ImmuniWeb® MobileSuite

ImmuniWeb® MobileSuite leverages our award-winning Machine Learning technology to accelerate and enhance mobile penetration testing. Every pentest is easily customizable and provided with a zero false-positives SLA. Unlimited patch verifications and 24/7 access to our security analysts are included into every project.

www.immuniweb.com

Gartner Cool Vendor™

IDC Innovator

AIFINTECH 100 2021

Mobile Penetration Testing Made Simple

In-Depth Testing

Business logic testing, SANS Top 25, PCI DSS & OWASP coverage

Zero False Positives SLA

Money-Back Guarantee for a single false-positive

Actionable Reporting

Tailored remediation guidelines and 24/7 access to analysts

Rapid Delivery SLA

Guaranteed execution schedule and report delivery

DevSecOps Native

SDLC and CI/CD tools integration, WAF for mobile backend flaws

1. Configure and schedule pentest in a few clicks
2. Get your pentest report and re-test at no cost
3. Receive your pentest compliance certificate

Actionable Report. Simple Remediation.

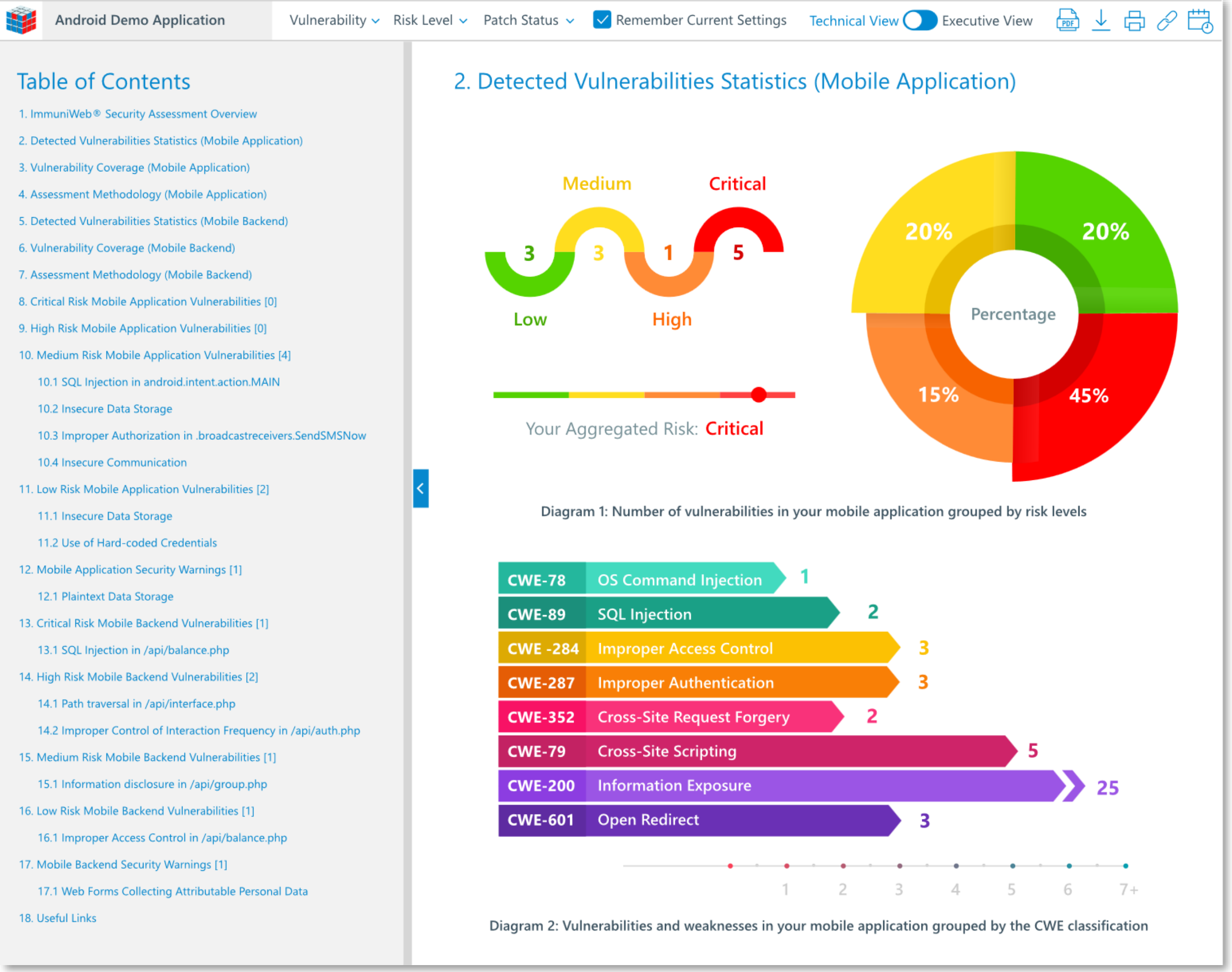


Table of Contents

2. Detected Vulnerabilities Statistics (Mobile Application)

Your Aggregated Risk: Critical

Diagram 1: Number of vulnerabilities in your mobile application grouped by risk levels

CWE-78 OS Command Injection 1
CWE-89 SQL Injection 2
CWE -284 Improper Access Control 3
CWE-287 Improper Authentication 3
CWE-352 Cross-Site Request Forgery 2
CWE-79 Cross-Site Scripting 5
CWE-200 Information Exposure 25
CWE-601 Open Redirect 3
1
2
3
4
5
6
7+

