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:

1) Log in

4) Browser sends the

cookie>

POST /transfer.jsp HTTP/1.1

Cookie: <mybank authentication

recipient=attacker&amount=1000

request to mybank.com

\$

mybank.com

Victims browser

2) Victim visits attacker.com

3) Page contains CSFR code

<form action=http://mybank.com/transfer.jsp method=POST>

- <input name=recipient value=attacker>
- <input name=amount value=1000>
- </form>
- <script>document.forms[0].submit()</scrip>



attacker.com

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 <u>NO</u> _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 envio





IMUCHAS GRACIAS!