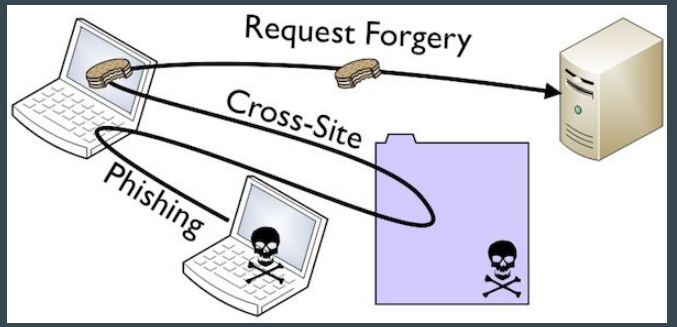
CSRF

(Cross-site request forgery o falsificación de petición en sitios cruzados)

Seguridad e Integridad de Sistemas



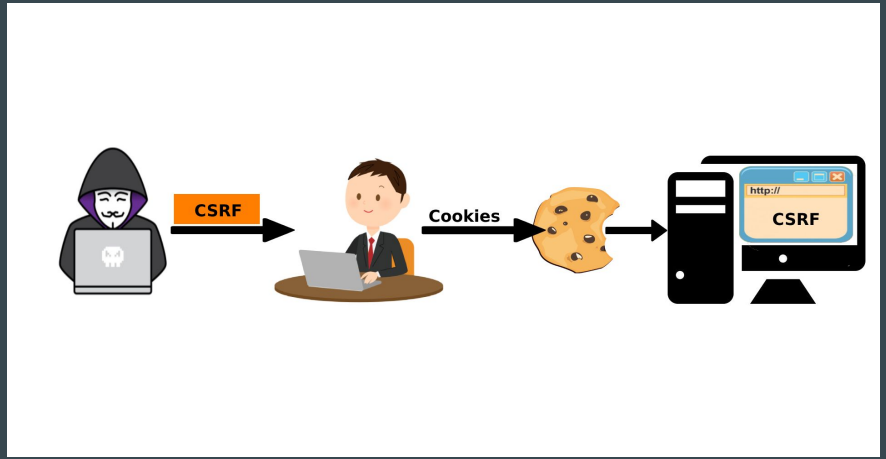
Prof. GIANNI, Fernando Julian

¿Qué es una vulnerabilidad CSRF?

Cross-site request forgery o falsificación de petición en sitios cruzados es un tipo de ataque que engaña al navegador de una víctima para que realice acciones no deseadas en una aplicación web donde está autenticada.

Características:

- Engaño al Usuario: El atacante induce al usuario a ejecutar acciones sin su conocimiento.
- Explotación de la Confianza: Aprovecha la confianza que una aplicación tiene en el navegador del usuario.



¿Cómo se explota?

1- El atacante crea una solicitud maliciosa (GET o POST) dirigida a la aplicación vulnerable.

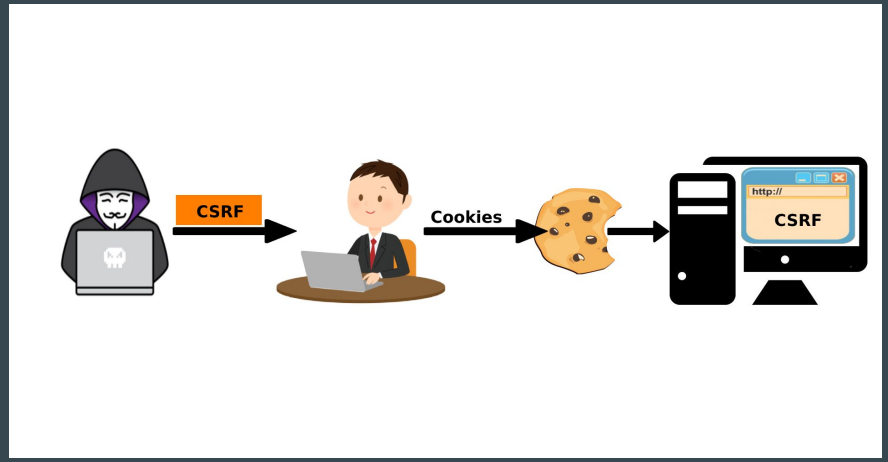
2- Entrega del Exploit:

Métodos de Entrega:

- Correos electrónicos con enlaces maliciosos.
- Páginas web controladas por el atacante.
- Mensajes en redes sociales.

3- La víctima, autenticada en la aplicación, interactúa con el exploit (clic en enlace, carga de imagen, etc.).

4- La solicitud se ejecuta con los privilegios de la sesión autenticada de la víctima.



Impacto

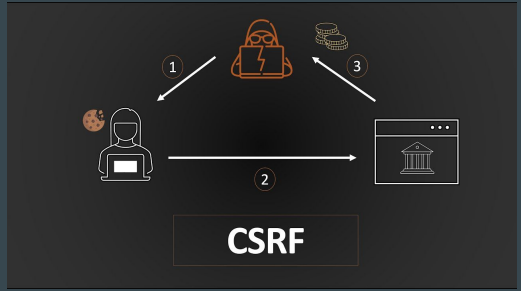
- Ejecución de acciones no autorizadas (cambios de configuración, transferencias de dinero, etc.).
- Pérdida de confianza de los usuarios.
- Daños financieros.
- Reputación afectada.

