Writeup – UAM – DRAGON BALL

EPISODIO 1

950

Célula, desde un universo paralelo, ha vuelto al futuro de nuestros héroes en búsqueda de su cuerpo perfecto, para ello necesita una información que sólo una persona es capaz de proporcionarle. En la búsqueda de la información, y tras un enfrentamientos con uno de nuestros héroes, Célula consigue escapar con vida jurando que volvería con el cuerpo perfecto y eliminaría la Tierra por completo.

Debes ayudar a los héroes de la Tierra con el fin de evitar que Célula consiga su objetivo. Llegan a la conclusión de que han de encontrar a la persona buscada por Célula antes que éste. Para ello, y con la ayuda del radar de Bulma, deciden ir en busca de las bolas de dragón para conocer quién es el objetivo de Célula a través de Shenron. ¿Serás capaz de conseguir el nombre?

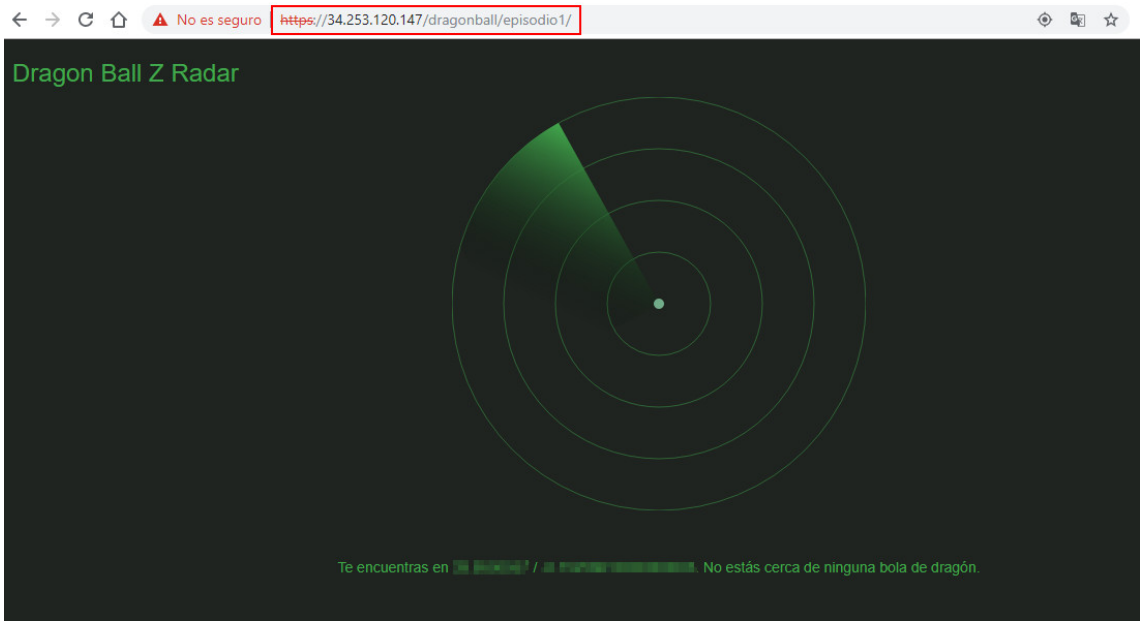
** Es necesario que deis acceso a vuestra ubicación para que funcione correctamente **

Servicio contra el que comprobar el nombre: 34.253.120.147:9999
Radar de Bulma: https://34.253.120.147/dragonball/episodio1/

