ETHICAL HACKING WEB APPLICATION (EHWEB)

DESCRIÇÃO

(Nível Básico/Intermediário)

Carga Horária: 40 hrs

No Ethical Hacking Web Application (EHWEB), o aluno aprenderá, de forma prática, a executar testes de vulnerabilidades em aplicações web, com o intuito de encontrar falhas e reportá-las para as devidas correções.

As aplicações web desempenham um papel vital em todas as organizações (pequeno, médio ou grande porte), dessa forma, se estas aplicações não forem corretamente testadas e protegidas, podem ser alvos de ataques com objetivos de comprometê-las, danificar as funcionalidades do negócio, roubar dados entre outros. Realizar testes de segurança nessas aplicações é uma das principais demandas no cenário de Segurança Ofensiva em auxílio à proteção de uma organização.

Este treinamento tem por objetivo apresentar metodologias para testes de aplicações web, explicar as principais vulnerabilidades encontradas, entender como funcionam os ataques a aplicações web, abordar ferramentas e técnicas para realização dos testes e desenvolver a capacidade de encontrar falhas ao analisar uma aplicação e reportá-las de acordo com o impacto para o negócio.

O conteúdo do curso está alinhado com as boas práticas de segurança do Open Web Application Security Project (OWASP), possui conteúdo 100% prático (*hands-on*) com laboratórios de nível Básico/Intermediário e é indicado para os alunos que estão iniciando na área de Teste de Invasão (Pentest) em Aplicações Web.

MÓDULO 1 – APLICAÇÕES WEB

- Fundamentos de Aplicações Web
- OWASP Top 10
- Aprendendo a usar o Burp Suite
- Como Funciona o HTTP/HTTPS e o HTTP 2
- Como funciono o HTML, CSS e o Javascript
- Linguagens de programação Server-Side e Client-side
- Servidores Web
- Server-Side Databases
- Client-Side Data Stores
- REST *Application Programming Interface* (API)
- O modelo de micro serviços
- O que são os frameworks?
- Server-Side Frameworks
- Client-Side Frameworks
- Web Sockets
- Aplicações Modernas Versus Aplicações legadas
- Codificação de Strings
- A política de mesma origem dos navegadores
- Cross-Origin Resource Sharing (CORS)
- Metodologias para Pentest Web
- Black Box vs White Box

MÓDULO 2 – WEB APPLICATION RECONNAISSANCE (RECON)

- Coleta passiva e ativa de informação.
- Mapeamento de DNS
- Mapeamento de Aplicações Web
- Mapeamento de APIs
- Análise de código no frontend
- Engenharia social para ataques web
- Escaneamento automatizado de sistemas web
    - ✔ Laboratório

MÓDULO 3 – CLIENT-SIDE EXPLOITATION

- Ataque de redirecionamento de URLs (Open-Redirect)
    - ✔ Laboratório
- Cross-Site Scripting (XSS)
    - ✔ Laboratório
- Client-Side Template Injection (CSTI)
    - ✔ Laboratório
- Cross-Site Request Forgery (CSRF)
    - ✔ Laboratório
- Combinando ataques no lado cliente para provar impacto
    - ✔ Laboratório

MÓDULO 4 – AUTHENTICATION, AUTHORIZATION AND SESSION EXPLOITATION

- Escalação de privilégio em Aplicações Web
  - ✔ Laboratório
- Manipulando parâmetros de administração
  - ✔ Laboratório
- Burlando mecanismos de autenticação baseados em hash
  - ✔ Laboratório Hash Client-Side Bypass Auth
- Enumeração de usuários em formulários web
  - ✔ Laboratório
- Ataques de dicionário & força bruta em formulários
  - ✔ Laboratório
- Ataques de dicionários com Anti-CSRF Token
  - ✔ Laboratório
- Bypass de captcha texto nos ataques de dicionário & força bruta
  - ✔ Laboratório
- Usando valores de cache para Captcha Bypass
  - ✔ Laboratório
- Ataques de dicionário com bypass de captcha em imagem
  - ✔ Laboratório

MÓDULO 5 – INJECTIONS EXPLOITATION

- Injeção de SQL - SQL Injection (SQLi)
  - ✔ Laboratório
- Injeção Remota de Comandos – Remote Command Injection (RCE)
  - ✔ Laboratório de RCE e SQLi – Combinando as vulnerabilidades
- Introdução à Banco de Dados Orientados a Objetos
- Injeção de NoSQL
  - ✔ Laboratório
- Injeção de código PHP
  - ✔ Laboratório