¿Cómo encontrarla?

1) Inspeccionar formularios y solicitudes que realizan acciones sensibles.
2) Verificar la presencia de tokens anti-CSRF.
3) Burp Suite: Utilizar el módulo de "CSRF Scanner".
4) OWASP ZAP: Plugins específicos para detectar CSRF.
5) Revisar el manejo de tokens y validaciones en el código fuente.
6) Simular ataques CSRF para identificar vulnerabilidades reales.

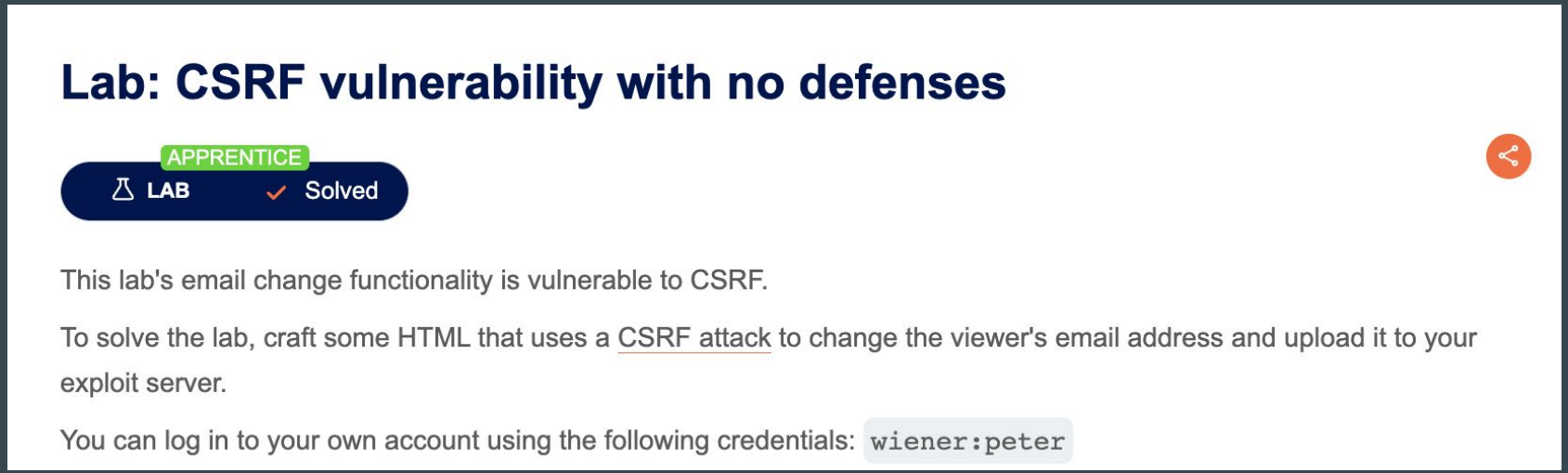
Mitigación

- Tokens Anti-CSRF:
  - Generar tokens únicos y secretos por sesión.
  - Incluir los tokens en formularios y verificar su validez en el servidor.
- Configuración de Cookies SameSite:
  - Establecer el atributo SameSite en las cookies para restringir su envío en solicitudes cross-site.
- Autenticación Fuera de Banda:
  - Requerir pasos adicionales de autenticación para acciones sensibles.
- Políticas de Seguridad de Contenido (CSP):
  - Restringir las fuentes desde las cuales se pueden cargar recursos en la aplicación.



Laboratorio

https://portswigger.net/web-security/csrf/lab-no-defenses



Laboratorio

https://portswigger.net/web-security/csrf/bypassing-token-validation/lab-token-validation-depends-on-request-method

Lab: CSRF where token validation depends on request method

PRACTITIONER

LAB ✓ Solved

This lab's email change functionality is vulnerable to CSRF. It attempts to block CSRF attacks, but only applies defenses to certain types of requests.

To solve the lab, use your exploit server to host an HTML page that uses a CSRF attack to change the viewer's email address.

You can log in to your own account using the following credentials: `wiener:peter`

Mitigación

- Verificación de Encabezados Origin y Referer
  - Validar que las solicitudes provienen de dominios autorizados.

- Encabezado Origin:
  - Contiene el origen de la solicitud (esquema, host y puerto).

- Encabezado Origin:
  - Indica la URL de la página desde la que se realizó la solicitud.
  - Puede ser útil, pero menos confiable que Origin ya que algunos navegadores o configuraciones de privacidad pueden omitirlo.

```python
from flask import request, abort

@app.route('/transfer', methods=['POST'])
def transfer():
    origin = request.headers.get('Origin')
    if origin != 'https://tu-dominio.com':
        abort(403)
```

```python
from flask import request, abort

@app.route('/transfer', methods=['POST'])
def transfer():
    referer = request.headers.get('Referer')
    if not referer.startswith('https://tu-dominio.com'):
        abort(403)
```

Conclusiones

- CSRF es una vulnerabilidad crítica que puede tener graves impactos.
- La explotación depende de la interacción del usuario y de la falta de validaciones adecuadas.
- Importancia de la Mitigación: proteger a los usuarios y mantener la integridad de la aplicación.
- Implementar tokens anti-CSRF.