Cyberous

Duration: 2 Months

WEB APPLICATION PENETRATION TESTING

Overview:

Web penetration testing replicates cyberattacks on web applications to unveil vulnerabilities exploitable by malicious actors. It encompasses assessing the application's infrastructure, code, and configurations. By conducting penetration testing, organizations proactively tackle weaknesses, bolster their security posture, and shield sensitive data from potential breaches. This proactive approach is critical in today's cyber landscape, where threats are increasingly sophisticated and prevalent. Through rigorous testing, organizations can identify and rectify vulnerabilities before they are exploited, minimizing the risk of costly data breaches and reputational damage.

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

Benifits

➢**Hands-on practical:** Engage in real-world exercises to apply theoretical knowledge directly.

➢**Internship opportunity:** Gain practical experience through internships to enhance skills and build a professional network.

➢**Expert trainers:** Receive guidance and instruction from seasoned professionals with extensive experience in the field.

➢**Job assistance:** Access support and resources to secure employment opportunities aligned with acquired skills. and expertise.

You can reach us at:

🌐 www.cyberous.in
✉ info@cyberous.in
📷 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

Module 05: Authentication and Authorization

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

Module 06: Cross-Site Scripting (XSS) Prevention

- Output encoding
- Content security policy
- XSS filtering

Module 07: Cross-Site Request Forgery (CSRF) Protection

- CSRF tokens
- SameSite cookie
- Anti-CSRF tokens

Module 08: SQL Injection (SQLi) Mitigation

- Prepared statements
- Parameterized queries
- Input validation

Module 09: 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

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