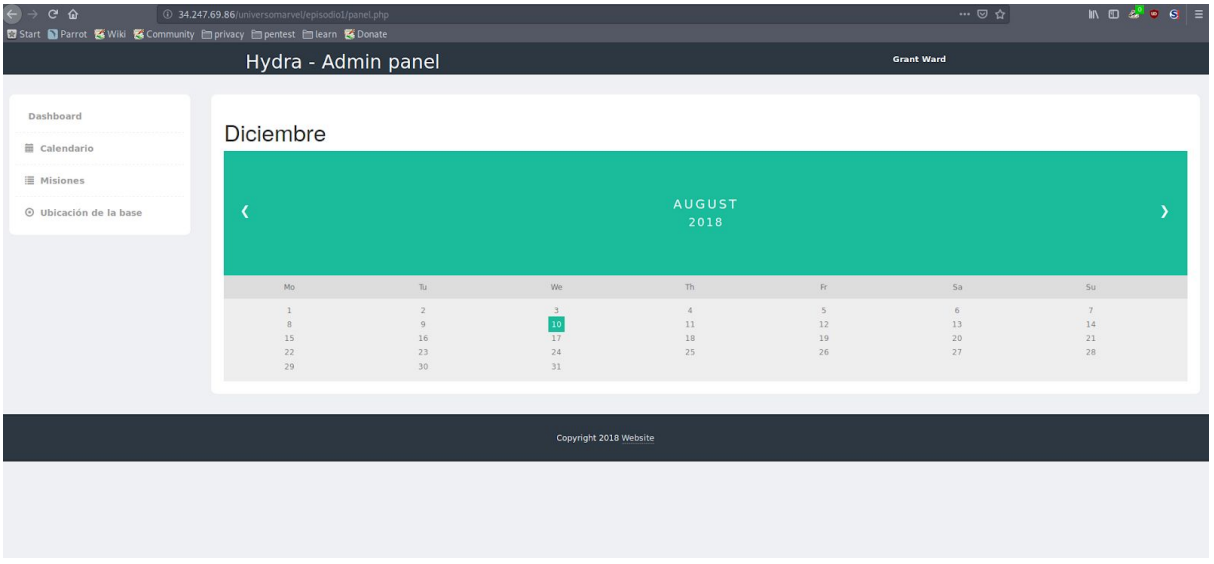


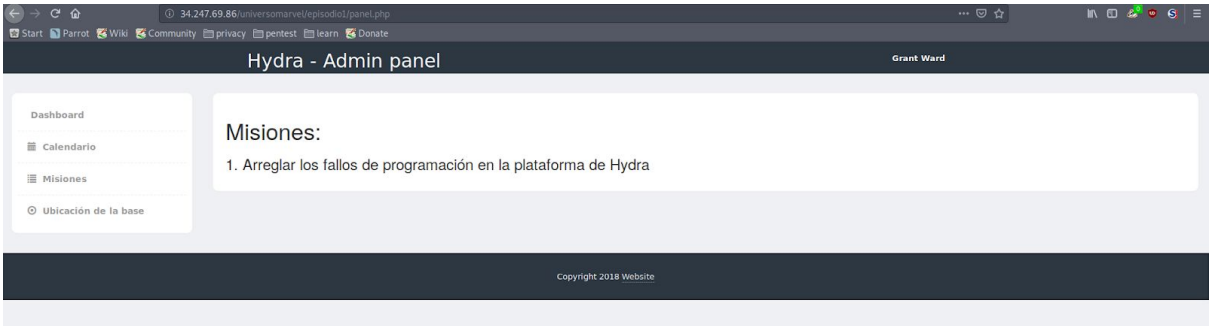
Logamos con la url que aparece en el archivo, que parece que pasa las credenciales por get (facepalm). Estamos dentro:

http://34.247.69.86/universomarvel/episodio1/authenticate.php%3fusername=qward%40hydra.com&password=rUHp6e7FVds2nRPZ

