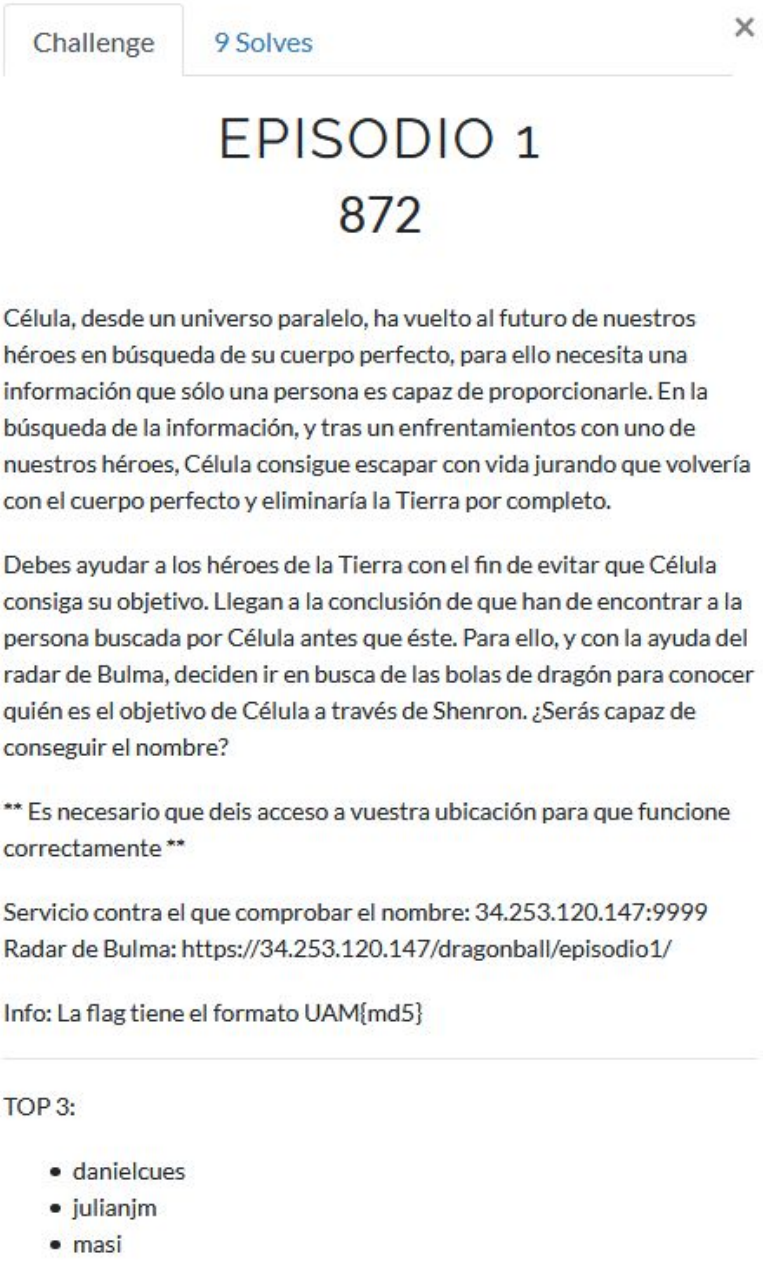
Dragon Ball - Episodio 1

UAM CTF 2019-7-15

El reto

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



Challenge | 9 Solves

EPISODIO 1

872

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}

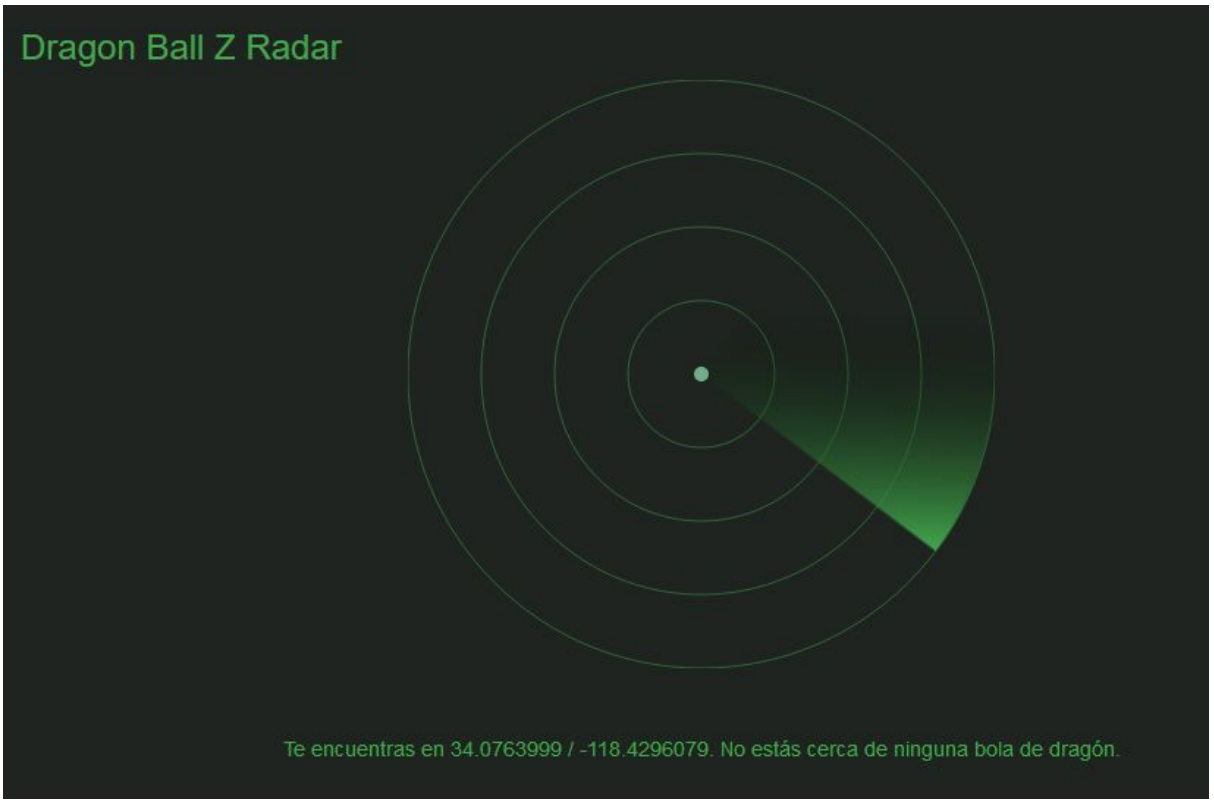
TOP 3:

- danielcues
- julianjm
- masi

Tenemos que buscar a una persona antes de que Célula la encuentre, y nos dan un radar y un servicio contra el que comprobar el nombre.

El radar

Entramos en la web y nos solicitan ubicación, pero parece que no tenemos ninguna bola cerca...



Si abrimos la consola del navegador y en el apartado de red miramos las peticiones, podemos ver una llamada a https://34.253.120.147/dragonball/episodio1/server.php con los parámetros de longitud y latitud que tenemos en el navegador.

hacemos un curl con los datos de la petición que realiza la web, poniendo una latitud y longitud al azar.

```
curl http://34.253.120.147/dragonball/episodio1/server.php --data "lat=0&lng=0" -k
```

(usamos -k para ignorar la validez del certificado ssl autofirmado)

La respuesta es un bonito: `{"success":0}`

Tras probar a enviar las coordenadas de varias ciudades grandes, no encuentro nada. Voy a bajarme una base de datos de ciudades con sus coordenadas para que me automatice las peticiones… y encuentro una en https://simplemaps.com/data/world-cities con 13k ciudades. Me descargo el zip y extraigo un csv que voy a procesar con un pequeño script de bash. Tiene este aspecto:

```
"city","city_ascii","lat","lng","country","iso2","iso3","admin_name","capital","population","id"
"Malishevë","Malisheve","42.4822","20.7458","Kosovo","XK","XKS","Malishevë","admin","","1901597212"
"Prizren","Prizren","42.2139","20.7397","Kosovo","XK","XKS","Prizren","admin","","1901360309"
"Zubin Potok","Zubin Potok","42.9144","20.6897","Kosovo","XK","XKS","Zubin Potok","admin","","1901608808"
