ETHICAL HACKING WEB API (EHAPI)

DESCRIÇÃO

(Nível Básico/Intermediário)

Carga Horária: 12 hrs

O curso Ethical Hacking Web API (EHAPI) ensina, de forma prática, a executar testes de vulnerabilidades em *Application Programming Interface* (API) de sistemas 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), o que as tornam um alvo frequente de ataques cibernéticos. E o emprego dessas aplicações, normalmente, envolve a utilização de APIs. Dessa forma, realizar testes de segurança nessas estruturas é uma tarefa crucial para a proteção de qualquer empresa.

Este treinamento tem por objetivo apresentar metodologias para testes em APIs web, explicar as principais vulnerabilidades encontradas na implementação de APIs, entender como funcionam os ataques a APIs web, abordar ferramentas e técnicas para realização dos testes e desenvolver a capacidade de encontrar e corrigir falhas ao analisar uma API.

O conteúdo do curso está alinhado com as boas práticas de segurança do Open Web Application Security Project (OWASP), com uma abordagem 100% prático (*hands-on*), incluindo 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 – FUNDAMENTOS DE API

1. O que é uma *Application Programming Interface* (API) Web
2. Definição e principais utilizações de APIs
3. Métodos HTTP e estrutura de requisições API
4. API RESTful

MÓDULO 2 – FERRAMENTAS

1. Visão geral de ferramentas para análise de APIs
2. Utilização de Postman e Burp Suite
3. Configuração e utilização básica de ferramentas

MÓDULO 3 – EXPLORAÇÃO

1. Técnicas de reconhecimento de APIs
2. OWASP API Security Top 10
3. Técnicas de Invasão para vulnerabilidades do OWASP Top 10 API
4. *Server Side Template Injection* (SSTI) em APIs
5. Exploração de autenticação baseada em *hash* do lado do cliente
6. Ferramentas e técnicas de debug
7. Introdução ao debug do lado do cliente
8. Identificação de pontos de exploração através do debug com Postman e Burp Suite
9. Engenharia reversa de APIs
10. Fundamentos de GraphQL
11. Exploração de GraphQL

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 02 (duas) 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 APIs Web
- Entender os principais aspectos do OWASP API Security Top 10
- Entender as principais vulnerabilidades existentes em APIs de Aplicações Web
- Mapear as principais falhas em APIs Web
- Explorar vulnerabilidades em APIs Web
- Compreender a importância das atividades de Teste de Invasão (Pentest) em APIs 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 de API Web e produzir relatório de forma adequada

JOSÉ AUGUSTO DE ALMEIDA JUNIOR