ventas@xnet.com.pe

“Programa de Capacitación Pentesting de Aplicaciones Web Avanzado”

XNET SOLUTIONS

Presentado a:

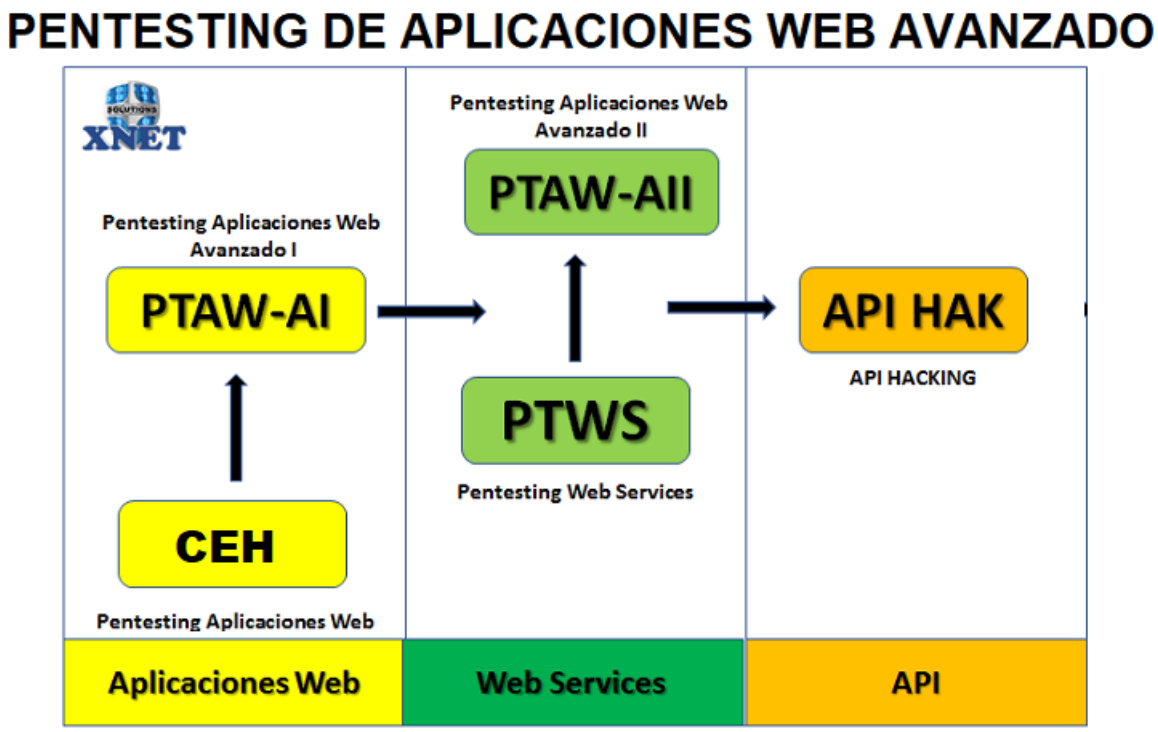
PROPUESTA TÉCNICA

CURSOS DE PENTESTING DE APLICACIONES WEB AVANZADO

2021

Av Del Parque Sur 185, Oficina 501 - San Isidro

CURSOS DE PENTESTING DE APLICACIONES WEB AVANZADO



CURSOS DE PENTESTING EN APLICACIONES WEB AVANZADO				
CODIGO	CURSO	DURACION	PRECIO * sin IGV	Pre Requisitos
PTAW-AI	Pentesting Aplicaciones Web Avanzado I	24 H	US$ 400	CEH o PTAN
PTWS	Pentesting Web Services	24 H	US$ 400	PTAN
PTAW-AII	Pentesting Aplicaciones Web Avanzado II	24 H	US$ 400	PTWS
API HAK	API Hacking	24 H	US$ 600	PTAN