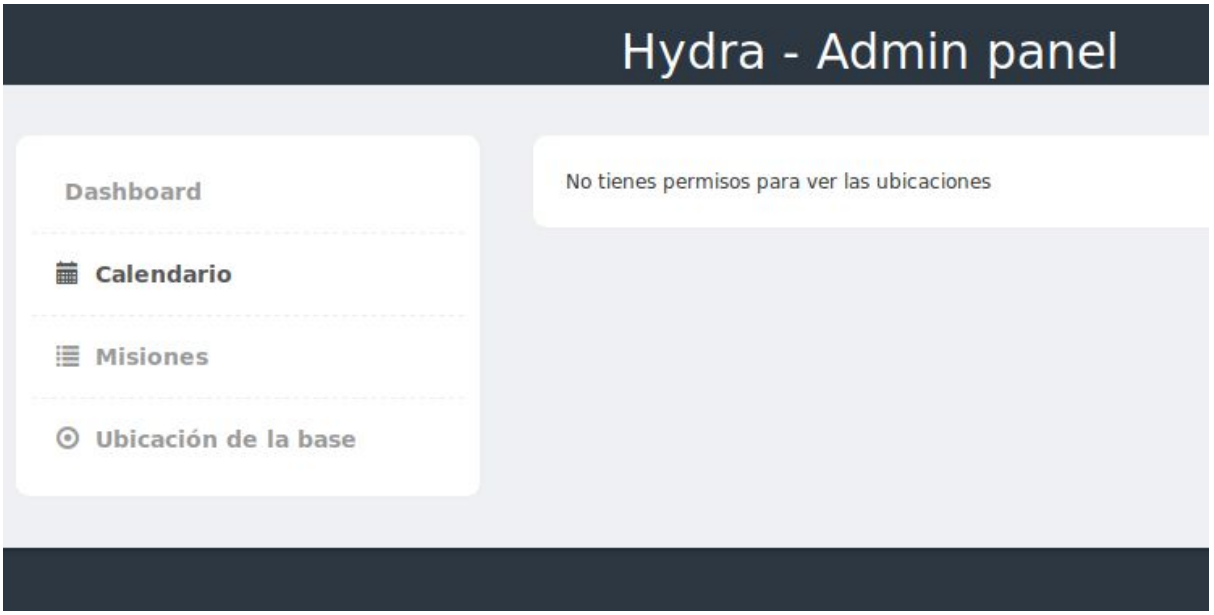

34.247.69.86/universomarvel/episodio1/panel.php
Start Parrot Wiki Community privacy pentest learn Donate
Hydra - Admin panel
Grant Ward
Dashboard
Calendario
Misiones
Ubicación de la base
Bienvenido Grant Ward
34.247.69.86/universomarvel/episodio1/index.html

Paneles:


34.247.69.86/universomarvel/episodio1/panel.php
Start Parrot Wiki Community privacy pentest learn Donate
Hydra - Admin panel
Grant Ward
Dashboard
Calendario
Misiones
Ubicación de la base
Diciembre
AUGUST
2018
Mo Tu We Th Fr Sa Su
1 2 3 4 5 6 7
8 9 10 11 12 13 14
15 16 17 18 19 20 21
22 23 24 25 26 27 28
29 30 31
Copyright 2018 Website


34.247.69.86/universomarvel/episodio1/panel.php
Start Parrot Wiki Community privacy pentest learn Donate
Hydra - Admin panel
Grant Ward
Dashboard
Calendario
Misiones
Ubicación de la base
Misiones:
1. Arreglar los fallos de programación en la plataforma de Hydra
Copyright 2018 Website

Ubicación de la base



Si nos fijamos en el php que nos dejan, aparecen algunas llamadas a databases.php?load=...

http://34.247.69.86/universomarvel/episodio1/databases.php?load=NVQXAYLT

nos muestra el texto

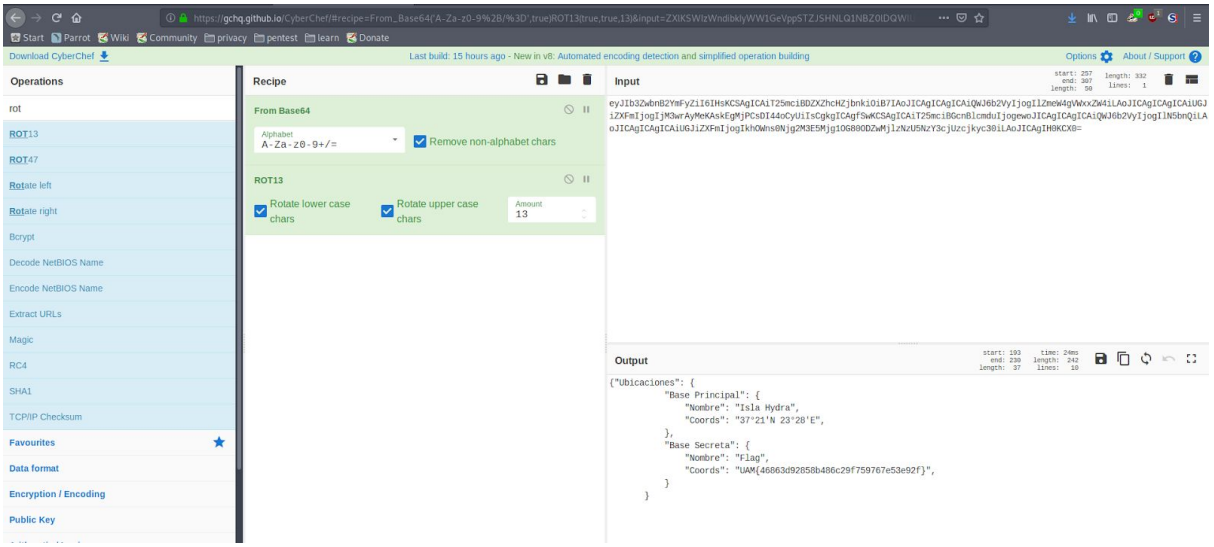
No tienes permisos para ver las ubicaciones

