

Proposal for Mobile Application Penetration Testing Aligned with OWASP MASVS

Overview:

We are pleased to present this proposal for conducting a thorough mobile application penetration testing engagement aligned with the OWASP Mobile Application Security Verification Standard (MASVS). Our experienced team will assess the security posture of your mobile application, identify vulnerabilities, and provide actionable recommendations to mitigate risks.

Objectives:

- Perform a comprehensive security assessment of the All house mobile application in alignment with OWASP MASVS requirements.
- Identify and prioritize vulnerabilities based on their impact and relevance to MASVS security controls.
- Provide detailed documentation and reporting, including actionable recommendations for improving security posture.
- Enhance overall security and ensure compliance with industry standards.

Scope of Work:

1. Pre-engagement Activities:

- Align penetration testing scope with MASVS requirements.
- Obtain necessary authorization and document specific MASVS requirements to be tested.

2. Testing Phases:

Reconnaissance:

- Gather information about the mobile application's technologies, entry points, and architecture.

Scanning:

- Perform automated scanning using tools such as MobSF, Drozer, and QARK, aligned with MASVS requirements.

Initial Vulnerability Analysis:

- Analyze automated scan results and prioritize vulnerabilities based on MASVS levels.

Manual Testing:

- Conduct manual testing to address specific MASVS requirements not comprehensively covered by automated tools.

Exploitation and Post-Exploitation:

- Attempt to exploit identified vulnerabilities, focusing on those directly related to MASVS requirements.

3. Documentation and Reporting

- Document findings, emphasizing their alignment with MASVS requirements.
- Classify and prioritize findings based on MASVS levels.

4. Post-engagement Activities

Review and Validation

- Review findings with stakeholders and validate coverage of MASVS requirements.

Final Reporting

- Generate the final penetration testing report, structured according to MASVS guidelines.

Debriefing and Knowledge Transfer

- Conduct a debriefing session to discuss testing results and provide insights into integrating MASVS requirements into development and security processes.

Deliverables:

- Penetration Testing Plan aligned with MASVS requirements.
- Detailed Penetration Testing Report structured according to MASVS guidelines.
- Executive Summary highlighting key findings and recommendations.
- Recommendations for mitigating identified vulnerabilities and improving security posture.

Timeline:

The penetration testing engagement will be conducted over a period of 20-30 days, depending on the complexity of the application and the chosen approach (white-box or black-box testing).