

# WRITE-UP MARVEL – CTF UAM - HISPASEC

## EPISODIO-3

*Elaborado por: Arsenics*

### **Misión:**

**Sabemos que el ataque a la base de Haití se va a realizar entre el 15 y el 22 de febrero. ¡Es necesario pararlo!**

La web desde donde dirigen el lanzamiento es pública y por tanto su desactivación también. Necesitamos que encuentres algún fallo para colarte en el servidor, y una vez ahí encuentres algún código de desactivación válido.

Recuerda que Hydra suele usar sistemas de cifrados originales y creativos.

Mucha suerte soldado.

Nick Furia.

---

Enlace a la web de lanzamiento: <http://34.247.69.86/universomarvel/episodio3/index.php>

Info: La flag tiene el formato UAM{md5}

### **Tools:**

-Burpsuite: <https://portswigger.net/burp/>

-Dirb: <https://sourceforge.net/projects/dirb/>

-Put2win: <https://github.com/sysdevploit/put2win>

-Md5: <https://www.md5online.org/>

### **Walktrough:**

El enlace nos lleva a una web que nos solicita el código de desactivación del ataque a Haití.

A screenshot of a web interface with a dark, textured background. In the center, there is a white rectangular box. Inside this box, at the top, is a text input field followed by the label "Codigo de desactivacion". Below the input field is a prominent red button with the white text "DESACTIVAR LANZAMIENTO".

En primer lugar revisamos el código fuente para ver si nos proporciona alguna pista, pero no encontramos nada interesante. En segundo lugar se realiza un poco de fuzzing para revisar que información podemos recopilar que nos muestre el camino. Hay varias aplicaciones con la que podemos hacer fuzzing Nikto, dirb, dirbuster, gobuster, wfuzz, Cualquiera de ellas es válida para la obtención de los resultados la clave estriba en el diccionario que utilices.

dirb <http://34.247.69.86/universomarvel/episodio3/> usr/share/dirb/wordlists/big.txt -r

<http://34.247.69.86/universomarvel/episodio3/logs/>



<http://34.247.69.86/universomarvel/episodio3/js/>

<http://34.247.69.86/universomarvel/episodio3/robots.txt/>

<http://34.247.69.86/universomarvel/episodio3/imagenes/>

Nos han ido dejando mensajes en diferentes apartados. En el robots.txt por ejemplo aparecía un mensaje que decía “No cuela. Se que eres agente de Shield y aquí no vas encontrar nada”. En la carpeta imagenes habían montón de fotos guapas de Hydra, pero que no nos proporcionaba la información que andábamos buscando para el reto. En el directorio examples hay varias cosas que captan mi atención.

## Index of /universomarvel/episodio3/examples

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 <a href="#">Parent Directory</a>		-	
 <a href="#">fbuasnakdqudbnqdkqwdnm/</a>	2019-02-14 16:34	-	
 <a href="#">jquwndaksduiawndqldnqwkldqwn/</a>	2019-02-14 16:34	-	
 <a href="#">jungasdjashdaskdansdkasdkl/</a>	2019-02-15 16:01	-	
 <a href="#">pounaslduqndqlwdjqwdqw/</a>	2019-02-14 16:34	-	
 <a href="#">quyertuqnwemqwejgwnsak/</a>	2019-02-14 16:34	-	
 <a href="#">tqhqwnduansdamdioqwmq/</a>	2019-02-14 16:34	-	
 <a href="#">uaysdnqdmqowdqnqkdqopwdj/</a>	2019-02-14 16:34	-	
 <a href="#">ukasnflkianfiansfuinasfiunasf/</a>	2019-02-14 16:34	-	
 <a href="#">unyxbaiksdqhdqiwwqwdnqkwd/</a>	2019-02-14 16:34	-	
 <a href="#">uqwywebasdmassnfiewufbwefew/</a>	2019-02-14 16:34	-	

