

VULNERABILIDADES EN APLICACIONES WEB

XSS - CSRF - DDoS

José Moisés Granados Guevara




USAC - CUNOC / Guatemala

Agenda

Vulnerabilidades a cubrir:

- XSS: Cross-Site scripting
- CRSF: Cross-Site Request Forgery
- DDoS: Denial-of Service

Metodología por vulnerabilidad

1.  Teoría Fundamental - Conceptos técnicos
2.  Demostración Práctica - Aplicación JSP vulnerable
3.  Laboratorio - implementación segura

Tecnología: JSP + Servlets

Metodología por vulnerabilidad

Repo:

XSS: Cross-Site Scripting

XSS es una vulnerabilidad de seguridad que permite a atacantes inyectar scripts maliciosos en páginas web vistas por otros usuarios, ejecutándose en el contexto de seguridad de la aplicación víctima.

XSS: Cross-Site Scripting

Fases del ataque:

1. Inyección
2. Almacenamiento
3. Victimizacion
4. Ejecución
5. Explotacion

XSS Reflected

El payload malicioso es incluido inmediatamente en la respuesta del servidor, sin ser almacenado persistentemente. El ataque requiere que la víctima visite una URL especialmente crafted o envíe datos maliciosos.

XSS Reflected: Características

Ventajas para el Atacante:

- Fácil de crear y probar
- No deja rastro persistente en el servidor
- Puede ser altamente dirigido
- Funciona incluso con autenticación

XSS Reflected: Características

Desventajas para el Atacante:

- Requiere ingeniería social
- Menor escalabilidad (una víctima a la vez)
- Fácil de detectar en logs
- La víctima puede notar el comportamiento extraño

Jueguen (ataquen) un poco



XSS Stored

El payload malicioso se almacena permanentemente en el servidor (generalmente en una base de datos) y luego se sirve automáticamente a múltiples usuarios en respuestas futuras.

XSS Stored: Características

Persistencia

- Almacenamiento permanente en el servidor
- Sobrevive a reinicios de aplicación
- No requiere re-inyección del payload
- Persiste hasta que sea eliminado manualmente

XSS Stored: Características

Automatización

- Ejecución automática sin interacción del usuario
- No requiere ingeniería social
- Funciona en segundo plano
- Afecta a usuarios legítimos

XSS Stored: Características

Escalabilidad

- Afecta a TODOS los usuarios que accedan al contenido
- Impacto masivo potencial
- Propagación automática

Jueguen (ataquen) un poco



XSS: Mitigación

- Siempre desconfiar de lo que ingresa el usuario.
- Usar encoders.
- Es más difícil realizar XSS en SPA pero es posible.

CSRF: Cross-Site Request Forgery

Es un ataque que obliga al usuario a ejecutar acciones no deseadas en una aplicación web en la que está autenticado. El ataque explota la confianza que la aplicación tiene en el navegador del usuario.

CSRF: Cross-Site Request Forgery

Fases del ataque:

1. Víctima inicia sesión en sitio seguro, se obtiene cookie de session
2. Victima visita sitio malicioso
3. Víctima ejecuta un request automatico con cookies válidas al sitio seguro
4. El sitio seguro recibe cookies validas y ejecuta la accion.

CSRF: Condiciones necesarias

1. Autenticación Basada en Cookies
2. No Verificación de Origen
3. Acciones Sensibles via GET/POST
4. Usuario Autenticado Visita Sitio Malicioso

Jueguen (ataquen) un poco



CSRF: Mitigación

- Same-Origin Policy o limitar el origen de los request.
- Implementar token CSRF.

DDoS: Distributed Denial of Service

Ataque que busca hacer que un servicio o recurso no esté disponible para usuarios legítimos mediante tráfico masivo coordinado desde múltiples fuentes.

DDoS: Evolucion

1990s: DoS (Denial of Service)

2000s: DDoS (Distributed DoS)

2010s: DDoS Masivo

DDoS: Ataques volumetricos

El objetivo es saturar el ancho de banda para que se agote la cuota de ancho de banda.

Capa 3 y 4 del modelo OSI

DDoS: Ataques de Protocolo

El objetivo es agotar recursos del servidor.

Capa 3 y 4 del modelo OSI

DDoS: Ataques de Aplicacion

El objetivo es consumir recursos de aplicación para que el servidor esté lento o inaccesible.

Capa 3 y 4 del modelo OSI

DDoS: Uso de bots

Red de dispositivos comprometidos y controlados remotamente por un atacante para realizar actividades maliciosas.

Botnet Mirai

Jueguen (ataquen) un poco



DDoS: Mitigación

- Límites por IP.
- Filtrado y Filtrado automático con listas negras.
- Infraestructuras como firewalls y balanceador de cargas, entre otros.

Bonus

<https://tinyurl.com/79c4evxk>