Web Application Hacking and Security (WAHS)

Zetlan Technologies

Online Course

ZETLAN TECHNOLOGIES
www.zetlantech.com

Web Application Hacking and Security (WAHS)

Course Modules

- Advanced Web Application Penetration Testing
- Advanced SQL Injection (SQLi)
- Reflected, Stored and DOM-based Cross Site Scripting (XSS)
- Cross Site Request Forgery (CSRF) – GET and POST Methods
- Server-Side Request Forgery (SSRF)
- Security Misconfigurations
- Directory Browsing/Brute forcing
- CMS Vulnerability Scanning
- Network Scanning
- Auth Bypass
- Web App Enumeration
- Dictionary Attack
- Insecure Direct Object Reference Prevention (IDOR)
- Broken Access Control
- Local File Inclusion (LFI)
- Remote File Inclusion (RFI)
- Arbitrary File Download
- Arbitrary File Upload
- Using Components with Known Vulnerabilities

Web Application Hacking and Security (WAHS)

For Enquiry: +91 8680961847

- Command Injection
- Remote Code Execution
- File Tampering
- Privilege Escalation
- Log Poisoning
- Weak SSL Ciphers
- Cookie Modification
- Source Code Analysis
- HTTP Header modification
- Session Fixation
- Clickjacking

Zetlan Technologies

LEARN REMOTELY!!

The efficiency of online learning in terms of time management, flexibility, and the ability to access resources anytime, anywhere can be compelling.

ZETLAN TECHNOLOGIES

www.zetlantech.com

For contact: +91 8680961847
+91 9600579474