RED TEAM SIMULATION REPORT

Mobile Application Security Assessment

Report Date:	2024-11-30 13:25:52
Target Application:	Android InsecureBankv2
Risk Level:	Medium
Total Attacks:	3
Vulnerabilities Found:	0

Executive Summary

This report presents the findings of a comprehensive Red Team simulation conducted on the Android InsecureBankv2 application. The assessment focused on identifying vulnerabilities through XSS, SQL injection, and password attacks. Key Findings: • Total Attacks Performed: 3 • Vulnerabilities Identified: 0 • Overall Risk Assessment: Medium

Attack Details

1. Cross-Site Scripting (XSS) Attacks

Payload	Status	Details
<script>alert("XSS")</script>	Potentially Vulnerable	WebView accepted malicious payload
<img src="x" onerror="alert('XSS')">	Potentially Vulnerable	WebView accepted malicious payload
"><script>alert(document.cookie)</script>	Potentially Vulnerable	WebView accepted malicious payload
<svg onload="alert(1)">	Potentially Vulnerable	WebView accepted malicious payload
javascript:alert(document.domain)	Potentially Vulnerable	WebView accepted malicious payload

2. SQL Injection Attacks

Payload	Status	Details

3. Password Attacks

Password	Status	Details

Identified Vulnerabilities

Type	Risk Level	Details

Blue Team Mitigation Strategies

XSS Mitigation

- Implement proper input validation
- Use Content Security Policy in WebViews
- Sanitize all user inputs
- Enable WebView security flags

SQL Injection Mitigation

- Use parameterized queries
- Implement proper input validation
- Use ORM frameworks
- Minimal SQL privileges

Password Attack Mitigation

- Implement rate limiting
- Use strong password policies
- Implement account lockout
- Use multi-factor authentication

Report Generated: 2024-11-30 13:26:31 | Confidential