Diagram 2: Vulnerabilities and weaknesses in your mobile application grouped by the CWE classification

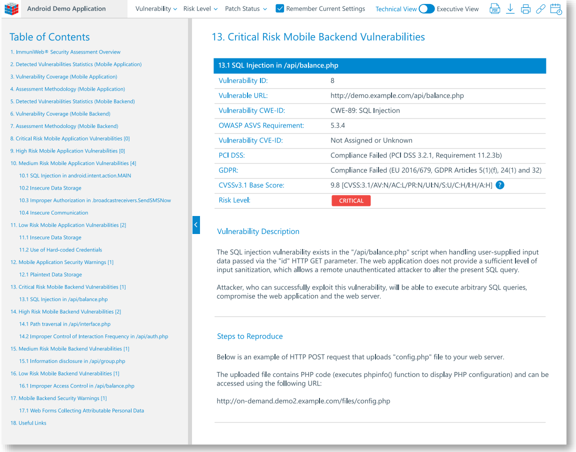


Table of Contents
1. ImmuniWeb® Security Assessment Overview
2. Detected Vulnerabilities Statistics (Mobile Application)
3. Vulnerability Coverage (Mobile Application)
4. Assessment Methodology (Mobile Application)
5. Detected Vulnerabilities Statistics (Mobile Backend)
6. Vulnerability Coverage (Mobile Backend)
7. Assessment Methodology (Mobile Backend)
8. Critical Risk Mobile Application Vulnerabilities [0]
9. High Risk Mobile Application Vulnerabilities [0]
10. Medium Risk Mobile Application Vulnerabilities [4]
10.1 SQL Injection in android.intent.action.MAIN
10.2 Insecure Data Storage
10.3 Improper Authorization in .broadcastreceivers.SendSMSNow
10.4 Insecure Communication
11. Low Risk Mobile Application Vulnerabilities [2]
11.1 Insecure Data Storage
11.2 Use of Hard-coded Credentials
12. Mobile Application Security Warnings [1]
12.1 Plaintext Data Storage
13. Critical Risk Mobile Backend Vulnerabilities [1]
13.1 SQL Injection in /api/balance.php
14. High Risk Mobile Backend Vulnerabilities [2]
14.1 Path traversal in /api/interface.php
14.2 Improper Control of Interaction Frequency in /api/auth.php
15. Medium Risk Mobile Backend Vulnerabilities [1]
15.1 Information disclosure in /api/group.php
16. Low Risk Mobile Backend Vulnerabilities [1]
16.1 Improper Access Control in /api/balance.php
17. Mobile Backend Security Warnings [1]
17.1 Web Forms Collecting Attributable Personal Data
18. Useful Links

