Advance Web Penetration Testing

Course Overview

Welcome to the **Advanced Web Application Penetration Testing course**. This course is designed to teach you how to identify, exploit, and mitigate security vulnerabilities in web applications. You only need a positive attitude and a desire to learn; no prior hacking knowledge is required. **While prior experience in web development or basic cybersecurity is beneficial**, this course covers both foundational and advanced topics, making it suitable for everyone. By the end of this course, you'll have a solid understanding of web application security and be ready to handle real-world challenges in web penetration testing.

Requirements

1. Join Our Official Telegram
2. Basic IT knowledge.
3. A minimum of 8GB of RAM is suggested.
4. For Lab Build: A minimum of 16GB of RAM is suggested. Students can still participate in the course but may experience slow lab environments.

Course Curriculum

▢ Module 01: Introduction to Web Application Security

- **Request Handling Basics**

    - Fundamentals of how web applications handle requests.
    - Understanding request and response cycles.
- **Understanding URLs and Navigation**
    - Detailed explanation of URL components.
    - Techniques for URL manipulation.
- **Introduction to Web Domains**
    - Understanding domain structures and DNS.
    - Techniques for discovering subdomains.
- **Overview of Lab Environments**
    - Setting up and navigating through lab environments for testing.
- **Security Reporting Fundamentals**
    - Writing effective security reports.
    - Key elements of a good vulnerability report.

▢ Module 02: Information Gathering and Target Selection

- **Reconnaissance Techniques**
- **Active and Passive Reconnaissance Methods**
    - Cyber Threat Intelligence
    - WHOIS Information Gathering
    - DNS Information Gathering
    - Social Media Information Gathering
- **Target Selection and Analysis**
- **Scope Analysis**
- **Setting Up Automation For Information Gathering**

▢ Module 03: Subdomain Enumeration

- **Using Search Engines & Google Dorks**
    - Techniques for finding subdomains using search engines.
    - Search Engine Information Gathering
    - Dark Web Investigation
    - Google Dorking
    - Shodan, FOFA, Censys Dorking
- **Publicly Available Data**
    - Leveraging public records and databases for subdomain discovery.
- **Certificate Transparency**
    - Using certificate transparency logs for subdomain enumeration.

- **Dictionary-Based Enumeration**
  - Techniques and tools for dictionary-based subdomain enumeration.
- **Setting Up Automation For Subdomain Enumeration**

▢ Module 04: Port Scanning

- **Using Kali Linux for Port Scanning**
  - Tools and techniques in Kali Linux for effective port scanning.
- **Using Various Open Source Tools**
  - Exploring different open-source tools for port scanning and their configurations.
- **Setting Up Automation For Port Scanning**

▢ Module 05: Installing and Understanding Burp Suite

- **Proxy -** Setting up and configuring Burp Suite Proxy.
- **Target -** Using the Target tool for site mapping and analysis.
- **Spider -** Automating the discovery of content with the Spider tool.
- **Scanner -** Automated scanning for vulnerabilities.
- **Repeater -** Crafting and sending custom requests with the Repeater tool.
- **Intruder -** Automated customized attacks with the Intruder tool.
- **Decoder -** Encoding and decoding data with the Decoder tool.
- **Comparer -** Comparing different sets of data with the Comparer tool.
- **Sequencer -** Analyzing the randomness of tokens.

▢ Module 06: OWASP Top 10

- Introduction to OWASP Top 10
- Injection Attacks
- Broken Authentication
- Sensitive Data Exposure
- XML External Entities (XXE)
- Broken Access Control
- Security Misconfigurations
- Cross-Site Scripting (XSS)
- Insecure Deserialization
- Using Components with Known Vulnerabilities

- Insufficient Logging and Monitoring

▢ Module 07: HTML Injection

- **Explanation and Demo of HTML Injection**
  - Understanding the impact and exploitation of HTML injection vulnerabilities.

▢ Module 08: Cross-Site Scripting (XSS)

- **Detailed Concept about XSS**
  - In-depth understanding of XSS vulnerabilities.
- **Reflected XSS**
  - Techniques and examples of Reflected XSS.
- **Stored XSS**
  - Understanding and exploiting Stored XSS.
- **DOM-based XSS**
  - Techniques for finding and exploiting DOM-based XSS.
- **Basic XSS on Lab**
  - Practical lab for basic XSS exploitation.
- **The Exploitation of XSS URL Redirection**
  - Using XSS for URL redirection attacks.
- **The Exploitation of XSS Phishing Through XSS**
  - Crafting phishing attacks using XSS.
- **The Exploitation of XSS Cookie Stealing**
  - Stealing cookies using XSS vulnerabilities.
- **XSS Through Remote File Inclusion**
  - Combining XSS with remote file inclusion.
- **XSS Through File Uploading**
  - Exploiting file upload functionalities for XSS.
- **Setting Up Automation For Cross-Site Scripting**

▢ Module 09: Host Header Injection

- **XSS Through Host Header Injection**
  - Exploiting XSS using host header injection.
- **Host Header Attack Open Redirection**
  - Leveraging host header manipulation for open redirection.