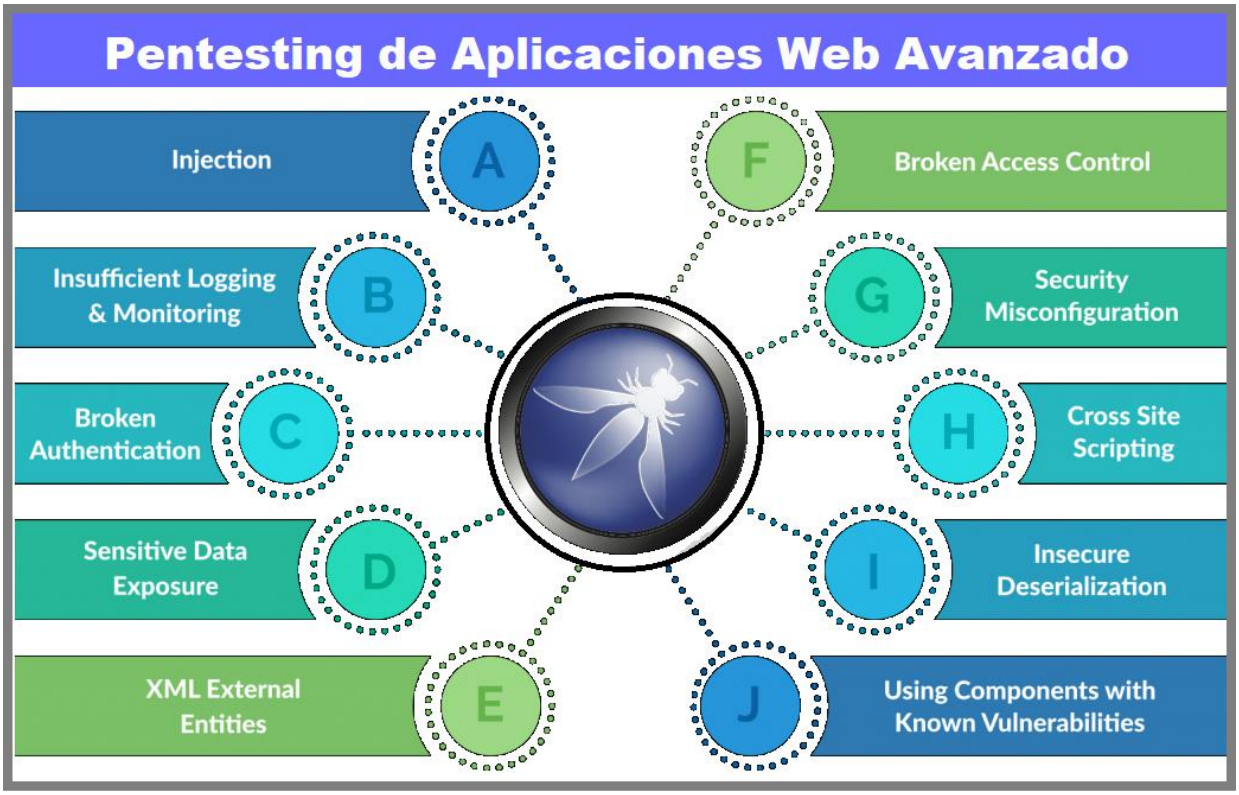
Pentesting de Aplicaciones Web - Avanzado

CURSO : Pentesting de Aplicaciones Web – Avanzado I

Duración : 24 Horas

Observaciones:

- Basado en aprox 60 vulnerabilidades identificadas en el proyecto de Owasp referido a Aplicaciones Web Avanzadas.
- El curso es 100% practico y de nivel Avanzado, es necesario tener conocimientos básicos de vulnerabilidades de aplicaciones web
- Se entregará Guía de Laboratorio de Técnicas de Pentesting de Aplicaciones Web



DESCRIPCION DEL CURSO

Este curso está diseñado para capacitar a profesionales y técnicos en TI en las técnicas avanzadas y uso de herramientas para realizar tareas de Auditoria o Pentesting de Aplicaciones web.

Durante el curso se revisarán mas de 60 vulnerabilidades identificadas en el proyecto de Owasp y que forman parte de las Guía de Pruebas de OWASP dentro de las cuales esta el Top Ten de Owasp.

Objetivo:

Desarrollar habilidades prácticas en Auditoria de Aplicaciones Web que permita desarrollar las competencias necesarias para realizar un proceso controlado de Pentesting de Aplicaciones Web Avanzado que permita conocer las vulnerabilidades y de esta manera tomar las medidas preventivas.

