THROUGHSEC

Web Application Penetration testing

Course Overview:

This course provides a comprehensive foundation in web security, starting with web basics and advancing through various common web vulnerabilities, including Local File Inclusion, SQL Injection, Command Injection, and more. Through a mix of theory, hands-on labs, and challenges on platforms like Root-Me and PortSwigger, participants will learn to identify, exploit, and understand the impact of these vulnerabilities in real-world scenarios. By the end of this course, students will be equipped with the knowledge and tools needed to assess and secure web applications effectively.

Module 1: Web Basics & Burp Suite Fundamentals

- **Objectives:**
    - Understand the basics of HTTP, HTML, and how the web works.
    - Introduction to Burp Suite for intercepting and analyzing traffic.
- **Topics Covered:**
    - HTTP Methods, Status Codes, Cookies, and Sessions.
    - Setting up and configuring Burp Suite for web security testing.
    - Basic Burp Suite tools: Proxy, Repeater, Intruder.
- **Hands-on Practice:**
    - Solve basic challenges on Root-Me to reinforce web basics.

Module 2: Local File Inclusion (LFI) / Path Traversal

- **Objectives:**
    - Understand LFI and Directory Traversal vulnerabilities.
- **Topics Covered:**
    - Recognizing LFI vulnerabilities and crafting path traversal payloads.
    - Exploiting LFI for sensitive file exposure and understanding risk mitigation.
- **Hands-on Labs:**
    - Root-Me and PortSwigger Labs: Explore and complete LFI challenges.

Module 3: SQL Injection

- **Objectives:**
    - Identify and exploit SQL Injection (SQLi) vulnerabilities.
- **Topics Covered:**
    - SQL Injection basics, common payloads, and methods for exploitation.
    - Different types of SQLi: Union-based, Error-based, Blind SQL Injection.
- **Hands-on Labs:**
    - Practice SQL Injection rooms on Root-Me and PortSwigger.

Module 4: Command Injection

- **Objectives:**
    - Understand Command Injection vulnerabilities and exploit them.
- **Topics Covered:**
    - Identifying command injection and bypass techniques.
    - Risks of command injection and common mitigation strategies.
- **Hands-on Labs:**
    - Root-Me and PortSwigger rooms focused on Command Injection.

Module 5: File Upload Vulnerabilities

- **Objectives:**
    - Explore file upload vulnerabilities and their impact on web security.
- **Topics Covered:**
    - Exploiting unrestricted file uploads and bypassing restrictions.
    - Malicious file upload techniques: web shells, script injections.
- **Hands-on Labs:**
    - Rooms on Root-Me and PortSwigger that involve file upload vulnerabilities.

Module 6: XML External Entity (XXE) Injection

- **Objectives:**
    - Identify and exploit XXE vulnerabilities in web applications.
- **Topics Covered:**
    - Introduction to XML and XXE basics.

  - Techniques for detecting and exploiting XXE.
- **Hands-on Labs:**
  - Practice XXE scenarios on Root-Me and PortSwigger.

Module 7: NoSQL Injection

- **Objectives:**
  - Understand NoSQL databases and exploit NoSQL Injection vulnerabilities.
- **Topics Covered:**
  - Basics of NoSQL databases and injection attacks.
  - Identifying NoSQL Injection in web applications.
- **Hands-on Labs:**
  - Root-Me and PortSwigger NoSQL Injection challenges.

Module 8: Cross-Site Scripting (XSS)

- **Objectives:**
  - Explore Cross-Site Scripting (XSS) vulnerabilities.
- **Topics Covered:**
  - XSS types: Reflected, Stored, and DOM-based.
  - Techniques for detecting and exploiting XSS.
  - XSS impact and prevention techniques.
- **Hands-on Labs:**
  - XSS challenges in Root-Me and PortSwigger.

Note: Each module includes practical labs, quizzes, and assignments designed to reinforce key concepts and provide real-world application. The course culminates in a hands-on project, offering students the opportunity to showcase their skills in a real-world scenario.

Key Target Audience:

1. **Aspiring Penetration Testers**: Those new to penetration testing and interested in focusing on web applications, learning the latest techniques and methodologies.
2. **Cybersecurity Students**: College or university students pursuing cybersecurity or ethical hacking programs who want to specialize in web application security.
3. **Security Analysts**: Professionals already working in a security operations center (SOC) or network security role who wish to transition into application security.
4. **Web Developers**: Developers looking to improve their understanding of common security flaws in web applications and how to avoid them.
5. **Red Team Members**: Security professionals involved in red teaming who want to deepen their knowledge of web application exploitation techniques.
6. **Bug Bounty Hunters**: Individuals looking to enhance their skills in identifying vulnerabilities in web applications for bug bounty programs.
7. **Security Consultants**: Consultants working with organizations to assess the security of web applications, looking to improve their technical penetration testing skills.