13. Critical Risk Mobile Backend Vulnerabilities

13.1 SQL Injection in /api/balance.php	
Vulnerability ID:	8
Vulnerable URL:	http://demo.example.com/api/balance.php
Vulnerability CWE-ID:	CWE-89: SQL Injection
OWASP ASVS Requirement:	5.3.4
Vulnerability CVE-ID:	Not Assigned or Unknown
PCI DSS:	Compliance Failed (PCI DSS 3.2.1, Requirement 11.2.3b)
GDPR:	Compliance Failed (EU 2016/679, GDPR Articles 5(1)(f), 24(1) and 32)
CVSSv3.1 Base Score:	9.8 [CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H] ?
Risk Level:	CRITICAL

Vulnerability Description

The SQL injection vulnerability exists in the "/api/balance.php" script when handling user-supplied input data passed via the "id" HTTP GET parameter. The web application does not provide a sufficient level of input sanitization, which allows a remote unauthenticated attacker to alter the present SQL query.

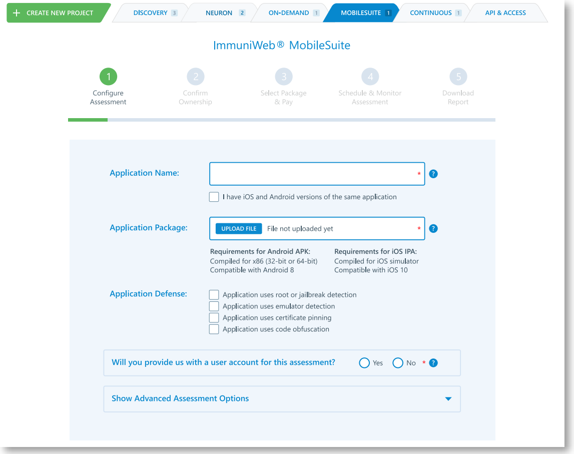
Attacker, who can successfully exploit this vulnerability, will be able to execute arbitrary SQL queries, compromise the web application and the web server.

Steps to Reproduce

Below is an example of HTTP POST request that uploads "config.php" file to your web server.

The uploaded file contains PHP code (executes phpinfo() function to display PHP configuration) and can be accessed using the following URL:

http://on-demand.demo2.example.com/files/config.php



ImmuniWeb® MobileSuite

Application Name: * ?

□ I have iOS and Android versions of the same application

Application Package: UPLOAD FILE File not uploaded yet * ?

Requirements for Android APK:
Compiled for x86 (32-bit or 64-bit)
Compatible with Android 8

Requirements for iOS IPA:
Compiled for iOS simulator
Compatible with iOS 10

Application Defense:
□ Application uses root or jailbreak detection
□ Application uses emulator detection
□ Application uses certificate pinning
□ Application uses code obfuscation

Will you provide us with a user account for this assessment? ○ Yes ○ No * ?

Show Advanced Assessment Options ▾

Mobile Penetration Test for Any Need

Mobile App Security

Static, dynamic and interactive security testing with SCA

Mobile Backend Security

Comprehensive testing of mobile app’s endpoints

Privacy and Encryption

Detailed analysis of privacy and encryption problems

Black & White Box

Authenticated (including MFA/SSO) or Black Box testing

Open Source Security

Software Composition Analysis (SCA) tests for 20,000+ known CVE-IDs

Red Teaming

Breach and attack simulation per MITRE ATT&CK® Mobile

Proven Methodology and Global Standards

- OWASP Mobile Security Testing Guide (MSTG)
- NIST SP 800-115 Technical Guide to Information Security Testing & Assessment
- PCI DSS Information Supplement: Penetration Testing Guidance
- MITRE ATT&CK® Matrices for Mobile and Enterprise
- FedRAMP Penetration Test Guidance
- ISACA’s How to Audit GDPR

- OWASP Application Security Verification Standard (ASVS v4.0.2) Mapping
- Common Vulnerabilities and Exposures (CVE) Compatible
- Common Weakness Enumeration (CWE) Compatible
- Common Vulnerability Scoring System (CVSS v3.1)

ImmuniWeb® MobileSuite Setup and Packages

1. Configure and schedule your pentest in a few clicks →
2. Get your pentest report and re-test at no cost →
3. Receive your pentest compliance certificate

ImmuniWeb® MobileSuite Packages for any need	Corporate Pro	Corporate	Express Pro	Express
OWASP MASVS Testing	Level 2	Level 2	Level 1	Level 1
OWASP ASVS Testing	Level 3	Level 2	Level 1	Level 1
Manual Penetration Testing	5 days	5 days	3 days	1 day
Report Writing	8 hours	4 hours	2 hours	1 hour

Corporate Pro

Designed for mobile application of large size and complexity, with multiple endpoints (e.g. APIs or web services) or several user roles.