Competencias:

- Comprende un ataque a servidores web y aplicaciones a través de Internet
- Realizar una prueba de penetración a Aplicaciones Web.
- Utiliza las herramientas idóneas para realizar un proceso de Auditoria a Aplicaciones Web
- Entender el funcionamiento de los ataques más comunes como SQL Injection, Cross Site Scripting, Path Traversal, Session Hijacking, entre otros
- Uso de Herramientas para Pentesting de Aplicaciones web como Burp Suite, OWASP ZAP, SQL MAP , entre otras.
- Reconoce las ventajas de la tecnología y los peligros al no tener una cultura de seguridad

Dirigido a:

- Profesionales en Tecnologías de la Información
- Desarrolladores de Aplicaciones Web
- Administradores de TI, Programadores
- Ingenieros de Testing de Aplicaciones Web

Pre Requisito:

Debido a que durante el curso es 100% practico y avanzado, es necesario que los participantes tengan conocimiento de:

- Conocimiento de Vulnerabilidades de Aplicaciones Web
- Haber llevado o tener conocimiento de Ethical Hacker
- Entender como funciona una Pagina Web
- Tener conocimiento del uso de Proxy para Pentesting

DETALLES DEL CURSO

/ A1 -Injection /

- HTML Injection -Reflected (GET)
- HTML Injection -Reflected (POST)
- HTML Injection -Reflected (Current URL)
- HTML Injection -Stored (Blog)
- iFrame Injection
- LDAP Injection (Search)
- Mail Header Injection (SMTP)
- OS Command Injection
- OS Command Injection -Blind
- PHP Code Injection
- Server-Side Includes (SSI) Injection
- SQL Injection (GET/Search)
- SQL Injection (GET/Select)
-

/ A2 -Broken Auth. & Session Mgmt. /

- Broken Authentication -CAPTCHA Bypassing
- Broken Authentication -Forgotten Function
- Broken Authentication -Insecure Login Forms
- Broken Authentication -Logout Management
- Broken Authentication -Password Attacks

/ A3 -Cross-Site Scripting (XSS) /

- Cross-Site Scripting -Reflected (GET)
- Cross-Site Scripting -Reflected (POST)
- Cross-Site Scripting -Reflected (Back Button)
- Cross-Site Scripting -Reflected (Custom Header)
- Cross-Site Scripting -Reflected (Eval)
- Cross-Site Scripting -Reflected (HREF)
- Cross-Site Scripting -Reflected (Login Form)
- Cross-Site Scripting -Reflected (phpMyAdmin)
- Cross-Site Scripting -Stored (Blog)
- Cross-Site Scripting -Stored (Change Secret)
- Cross-Site Scripting -Stored (User-Agent)

/ A4 -Insecure Direct Object References /

- Insecure DOR (Change Secret)
- Insecure DOR (Reset Secret)

/ A5 -Security Misconfiguration /

- Arbitrary File Access (Samba)
- Cross-Domain Policy File (Flash)
- Denial-of-Service (Large Chunk Size)

- Denial-of-Service (Slow HTTP DoS)
- Denial-of-Service (SSL-Exhaustion)
- Local Privilege Escalation (sendpage)
- Local Privilege Escalation (udev)
- Man-in-the-Middle Attack (HTTP)
- Robots File

/ A6 -Sensitive Data Exposure /

- Base64 Encoding (Secret)
- BEAST/CRIME/BREACH Attacks
- Clear Text HTTP (Credentials)
- HTML5 Web Storage (Secret)
- Text Files (Accounts)

/ A7 -Missing Functional Level Access Control /

- Directory Traversal -Directories
- Host Header Attack (Cache Poisoning)
- Host Header Attack (Reset Poisoning)
- Local File Inclusion (SQLiteManager)
- Remote & Local File Inclusion (RFI/LFI)
- Restrict Device Access

/ A8 -Cross-Site Request Forgery (CSRF) /

- Cross-Site Request Forgery (Change Password)
- Cross-Site Request Forgery (Change Secret)

/ A9 -Using Known Vulnerable Components /

- Buffer Overflow (Local)
- Buffer Overflow (Remote)
- Drupal SQL Injection (Drupageddon)
- PHP CGI Remote Code Execution
- PHP Eval Function
- SQLiteManager PHP Code Injection

/ A10 -Unvalidated Redirects & Forwards /

- Unvalidated Redirects & Forwards (1)
- Unvalidated Redirects & Forwards (2)

Curso Avanzado – Pentesting to Web Services

CURSO : Pentesting to Web Services

Duración : 24 Horas

Observaciones:

- El curso incluye manuales del curso
- Guía de Laboratorio de Web Services

DESCRIPCION DEL CURSO

Este curso está diseñado para capacitar a profesionales en TI como realizar tareas de Auditoria o Pentesting de Web Services.

