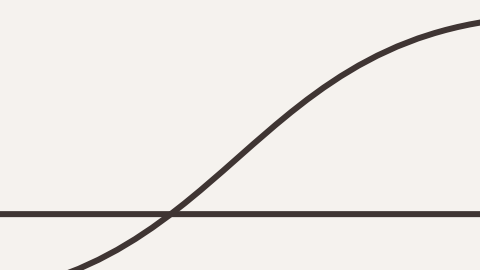




Seguridad de aplicaciones web: Principios y riesgos OWASP

Javier Abella, Xavier Leonardo, Alex López, Sergio Utrero



Índice

1. Objetivos de la seguridad informática
2. ¿Qué es OWASP?
3. Principios de seguridad
4. OWASP Top 10
5. OWASP Juice shop
6. Bibliografía
7. Reparto de tareas

Seguridad informática - Objetivos

- Proteger los datos de los usuarios
- Prevenir ataques externos
- Garantizar la disponibilidad continua del servicio



¿Qué es OWASP?

Open Worldwide Application Security Project

- Fundación sin ánimo de lucro
- Dedicada a la seguridad de las aplicaciones
- Proporciona recursos educativos

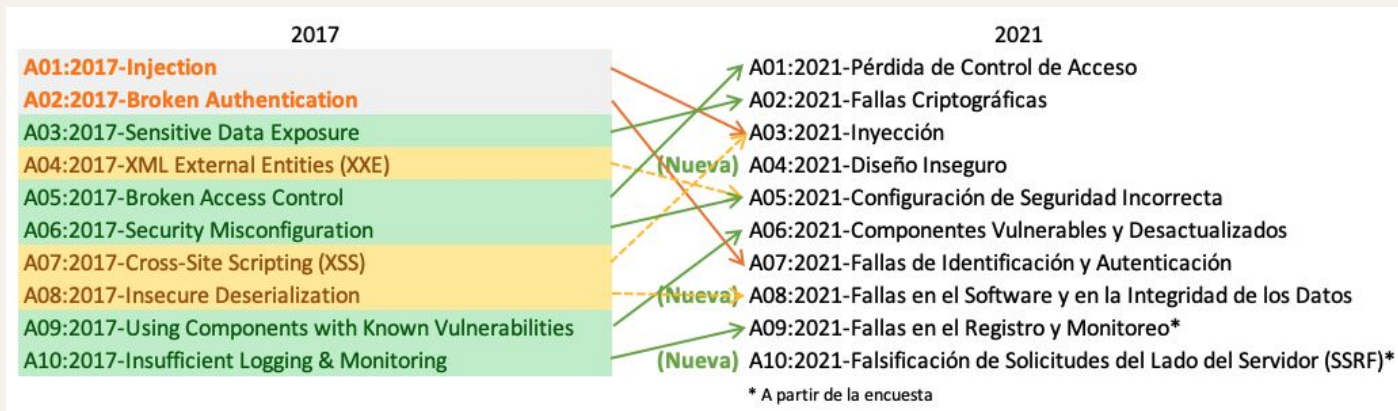


Principios de seguridad OWASP

1. El principio de Menor Privilegio y Separación de Funciones
2. El principio de Defensa en Profundidad
3. El principio de Confianza Cero
4. El principio de Seguridad en Abierto

Riesgos - OWASP Top 10

- Lista de los 10 riesgos de seguridad más críticos
- Última actualización en 2021



A01 Pérdida de Control de Acceso

- Cumplimiento de política de modo que los usuarios no pueden actuar fuera de los permisos que le fueron asignados
- Prevención:
 - Implementar control de acceso en servidor o API
- Escenario de ataque:

```
https://example.com/app/getappInfo  
https://example.com/app/admin_getappInfo
```

A02 Fallas Criptográficas

- Exposición de datos sensibles
- Prevención:
 - No guardar datos sensibles innecesariamente
 - Cifrar todos los datos sensibles en reposo
- Escenario de ataque:
 - Cifrado de números de tarjetas de crédito

A03 Inyección

- Infiltración de código intruso para realizar operaciones sobre una BD
- Prevención:
 - Utilizar una API segura que use ORM
 - Utilizar controles SQL como LIMIT
- Escenario de ataque:

```
String query = "SELECT \* FROM accounts WHERE custID='" + request.getParameter("id") + "'";
```

```
http://example.com/app/accountView?id=' UNION SELECT SLEEP(10);--
```

A04 Diseño Inseguro

- Riesgos relacionados con el diseño y fallos de arquitectura
- Prevención:
 - Establecer y utilizar patrones de diseño seguro
 - Separar correctamente las capas del sistema
- Escenario de ataque:
 - Descuentos en la reserva de grupos en un cine

