Web Application Penetration Tester Roadmap

An in-depth guide on becoming a proficient web application penetration tester.

lyself

. M. Faruk Ahmed

SSP, CC, CISA, CDCP, ITAF Reviewer
Sc in CSE (IU), M.Sc in SE, CEMBA, DAIBB

ofessional Details:

am Lead, IT Audit & Cyber Security
nior Principal Officer (Senior Programmer),
pali Bank Limited.
om Feb, 2012 – Till now

oject: CBS, DC, DR, ICT Security Policy, BCP

ftware Engineer
ADS Corporation Limited
om Dec, 2008 to Feb, 2012

oject: Core Banking Solution

linkedin.com/in/gmfaru

Youtube.com/learnspla

https://www.gmfaruk.

Agenda

1
Introduction

2
Getting Started

3
Learning Programming

4
Networking Fundamentals

5
Operating Systems Knowledge

6
Introduction to Cybersecurity

7
Sensitive Data Exposure

8
Tools for Pentesting

9
Web Application Firewalls (WAF)

10
Career Path Options

11
Conclusion

12
Soft Skills Development

Introduction

Overview of web application penetration testing.

Importance and growing demand in cybersecurity.

Getting Started

Fundamental skills and prerequisites.

Basic understanding of networks, OS, and cybersecurity concepts.

Learning Programming

Recommended languages: Python, JavaScript, and SQL.

Role of coding skills in penetration testing.

Networking Fundamentals

Understanding TCP/IP, HTTP/S, DNS.

Network layers and protocols vital for testing.

Operating Systems Knowledge

Familiarity with Linux, Windows, and macOS.

Basics of command-line interfaces.

Introduction to Cybersecurity

Concepts like CIA triad, risk management, and encryption.

Basic security protocols and frameworks.

Web Application Basics

Understanding web architecture, servers, and databases.

Common platforms: Apache, Nginx, SQL databases.

Setting Up Lab Environment

Using virtual machines and Docker.

Testing tools: Burp Suite, OWASP ZAP, Metasploit.

Web Technologies

Familiarity with HTML, CSS, JavaScript.

Backend languages: PHP, Python, Ruby, Node.js.

Authentication & Session Management

Understanding login mechanisms and session cookies.

Common vulnerabilities in authentication.

Input Validation

Importance of sanitizing inputs to prevent injections.

Introduction to SQL and command injection vulnerabilities.

Cross-Site Scripting (XSS)

Understanding XSS and its types (Reflected, Stored, DOM).

Techniques for detecting and exploiting XSS.

Cross-Site Request Forgery (CSRF)

How CSRF attacks occur and their impacts.

Mitigation techniques and prevention strategies.

Broken Access Control

Testing access control flaws in web applications.

OWASP guidelines for proper access management.

Security Misconfigurations

Identifying and fixing security misconfigurations.

Examples: error messages, default settings, open ports.

Sensitive Data Exposure

Importance of encrypting sensitive data.

Techniques to detect unencrypted data and mitigate risks.

Tools for Pentesting

Overview of Burp Suite, Nmap, Nikto, and more.

Using automated tools for vulnerability detection.

Web Application Firewalls (WAF)

Role of WAFs in protecting web apps.

Testing bypass techniques for WAFs.

API Security Testing

Testing REST and SOAP APIs.

Common API vulnerabilities: improper authentication, rate limiting.

Bug Bounty Programs

Getting started with bug bounty platforms.

Practicing and gaining real-world experience.

OWASP Top 10

Understanding and testing OWASP Top 10 vulnerabilities.

Why these vulnerabilities are prioritized.

Reporting Findings

Importance of clear and concise reporting.

Creating executive summaries and detailed technical reports.

Maintaining Confidentiality

Ethical considerations and legal implications.

Non-disclosure agreements and client privacy.

Continuous Learning

Staying updated with the latest vulnerabilities and tools.

Joining cybersecurity communities and forums.

Certifications

Recommended certifications: CEH, OSCP, GWAPT.

Importance of certifications in career growth.

Penetration Testing Methodologies

Popular methodologies: PTES, OWASP Testing Guide.

Following structured approaches in tests.

Soft Skills Development

Communication, problem-solving, and analytical skills.

Importance of presenting findings effectively.

Career Path Options

Different roles: security analyst, consultant, researcher.

Average salaries and growth potential.

Conclusion

Summary of skills and steps to become a web application penetration tester.

Encouragement for continuous improvement and ethical responsibility.

Thank You!

linkedin.com/in/gmfaruk/