Durante el curso se revisarán los conceptos y vulnerabilidades asociadas a Web Services identificadas en el proyecto de OWASP.

Objetivo:

Desarrollar habilidades prácticas en Auditoria de Web Services que permita desarrollar las competencias necesarias para realizar un proceso controlado de Pentesting de Aplicaciones Web basado en Web Services.

Competencias:

- Comprende un ataque a Aplicaciones con Web Services a través de Internet
- Realizar una prueba de penetración a Web Services.
- Utiliza las herramientas idóneas para realizar un proceso de Auditoria a Aplicaciones Web y Web Services asociados.
- Entender el funcionamiento de los ataques más comunes como Enumeración de WSDL, XPATH Injection, REST API SQL Injection, JSON Web Token Secret Key Brute Force, XML External Entity Attack, Command Injection, entre otros
- Uso de Herramientas para Pentesting de Aplicaciones web como Burp Suite, Owasp ZAP, SQL MAP, Plugin de Burp Suite para SOAP o REST, entre otras.

Dirigido a:

- Profesionales en Tecnologías de la Información
- Desarrolladores de Aplicaciones Web
- Administradores de TI, Programadores
- Ingenieros de Testing de Aplicaciones Web

Pre Requisito:

Los participantes deberán tener conocimiento de:

- Conocimiento de Vulnerabilidades de Aplicaciones Web básicas.
- Haber llevado o tener conocimiento de Ethical Hacker o similares.
- Entender cómo funciona una Página Web.

SYLABUS DEL CURSO:

Mod 1. Web Services

- Que son los Web Services
  - Descripcion General
  - Entendiendo XML
- Implementaciones de Web Services
  - XML-RPC / JSON - RPC / RESTful / SOAP
  - SOAP
  - Entendiendo SOAP
- Entendiendo WSDL
  - Objectos en WSDL
  - Binding / Port Type / Operation / Interface
  - SOAP en Action
- Ataques a Web Services
  - Divulgacion WSDL
  - WSDL Google Hacking
  - Identificando WSDL File
  - Escaneando WSDL
  - SOAPAction Spoofing
  - Request Spoofed
  - SQL Injection con SOAP

Mod2. XML 101

- Documentos y BD XML
  - Documentos XML
  - BD XML
  - XPath
  - Expresion y sintaxis
  - XPath vs SQL
- Detectando XPath Injection
  - Detectando XPath Injection
  - Injection basado en Error
  - Blind Injection
- Explotacion
  - Bypass XPath Query
  - Extrayendo XML Documents
  - Encontrando Nodos/Sub Nodos

Mod3 Ataques a Web Services con DVWS

- Divulgacion de WSDL
- WSDL Enumeration
- XML Bomb DoS
- XPath Injection

Mod 4. XML Attacks

- Introduccion a XML Attacks
  - Intriduccion
  - Entities Block
- XML Tag Injection
  - XML Injection
  - XSS con CDATA
- XML External Entity
  - Taxonomia
  - External Entities : Private vs Public
  - Inclusion de Recursos
  - File, CDATA, I/O Streams, OOB via HTTP
- XML Entity Expansion
  - XML Entity Expansion
  - Ataque DoS
  - Quadratic Blowup Attack
- XPath Injection
  - XPath v1.0 vs v2.0
  - XPath Injection
- Advaced XPath Exploitation
  - Blind Exploitation
  - OOB Exploitation

Pentesting de Aplicaciones Web – Avanzado II

CURSO : Pentesting de Aplicaciones Web – Avanzado II

Duración : 24 Horas

Observaciones:

- Basado en aprox 60 vulnerabilidades identificadas en el proyecto de Owasp referido a Web Services y Aplicaciones Web Avanzadas.
- El curso es 100% practico y de nivel Avanzado, es necesario tener conocimientos básicos de vulnerabilidades de Web Services, SOAP, REST.
- Se entregará Guía de Laboratorio de Técnicas de Pentesting de Aplicaciones Web y Web Services.