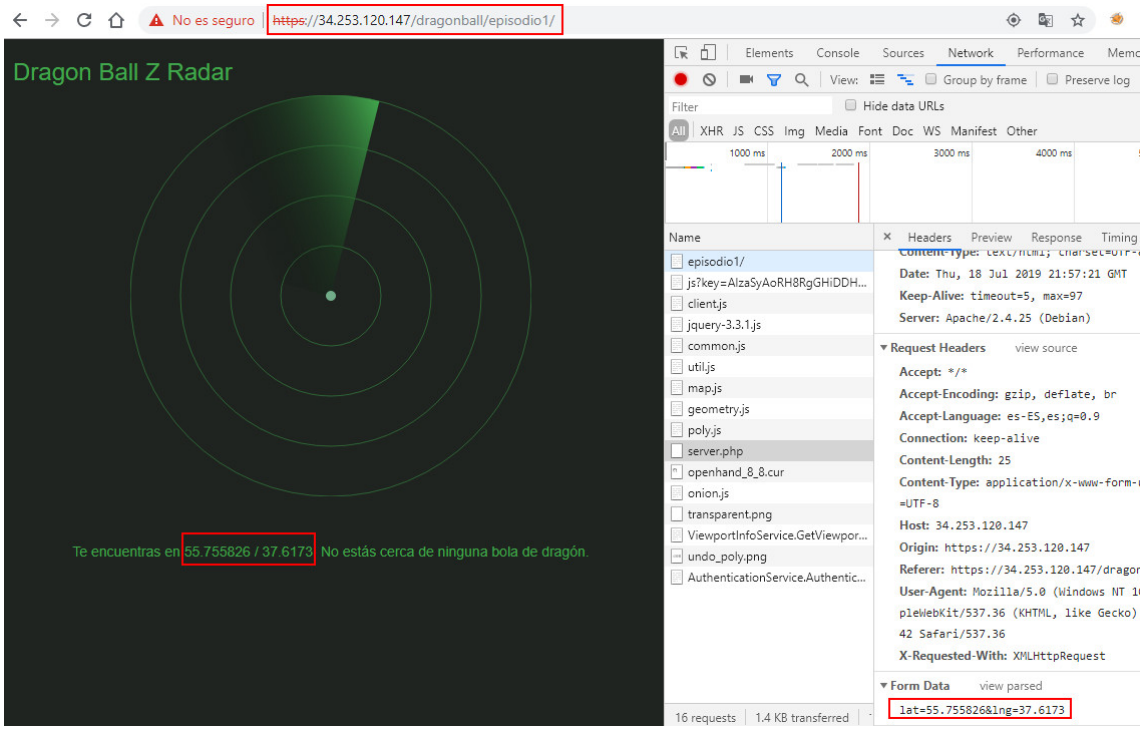
Info: La flag tiene el formato UAM{md5}

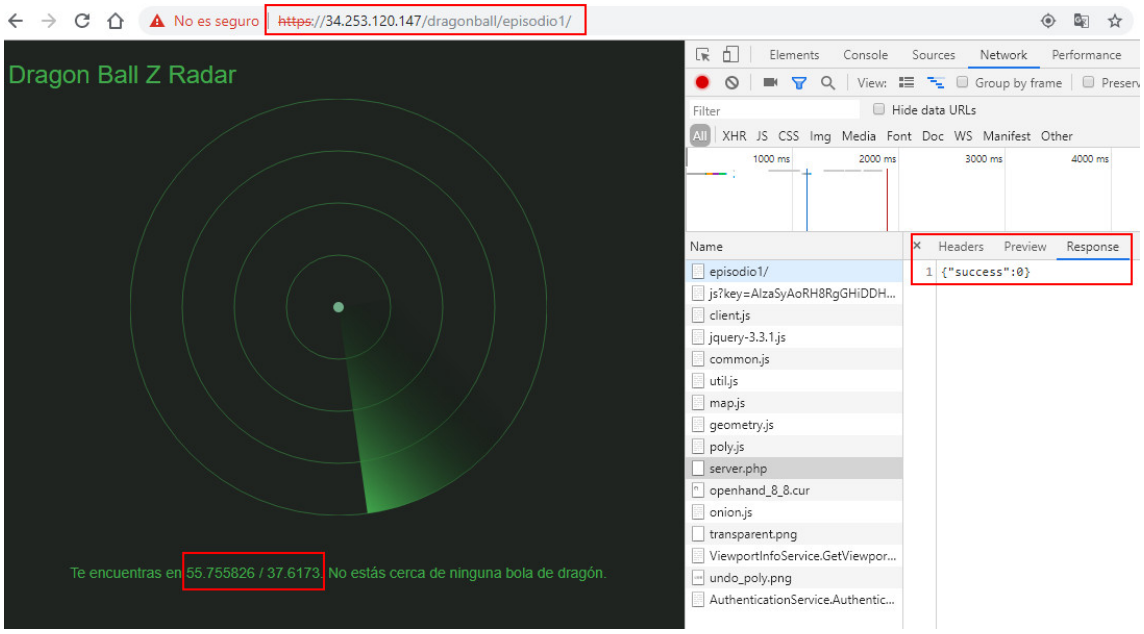
Para los fans como yo de Dragon Ball, tendremos la oportunidad de buscar las siete bolas del dragón por todo el planeta, conseguir el nombre del personaje y con este, la flag.

