

AUDITORÍA DE UNA APLICACIÓN WEB:

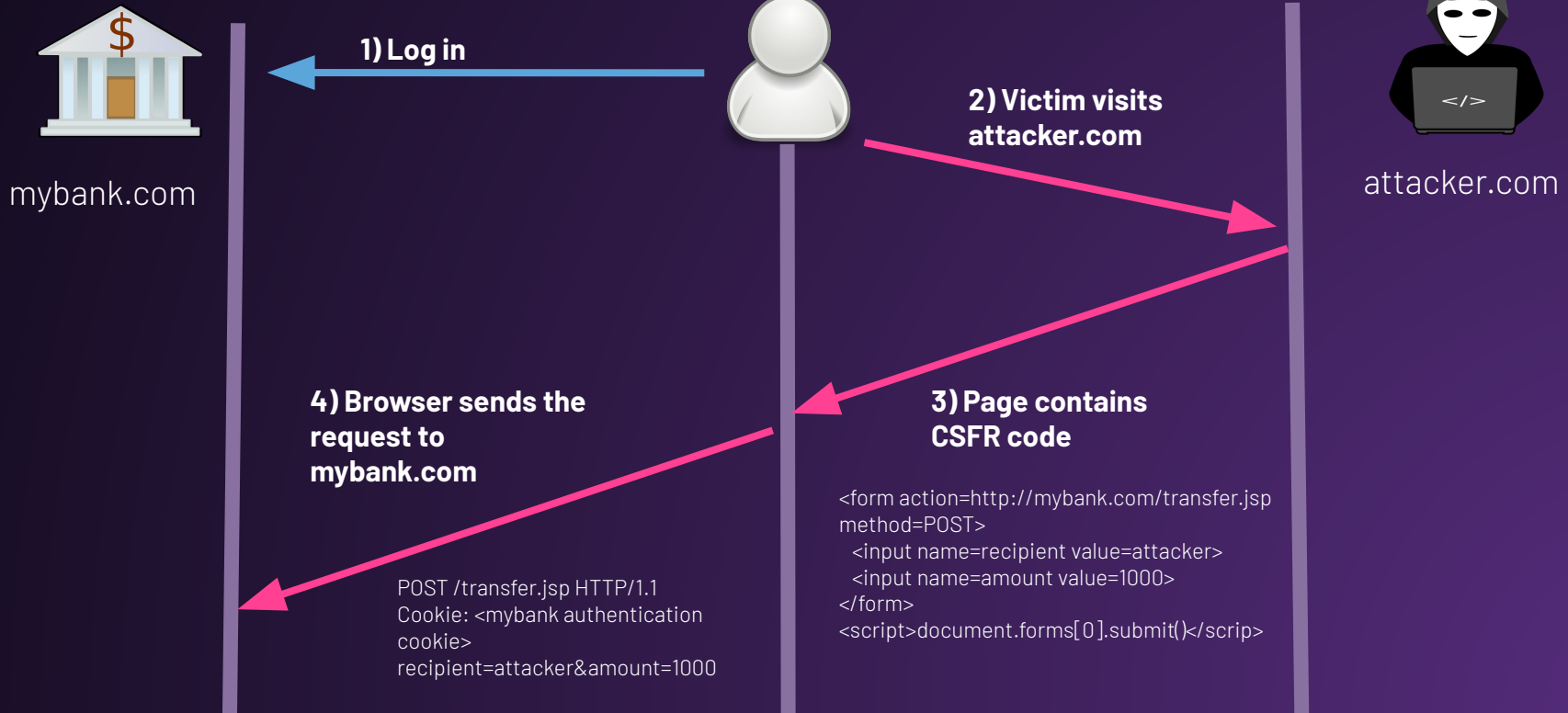
CROSS SITE REQUEST
FORGERY

¿Qué es Cross Site Request Forgery?

Es un tipo de ataque que se suele usar para estafas por Internet. Engaña a la víctima para que envíe una solicitud maliciosa. Hereda la identidad y los privilegios de la víctima para realizar una función no deseada en nombre de la víctima.



— ATAQUE:



VULNERABILIDAD

Tienen como objetivo las solicitudes de cambio de estado. Explota las vulnerabilidades denominadas "**defectos CSRF almacenados**". Esto se puede lograr simplemente almacenando una etiqueta IMG o IFRAME en un campo que acepte HTML, o mediante un ataque de scripting entre sitios más complejo.



MEDIDAS DE PREVENCIÓN QUE NO —FUNCIONAN

COOKIE SECRETA



ACEPTAR SOLO SOLICITUD POST



TRANSACCIONES DE VARIOS PASOS



REESCRITURA DE URL



TESTING: — CASO PRÁCTICO

DAMN VULNERABLE
WEB APPLICATION
(DVWA)



— ¿Cómo prevenir las vulnerabilidades CSRF?

Incorporar protección CSRF



Usar patrón de token de sincronizador



Usar cookies de doble envío





¡MUCHAS GRACIAS!