DESCRIPCION DEL CURSO

Este curso está diseñado para capacitar a profesionales y técnicos en TI en las técnicas avanzadas y uso de herramientas para realizar tareas de Auditoria o Pentesting de Aplicaciones web, Web Services y Mas.

Durante el curso se revisarán más de 60 vulnerabilidades identificadas en el proyecto de OWASP y que forman parte de las Guía de Pruebas de OWASP dentro de las cuales esta el Top Ten de Owasp.

Objetivo:

Desarrollar habilidades prácticas en Auditoria de Aplicaciones Web que permita desarrollar las competencias necesarias para realizar un proceso controlado de Pentesting de Aplicaciones Web Avanzado y Web Services que permita conocer las vulnerabilidades y de esta manera tomar las medidas preventivas.

Competencias:

- Comprende un ataque a servidores web y Web Services a través de Internet
- Realizar una prueba de penetración a Web Services.
- Utiliza las herramientas idóneas para realizar un proceso de Auditoria a Aplicaciones Web y Web Services asociados.
- Entender el funcionamiento de los ataques más comunes como SQL Injection, Cross Site Scripting, Path Traversal, Session Hijacking, entre otros
- Uso de Herramientas para Pentesting de Aplicaciones web como Burp Suite, Owasp ZAP, SQL MAP, Plugin de Burp Suite para SOAP o REST, entre otras.
- Reconoce las ventajas de la tecnología y los peligros al no tener una cultura de seguridad

Dirigido a:

- Profesionales en Tecnologías de la Información
- Desarrolladores de Aplicaciones Web
- Administradores de TI, Programadores
- Ingenieros de Testing de Aplicaciones Web

Pre Requisito:

Debido a que durante el curso es 100% practico y avanzado, es necesario que los participantes tengan conocimiento de:

- Conocimiento de Vulnerabilidades de Aplicaciones Web y Web Services
- Haber llevado o tener conocimiento de Ethical Hacker
- Entender cómo funciona una Página Web y Web Services asociados.
- Tener conocimiento del uso de Proxy para Pentesting

DETALLES DEL CURSO

/ A1 -Injection /

- SQL Injection (POST/Search)
- SQL Injection (POST/Select)
- SQL Injection (AJAX/JSON/jQuery)
- SQL Injection (CAPTCHA)
- SQL Injection (Login Form/Hero)
- SQL Injection (Login Form/User)
- SQL Injection (SQLite)
- SQL Injection (Drupal)
- SQL Injection -Stored (Blog)
- SQL Injection -Stored (SQLite)
- SQL Injection -Stored (User-Agent)
- SQL Injection -Stored (XML)
- SQL Injection -Blind -Boolean-Based
- SQL Injection -Blind -Time-Based
- SQL Injection -Blind (SQLite)
- SQL Injection -Blind (Web Services/SOAP)
- XML/XPath Injection (Login Form)
- XML/XPath Injection (Search)

/ A2 -Broken Auth. & Session Mgmt. /

- Broken Authentication -Weak Passwords
- Session Management -Administrative Portals
- Session Management -Cookies (HTTPOnly)
- Session Management -Cookies (Secure)
- Session Management -Session ID in URL

- Session Management -Strong Sessions

/ A3 -Cross-Site Scripting (XSS) /

- Cross-Site Scripting -Reflected (JSON)
- Cross-Site Scripting -Reflected (AJAX/JSON)
- Cross-Site Scripting -Reflected (AJAX/XML)
- Cross-Site Scripting -Reflected (AJAX/XML)
- Cross-Site Scripting -Reflected (PHP_SELF)
- Cross-Site Scripting -Reflected (Referer)
- Cross-Site Scripting -Reflected (User-Agent)
- Cross-Site Scripting -Stored (Cookies)
- Cross-Site Scripting -Stored (SQLiteManager)

/ A4 -Insecure Direct Object References /

- Insecure DOR (Reset Secret)
- Insecure DOR (Order Tickets)