Accediendo al radar de Bulma podemos ver lo siguiente:



Si observamos el código del sitio, la aplicación hace una petición con las coordenadas a un archivo llamado “server.php” donde comprueba las coordenadas y nos devuelve una información en json.





Aunque podríamos ir cambiando las coordenadas desde el navegador, nos volveríamos locos ir introduciendo coordenadas por coordenadas de cada ciudad del mundo.

Por este caso, me monté un sencillo script en **Bash Scripting** que básicamente lo que hace es ir haciendo petición POST con las variables "**lat**" y "**lng**" y sustituyendo su valor por el de las coordenadas… Ahora nos falta lo importante, conseguir un listado de la geolocalización de todas las ciudades del mundo. xD

Pues tras un buen rato buscando por la red, encontré esto https://dev.maxmind.com/geoip/geoip2/geolite2/ una base de datos (también en Excel) con un listado de 1.048.576 de coordenadas (casi nada). De este listado, sólo me he quedado con las columnas longitud y latitud, las he pasado a un archivo de texto para después utilizarlo con el script.

```
C:\Users\M3n0s_D0n4ld\Downloads\CTF\UAM\dragonball2
> cat coordenadas-ok.txt | more
55.6108&lng=37.9722
55.6125&lng=11.7703
55.6139&lng=12.3895
55.6154&lng=12.3518
55.6167&lng=12.3500
55.6167&lng=-3.5167
55.6167&lng=40.6667
55.6180&lng=9.3010
55.6185&lng=11.2145
55.6194&lng=-4.6551
55.6211&lng=8.4807
55.6223&lng=-4.5008
55.6268&lng=8.2876
55.6299&lng=9.0824
55.6314&lng=13.7062
55.6325&lng=13.0714
55.6333&lng=12.3667
55.6333&lng=13.4833
55.6333&lng=-3.1167
55.6339&lng=11.8712
55.6352&lng=12.6489
55.6362&lng=-4.7859
55.6368&lng=11.3172
```

Este es código del script: (**Aviso!** Es bastante cutre el código, lo sé, pero funciona!)

dragonball2.sh

```
#!/bin/bash

url="https://34.253.120.147/dragonball/episodio1/server.php"


#!/bin/bash
intentos=0
for line in $(cat coordenadas-ok.txt); do
    echo $line >> resultado2.log
    resultado=$(curl --insecure -d "lat=$line" $url >> resultado2.log)
    echo $resultado >> resultado2.log
    let intentos=$intentos+1
    if [[ $intentos -eq 10 ]]; then
        sleep 5
        let intentos=0
    fi
done
```

Con el script ya en marcha solo tendremos que esperar a que vaya probando todas las coordenadas y empezará a mostrarnos las bolas del dragón que va encontrando:

