

Duration: 2 Month

# Web Application Security

## Overview:

Web penetration testing involves simulating cyberattacks on web applications to identify vulnerabilities that could be exploited by malicious actors.

This process includes assessing the security of the application's infrastructure, code, and configurations.

By conducting penetration testing, organizations can proactively address weaknesses, enhance their security posture, and safeguard sensitive data from potential breaches.

### What you'll learn

- Importance of Web Application Security: Understanding why safeguarding web applications is crucial for protecting sensitive data and maintaining user trust.
- Common Vulnerabilities: Identifying and addressing prevalent security weaknesses like injection attacks, broken authentication, and sensitive data exposure.
- Impact of Breaches: Recognizing the serious consequences of security breaches, including financial losses, reputational damage, and legal liabilities.
- OWASP Top 10: Familiarizing with the top ten web application security risks outlined by OWASP, including injection attacks, broken authentication, and XSS vulnerabilities.
- Security Best Practices: Learning essential techniques such as input validation, session management, secure coding practices, and security testing to mitigate risks and enhance overall security posture.

### Target Audience:





The Web Application Security course will significantly benefit:

- Target audience for the PDF: Web developers, security professionals, penetration testers, and individuals interested in understanding and mitigating web application vulnerabilities.

### Prerequisite Knowledge:

- Familiarity with Linux, web application testing, and cybersecurity basics.

## You can reach us:

-  [www.cyberous.in](http://www.cyberous.in)
-  [info@cyberous.in](mailto:info@cyberous.in)
-  [@cyberous](https://www.instagram.com/cyberous)
-  [Cyberous](https://www.youtube.com/Cyberous)



CyberouS

## Course Outline:

### Module 01: Understanding Web Application Security

- Importance.
- Common vulnerabilities.
- Impact of breaches.

### Module 02: OWASP Top 10

- Injection attacks.
- Broken authentication.
- Sensitive data exposure.

### Module 03: Input Validation and Sanitization

- Validating inputs.
- Sanitizing data.
- Preventing injections.

### Module 04: Session Management

- Secure handling.
- Fixation prevention.
- Hijacking detection.



CyberouS

## Module 5: Authentication and Authorization

- Secure methods.
- Multi-factor auth.
- Role-based access.

## Module 6: Cross-Site Scripting (XSS) Prevention

- Output encoding.
- Content security policy.
- XSS filtering.

## Module 7: Cross-Site Request Forgery (CSRF) Protection

- CSRF tokens.
- SameSite cookie.
- Anti-CSRF tokens.

## Module 8: SQL Injection (SQLi) Mitigation

- Prepared statements.
- Parameterized queries.
- Input validation.



CyberouS

## Module 9: Security Headers Implementation

- Content Security Policy.
- Strict-Transport-Security.
- X-Content-Type-Options.

## Module 10: Secure File Uploads

- File validation.
- Renaming uploads.
- Secure storage.

## Module 11: Secure Coding Practices

- Least privilege.
- Coding standards.
- Code reviews.

## Module 12: Error Handling and Logging

- Proper handling.
- Sensitive info logging.
- Monitoring.



CyberouS

### Module 13: Security Testing Techniques

- Vulnerability scanning.
- Penetration testing.
- Code review.

### Module 14: HTTPS Implementation

- SSL/TLS certificates.
- HTTPS redirection.
- Configuration.

### Module 15: Security Headers Configuration

- HSTS.
- X-Content-Type-Options.
- X-Frame-Options.

### Module 16: API Security

- Authentication.
- Rate limiting.
- Validation.



## Module 17: Content Security Policy (CSP)

- Content sources.
- XSS mitigation.
- Violation reporting.

## Module 18: Server-Side Request Forgery (SSRF) Prevention

- Domain whitelisting.
- URL parameter validation.
- Network limits.

## Module 19: Browser Security

- Sandboxing.
- Security features.
- Same-origin policy.

## Module 20: Security Education and Training

- Awareness programs.
- Developer training.
- Continuous improvement.