

Advanced Web Hacking (AWH)

Course Duration : 32 Hours

Course code : AWH

1. Course Overview

The **Advanced Web Hacking (AWH)** course is designed to provide in-depth knowledge of advanced web application attack techniques. This course focuses on identifying complex vulnerabilities, exploiting real-world web application flaws, and understanding advanced attack scenarios while following ethical hacking practices.

2. What you'll learn?

- Advanced web application security concepts
- Deep understanding of OWASP vulnerabilities
- Advanced exploitation techniques
- Bypassing security controls
- Web application attack automation
- Secure application defense strategies

3. Target Audience

- Ethical hackers
- Penetration testers
- Bug bounty hunters
- Cybersecurity professionals
- Security researchers

4. Pre-Requisites

- Basic web application security knowledge
- Experience with ethical hacking tools
- Understanding of HTTP/HTTPS protocols

5. Course Content (Modules)

Module 1: Advanced Web Application Architecture

- Modern web technologies
- Client-server communication

Module 2: Advanced OWASP Attacks

- SQL injection advanced
- Cross-site scripting (XSS) advanced

Module 3: Authentication and Authorization Attacks

- Session hijacking
- Access control bypass

Module 4: Business Logic Flaws

- Logic abuse techniques
- Real-world scenarios

Module 5: Automation and Advanced Tools

- Burp Suite advanced usage
- Custom attack scripts

Module 6: Web Application Defense

- Secure coding practices
- Defense and mitigation strategies