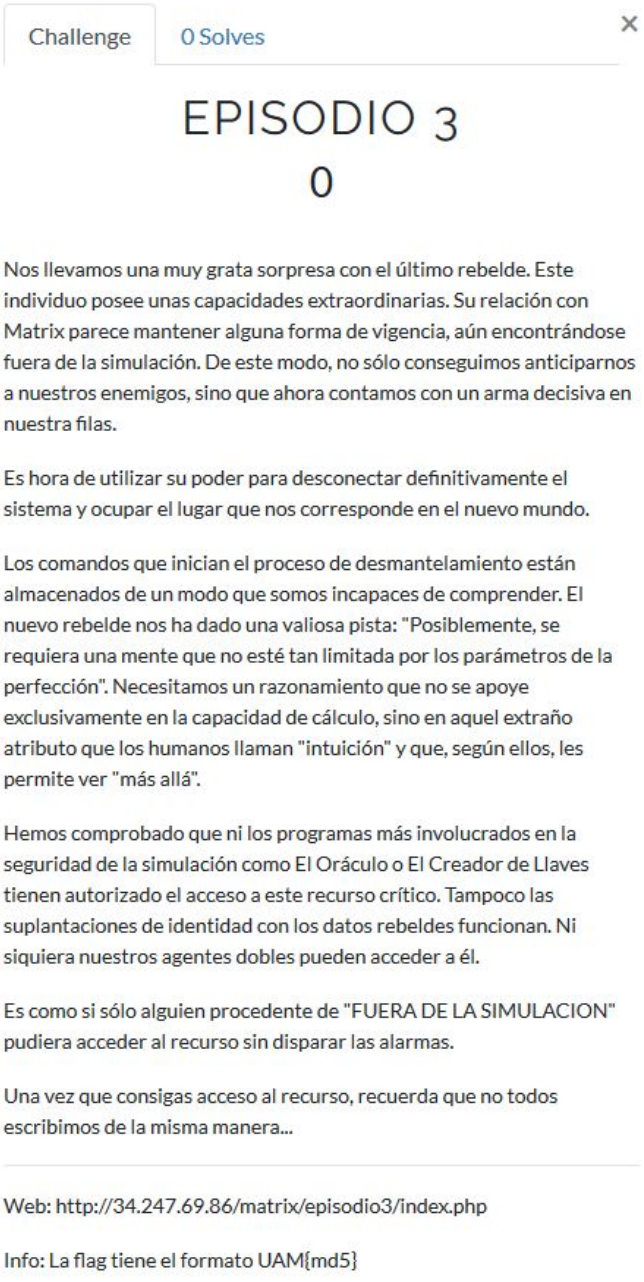
Matrix - Episodio 3

UAM CTF 2019-5-15

El reto

https://unaalmes.hispasec.com/challenges#EPISODIO%203



Challenge | 0 Solves

EPISODIO 3

0

Nos llevamos una muy grata sorpresa con el último rebelde. Este individuo posee unas capacidades extraordinarias. Su relación con Matrix parece mantener alguna forma de vigencia, aún encontrándose fuera de la simulación. De este modo, no sólo conseguimos anticiparnos a nuestros enemigos, sino que ahora contamos con un arma decisiva en nuestra filas.

Es hora de utilizar su poder para desconectar definitivamente el sistema y ocupar el lugar que nos corresponde en el nuevo mundo.

Los comandos que inician el proceso de desmantelamiento están almacenados de un modo que somos incapaces de comprender. El nuevo rebelde nos ha dado una valiosa pista: "Posiblemente, se requiera una mente que no esté tan limitada por los parámetros de la perfección". Necesitamos un razonamiento que no se apoye exclusivamente en la capacidad de cálculo, sino en aquel extraño atributo que los humanos llaman "intuición" y que, según ellos, les permite ver "más allá".

Hemos comprobado que ni los programas más involucrados en la seguridad de la simulación como El Oráculo o El Creador de Llaves tienen autorizado el acceso a este recurso crítico. Tampoco las suplantaciones de identidad con los datos rebeldes funcionan. Ni siquiera nuestros agentes dobles pueden acceder a él.

Es como si sólo alguien procedente de "FUERA DE LA SIMULACION" pudiera acceder al recurso sin disparar las alarmas.

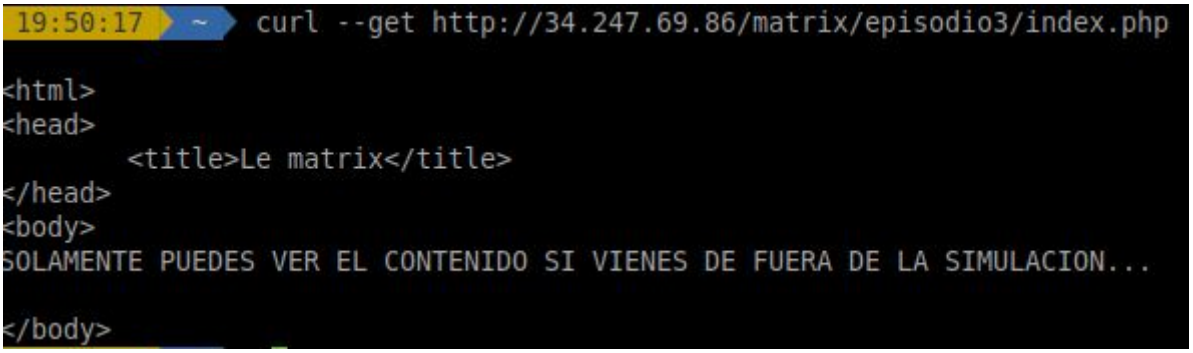
Una vez que consigas acceso al recurso, recuerda que no todos escribimos de la misma manera...