Corporate

Designed for mobile application of medium size and complexity, with several endpoints (e.g. APIs or web services) or a couple of user roles.

Express Pro

Designed for mobile application of small size and complexity, with one or two endpoints (e.g. APIs or web services) and one user role.

Express

Designed for mobile application of very small size and complexity, with one main endpoint (e.g. API or web service) and one simple user role.

ImmuniWeb® MobileSuite Setup and Packages

Penetration Testing

- ✓ OSINT Search of Stolen Credentials
- ✓ Mobile Penetration Testing
  - SANS Top 25 Full Coverage
  - PCI DSS 6.5.1-6.5.10 Full Coverage
  - OWASP Mobile Top 10 Full Coverage
  - Backend Testing (REST/SOAP/GraphQL APIs)
  - AI Augments Human Testing and Analysis
  - Machine Learning Accelerates Testing
  - Authenticated Testing (OTP / MFA)
  - Business Logic Testing
- ✓ Full Customization of Testing
- ✓ Rapid Delivery SLA Money back
- ✓ Privacy Review

Reporting

- ✓ Threat-Aware Risk Scoring
- ✓ Step-by-Step Instructions to Reproduce
- ✓ Web Interface, PDF and XML Formats
- ✓ Tailored Remediation Guidelines
- ✓ PCI DSS and GDPR Compliances
- ✓ CVE, CWE and CVSS Scores
- ✓ OWASP ASVS Mapping
- ✓ Zero False-Positives SLA Money back

Remediation

- ✓ Unlimited Patch Verifications
- ✓ 24/7 Access to Our Security Analysts
- ✓ DevSecOps & CI/CD Tools Integration
- ✓ One-Click Virtual Patching (Backend)
- ✓ Multirole RBAC Dashboard with 2FA
- ✓ Penetration Test Certificate

INSTANT START
24/7
RAPID DELIVERY

Why Choosing ImmuniWeb ® AI Platform

Instant start. Rapid Delivery. 24/7.

Award-Winning

Gartner Cool Vendor
SC Awards Winner
IDC Innovator

Globally Trusted

1,000+ Enterprise Clients
250+ Business Partners
50+ Countries

Proven Success

90% Customer Retention
70% YoY Sales Growth
Zero Breaches of SLA

> *At ImmuniWeb, we always carefully listen to all our customers to continuously make our award-winning Platform even better to stay ahead of the rapidly evolving cyber threats. This unique synergy helps us maintain the customer retention rate above 90%.*

Dr. Ilia Kolochenko
Chief Architect & CEO

Frequently Asked Questions

Q Do I need two packages for iOS and Android versions of the same app?

A Normally yes, however, the second package will be offered with a 50% discount. Recurrent penetration testing of the same mobile app also has special discounts. Please get in touch with us to learn more and get a custom quote for your mobile security testing needs.

Q How can customize my mobile pentesting requirements?

A At the first step of project creation, you can easily configure special requirements for mobile penetration testing. For example, you can select authenticated (White Box) testing with 2FA/SSO if you mobile app supports authentication, try some specific attack vectors, such as extracting protected content or activate features that are only available to premium users.

Q What is the difference between the packages?

A Packages (from right to left) include gradually more human time and other resources that will be allocated for the penetration test. Generally, the bigger your scope is, the bigger package you need to comprehensively test your mobile application and its backend for all know vulnerabilities and attack vectors. Please reach out to us for a quote tailored for your specific needs and scope.

Q Can you test mobile applications built with Xamarin or Flutter?

A Yes, we can test applications built with any mobile frameworks or technologies. However, complicated cross-platform frameworks, such as Xamarin and Flutter, impose additional challenges that usually require supplementary resources and human time for comprehensive testing of the application. Therefore, the minimum required package for those frameworks is MobileSuite Corporate.

Q How are you different from other penetration testing companies?