MÓDULO 6 – EXTRA EXPLOITATION

- Insecure Direct Object References (IDOR)
  - ✔ Laboratório
- Server-Side Request Forgery (SSRF)
  - ✔ Laboratório
- XML eXternal Entity (XXE)
  - ✔ Laboratório
- Exploração de Content Management System (CMS)
  - ✔ Laboratório

MÓDULO 7 – EXPLOITATION

- Injeção de arquivos - Local/Remote File Inclusion (LFI/RFI)
    - ✔ Laboratório de RFI e LFI – Desafio com combinações
- Ataque de desserialização com Python
    - ✔ Laboratório
- Server-Side Template Injection (SSTI)
    - ✔ Laboratório de SSTI
- Entendendo a utilidade de se poluir parâmetros (Parameter Pollution)
- DoS | Stress
    - ✔ Laboratório de Negação de serviço

MÓDULO 8 – EXPLORAÇÃO DE API WEB

- Entendendo *Application Programming Interface* (API) Web
- Montando o meu arsenal
- Reconhecimento
    - ✔ Laboratório de API Recon
- OWASP API Security Top 10
    - ✔ Laboratório de Ataques a APIs
    - ✔ ChatGPT Prompt Injection
- Fundamentos de GraphQL
    - ✔ Laboratório de exploração de GraphQL

MÓDULO 9 – REPORTING (RELATÓRIO)

- Dicas para elaboração de um relatório de qualidade
- Classificação e pontuação (*scoring*) de vulnerabilidades
- CVE, CWE e CVSS
- Sugestões de formato do relatório
- Links e sugestões extras

PRÉ-REQUISITOS

- Conhecimentos básicos em Sistema Operacional Windows e Linux
- Estrutura de diretórios, comandos básicos do prompt/shell, configuração de rede, verificação de serviços e processos, gerenciamento de usuários locais, permissão de arquivos
- Conhecimentos básicos de Rede de Computadores, Serviços de Rede e Programação
- Conhecimentos básicos de protocolos TCP/IP, HTTP, HTTPS, SSH, DNS, ICMP
- Conhecimentos em lógica de programação
- Conhecimentos básicos de programação
- Familiaridade com a distribuição Kali Linux
- Familiaridade com ferramentas de Virtualização – VMWare

PÚBLICO ALVO

- Especialistas em Segurança da Informação
- Analista de Segurança da Informação
- Pentesters
- Desenvolvedores de Aplicações Web
- Membros de Red Team / Blue Team
- Membros de CSIRT
- Analista de SOC
- Profissionais de TI com interesse e afinidade na área de Segurança da Informação
- Profissionais com interesse na área de Bug Bounty Web

MATERIAL NECESSÁRIO

- Os alunos devem utilizar suas próprias estações de trabalho (Windows, Linux ou Mac OS), com a capacidade de executar até 03 (três) Máquinas Virtuais (VM) simultaneamente.
- Configuração mínima de 8GB de RAM, 50 GB de espaço livre em disco, porta USB e placa de rede (RJ45 ou *wireless*) para acesso à Internet.
- Desejável 02 (dois) monitores para incremento na produtividade.
- Software de Virtualização: VMWare, preferencialmente, a versão mais atualizada.

MATERIAL RECEBIDO

- Slides do Curso no formato PDF
- Acesso ao portal do aluno, o GoHacking Academy
- Gravação das sessões ao vivo
- Acesso aos laboratórios online
- Certificado de Conclusão do Curso no formato PDF (com a carga horária e ementa)

CAPACIDADES ALCANÇADAS

No final do curso, o aluno estará apto a:

- Entender o funcionamento de Aplicações Web
- Analisar os principais componentes de uma Aplicação Web
- Compreender o funcionamento de APIs Web
- Entender aspectos da Segurança Ofensiva aplicados em Serviços e Aplicações Web
- Compreender os principais modelos e frameworks para testes de segurança em Serviços e Aplicações Web
- Entender as principais vulnerabilidades existentes em Aplicações Web
- Mapear as principais falhas em Serviços e Aplicações Web
- Identificar e explorar vulnerabilidades em Aplicações Web
- Explorar vulnerabilidades em APIs Web
- Compreender a importância das atividades de Teste de Invasão (Pentest) Web
- Planejar um Teste de Invasão (Pentest) em Aplicações Web
- Adotar metodologia sólida para testes de segurança em Aplicações Web
- Dominar os principais aspectos de exploração de falhas de Aplicações Web
- Realizar um Pentest Web e produzir relatório de forma adequada

JOSÉ AUGUSTO DE ALMEIDA JUNIOR