

Challenge

294 Solves



# Buckets of fun

## 100

<http://bucketsoffun-ctf.s3-website-us-east-1.amazonaws.com>

Author: scriptingislife

Flag

Submit

Tras entrar en la web nos encontramos que está protegida por una contraseña,

## Welcome to the challenge!

**Password**

Enter

Al probar con una contraseña aleatoria la web nos devuelve el siguiente mensaje

You won't be getting around this auth.

Tras probar varios métodos sin éxito para acceder al contenido protegido decidí buscar otro enfoque y centrarme en la url, ya que es la única web de todos los retos alojada en aws, al rato encontré esta web <https://medium.com/@cvignesh28/aws-s3-bucket-misconfiguration-c11e8f86e9a7> la cual nos explica como aprovechar los buckets de amazon mal configurados, para ello descargué awscli y tras loguearme con mis credenciales probe a acceder al bucket que nos dan y ...

```
[MacBook-Air-de-Juanjo: Buckets of fun juanjo$ aws s3 ls s3://bucketsoffun-ctf
2019-11-25 11:50:22          630 index.html
2019-11-25 11:50:22           25 youfoundme-asd897kjm.txt
```

podemos ver lo que contiene. El archivo .txt parece una flag, así que vamos a descargarlo.

```
[MacBook-Air-de-Juanjo: Buckets of fun juanjo$ aws s3 cp s3://bucketsoffun-ctf/youfoundme-asd897kjm.txt flag.txt  
download: s3://bucketsoffun-ctf/youfoundme-asd897kjm.txt to ./flag.txt
```

Vemos que contiene y obtenemos la flag.

**RITSEC{LIST\_HIDDEN\_FILES}**