- **Host Header Attack Cache Poisoning**
  - Techniques for cache poisoning using host header attacks.
- **Host Header Attack Password Reset Poisoning**
  - Exploiting password reset mechanisms via host header injection.

▢ Module 10: SQL Injection

- **Detailed Concept of SQL Injection**
  - Comprehensive understanding of SQL injection.
- **SQL Injection Lab Setup**
  - Setting up a lab environment for SQL injection testing.
- **Injection Points for SQL Injection**
  - Identifying potential injection points.
- **SQL Injection on GET Parameter**
  - Exploiting SQL injection vulnerabilities in GET parameters.
- **SQL Injection on POST Parameter**
  - Techniques for POST parameter SQL injection.
- **Cookie-Based SQL Injection**
  - Exploiting SQL injection through cookies.
- **WAF Bypass in SQL Injection**
  - Techniques to bypass Web Application Firewalls during SQLi.
- **Authentication Bypass Using SQLi**
  - Using SQL injection to bypass authentication.
- **Setting Up Automation For SQL Injection**

▢ Module 11: Unvalidated Redirects and Forwards

- **Techniques for Identifying and Exploiting Unvalidated Redirects**
  - Finding and exploiting unvalidated redirects.
- **Setting Up Automation For Open Redirection**

▢ Module 12: File Uploading & Bypass Methods

- **Secure File Uploading Techniques**
  - Understanding and exploiting file upload vulnerabilities.

▢ Module 13: Rate Limits and Tricks

- **Techniques to Bypass Rate Limits**
  - Bypassing rate limit protections.

▢ Module 14: Parameter Tampering

- **Exploiting Parameter Tampering**
  - Identifying and exploiting parameter tampering vulnerabilities.

▢ Module 15: IDOR (Insecure Direct Object Reference)

- **Techniques to Exploit IDOR**
  - Finding and exploiting IDOR vulnerabilities.

▢ Module 16: SSRF (Server-Side Request Forgery)

- **What is SSRF?**
  - Understanding SSRF attacks.
- **Exploitation of SSRF**
  - Techniques for exploiting SSRF vulnerabilities.
- **Setting Up Automation For SSRF**

▢ Module 17: CORS Exploitation

- **Detailed Concept about CORS**
  - Understanding Cross-Origin Resource Sharing (CORS).
- **Insecure CORS by Checking Response Header**
  - Exploiting insecure CORS configurations via response headers.
- **Insecure CORS through Request Header**
  - Finding and exploiting CORS issues via request headers.
- **Same Origin Policy, All Scenarios**
  - Comprehensive coverage of same-origin policy and its exploitation.

▢ Module 18: Subdomain Takeover

- **Detailed Concept of Subdomain Takeover**
  - Understanding and exploiting subdomain takeovers.
- **Demo**
  - Practical demonstration of subdomain takeover.

▢ Module 19: Command Injection

- **The Detailed Concept of Command Injection**
  - Comprehensive understanding of command injection.
- **The Exploitation of Command Injection**
  - Techniques for exploiting command injection vulnerabilities.

▢ Module 20: Local File Inclusion & Remote File Inclusion

- **Techniques for LFI & RFI**
  - Exploiting local file & remote file inclusion vulnerabilities.

▢ Module 21: CSRF (Cross-Site Request Forgery)

- **Detailed Concept of CSRF**
  - In-depth understanding of CSRF attacks.
- **Injection Point for CSRF**
  - Identifying injection points for CSRF.
- **CSRF on Logout Page**
  - Techniques for exploiting CSRF on logout pages.

▢ Module 22: XXE (XML External Entity) Injection

- **What is the XXE Attack**
  - Understanding XML External Entity (XXE) injection.
- **The Exploitation of XXE Attack**
  - Techniques for exploiting XXE vulnerabilities.

▢ Module 23: Business Logic Flaw

- **Identifying Business Logic Vulnerabilities**

- Understanding and finding business logic flaws.

▢ Module 24: Privilege Escalation and Automation

- **Techniques for Privilege Escalation**
  - Understanding privilege escalation and automation techniques.