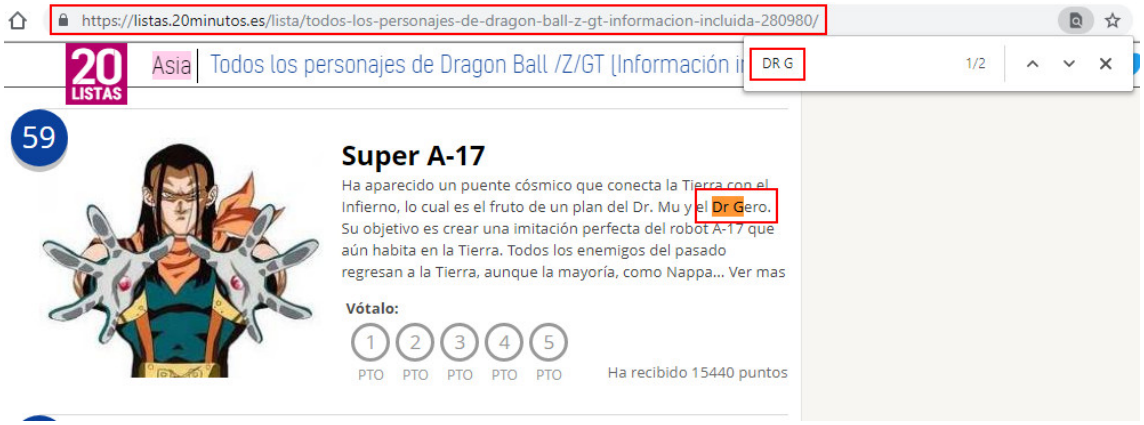
```
C:\Users\M3n0s_D0n4ld\Downloads\CTF\UAM\dragonball2
> cat resultado.log |grep stars
{"stars":2,"city":"Ronda","lat":36.745473,"lng":-5.161438,"locInRadar":"<circle cx=\"250\" cy=\"125\" r=\"10\"><\/circle>"}
{"stars":3,"city":"Guam","lat":13.440439,"lng":144.779184,"locInRadar":"<circle cx=\"125\" cy=\"270\" r=\"10\"><\/circle>"}
{"stars":7,"city":"Odessa","lat":46.482921,"lng":30.722892,"locInRadar":"<circle cx=\"30\" cy=\"280\" r=\"10\"><\/circle>"}
{"stars":4,"city":"Ulan Bator","lat":47.906641,"lng":106.895085,"locInRadar":"<circle cx=\"50\" cy=\"240\" r=\"10\"><\/circle>"}
```

Con estas 4 bolas fueron suficiente para poder resolver el reto…. Ya que contaba con la bola 2, 3, 4 y 7 (bolas del medio y la última).

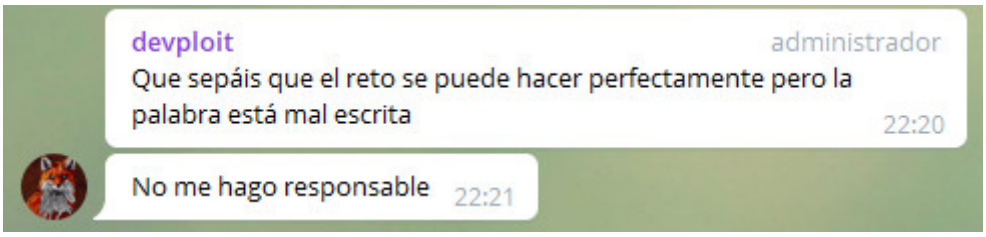
Visto que el reto consiste en descubrir el personaje de la serie, ponemos las primeras iniciales en el orden del número de estrellas de las bolas, quedando de esta manera.

_ R G U _ _ O

Con las 4 bolas en mi poder, paso a contrastar con la lista de todos los personajes de Dragon Ball en una web. Utilizando el buscador, nos encontramos con esto:

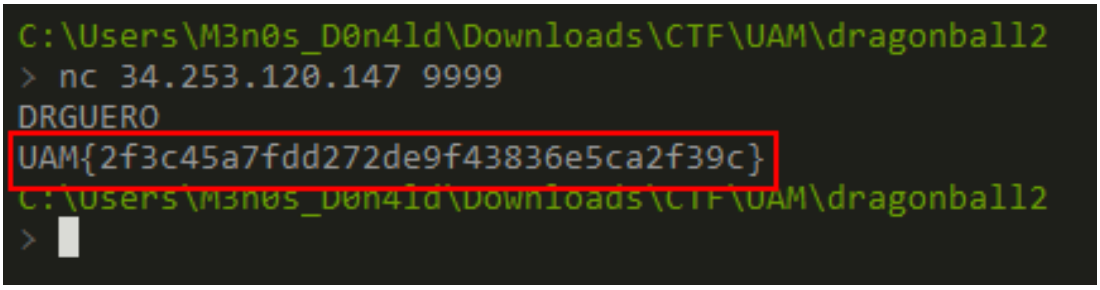


Si contamos el número de caracteres solo tiene 6, cuando las bolas son 7, pero recordé la pista que lanzó **@devploit**:



Por lo que el nombre del personaje podría ser: **D R G U E R O**

¡Por probar que no quede! Lanzamos el nombre al comprobador **34.253.120.147:9999** utilizando Netcat:



¡Y reto superado!