EDUCACIÓN IT

Seguridad Web: SQL Injection & XSS

Programa de Estudio

Seguridad Web: SQL Injection & XSS

Aprende las técnicas más utilizadas por los hackers para vulnerar aplicaciones web. Entiende cómo analizar la seguridad en empresas realizando ataques.

Contenido del curso

El curso comienza analizando el protocolo HTTP, para entender sus particularidades relacionadas con la seguridad, así como también las mejores prácticas al momento de implementar una aplicación web.
Más adelante veremos cómo funcionan las vulnerabilidades del tipo Cross-Site Scripting (XSS), sus diferentes variantes, y las técnicas que podría utilizar un atacante para tomar el control de un navegador a través de su explotación.
También analizaremos las vulnerabilidades del tipo SQL Injection, así como también otras variantes de inyección, como las Command Injections. Dentro de SQL Injection aprenderemos a detectarlas y a evitarlas. Realizaremos prácticas para, por ejemplo, ver cómo pueden ser robados los datos de una base a través de este tipo de ataques.
Se cubrirán temas como la correcta gestión de sesiones, para comprender cómo deben estar formados los identificadores de sesión y cómo podrían llegar a ser atacados con el objetivo de acceder a estas sesiones sin necesidad de autenticarse.
Para cada uno de los aspectos analizados, se estudiará cómo deberían ser implementadas correctamente las funcionalidades en el código de aplicación, a fin de estar protegidos contra cada uno de los ataques.
Por último, analizaremos las medidas de seguridad web que pueden ser implementadas del lado de la infraestructura, particularmente implementaremos un Web Application Firewall con ModSecurity.
PRÁCTICAS EN CLASE ::

Durante las clases realizaremos ataques sobre sitios web de práctica, que nos permitirán entrar en contacto directo con las técnicas, herramientas y comportamientos de las aplicaciones web existentes. Realizaremos ataques para saltar procesos de autenticación, inyectar información dentro de bases de datos, capturar datos de usuarios y más.

Requisitos

Conocimientos previos:
Tener conocimientos de seguridad informática o haber realizado el curso de Introducción a la seguridad Informática
Tener conocimientos de criptografía o haber realizado el curso de Criptografía y Blockchain

Tener conocimientos de seguridad en redes o haber realizado el curso de Seguridad en Redes: Network Hacking

Modalidad de cursado

Puedes tomar este curso en modalidad presencial o modalidad online - en vivo

¿Qué aprenderás?

- Fundamentos HTTP y ZAP Proxy
- Detectar qué tecnologías utiliza una aplicación Web
- Modificar las peticiones y respuestas HTTP
- Cross Site Scripting
- Utilización de Cookies para la seguridad de una App
- Detectar vulnerabilidades con XSS, CSRF y SQL Injection
- SQL/Command Injections
- Utilizar Zed Attack Proxy y Vega
- Inclusiones, Shells, Sesiones y Validaciones Client-Side
- Control de un navegador web a través de BeEF
- Crear archivos remotos en servidores vulnerables
- Protecciones con Apache + ModSecurity
- Uso de Web Application Firewalls
- Detener ataques con ModSecurity y ModEvasive para Apache

Plan de Estudios

1. HTTP y ZAP Proxy

HTTP - Fundamentos
Instalación de DVWA sobre Kali Linux
Acceso desde Ncat
Análisis de las Cabeceras HTTP
Obtener métodos con el verbo OPTIONS
ZAP - Peticiones y Respuestas
Zap - Configuración del Proxy
Zap - Configuración del Scope
Zap - Análisis de Peticiones y Respuestas
Zap - Modificar Peticiones al Vuelo (BreakPoints)
ZAP - Escaneo Pasivo
Zap - Configuración de Escaneo Pasivo
Zap - Spidering
Zap - Descubrir Directorios Ocultos (dirbuster)
Zap - Fuzzing de Peticiones Web
ZAP - Plugins y Escaneo Activo
Zap - Reenviar peticiones
Zap - Instalación de Plugins
Zap - Configuración de Escaneo Activo
Zap - Lanzamiento de Escaneos Activos

2. Cross Site Scripting

XSS - Introducción
XSS Reflejado
Análisis de código
Nivel Medio
Nivel Alto
Nivel Imposible
XSS - Otras variantes
XSS Persistente
XSS Basado en DOM
Detección a través de Fuzzing
VLab
XSS Payloads

XSS DoS
Robo de Cookies
Keylogger
VLab - Redirección
BeEF - Browser Exploitation Framework
BeEF enganche (hook.js)
BeEF - GetCookie y GetFormValues
BeEF - Redirect Browser
BeEF - Detect Virtual Machine
XSS Payloads
XSS Persistente
XSS Persistente
XSS DoS
XSS Con Redirect
Via HTTP Headers (Show log)
Robo de Cookies
XSS Alert con Cookies
Robo de Cookies a través de json request
Atributo httponly para evitar el robo
Robo de Cookies via img o algún otro request

3. SQL/Command Injections

SQLi Básico
Análisis de código nivel Low
Generación de Errores
Lógica del 1=1 (mostrar en mysql console)
Ataque por 1=1
SQLi Payloads
Mostrar nombre de base de datos, versión y usuario
Mostrar todas las tablas de la base
Mostrar todas las columnas
Mostrar todos los datos de las columnas
SQLi - Contramedidas
Nivel Medio
Nivel Alto
Nivel Imposible
Algún lab
Command Injection

Inyección básica de comandos
Crear archivos en el sistema
Crear una conexión shell con NetCat
Identificar la password de la base de datos

4. Inclusiones, Shells, Sesiones y Validaciones Client-Side

File Inclusions
Local File Inclusion (LFI)
Remote File Inclusion (RFI)
Nivel Medio
Nivel Alto
Shells PHP
Creación de una shell en PHP
Subir a través de File Upload
Remote Hell - Análisis de Código
Utilización de Remote Hell (rhell)
Cookies de Sesión
El atributo ?secure?
El atributo ?httponly?
Cambio de contenido (user=admin, etc)
Enumerar los usuarios del sistema
Validaciones Client-Side
Saltar Restricciones de Longitud en Formularios
Saltar validaciones JavaScript 1
Saltar validaciones JavaScript 2
Enviar un XSS con el nivel de seguridad 3

5. Protecciones con Apache + ModSecurity

Configuración Segura de Apache
X-Frame Options
X-Content-Type-Options
Content Security Policy
Cookies
HTTPS Strict Transport Security
Public-Key-Pins

Mod Security - Instalación
Instalación de ModSecurity y el CRS
Habilitar ModSecurity en Modo Detection Only
Navegar la aplicación y mirar los logs de ModSecurity
Lab: Habilitar en On y probar
Mod Security - Configuración
XSS vs ModSecurity
SQLi vs ModSecurity
PHPInfo vs ModSecurity (Outbound)
Lab: LFI vs ModSecurity
Mod Security - Reglas Personalizadas
Análisis de 913100 - Found User-Agent associated with security scanner
Análisis de 920160 - Content-Length HTTP header is not numeric.
Análisis de 950130 - Directory Listing
Describir el comportamiento de una regla (sin ver los comentarios ni el msg)

Lavalle 648 Piso 8, Microcentro, CABA
0810-220-8148
info@educacionit.com