A ImmuniWeb® MobileSuite leverages our award-winning Machine Learning technology for acceleration and intelligent automation of laborious and time-consuming testing tasks and processes, eventually saving a considerable amount of human time on our side. Eventually, compared to traditional penetration testing, you may expect to get your penetration testing report much faster and to get higher vulnerability detection rate, as our security experts will spend their valuable time to meticulously reverse engineer your application and try the most sophisticated attack vectors instead of wasting time on routine or automatable security checks.

DevSecOps, CI/CD and WAF Integrations

Developers Environment

Jira Software

hp Application Lifecycle Management

mantis BUG TRACKER

splunk>

GitHub

servicenow.

Mattermost.

ROCKET.CHAT

zapier

Web Application Firewalls

f5.

imperva

Barracuda.

FORTINET.

Qualys

and much more:

asana

MICRO FOCUS.

BROADCOM.

trac Integrated SCM & Project Management

REDMINE flexible project management

FOGBUGZ

ZOHO

JET BRAINS

PivotalTracker

Bugzilla

ROHDE&SCHWARZ

Testimonials and Customers References

We used ImmuniWeb for some of our products and we have been highly satisfied from the provided service as valid vulnerabilities with no false positives were identified. The report ImmuniWeb delivered to us was quite clear in terms of the classifications and the description of the identified vulnerabilities, linking to the corresponding CVE and the fix recommendations. We recommend ImmuniWeb to other vendors to make their web products secure

ebay

We believe ImmuniWeb platform would definitely address the common weaknesses seen in manual assessments. The AI-assisted platform not only automates the assessments, but also, executes them in a continuous, consistent and reliable fashion. Admittedly, the platform would definitely add quick wins and great ROI to its customers on their investment.

DP WORLD

The report was very detailed and clearly explained the risk at executive level, a great assistance in taking the report to senior management.
I would have no hesitation in recommending ImmuniWeb.

Celgene

ImmuniWeb is an efficient and very easy-to-use solution that combines automatic and human tests. The results are complete, straightforward and easy to understand. It's an essential tool for the development of the new digital activities

next bank
CRÉDIT AGRICOLE

Strategic Business and Technology Alliance Partners

pwc

softwareONE

BDO

imperva

FORTINET

f5

ITU

Qualys

GLOBAL CYBER ALLIANCE

Barracuda

CyberPeace Institute

ImmuniWeb Partners Directory

Cybersecurity and Data Protection Compliance

ImmuniWeb® AI Platform provides award-winning IT asset discovery and inventory, third-party risk management, continuous monitoring and security testing to help your organization meet emerging regulatory and compliance requirements in a simple and cost-effective manner.

EU & UK GDPR

California CCPA, CPRA

ISO 27001

Singapore MAS

HIPAA / HITECH

FTCA, GLBA, FCRA/FACTA

PCI DSS

NIST

South Africa POPIA

New York SHIELD, NYDFS

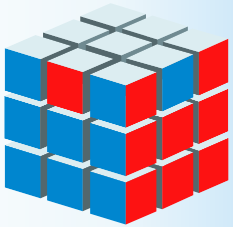
Brazil LGPD

Hong Kong PDPO

India IT Act

Singapore PDPA

1 Platform



5 SaaS Products

ImmuniWeb® Discovery

ImmuniWeb® Neuron

ImmuniWeb® On-Demand

ImmuniWeb® MobileSuite

ImmuniWeb® Continuous

20 Use Cases

- API Penetration Testing
- API Security Scanning
- Attack Surface Management
- Cloud Penetration Testing
- Cloud Security Posture Management
- Continuous Penetration Testing
- Cyber Threat Intelligence
- Dark Web Monitoring
- Digital Brand Protection
- GDPR Penetration Testing
- Mobile Penetration Testing
- Mobile Security Scanning
- Network Security Assessment
- PCI DSS Penetration Testing
- Red Teaming Exercise
- Software Composition Analysis
- Third-Party Risk Management
- WAF Security Testing
- Web Penetration Testing
- Web Security Scanning

ImmuniWeb®

AI for Application Security

www.immuniweb.com

CREST ACCREDITED

SYSTEM CERTIFICATION ISO/IEC 27001 SGS

UKAS MANAGEMENT SYSTEMS 005

> *ImmuniWeb outperformed IBM Watson for Cybersecurity and won in the “**Best Usage of Machine Learning and AI**” category*

SC awards 2018 EUROPE Winner

One Platform. All Needs.