

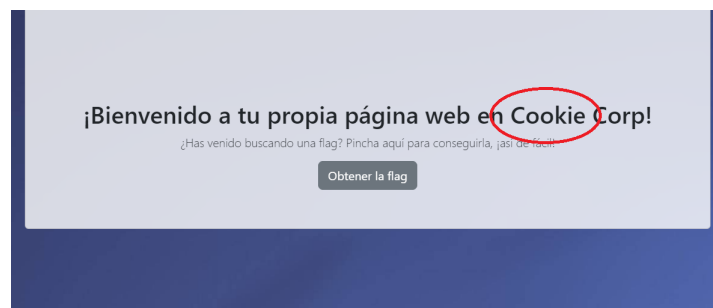
WriteUp Cookie Challenge

Fernando Rodríguez Martín - SUGUS

Al empezar este reto, lo primero que vemos es una pestaña de *login*, en la que no sabemos la contraseña.



Por tanto, lo más normal es intentar entrar como invitado, e intentar recabar información desde ahí. Lo primero que vemos al entrar es que la empresa es *Cookie Corp*, pista de que el reto tiene algo que ver con las *Cookies*.



Como vemos que no podemos hacer nada más en esta página, vamos a abrir las *DevTools* desde la página de *login*. Queremos mirar las cookies, por lo que nos iremos al apartado de **Aplicación** -> **Almacenamiento** -> **Cookies**, y vemos que tenemos una *cookie* de sesión y otra *cookie* de invitado.

Nombre	Valor	Domain	Path	Expires /...	Tamaño	HttpOnly	Secure	SameSite	SameParty	Partition...	Priority
guest	Z3Vlc3Q%3D	192.168...	/	2023-01...	15						Medium
PHPSESSID	8u9ud6k6sro4p3q36dfh9ajq2r	192.168...	/	Sesión	35						Medium

Normalmente, las *cookies* van **codificadas en Base64**, tal como especifica el **RFC** (*Request For Comments*) que define las *cookies*:

To maximize compatibility with user agents, servers that wish to store arbitrary data in a cookie-value SHOULD encode that data, for example, using Base64 [RFC4648].

Por tanto, lo lógico es pasar dicho valor por un decodificador de Base64 para ver su valor. Es importante ver que el % tiene un significado especial en las URL, ya que sirve para codificar caracteres especiales. (*tales como ' ' o '='*). Por tanto, el valor de la *cookie* **Z3Vlc3Q %3D**, es, en verdad, **Z3Vlc3Q=**.

URL Decode online

Input: Z3Vlc3Q%3D

Output: Z3Vlc3Q=

Ahora, si pasamos dicho valor por un decodificador de **Base64**, obtenemos:

Decode from Base64 format
Simply enter your data then push the decode button.

Input: Z3Vlc3Q%3D

Output: guest

Decode from Base64 format
Simply enter your data then push the decode button.

Input: Z3Vlc3Q=

Output: guest

Vemos que el valor de la *cookie* es **guest**. Por tanto, si el valor de la cookie es igual al nombre de la cookie, podemos pensar que funcionará igual si lo hacemos con la cookie del usuario **admin**:

Encode to Base64 format

Simply enter your data then push the encode button.

admin

To encode binaries (like images, documents, etc.) use the file upload form a little further down on this page.

UTF-8 Destination character set.

LF (Unix) Destination newline separator.

☐ Encode each line separately (useful for when you have multiple entries).

☐ Split lines into 76 character wide chunks (useful for MIME).

☐ Perform URL-safe encoding (uses Base64URL format).

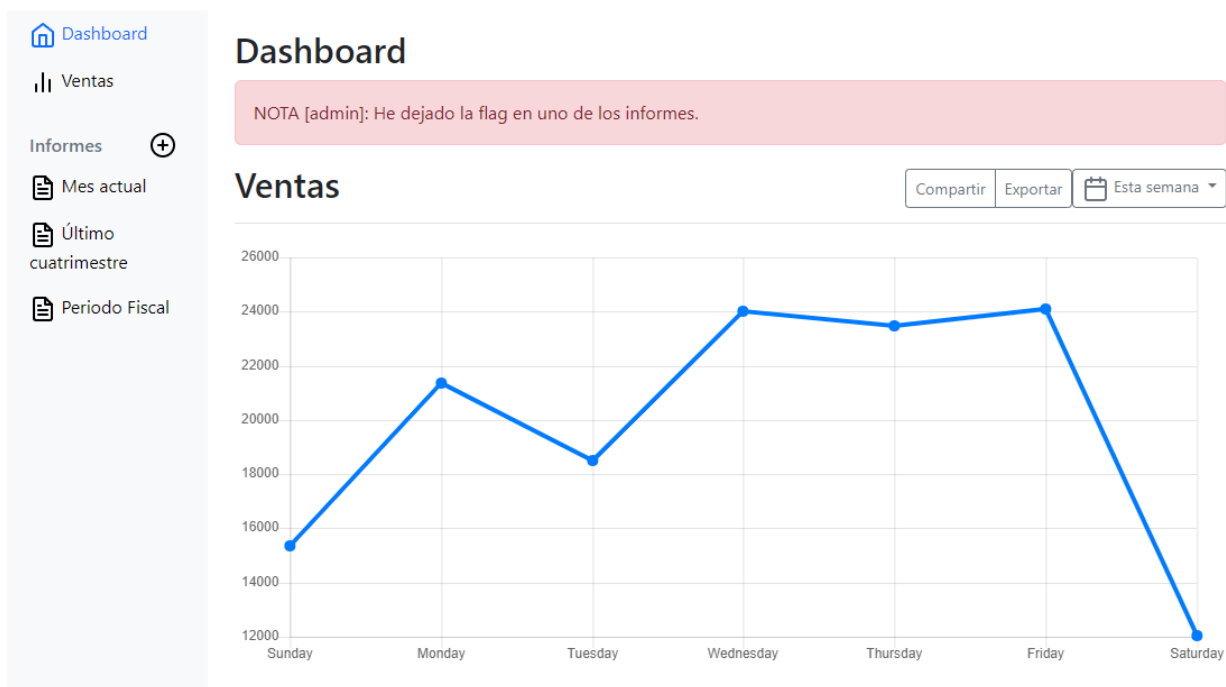
☒ Live mode OFF Encodes in real-time as you type or paste (supports only the UTF-8 character set).

> ENCODE < Encodes your data into the area below.

YWRtaW4=

Ahora, simplemente modificamos el valor de la cookie en *Almacenamiento*, e intentamos realizar un login:

Filtrar											
Mostrar solo cookies que tengan un problema											
Nombre	Valor	Domain	Path	Expires /...	Tamaño	HttpOnly	Secure	SameSite	SameParty	Partition...	Priority
admin	YWRtaW4=	192.168...	/	2023-01...	13						Medium



Por fin, hemos conseguido hacernos pasar por el administrador de **Cookie Corp.** Ahora, solo nos queda mirar uno de los informes (*cualquiera de los tres*) para conseguir la *flag*.