Apache/2.4.25 (Debian) Server at 34.247.69.86 Port 80

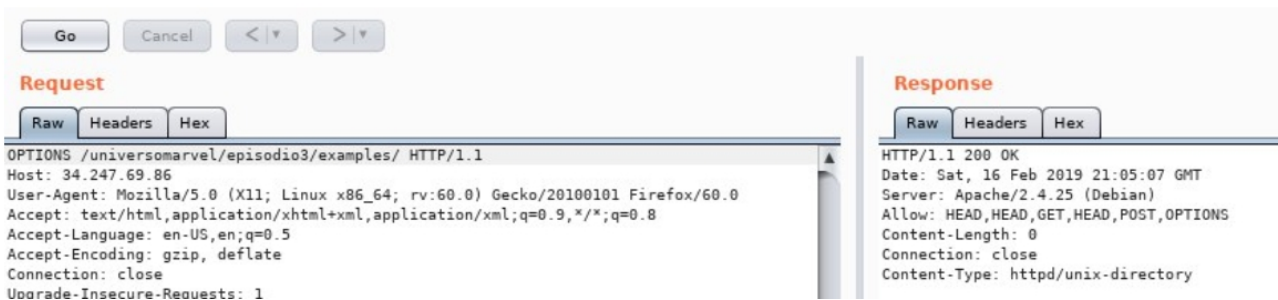
Por un lado vemos lickeada la info del server sin haber hecho uso de un nmap como si hubiésemos utilizado en otros casos. Por otro lado vemos que las carpetas tienen nombres de teclas pulsados al azar y que todas fueron creadas el día de San Valentín excepto una. Hay una única carpeta creada el mismo día 15 poco después tras la apertura de la prueba. Nos han dejado una pista!!

Al entrar en ella te enseña una imagen como en las otras pero se observa que hace un 301. Te redirecciona al puerto 8080 donde está el servidor con el código de desactivación. De forma que el nmap te lo puedes ahorrar totalmente xD.

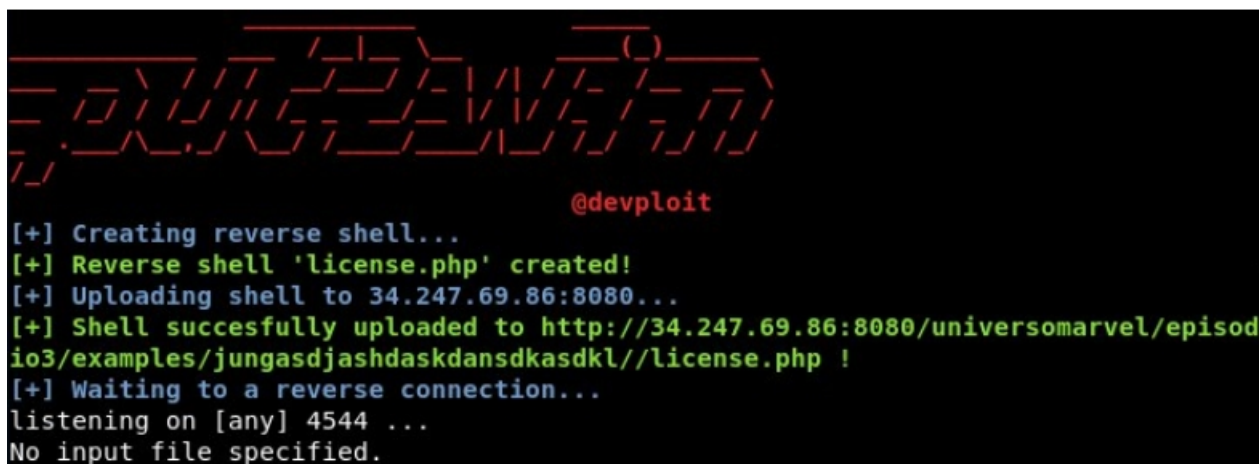


No es seguro | 34.247.69.86:8080/index.jpg

Llegados a este punto, tenemos clara la entrada al servidor. Hay que ver cómo. Mientras que en otras carpetas puedes observar con burp los diferentes métodos http permitidos GET, POST , etc en esta el OPTIONS no esta permitido y no nos deja... que curioso jaja