Web: http://34.247.69.86/matrix/episodio3/index.php

Info: La flag tiene el formato UAM{md5}

La web y los headers

Vamos a ver qué hay en esa web… http://34.247.69.86/matrix/episodio3/index.php



¿Venir de fuera de la simulación? ¿A qué se refiere?

Tras probar a escanear puertos, lanzar dirsearch y comerme el ban de 2 minutos varias veces (y hacer un poco el mal con proxychains, pero poco @devploit xDD), usando nikto y algunas cosas más… sin éxito, pruebo con las cabeceras.

https://en.wikipedia.org/wiki/List_of_HTTP_header_fields

Aquí encontramos algo interesante...

> **X-Forwarded-For:** A de facto standard for identifying the originating IP address of a client connecting to a web server through an HTTP proxy or load balancer. Superseded by Forwarded header.

Esta cabecera identifica el origen de la petición. ¿Cómo le digo que vengo de fuera de la simulación? Probando con diferentes ips y textos no cambia nada, solo veremos el contenido *si vienes de "FUERA DE LA SIMULACION"*, como nos dice la pista.

Ya que estamos probando cosas, voy a decirle que vengo de "FUERA DE LA SIMULACION"

¡Ehhh, tenemos una imagen!

La imagen

http://34.247.69.86/matrix/episodio3/iuo1h2eipu1h2ieuo12h890dhas89hd9i1n2opudniukbnaksfjbnahjklfbu12981hfi1.jpg

Si os fijáis bien en el código podréis ver a la rubia del vestido rojo y algo que llama la atención a simple vista: hay números en blanco en vez de el verde normal del resto.

Con un editor de imágenes, como este online: www.photopea.com podemos aislar estos números blancos ajustando un poco los niveles, haciendo que todos los tonos por debajo del blanco, sean más oscuros:

10101111100

Al mirar la imagen con steghide…

```
20:05:43 ~ steghide info iuo1h2eipu1h2ieuo12h890dhas89hd9i1n2opudniukbnaksfjbnahjklfbu12981hfi1.jpg
"iuo1h2eipu1h2ieuo12h890dhas89hd9i1n2opudniukbnaksfjbnahjklfbu12981hfi1.jpg":
  formato: jpeg
  capacidad: 33,5 KB
Intenta informarse sobre los datos adjuntos? (s/n) s
Anotar salvoconducto:
steghide: no pude extraer ningn dato con ese salvoconducto!
```

...parece que tenemos algo, y si usamos estos números como clave, obtenemos un archivo.

```
20:35:59 ~ steghide --extract -p 10101111100 -sf iuo1h2eipu1h2ieuo12h890dhas89hd9i1n2opudniukbnaksfjbnahjklfbu12981hfi1.jpg
anot los datos extrados e/"flag.txt".
```

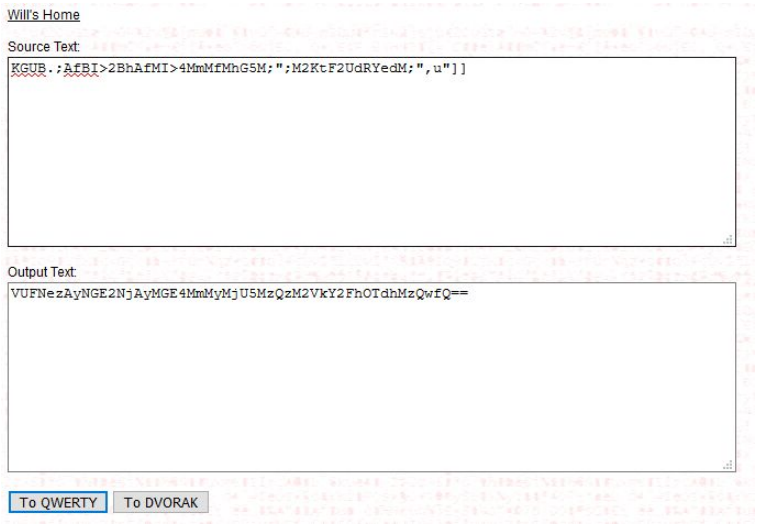
flag.txt

```
20:36:06 ~ cat flag.txt
KGUB.;AfBI>2BhAfMI>4MmMfMhG5M;";M2KtF2UdRYedM;",u"]]
```

Tiene el aspecto de un código esotérico como malbolge o befunge, pero nada funciona. Tampoco encuentro codificación alguna que me ayude :(

Hasta que volvemos a las pistas: *Una vez que consigas acceso al recurso, recuerda que no todos escribimos de la misma manera...*

La primera vez que leí la pista ya pensé en codificaciones y teclados pero no me acordé. Estuve perdiendo el tiempo buscando… pero releyendo el enunciado me acordé de esto, y probando el traductor de dvorak a qwerty de http://wbic16.xedoloh.com/dvorak.html



¡Apesta a base64!

```
20:48:23 ~ echo VUFNezAyNGE2NjAyMGE4MmMyMjU5MzQzM2VkY2FhOTdhMzQwfQ== | base64 -d
UAM{024a66020a82c22593433edcaa97a340}%
```

¡Yeah!

Flag

UAM{024a66020a82c22593433edcaa97a340}

Conclusión

Ha sido un reto *técnicamente más fácil pero a nivel de pensamiento lateral más jodida*. ¡Era cierto! Como dato adicional, sólo hizo falta una cerveza. Ha sido un reto más asequible y bastante chulo, volviendo a los retos más variados de antes, que parece que estos últimos han sido bastante duros… y nos bajan un poquito el listón técnico :)

¡Gracias por crear estos retos!

José Ángel Sánchez
@_j0n3