▢ Module 25: Source Code Disclosure

- **Techniques for Source Code Disclosure**
  - Methods for discovering and exploiting source code disclosure vulnerabilities.

▢ Module 25: Exam & Certification

- **Comprehensive Evaluation of Course Content**
- **Certification for Successful Completion**

Key Features

1. **Live Trainer-Led Online Training**: Engage in interactive sessions led by experienced trainers.
2. **50 Hours of Classes Over 2 Months**: Comprehensive coverage of Advance Web Application Penetration Testing topics spread over two months.
3. **90% Practical Oriented**: Emphasis on hands-on learning and practical application.
4. **Pay in 2 Installments**: Flexible payment options to make the course more accessible.
5. **Career Oriented Training**: Focused on building skills needed for a successful career in cybersecurity.
6. **Practical Assignments & Live Bug Hunting and Reporting**: Practical assessments to test and enhance your skills.

Frequently Asked Questions

1. **What is Advanced Web Penetration Testing?** Advanced Web Penetration Testing is a specialized field of cybersecurity focused on identifying, exploiting, and mitigating

vulnerabilities in web applications through comprehensive testing techniques.

2. **Who should take this course?** This course is ideal for IT professionals, cybersecurity enthusiasts, web developers, security analysts, and anyone interested in learning advanced techniques for web application security testing.
3. **Do I need any prior experience in cybersecurity to enroll in this course?** While prior experience in web development or basic cybersecurity is beneficial, the course covers both foundational and advanced topics, making it suitable for those with varying levels of experience.
4. **What tools and software will I need for this course?** You will need a computer with internet access, virtualization software (like VMware or VirtualBox), and various penetration testing tools such as Burp Suite, Nmap, OWASP ZAP, and SQLmap. Detailed setup instructions will be provided during the course.
5. **Will there be hands-on labs and practical assignments?** Yes, the course includes hands-on labs, practical assignments, and Capture The Flag (CTF) challenges to ensure you gain practical experience and apply the concepts learned.
6. **What topics are covered in the course?** The course covers a wide range of topics including reconnaissance, subdomain enumeration, port scanning, HTML injection, XSS, host header injection, SQL injection, file uploading, parameter tampering, IDOR, SSRF, CORS exploitation, subdomain takeover, command injection, LFI, RFI, CSRF, XXE injection, business logic flaws, privilege escalation, and source code disclosure.
7. **How is the course structured?** The course is divided into several modules, each focusing on specific areas of web penetration testing. Topics are presented in a logical progression, starting with foundational concepts and advancing to more complex techniques.
8. **Will I receive a certificate upon completion of the course?** Yes, participants who successfully complete the course and all required assessments will receive a certificate of completion.
9. **Can I access the course material after completing the course?** Yes, you will have continued access to the course materials, including lecture notes, videos, and lab exercises, even after you have completed the course.
10. **How can I get help if I have questions or face difficulties during the course?** You can seek help through the course's online forums, email support, and live Q&A sessions with instructors. Additionally, there are resources and guides available to assist you throughout the course.

⚠Non-Disclosure Agreement Disclaimer⚠

This training program on Vulnerability Assessment and Penetration Testing (VAPT) is intended for educational purposes only. The techniques, methodologies, and information shared in

this training are meant to increase understanding and awareness of cybersecurity practices and ethical hacking concepts. It is important to note the following:

1. Legal and Ethical Use: The techniques and knowledge gained from this training should be used only for legal and ethical purposes. Participants are strictly prohibited from engaging in any malicious, illegal, or unauthorized activities using the information acquired from this training.

2. Respect for Privacy and Consent: Participants must always respect the privacy of individuals and obtain proper authorization before testing or assessing any systems, networks, or devices. Unauthorized access to systems is illegal and unethical.

3. No Guarantees: While efforts are made to provide accurate and upto-date information, no guarantees are made regarding the accuracy, completeness, or timeliness of the content. The training content may not cover all possible scenarios or reflect the latest developments in the field.

4. No Liability: The trainers and organizers of this training program are not liable for any actions taken by participants based on the knowledge gained from this training. Participants assume full responsibility for their actions and the consequences thereof.

5. Independent Research: Participants are encouraged to conduct their own independent research and due diligence before implementing any techniques or methodologies discussed in the training.

By participating in this ethical hacking training program, you acknowledge that you have read and understood this disclaimer. You agree to use the knowledge gained from this training

responsibly, within legal and ethical boundaries. The trainers and organizers of this training program are not responsible for any misuse or misinterpretation of the information provided.

⚠⚠⚠This disclaimer is an integral part of the training program and applies to all participants.⚠⚠⚠