A05 Configuración de Seguridad Incorrecta

- Ausencia de parches de seguridad y configuraciones erróneas
- Prevención:
 - Arquitectura de aplicación segmentada
- Escenario de ataque:
 - El listado de directorios no se encuentra deshabilitado en el servidor

A06 Componentes Vulnerables y Desactualizados

- Componentes utilizados en una aplicación web desactualizados o con vulnerabilidades conocidas
- Prevención:
 - Herramientas de escaneo de dependencias
 - Política de actualización de componentes
 - Estar al tanto de los avisos de los proveedores
- Escenario de ataque:
 - Struts 2 permite la ejecución de código arbitrario en el servidor

A07 Fallas de Identificación y Autenticación

- Vulnerabilidades asociadas con procesos de verificación de identidad y acceso a sistemas
- Prevención:
 - Prácticas sólidas de gestión de identidades
 - Protocolos de autenticación
 - Monitorización constante
- Escenario de ataque:
 - Uso de contraseñas como único factor de autenticación

A08 Fallas en el Software y en la Integridad de los Datos

- Está relacionado con código e infraestructura no protegidos contra alteraciones
- Prevención:
 - Firmas digitales
 - Bibliotecas y dependencias confiables
- Escenario de ataque:
 - SolarWinds Orion distribuyó una actualización maliciosa a más de 18.000 organizaciones.

A09 Fallas en el Registro y Monitoreo

- Impiden detectar y combatir posibles brechas activas
- Prevención:
 - Sistema robusto de registro de eventos
 - Alertas y notificaciones para eventos críticos
- Escenario de ataque:
 - Una aerolínea India tuvo una brecha por más de 10 años en los que se filtraron datos de sus usuarios

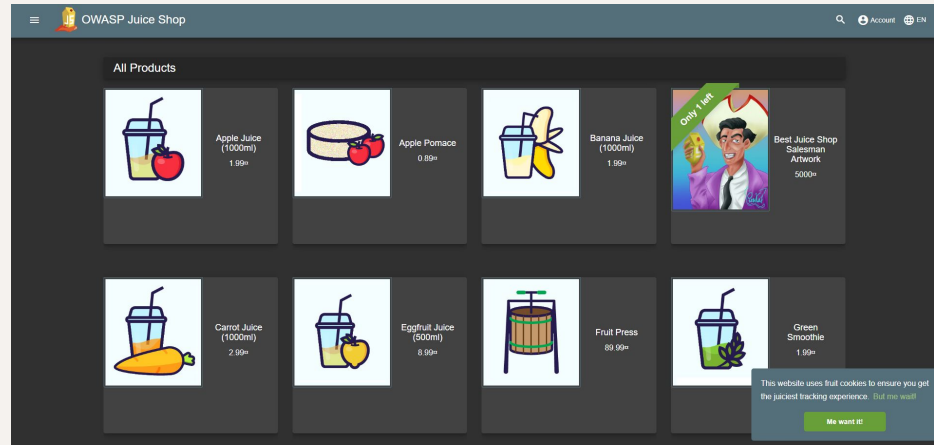
A10 Falsificación de Solicitud del Lado del Servidor (SSRF)

- Una aplicación web obtiene un recurso remoto sin validar la URL proporcionada por el usuario
- Prevención:
 - Validar los datos de entrada del cliente
 - Segmentar la funcionalidad de acceso a recursos remotos
- Escenario de ataque:
 - Los atacantes se conectan a servicios internos de la aplicación

Owasp Juice shop



- Aplicación insegura utilizada en entrenamientos de ciberseguridad
- Abarca vulnerabilidades de todo el OWASP Top Ten y otras encontradas en otras páginas reales



Conclusiones

- Conciencia en la seguridad informática
- Importancia de un desarrollo seguro
- Mantener actualizado el entorno
- Conocer los riesgos que corremos al desarrollar

Bibliografia

OWASP: <https://owasp.org/>

OWASP Principles:

https://cheatsheetseries.owasp.org/cheatsheets/Secure_Product_Design_Cheat_Sheet.html

OWASP Top 10: <https://owasp.org/www-project-top-ten/>

Juice shop: <https://owasp.org/www-project-juice-shop/>

Reparto de tareas

| Javier Abella | Xavier Leonardo | Alex López | Sergio Utrero |
|----------------------|------------------------|-------------------|----------------------|
| Transparencias | Orador | Transparencias | Orador |
| Investigación | Investigación | Investigación | Investigación |