Mobile OWASP Application Testing

0% Percent Complete

Questionnaire Instructions:
For each question choose either Yes, No or N/A from the drop-down menu provided. If N/A is chosen, an explanation is mandatory. Use the "Additional Information" field to the right of the question. Click on the instruction pop-up box and drag if necessary.

Ques Num	Question/Request	Response	Additional Information
M.1	Testing performed to verify Application is not vulnerable to Reverse Engineering Attack/Lack of Code	Yes	
M.2	Testing performed for Hard coded sensitive information in Application Code (including Crypt)	Yes	
M.3	Testing performed to Verify MSISDN (WAP)	No	
M.4	Testing performed if Attacker can bypass Second Level Authentication	Yes	
M.5	iOS snapshot/backgrounding testing performed	No	No sensitive content as part of screenshots
M.6	Testing performed to verify Debug is set to TRUE (Android Only)	Yes	
M.7	Clear text information under SSL Tunnel testing performed	Yes	Limited timeframe due to flutter framework
M.8	Testing performed to verify Client Side Validation cannot be bypassed	Yes	
M.9	Testing performed for Sensitive Information sent as Clear Text over network/Lack of Data	Yes	
M.10	Testing performed for Improper or NO implementation of Change Password Page	No	No password change available via mobile app
M.11	URL Modification testing performed	Yes	
M.12	Sensitive information in Memory Dump testing performed	Yes	
M.13	Testing performed for accessibility on Rooted or Jail Broken Device	Yes	
M.14	Back-and-Refresh attack testing performed	Yes	
M.15	Directory Browsing testing performed	No	
M.16	Open URL Redirects testing performed	No	
M.17	Insecure Application Permissions testing performed	Yes	
M.18	Testing performed if Application build contains Obsolete Files	No	
M.19	Private IP Disclosure testing performed	Yes	
M.20	UI Impersonation through RMS file modification (JAVA) testing performed	No	
M.21	UI Impersonation through JAR file modification (Android) testing performed	Yes	
M.22	Operation on a resource after expiration or release	Yes	
M.23	ASLR testing performed (iOS)	Yes	
M.24	Cache smashing protection testing performed (oOS)	No	
M.25	Android Backup Vulnerability testing performed (Android)	Yes	
M.26	Global File Permission on App Data testing performed (Android)	Yes	
M.27	Testing performed to Store Encryption Key Locally/Store Sensitive Data in ClearText	Yes	
M.28	Third-party Data Transit on Unencrypted Channel testing performed	No	
M.29	Testing performed for Failure to Implement Trusted Issuers (Android)	Yes	
M.30	Hostname Verifier testing performed (Android)	Yes	
M.31	Weak Custom Hostname Verifier testing performed (Android)	Yes	
M.32	App/Web Caches Sensitive Data Leak testing performed	Yes	
M.33	Leaking Content Provider testing performed	Yes	
M.34	Redundancy Permission Granted testing performed (Android)	Yes	
M.35	Spoof-able Values for Authenticating User testing performed (IMEI, UDID)	No	IMEI / UDID not required for application
M.36	Activity Hijacking testing performed (Android)	Yes	
M.37	Service Hijacking testing performed (Android)	Yes	
M.38	Broadcast Thief testing performed (Android)	Yes	
M.39	Malicious Broadcast Injection testing performed (Android)	Yes	
M.40	Malicious Activity/Service Launch testing performed (Android)	Yes	
M.41	Using Device Identifier as Session testing performed	Yes	
M.42	Symbols Remnant testing performed (iOS)	No	
M.43	Lack of Check-sum Controls/Altered Detection testing performed (Android)	Yes	
M.44	Insecure permissions on Unix domain sockets testing performed (Android)	Yes	
M.45	Insecure use of network sockets testing performed (Android)	Yes	
M.46	Cleartext password in Response testing performed	Yes	
M.47	Direct Reference to internal resource without authentication testing performed	Yes	
M.48	Testing that Application has NO or improper Session Management/Failure to Invalid performed	Yes	
M.49	Cross Domain Scripting Vulnerability testing performed	No	
M.50	Cross Origin Resource Sharing testing performed	Yes	
M.51	Improper Input Validation testing performed - Server Side	Yes	
M.52	Cross Site Request Forgery (CSRF)/SSRF testing performed	Yes	
M.53	Cacheable HTTPS Responses testing performed	Yes	
M.54	Path Attribute not set on a Cookie testing performed	Yes	
M.55	Http Only Attribute not set for a cookie testing performed	Yes	
M.56	Secure Attribute not set for a cookie testing performed	Yes	
M.57	Application is Vulnerable to Clickjacking/Tapjacking attack testing performed	Yes	
M.58	testing that Server/OS fingerprinting is possible performed	Yes	
M.59	Testing for Lack of Adequate Timeout Protection performed	Yes	
M.60	Testing Number of Times a Function Can be Used Limits performed	No	
M.61	Testing Defenses Against Application Miss-use performed	Yes	
M.62	Testing for Client Side Resource Manipulation	Yes	