Cyberous

Duration: 2 Months

MOBILE APPLICATION PENETRATION TESTING

Overview:

Mobile application penetration testing involves scrutinizing app security to unearth vulnerabilities and weaknesses exploitable by attackers. Employing techniques like code analysis, network traffic monitoring, and reverse engineering, testers unveil potential security flaws. Thorough penetration testing enables organizations to proactively identify and mitigate security risks, thereby safeguarding the confidentiality, integrity, and availability of their mobile applications. This proactive approach enhances overall security posture and fosters user confidence in the app's resilience against potential threats.

What you'll learn

➢Importance of Mobile App Security: Understanding why securing mobile applications is essential for safeguarding sensitive data and user privacy.

➢Common Vulnerabilities: Identifying prevalent security weaknesses like insecure data storage, authentication flaws, and insecure communication channels.

➢Impact of Breaches: Recognizing the serious consequences of mobile app breaches, including data theft, financial losses, and damage to reputation.

➢OWASP Mobile Top 10: Familiarizing with the top ten mobile app security risks outlined by OWASP, covering areas such as data storage, authentication, and network security.

➢Security Best Practices: Learning essential techniques such as secure coding practices, authentication methods, and secure update mechanisms 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 Mobile App Security

- Importance
- Common vulnerabilities
- Impact of breaches

Module 02: OWASP Mobile Top 10

- Data storage
- Server-side controls
- Transport layer protection

Module 03: Authentication and Authorization

- Secure methods
- Role-based access
- Token-based authentication

Module 04: Secure Data Storage

- Encryption
- Key management
- Data leak prevention

Module 05: Network Security

- Secure protocols
- Certificate pinning
- Network configuration

Module 06: Secure Coding Practices

- Input validation
- Output encoding
- Avoiding hardcoding

Module 07: Authentication Bypass

- Weak mechanisms
- Session vulnerabilities
- Biometric security

Module 08: Authorization Flaws

- Access control assessment
- Privilege escalation
- Access control checks

Module 09: Insecure Communication

- SSL/TLS assessment
- Man-in-the-middle
- Data interception

Module 10:Code Tampering

- App integrity
- Code modification
- Anti-tampering measures

Module 11: Reverse Engineering

- Code obfuscation
- Data storage
- Decompilation prevention

Module 12: Input Validation

- User input sanitization
- Injection prevention
- External data validation

Module 13: Side Channel Data Leakage

- App permissions
- Data exposure
- Clipboard security

Module 14: Sensitive Information Disclosure

- Memory security
- Log protection
- Error message security

Module 15: Session Handling

- Fixation prevention
- Secure management
- Timeout settings

Module 16: Client-Side Security Controls

- Data storage
- WebView controls
- Injection prevention

Module 17: Push Notification Security

- Secure handling
- Data in notifications
- Prevention measures

Module 18: Mobile App Testing Techniques

- Dynamic analysis
- Static analysis
- Manual testing

Module 19: Secure Update Mechanisms

- Update security
- Authenticity validation
- Secure channels

Module 20: Security Education and Awareness

- Developer training
- User education
- Promoting awareness