

Hackeando Aplicaciones Web

Código: HACK-104

Propuesta de Valor: SEGURIDAD INFORMÁTICA

Duración: 15 Horas



Este curso está orientado a toda persona que esté interesada en comprender las técnicas y herramientas de ataque a aplicaciones web que utilizan los hackers actualmente, así como también sacar provecho de las mismas para aumentar la seguridad de las organizaciones.

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.

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.

Más información: [AQUÍ](#)

Reserve su plaza: [AQUÍ](#)



AUDIENCIA

Profesionales del área de seguridad de la información.



PRE REQUISITOS

Conocimientos en seguridad de la información.



OBJETIVOS

- En este curso se enseña a los participantes a entender las principales fallas en las aplicaciones web y su explotación; y lo más importante; aprender a realizar un proceso repetible y verificado en la realidad, para encontrar de manera consistente estas fallas en sus organizaciones.



CERTIFICACIÓN DISPONIBLE



CONTENIDO

1. CYBERSECURITY & RISK MANAGEMENT
2. COMMON ATTACKS TYPES & VECTORS
3. CYBERSECURITY CONTROLS
4. TYPES OF DEFENSE IN DEPTH IMPLEMENTATIONS
5. VULNERABILITY WEB SCANNING
6. SEGURIDAD EN CMS
7. SEGURIDAD EN HTML 5
8. TOP VULNERABILITIES & MANAGEMENT
 - 8.1. INJECTION
 - 8.2. BROKEN AUTHENTICATION AND SESSION MANAGEMENT
 - 8.3. CROSS SITE SCRIPTING
 - 8.4. INSECURE DIRECT OBJECTS REFERENCES
 - 8.5. SECURITY MISCONFIGURATION
 - 8.6. SENSITIVE DATA EXPOSURE
 - 8.7. MISSING FUNCTIONS LEVEL ACCESS CONTROL
 - 8.8. CROSS SITE REQUEST FORGERY
 - 8.9. USING COMPONENTS WITH KNOWING VULNERABILITIES
 - 8.10. UNVALIDATED REDIRECTS AND FORWARDS



BENEFICIOS

