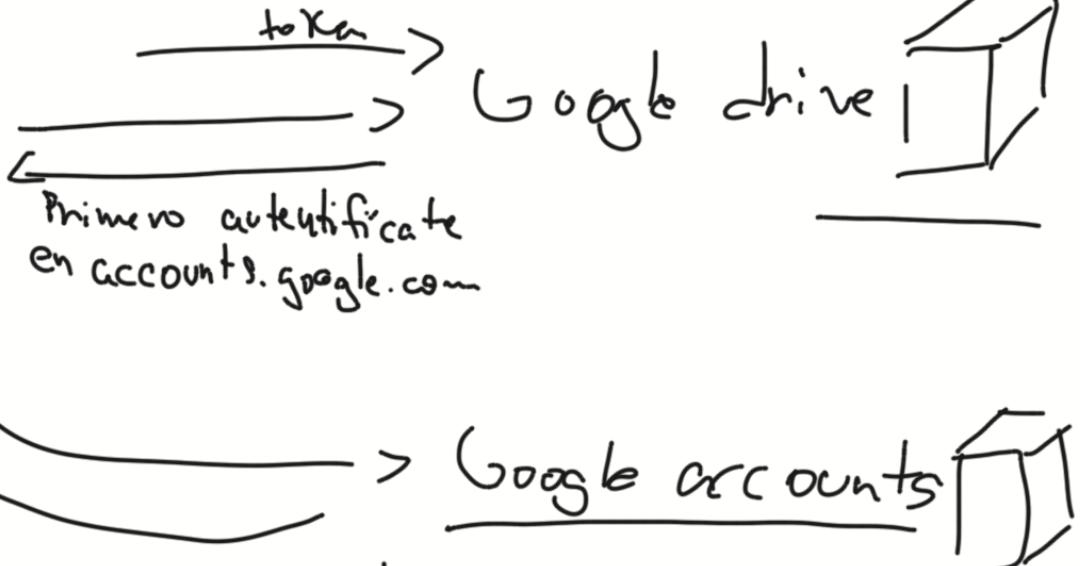


Seguridad en la Web - Parte 2



- 1) El servidor guarda mi contraseña en texto plano. Peor idea!!!
- 2) El servidor guarda el hash de mi contraseña. Mala idea!! Rainbow tables, misma clave, etc.
- 3) El serv. guarda mi contraseña "hasheada y salteada"
$$h(\text{clave} \parallel \text{salt}) \checkmark \checkmark$$
- 4) PBKDF2 $\checkmark \checkmark \checkmark$

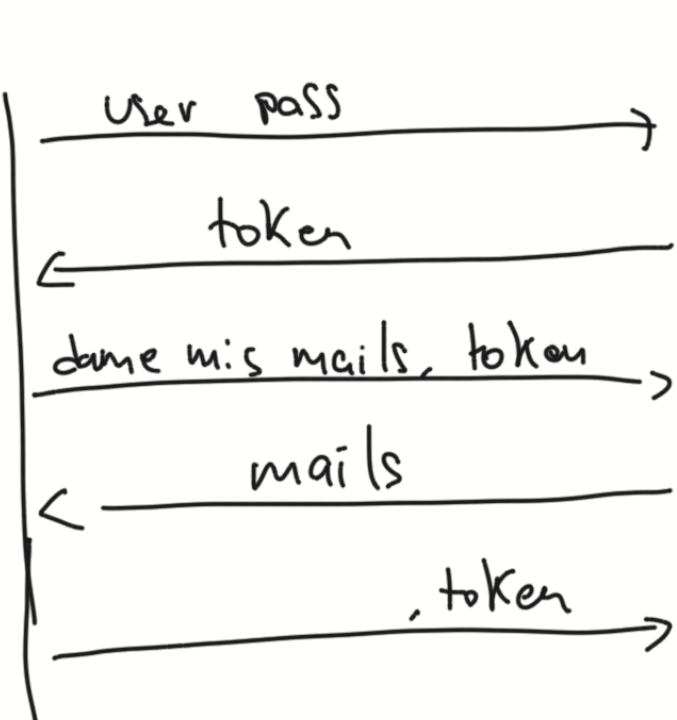
Problema con username
y password es la
AUDITABILIDAD



OAuth 2, pendiente



Guardar token como cookie



facebook.

1) Verificar ✓
2) Gen. token aleatorio
3) Guardar user, token

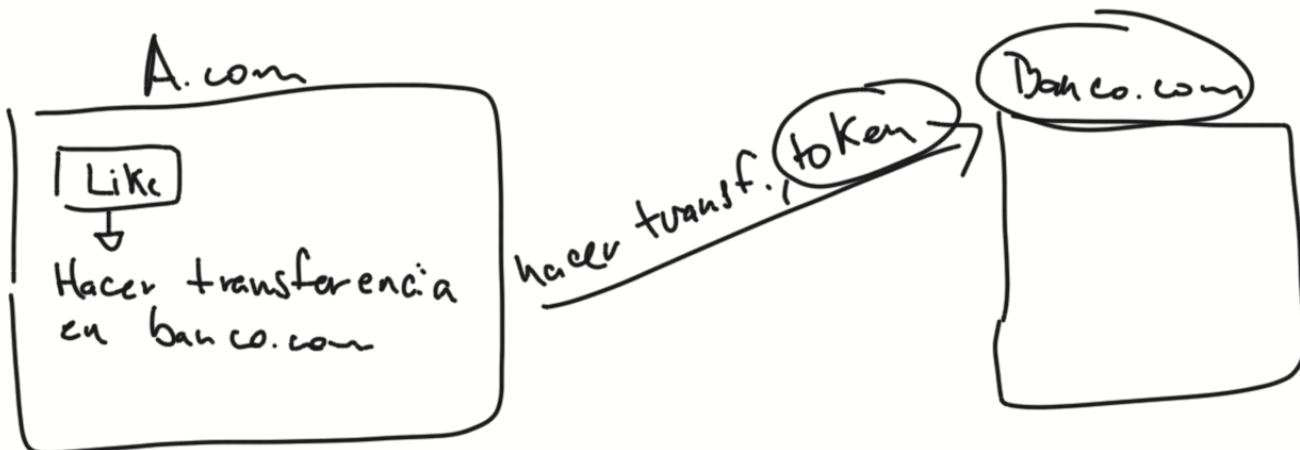
Tengo el token y corresponde al usuario? ✓



Cross-site request.