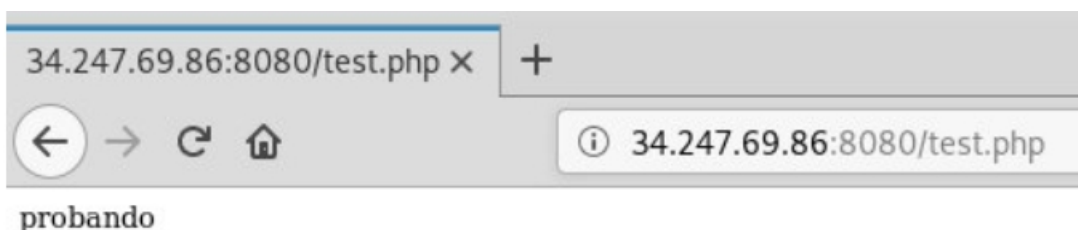


Aquí intento varias opciones, montando un SimpleHTTPServer en python e intentado hacer un put que no termina de funcionar. Pruebo también con el put2win pero me devuelve en el que crea la reverse shell y la sube, pero me devuelve un "No input file" y no logro el objetivo.



Tras un aire y darle unas vueltas finalmente hago una prueba con curl y se sube el archivo sin devolver error.

Curl - T test.php http://34.247.69.86



Abro los puertos, subo la reverse shell y consigo entrar. Aquí si se está acostumbrado a hacer este tipo de retos en otros lugares sueles hacer escalada de privilegios. Pero el primer paso es recoger información des del usuario obtenido para intentar ubicar el archivo del código de desactivación. Si hay dudas sobre lo que se puede o no hacer siempre se puede contactar con el admin en cuestión.

Al hacer un primer reconocimiento de las primeras cosas que suelo mirar es whoami para saber el user en el que estoy; nginx en este caso y bash\_history, a ver que se ha picado para recuperar lo que pueda ser interesante. Nada más verlo vemos que entra en:

*Var/www/html y el archivo que nos interesa resulta ser: hydra-encrypt.txt.*

Nos dirigimos directamente a esta ruta pero en un primer momento al hacer ls-la no aparece.

Tras mirar otras opciones y volverlo a intentar se muestra el ansiado archivo:

```
/var/www/html $ ls -la
total 124
drwxr-xr-x  1 nginx  nginx    4096 Feb 17 16:21 .
drwxr-xr-x  1 root   root     4096 Oct 31 14:42 ..
-rw-r--r--  1 nginx  nginx    2059 Feb 15 11:58 .hydra-encrypt.txt
-rw-r--r--  1 nginx  nginx  110201 Feb 13 16:39 index.jpg
-rw-----  1 nginx  nginx    3465 Feb 17 16:21 index.php
```

Cat al archivo y nos lo copiamos para estudiarlo que parecen unas coordenadas geográficas. Pienso ver claro la obtención de la flag. Buscar la primera inicial de los países así como hicimos en el reto anterior con los prefijos del listín telefónico.

```
/var/www/html $ cat .hydra-encrypt.txt
-51.2263816202, 8.10899805433
-3.396936473, 7.87198824054
45.1590246548, 7.93243330727
45.7384951953, -73.2066721802
-3.42714386964, -72.9107266853
-2.77172800229, 7.52185701112
19.1399952, -72.3570972
44.5607307927, -73.0205921546
43.6100611723, 6.58946301884
-2.73141067245, 8.27764655993
-50.3213413202, 7.07393246568
-51.2758314025, -73.091160021
-2.47453022387, -72.4698275544
44.2979255136, -72.4873645117
19.1399952, -72.3570972
-50.505288471, 7.6154200698
-2.77032857828, 8.45085972386
43.3953722545, 7.12287052714
45.8072900754, -73.1907339308
-2.95197936965, -72.2507948297
-3.37159885987, 7.61851969812
19.1399952, -72.3570972
44.9471915554, -71.7312374845
43.434079994, 7.05564264826
-3.77755921359, 7.3140029803
-2.1765448219, -72.9980908924
45.5157039055, -72.0750205454
-2.6665636247, -71.758301384
-52.4282156352, -73.7745944789
-50.711316091, 8.37083156669
-2.51838084051, 7.54880895033
19.1399952, -72.3570972
45.0778663225, -72.5092560673
-3.09237153981, -71.5875397405
-2.54013043815, 8.29075062273
-51.2650141235, 7.38182033986
-51.3843804847, -72.6927837569
-3.47113449173, -73.2910711802
19.1399952, -72.3570972
43.951979572, 7.34734479231
45.0774665767, -72.6653555968
-1.64013868935, -71.880258046
-2.5651543193, 7.15699499792
-51.1302541808, 6.61409584651
-51.6645314915, -72.2889667536
19.1399952, -72.3570972
50.8557663054, 7.86605255465
```

