OWASP Mobile Security Project

BY OWASP MOBILE SECURITY TEAM

OWASP MOBILE APPLICATION SECURITY GUIDE

CLIENT SIDE CHECKS

Sr.	Vulnerability Name	Applicable Platform	Compliant ? Yes/No/NA	Classification
1	Application is Vulnerable to Reverse Engineering Attack/Lack of Code	All		Static Checks
2	Account Lockout not Implemented	All		Dynamic Checks
3	Application is Vulnerable to XSS	All		Static + Dynamic Chec
4	Authentication bypassed	All		Dynamic Checks
5	Hard coded sensitive information in Application Code (including Crypt	All		Static Checks
6	Malicious File Upload	All		Dynamic Checks
7	Session Fixation	All		Dynamic Checks
8	Application does not Verify MSISDN	WAP		Unknown
9	Privilege Escalation	All		Dynamic Checks
10	SQL Injection	All		Static + Dynamic Chec
11	Attacker can bypass Second Level Authentication	All		Dynamic Checks
12	Application is vulnerable to LDAP Injection	All		Dynamic Checks
13	Application is vulnerable to OS Command Injection	All		Dynamic Checks
14	iOS snapshot/backgrounding Vulnerability	iOS		Dynamic Checks
15	Debug is set to TRUE	Android		Static Checks
16	Application makes use of Weak Cryptography	All		Static Checks
17	Cleartext information under SSL Tunnel	All		Dynamic Checks

18	Client Side Validation can be bypassed	All		Dynamic Checks
19	Invalid SSL Certificate	All		Static Checks
20	Sensitive Information is sent as Clear Text over network/Lack of Data	All		Dynamic Checks
21	CAPTCHA is not implemented on Public Pages/Login Pages	All		Dynamic Checks
22	Improper or NO implementation of Change Password Page	All		Dynamic Checks
23	Application does not have Logout Functionality	All		Dynamic Checks
24	Sensitive information in Application Log Files	All		Dynamic Checks
25	Sensitive information sent as a querystring parameter	All		Dynamic Checks
26	URL Modification	All		Dynamic Checks
27	Sensitive information in Memory Dump	All		Dynamic Checks
28	Weak Password Policy	All		Dynamic Checks
29	Autocomplete is not set to OFF	All		Static Checks
30	Application is accessible on Rooted or Jail Broken Device	All		Dynamic Checks
31	Back-and-Refresh attack	All		Dynamic Checks
32	Directory Browsing	All		Static + Dynamic Chec
33	Usage of Persistent Cookies	All		Dynamic Checks
34	Open URL Redirects are possible	All		Dynamic Checks
35	Improper exception Handling: In code	All		Static Checks
36	Insecure Application Permissions	All		Static Checks
37	Application build contains Obsolete Files	All		Static Checks
38	Certificate Chain is not Validated	All		Static + Dynamic Chec
39	Last Login information is not displayed	All		Dynamic Checks
40	Private IP Disclosure	All		Static Checks
41	UI Impersonation through RMS file modification [1]	JAVA		Dynamic Checks
42	UI Impersonation through JAR file modification	Android		Dynamic Checks
43	Operation on a resource after expiration or release	All		Dynamic Checks
44	No Certificate Pinning	All		Dynamic Checks
45	Cached Cookies or information not cleaned after application removal/	All		Dynamic Checks
46	ASLR Not Used	iOS		Static Checks

47	Clipboard is not disabled	All		Dynamic Checks
48	Cache smashing protection is not enabled	iOS		Static Checks
49	Android Backup Vulnerability	Android		Static Checks
50	Unencrypted Credentials in Databases (sqlite db)	All		Dynamic Checks
51	Store sensitive information outside App Sandbox (on SDCard)	All		Dynamic Checks
52	Allow Global File Permission on App Data	Android		Dynamic Checks
53	Store Encryption Key Locally/Store Sensitive Data in ClearText	All		Dynamic Checks
54	Bypass Certificate Pinning	All		Dynamic Checks
55	Third-party Data Transit on Unencrypted Channel	All		Dynamic Checks
56	Failure to Implement Trusted Issuers	Android		Static Checks
57	Allow All Hostname Verifier	Android		Static Checks
58	Ignore SSL Certificate Error	All		Static Checks
59	Weak Custom Hostname Verifier	Android		Static Checks
60	App/Web Caches Sensitive Data Leak	All		Dynamic Checks
61	Leaking Content Provider	Android		Dynamic Checks
62	Redundancy Permission Granted	Android		Static Checks
63	Use Spoof-able Values for Authenticating User (IMEI, UDID)	All		Dynamic Checks
64	Use of Insecure and/or Deprecated Algorithms	All		Static Checks
65	Local File Inclusion (might be through XSS Vulnerability)	All		Static + Dynamic Chec
66	Activity Hijacking	Android		Static Checks
67	Service Hijacking	Android		Static Checks
68	Broadcast Thief	Android		Static Checks
69	Malicious Broadcast Injection	Android		Static Checks
70	Malicious Activity/Service Launch	Android		Static Checks
71	Using Device Identifier as Session	All		Dynamic Checks
72	Symbols Remnant	iOS		Static Checks
73	Lack of Check-sum Controls/Altered Detection	Android		Dynamic Checks
74	Insecure permissions on Unix domain sockets	Android		Static Checks
75	Insecure use of network sockets	Android		Static Checks

SERVER SIDE CHECKS

Sr.	Vulnerability Name	Applicable Platform	Compliant ? Yes/No/NA	
76	Cleartext password in Response	All		Dynamic Checks
77	Direct Reference to internal resource without authentication	All		Dynamic Checks
78	Application has NO or improper Session Management/Failure to Invali	All		Dynamic Checks
79	Cross Domain Scripting Vulnerability	All		Dynamic Checks
80	Cross Origin Resource Sharing	All		Dynamic Checks
81	Improper Input Validation - Server Side	All		Dynamic Checks
82	Detailed Error page shows internal sensitive information	All		Dynamic Checks
83	Application allows HTTP Methods besides GET and POST	All		Dynamic Checks
84	Cross Site Request Forgery (CSRF)/SSRF	All		Dynamic Checks
85	Cacheable HTTPS Responses	All		Dynamic Checks
86	Path Attribute not set on a Cookie	All		Dynamic Checks
87	HttpOnly Attribute not set for a cookie	All		Dynamic Checks
88	Secure Attribute not set for a cookie	All		Dynamic Checks
89	Application is Vulnerable to Clickjacking/Tapjacking attack	All		Dynamic Checks
90	Server/OS fingerprinting is possible	All		Dynamic Checks
91	Lack of Adequate Timeout Protection	All		Dynamic Checks

By OWASP Mobile Team