

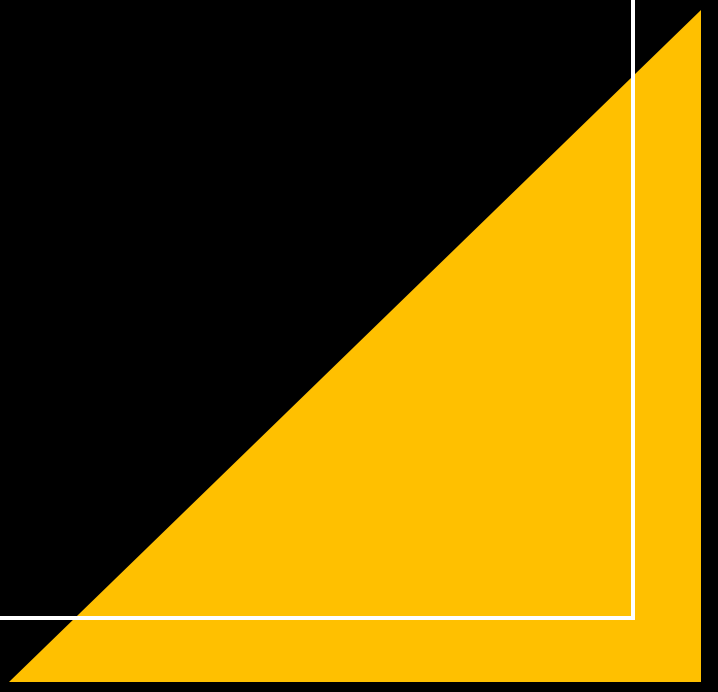
Web Penetration Testing Course

Boni Security




AGENDA

- Module 1: Introduction to Web Security and Penetration Testing
 - Module 2: Setting Up the Penetration Testing Environment
 - Module 3: Information Gathering and Footprinting
 - Module 5: Web Application Architecture and Technologies
 - Module 6: Web Application Fingerprinting and Analysis
 - Module 7: Vulnerability Assessment
 - Module 8: Exploitation Techniques
- 
- A large yellow right-angled triangle is positioned in the bottom right corner of the slide, pointing towards the top right.





AGENDA

- Module 9: Web Application Firewalls (WAFs) and Bypass Techniques
 - Module 10: Session Management and Authentication
 - Module 11: Web Application Security Best Practices
 - Module 12: Reporting and Documentation
 - Module 13: Advanced Topics
 - Module 14: Capture The Flag (CTF) Challenges]
 - Module 15: Legal and Ethical Considerations
- 
- A large yellow right-angled triangle is positioned in the bottom right corner of the slide, pointing towards the top right.




Final Project

-  Apply knowledge and skills acquired throughout the course
-  Conduct a comprehensive penetration test on a provided web application
-  Create a detailed report with findings and recommendations





Module 1: Introduction to Web Security and Penetration Testing

-  Overview of web security fundamentals
-  Importance of penetration testing
-  Legal and ethical considerations
-  Types of vulnerabilities in web applications




Module 2: Setting Up the Penetration Testing Environment

-  Installing and configuring Kali Linux
-  Setting up virtual environments
-  Introduction to essential tools (Burp Suite, OWASP ZAP, Nikto, etc.)




Module 3: Information Gathering and Footprinting

-  Passive reconnaissance techniques
-  Active reconnaissance techniques
-  DNS enumeration
-  WHOIS lookup and analysis




Module 5: Web Application Architecture and Technologies

-  Understanding web application architecture
-  Overview of common web technologies (HTML, CSS, JavaScript, AJAX, etc.)
-  Server-side vs. client-side technologies





Module 6: Web Application Fingerprinting and Analysis

-  Identifying web application frameworks
-  Analyzing HTTP headers
-  Extracting information from error messages




Module 7: Vulnerability Assessment

-  Manual and automated vulnerability assessment
-  Common web application vulnerabilities (SQL injection, Cross-Site Scripting, Cross-Site Request Forgery, etc.)
-  Assessing the security of third-party components (libraries, plugins)

Module 8: Exploitation Techniques

-  Advanced SQL injection
-  Cross-Site Scripting (XSS) exploitation
-  Command injection
-  File inclusion vulnerabilities





Module 9: Web Application Firewalls (WAFs) and Bypass Techniques

-  Understanding WAFs
-  Techniques to bypass WAFs
-  Evading detection and filtering





Module 10: Session Management and Authentication

-  Session management vulnerabilities
-  Cookie security
-  Password security and cracking techniques
-  Two-factor authentication (2FA) bypass




Module 11: Web Application Security Best Practices

-  Secure coding practices
-  Input validation and output encoding
-  Security headers implementation
-  Content Security Policy (CSP)




Module 12: Reporting and Documentation

-  Creating a penetration testing report
-  Prioritizing vulnerabilities
-  Communicating findings to stakeholders
-  Ethical disclosure and responsible reporting




Module 13: Advanced Topics

-  Mobile application security testing
-  API security testing
-  Web-sockets and other emerging technologie




Module 14: Capture The Flag (CTF) Challenges]

-  Hands-on practical exercises
-  Real-world scenarios
-  Building and solving CTF challenges

Module 15: Legal and Ethical Considerations

-  Ethical hacking and responsible disclosure
-  Legal aspects of penetration testing
-  Professional certifications and code of conduct

Final Project: Web Application Penetration Test

-  Apply knowledge and skills acquired throughout the course
-  Conduct a comprehensive penetration test on a provided web application
-  Create a detailed report with findings and recommendations

Thank You!