"Kamenicë","Kamenice","42.5781","21.5803","Kosovo","XK","XKS","Kamenicë","admin","","1901851592"
"Viti","Viti","42.3214","21.3583","Kosovo","XK","XKS","Viti","admin","","1901328795"
"Shtërpcë","Shterpce","42.2394","21.0272","Kosovo","XK","XKS","Shtërpcë","admin","","1901828239"
"Shtime","Shtime","42.4331","21.0397","Kosovo","XK","XKS","Shtime","admin","","1901598505"
"Vushtrri","Vushtrri","42.8231","20.9675","Kosovo","XK","XKS","Vushtrri","admin","","1901107642"
"Dragash","Dragash","42.0265","20.6533","Kosovo","XK","XKS","Dragash","admin","","1901112530"
```

Nos interesa el primer campo (city), el tercero (lat) y el cuarto (lon)

Con un script en bash leo cada línea del csv y la parseo, guardando en variables estas tres cosas

```bash
#!/bin/env bash

while read -r line
do
    city=$(echo $line | awk -F',' '{printf "%s", $1}' | tr -d '"')
    lat=$(echo $line | awk -F',' '{printf "%s", $3}' | tr -d '"')
    lon=$(echo $line | awk -F',' '{printf "%s", $4}' | tr -d '"')

    echo -n $city @ $lat $lon
    curl "https://34.253.120.147/dragonball/episodio1/server.php" --data "lat=$lat&lng=$lon" -k
    echo
done < worldcities.csv
```

ejecuto el script y voy guardando las respuestas en un fichero:

```
sh cities.sh > result_cities.txt
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100    28  100    13  100    15     73     84 --:--:-- --:--:-- --:--:--   157
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
```

Tras poco más de 50 minutos, lo único que consigo es una respuesta válida: la estrella 6 en Reikiavik, en las coordenadas 64.145144 -21.942496

¿Solo una bola? ¿Acaso querrán que peinemos el planeta? Devploit nos ha comentado que el radar tiene una precisión de aproximadamente 1 grados, que son, dependiendo del lugar del planeta, ~100km de radio.

