UNIVERSIDAD NACIONAL DE INGENIERÍA
FACULTAD DE INGENIERÍA INDUSTRIAL Y SISTEMAS

SISTEMAS UNI
Tecnologías de la Información

WORKSHOP

ETHICAL HACKING SEGURIDAD EN APLICACIONES WEB

El curso de Ethical Hacking muestra técnicas para vulnerar y proteger aplicaciones:
-Técnicas básicas y avanzas de INYECCIONES sobre aplicaciones web.
-Gestión y ruptura de sesiones (Session Management).
-Ataques del tipo Cross Site Scripting (XSS).
-Malas conguraciones del servidor.

• Conocimientos Previos

Conocimiento básico del sistema Operativo Microsoft Windows. Conocimiento básico de algoritmos y estructura de datos.

• El participante al final del curso sera capaz de :

Aplicar los conocimientos y técnicas de seguridad informática para vulnerar y proteger aplicaciones web. Las técnicas se encuentran relacionadas a la metodología OTP (OWASP Testing Project).

- **Dirigido a:** Estudiantes, Profesionales y Publico en General
- **Duración del curso: 24 Hrs. / 5 sesiones**

Evaluación

Será totalmentepráctica. Se realizarán entre 4 o 5 prácticas de las cuales se eliminará la nota más baja y se obtendrá un promedio (PP). Durante la última sesión se realizará un examen final (EF), el cual se promediará con la nota de prácticas y de esta manera se tendrá la calificación final

PROMEDIO DE PRÁCTICAS:

PP=(PR1 + PR2 + PR3 + PR4 - MENOR (PR)

NOTA FINAL:

NF= PP + EF

Modalidad Online

Requiere una PC con las siguientes caracteristicas:

- Procesador - 1GHZ o más rapido / en un chip (SOC).
- RAM - 1GB para 32 Bits o 2GB para 64.
- Espacio Libre 16GB - SO de 32 bits / 32GB - SO de 64 bits.
- Una tarjeta gráfica - DirectX 9, posterior o controlador WDDM 1.0.
- Pantalla - 800x 600 resolución.
- Conexión a internet estable.

Conéctate a nuestras diferentes Plataformas Digitales:

Telf.: 200 - 9060 Opción 1 / E-mail: sisuni.info@uni.edu.pe

/ /

www.sistemasuni.edu.pe

“Aumenta tus conocimientos, desarrolla nuevas habilidades y construye hoy tu futuro”.

LISTA DE TEMAS

• Introducción al desarrollo seguro de aplicaciones web.
• Introducción a OTP (OWASP Testing Project).
• Inyecciones de código SQL.
• CTF 01: Desarrollo de ejercicio práctico.

LISTA DE TEMAS

• Cross Site Scripting (XSS).
-Técnicas avanzadas de explotación.
- Mapeo de computadores con JAVASCRIPT.
- Robo de sesiones con JAVASCRIPT.
-Ejecutables para obtener sesión remota con Metasploit.
-CTF 02: Desarrollo de ejercicio práctico.
• Manejo inadecuado de Carga de archivos.
-Concepto de la carga de archivos a través de formularios web.
- Manipulación de la extensión del archivo.
- Manipulación del tipo de archivo.
-Creación de imágenes con BACKDOORS y PAYLOADs.

LISTA DE TEMAS

• Gestión y ruptura de autenticación.
• Herramienta: BURPSUITE.
• Cross Site Scripting (XSS).
• Definición de los ataques del lado del cliente.
• Introducción al JAVASCRIPT.
• Tipos de Cross Site Scripting.

LISTA DE TEMAS

• Remote/Local File Inclusion.
• CTF 03: Desarrollo de ejercicio práctico.
• Examen FINAL.