Cookies: Información que guarda mi navegador en relación a un sitio, y las "adjunta" en cada request que hace mi navegador a dicho sitio.

Cookies con Banco.com: token: ~~~~~



No conoce mis cookies con Banco.com.

Si embargo, si A.com le dice a mi navegador que haga un request a Banco.com, dicho request tendrá mis cookies con Banco.com.

Banco.com

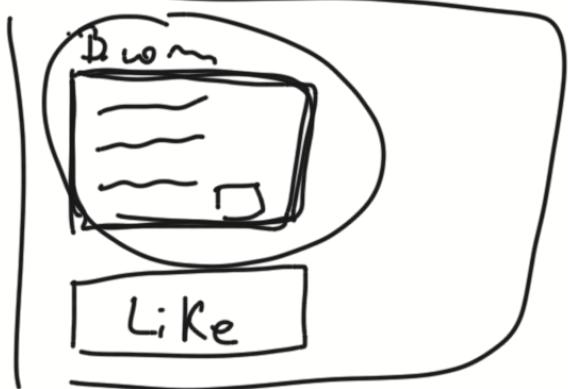


CSRF-token: Token aleatorio que se envía de Banco.com al cliente, y que el cliente tiene que incluir en su request.

g) adjuntar al hacer una transferencia.

→ Cross-site reference forgery

A.com

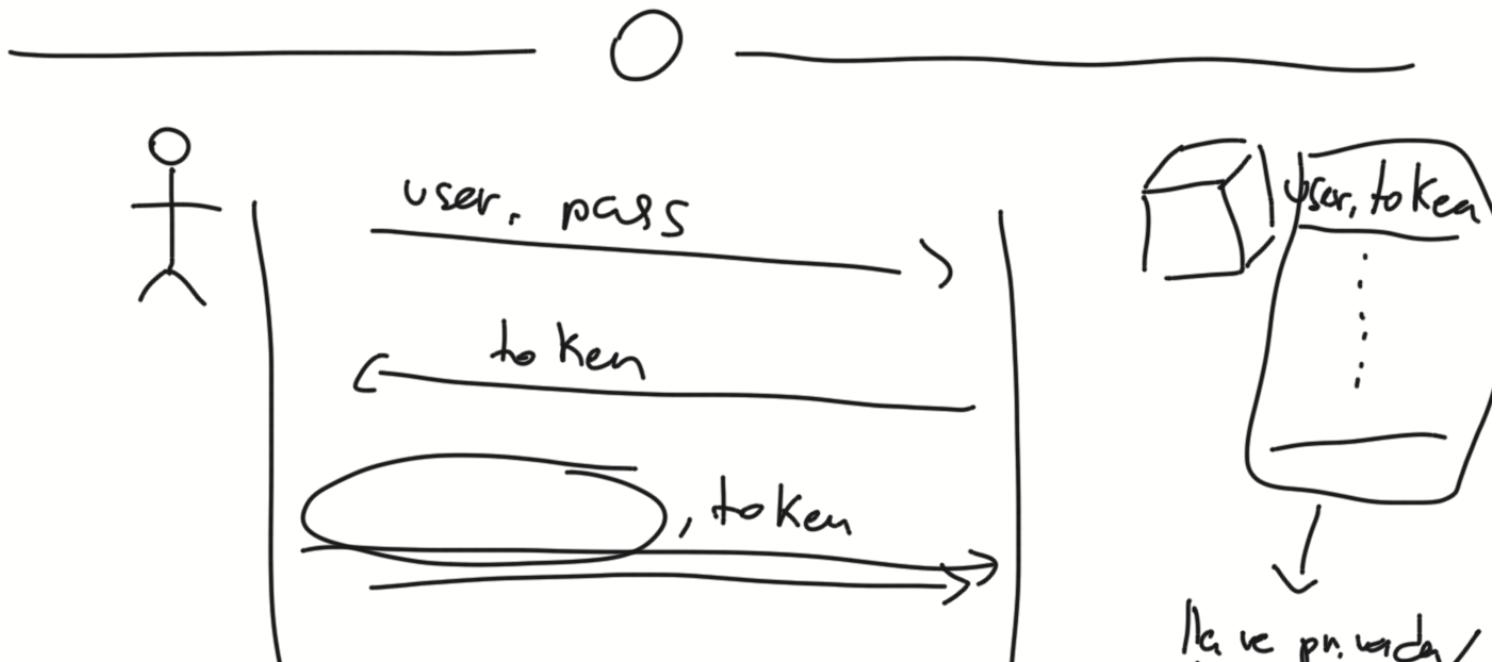


`<iframe src= >`
`<>`

El csrf_token se está reemplazando por el uso de cookies SAMESITE y HTTP-ONLY

↓
sólo se "adjunta" a requests que vienen del mismo sitio

→
No se pueden leer desde JS.



llave pública

El servidor se tiene que acordar de todos los tokens y a quienes pertenecen. Para evitar esto, podría dar al usuario un "token" con la información del usuario, que esté firmado por el servidor.

JWT

Jason Web Token