Voy a hacer un pequeño script en bash que peine el planeta…

Tenemos latitudes entre -85 y 85 grados y longitudes entre -180 y 180, así que hagamos un par de bucles y recorramos el planeta… en diminutos trocitos y millones de requests, pero voy a ser bueno y lanzaré solo un proceso, que eso de hacer brute force contra un server, con todos los que somos y lo brutos que se pondrán algunos, esta UAM veremos a servers y admins sudar xDDD

```
#!/bin/env bash

for lat in $(seq -85 .01 85); do
    for lon in $(seq -180 .01 180); do
        curl https://34.253.120.147/dragonball/episodio1/server.php --data "lat=$lat&lng=$lon" -k
        echo "$lat $lon"
    done
done
```

Aquí solo tenemos una cosa interesante: cómo hacer un bucle en bash con un step decimal… sec [desde] [paso/step] [hasta]

Tras un rato probándolo y haciendo algunos cálculos por la cantidad de requests y el tiempo que tardaría el script, decido pararlo. No puede ser necesario peinar el planeta.

Han pasado algunos días y el server ha petado varias veces. Durante este tiempo los admins, como medida paliativa ante la escasez de resultados por ataque de denegación que estamos haciendo entre todos al lanzar tantas peticiones, deciden ampliar el radio de acción del radar. Creo que fue una buena decisión.

No voy a hacer ninguna cosa más compleja aún, puedo lanzar mi script original otra vez, a ver si con el aumento de radio funciona mejor y… ¡vaya! obtengo todas las bolas en un rato :D

```
1: Nabatiye et Tahta @ 33.3833 35.4500{"stars":1,"city":"Damasco","lat":33.513645,"lng":36.276762,"locInRadar":"<circle cx=\"150\" cy=\"150\" r=\"10\"><\/circle>"}
2: Marbella @ 36.5166 -4.8833{"stars":2,"city":"Ronda","lat":36.745473,"lng":-5.161438,"locInRadar":"<circle cx=\"250\" cy=\"125\" r=\"10\"><\/circle>"}
3: Hagåtña @ 13.4745 144.7504{"stars":3,"city":"Guam","lat":13.440439,"lng":144.779184,"locInRadar":"<circle cx=\"125\" cy=\"270\" r=\"10\"><\/circle>"}
4: Ulaanbaatar @ 47.9167 106.9166{"stars":4,"city":"Ulan Bator","lat":47.906641,"lng":106.895085,"locInRadar":"<circle cx=\"50\" cy=\"240\" r=\"10\"><\/circle>"}
5: Stockholm @ 59.3508 18.0973{"stars":5,"city":"Estocolmo","lat":59.328694,"lng":18.068505,"locInRadar":"<circle cx=\"320\" cy=\"270\" r=\"10\"><\/circle>"}
6: Reikiavik @ 64.145144 -21.942496
7: Tiraspol @ 46.8531 29.6400{"stars":7,"city":"Odessa","lat":46.482921,"lng":30.722892,"locInRadar":"<circle cx=\"30\" cy=\"280\" r=\"10\"><\/circle>"}
```

El nombre

Si cogemos las primeras letras de las ciudades en las que hemos encontrado las bolas, ordenando por el número de estrellas obtenemos:

DRGUERO

Y si comprobamos este nombre contra el servicio…

```
echo DRGUERO | nc 34.253.120.147 9999
```

Obtenemos nuestra….

Flag

UAM{2f3c45a7fdd272de9f43836e5ca2f39c}

Décima posición pero reto superado!

Conclusión

El reto ha estado chulo pero quizá forzarnos a hacer brute force contra un servidor web pequeñito ha servido sobre todo para que nuestros admins se lo piensen antes de volver a crear una prueba donde tengamos que fundir un server a peticiones entre todos xDDD

También me doy cuenta de que podría haber procesado el csv para ordenarlo por población para acelerar la búsqueda, aunque tampoco ha tardado tanto.

Mis respetos para @danielcues, @julianjm, @masi y @asterixco, que consiguieron superar el reto cuando aún el rádar era una caca :D ¡Tengo ganas de ver vuestros writeups!

José Ángel Sánchez
@_j0n3