/ A5 -Security Misconfiguration /

- Cross-Origin Resource Sharing (AJAX)
- Cross-Site Tracing (XST)
- Denial-of-Service (XML Bomb)
- Insecure FTP Configuration
- Insecure SNMP Configuration
- Insecure WebDAV Configuration
- Man-in-the-Middle Attack (SMTP)
- Old/Backup & Unreferenced Files

/ A6 -Sensitive Data Exposure /

- Heartbleed Vulnerability
- Host Header Attack (Reset Poisoning)
- POODLE Vulnerability
- SSL 2.0 Deprecated Protocol

/ A7 -Missing Functional Level Access Control /

- Directory Traversal -Files
- Remote & Local File Inclusion (RFI/LFI)
- Restrict Folder Access
- Server Side Request Forgery (SSRF)
- XML External Entity Attacks (XXE)

/ A8 -Cross-Site Request Forgery (CSRF) /

- Cross-Site Request Forgery (Change Secret)
- Cross-Site Request Forgery (Transfer Amount)

/ A9 -Using Known Vulnerable Components /

- Heartbleed Vulnerability
- phpMyAdmin BBCode Tag XSS
- Shellshock Vulnerability (CGI)
- SQLiteManager Local File Inclusion
- SQLiteManager XSS

/ A10 -Unvalidated Redirects & Forwards /

- Unvalidated Redirects & Forwards (1)
- Unvalidated Redirects & Forwards (2)

Curso Avanzado – API Hacking

CURSO : API Hacking

Duración : 24 Horas

Observaciones:

- El curso incluye manuales del curso
- Guía de Laboratorio

DESCRIPCION DEL CURSO

Descripción del curso

API está siendo utilizada por todas las aplicaciones web/móviles/de_escritorio para comunicarse entre sí. Pero, como cualquier otra tecnología, tiene sus fortalezas y debilidades. En este curso nos centraremos en la API REST y revisaremos las técnicas utilizadas para encontrar debilidades y explotarlas, también las contramedidas utilizadas por los desarrolladores.

¿Que aprenderás?

- Estándares API (p. Ej., Autenticación, intercambio de datos, etc.)
- Ataques API y contramedidas

¿Qué habilidades ganarás?

- Experiencia práctica en pentesting REST API
- Cómo implementar API segura

Que necesitara?

- PC con un sistema operativo preferido (Mac OSX 10.5+, Windows 7+, Linux)
- Herramienta de prueba de API (por ejemplo, PostMan)
- Herramienta de proxy (p. Ej., Burp Suite, Fiddler)

¿Qué deben saber los estudiantes antes de unirse?

- Conocimiento previo de cómo funciona la web (p. Ej., Protocolo HTTP, métodos HTTP, etc.)
- Comprensión de las vulnerabilidades web básicas (por ejemplo, XSS, CSRF, Open Redirect, IDOR, etc.)

SYLABUS DEL CURSO:

Module 1: Introduction to API

- What is API/API Centric Applications?
- Intro to REST.
- REST API Fingerprinting / Fuzzing.
- Intro to API Authentication (Basic, JWT, OAuth).

Module 1 exercises:

- Fingerprinting API.
- REST Methods Manipulations.

Module 2: Authentication part 1

- Basic Authentication.
- Basic Digest Authentication.
- Session based vs Token based.
- JWT (Json Web Tokens) - Implementation & Attacks.

Module 2 exercises:

- Crack JWT Secret Key.
- Bypass JWT Hash Check.

Module 3: Authentication part 2 (Authorization)

- OAuth 1, 1.0a, 2 - Standards & Implementation.
- Stealing OAuth Access tokens.
- CSRF Attack on OAuth.
- Attacking authorization code grant flow.
- Open Redirect in OAuth.

Module 3 exercises:

- Steal OAuth tokens.
- Attack Authorization Flow.
- CSRF Attack on OAuth.

Module 4: Other Attacks On API

- DoS attacks on API.
- Bruteforcing Attacks.
- Attack Development/Staging API's.
- Traditional attacks (XSS, SQLI, IDOR, etc.).

Module 4 exercises:

- Basic sqli/xss attack on API.
- Finding Dev API and use it to bypass protection on production API.