Tenemos una cookie de sesión PHPSESSID

Si hacemos la petición sin esta sesión nos devuelve el texto:

eyJIb3ZwbnB2YmFyZiI6IHsKCSAgICAiT25mciBDZXZhcHZjbnkiOiB7IAoJICAgICAgICAiQWJ
6b2VyIjogIlZmeW4gVWxxZW4iLAoJICAgICAgICAiUGJiZXFmIjogIjM3wrAyMeKAskEgMjPCs
DI44oCyUiIsCgkgICAgfSwKCSAgICAiT25mciBGcnBlcmduIjogewoJICAgICAgICAiQWJ6b2VyI
jogIlN5bnQiLAoJICAgICAgICAiUGJiZXFmIjogIkhOWns0Njg2M3E5Mjg1OG80ODZwMjlzNzU
5NzY3cjUzcjkyc30iLAoJICAgIH0KCX0=

Base64 + rot13

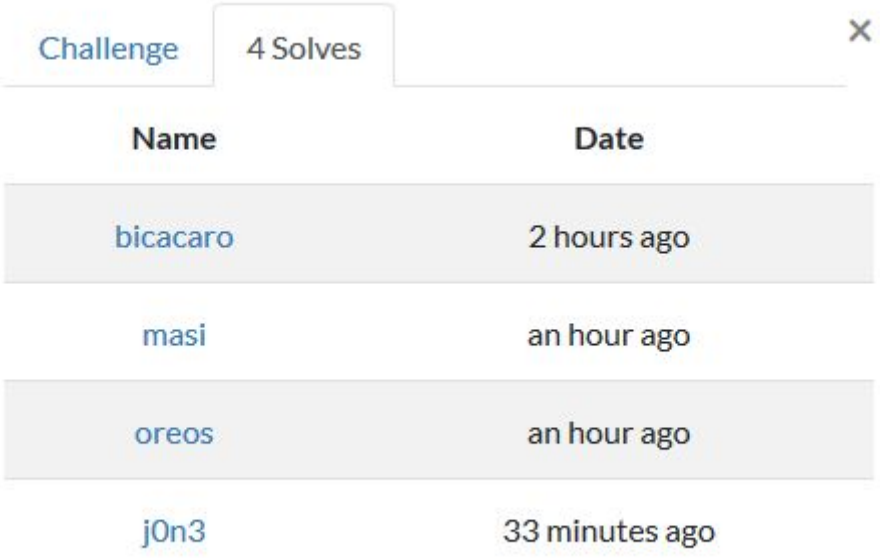


{"Ubicaciones": {
"Base Principal": {
"Nombre": "Isla Hydra",
"Coords": "37°21′ N 23°28′ E",
},
"Base Secreta": {
"Nombre": "Flag",
"Coords": "UAM{46863d92858b486c29f759767e53e92f}",
}
}

Flag

UAM{46863d92858b486c29f759767e53e92f}

4º puesto. ¡Qué velocidad tenéis!



Conclusión

Hemos hecho un ataque de diccionario contra una captura de paquetes de red wifi y extraído algunos ficheros interesantes. Hemos visto por qué no es buena idea usar GET para el envío de credenciales, ya que acceder simplemente a esa url nos da acceso a un servicio que requiera registro. Estas urls podrían quedar expuestas en el historial del navegador del usuario, por ejemplo.

Por otro lado vemos que el php que se encarga de permitirnos ver ciertos documentos está mal hecho. En caso de tener la cookie de sesión no nos deja, y si la quitamos, sí. Eso pasa por no hacer tests... :D

¡Gracias de nuevo, admins del remo! Esta vez se me ha hecho corto… ¡queremos más!

José Ángel Sánchez
@_j0n3