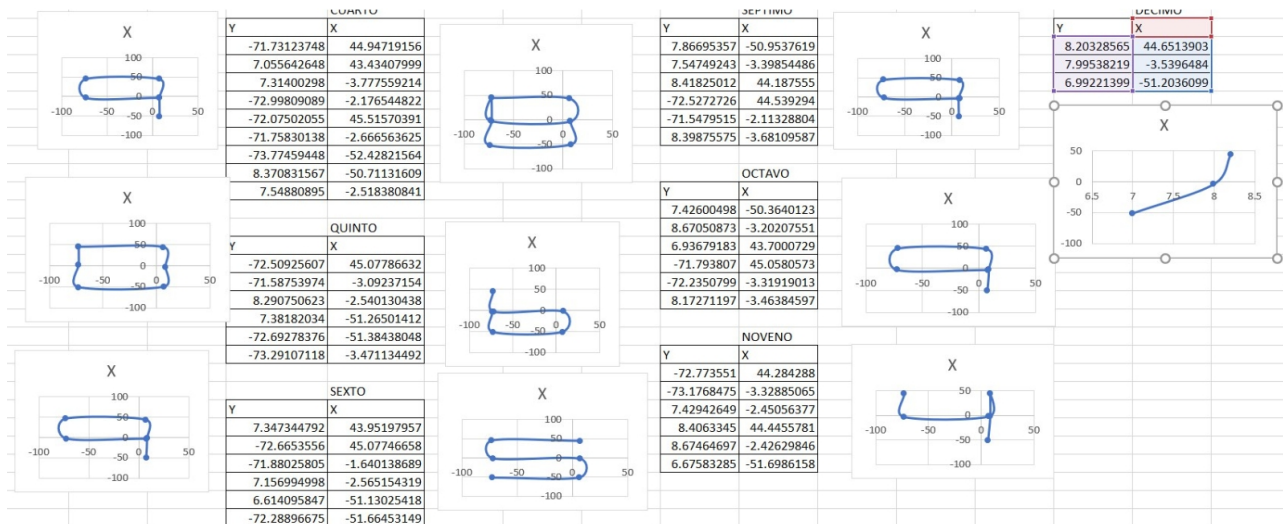
Craso error...Algunos no son países, es mar...Océano Atlántico Sur para ser exactos. OMG!

A partir de aquí vienen ralladas varias con ideas bastante locas. Mirar a ver si es un morse en el que el mar son los puntos y los países las rallas. Pensar si el mar son espacios y solo había que contar con la inicial de los países. Ver que hay un país que se repite sistemáticamente (Haití coordenada



19.1399952, -72.3570972) y pensar en funciones matemáticas a partir de formas triangulares, hexágonos y demás. Intentar transformar las coordenadas en hex para ver si forma alguna imagen y algunas barbaridades más que no vienen al caso porque no me fueron de utilidad xD.

Al final no eran coordenadas geográficas, pero si seguías los puntos que marcaban estas coordenadas daban como resultado figuras numéricas separadas por las coordenadas de Haití. Tela, telita tela, esto si que es un cifrado original y creativo! Este no lo encuentras aunque te surfees toda la red jaja.



Ingresamos el código en la web facilitada al inicio de este reto. Mencionada en el enunciado de la misión: <http://34.247.69.86/universomarvel/episodio3/index.php> 909865994..mmm ¿Pero cuál es el último? Probamos con coma, barra y no funciona. Pero todo són números! Debe ser 7 o 1. Y al ingresar 9098659941 obtenemos nuestra querida flag!!

**Enhorabuena, has parado el ataque. La flag es:**  
**UAM{e6570888dfb444f3bf2b50f6955b8eb5}**

Que si realizamos el decrypt en md5 es:

**Found : GG\_U\_Stopped\_the\_attack**  
 (hash = e6570888dfb444f3bf2b50f6955b8eb5)

Gracias admins por el esfuerzo en estas pruebas que nos hacen tener la mente activa, aprender y pasar un buen rato!

**Autoría: Arsenics**