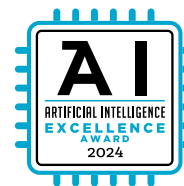




Compliance-Ready Mobile Application Penetration Testing

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

Copyright © 2025 ImmuniWeb SA

Quality. Efficiency. Value.



In-Depth Testing

SANS Top 25 & business logic
beyond OWASP Top 10



Threat-Led Testing

Simulation of real attacks relevant
to your business and industry



DevSecOps Native

Unlimited patch validation,
SDLC & CI/CD integration



Zero False-Positives SLA

100% validated findings
money-back guarantee



Rapid Delivery SLA

Always on-schedule testing
and report delivery



First-Class Reports

Zero noise, full exploitation cycle,
threat-aware risk scoring

1

Configure and schedule
your penetration test

2

Download your report and
get our help with patching

3

Get a letter of compliance
after validating the fixes

Control the Entire Process via a Multiuser Portal

Android Demo App

Vulnerability ▾ Risk Level ▾ Patch Status ▾ ☒ Remember Current Settings Technical View ☒ Executive View

PDF

↓

↩

🖨

🔗

Table of Contents

1. ImmuniWeb® Security Assessment Overview

2. Vulnerability Coverage (Mobile Application)

3. Assessment Methodology (Mobile Application)

4. Detected Vulnerabilities Statistics (Mobile Application)

5. Vulnerability Coverage (Mobile Backend)

6. Assessment Methodology (Mobile Backend)

7. Detected Vulnerabilities Statistics (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.SendSMSNowReceiver

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 Exposure 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 [0]

18. Useful Links

4. Detected Vulnerabilities Statistics (Mobile Application)

Medium

Critical

3

3

1

5

Low

High

Your Aggregated Risk: **Critical**

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

20%

20%

45%

15%

Percentage

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

CWE-78OS Command Injection1

CWE-89SQL Injection2

CWE -284Improper Access Control3

CWE-287Improper Authentication3

CWE-352Cross-Site Request Forgery2

CWE-79Cross-Site Scripting5

CWE-200Information Exposure25

CWE-601Open Redirect3

1

2

3

4

5

6

7+

 Android Demo Application	Risk Level >	Path Status >	Remember Current Settings	Executive View	   
Table of Contents					
1. Introduction & 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 asset action/MAN 10.2 Response Data Storage 10.3 Response Authentication in android/authenticate/SendAuthInfo 10.4 Response Communication 11. Low Risk Mobile Application Vulnerabilities [2] 11.1 Response Data Storage 11.2 Use of Hardcoded Credentials 12. Medium Application Security Warnings [1] 12.1 Response Data Storage 13. Critical Risk Mobile Backend Vulnerabilities [0] 14. High Risk Mobile Application Vulnerabilities [2] 14.1 Path traversal in /api/interface.php 14.2 Improper Content-Disposition frequency in /api/auth.php 15. Medium Risk Mobile Backend Vulnerabilities [1] 15.1 Information disclosure in /api/interface.php 16. Low Risk Mobile Backend Vulnerabilities [1] 16.1 Improper Access Control in /api/interface.php 17. Medium Backend Security Warnings [1] 17.1 Web Forms Collecting Attributes Personal Data 18. Useful Links					
13. Critical Risk Mobile Backend Vulnerabilities					
13.1 SQL Injection in /api/balance.php					
Vulnerability ID:		6			
Vulnerable URL:		http://demo.example.com/api/balance.php			
Vulnerability CVE-ID:		CVE-999-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 11.2.3)			
GDPR:		Compliance Failed (EU 2016/679, GDPR Articles 5(1)(b), 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					

Mobile Penetration Testing 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



Threat-Led Penetration Testing

Testing resilience of your systems to specific Tactics, Techniques & Procedures (TTPs)



Red Teaming

Breach and Attack Simulation (BAS) using MITRE ATT&CK® Mobile



IAM Testing

Full spectrum of cyber-attacks testing your Identity & Access Management (IAM)

Compliance-Ready Mobile Penetration Testing



US HIPAA, NYSDFS & NIST SP 800-171

Helps fulfill monitoring requirements
under the US laws & frameworks



EU DORA, NIS 2 & GDPR

Helps fulfill monitoring requirements
under the EU laws & regulations



PCI DSS, ISO 27001, SOC 2 & CIS Controls®

Helps fulfill monitoring requirements
under the industry standards

Proven Methodology and Standards of Testing

Testing Methodologies

- ✓ OWASP Mobile Security Testing Guide (MASTG)
- ✓ NIST SP 800-115 Technical Guide to Information Security Testing and 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
- ✓ ECB TIBER-EU



Covered Vulnerabilities

- ✓ CWE/SANS Top 25
- ✓ PCI DSS 4.0 (6.2.4)
- ✓ OWASP Mobile Top 10
- ✓ OWASP Top 10 API



Reporting Standards

- ✓ OWASP Application Security Verification Standard (ASVS v4.0.2) Mapping
- ✓ OWASP Mobile Application Security Verification Standard (MASVS v2.1.0) Mapping
- ✓ Common Vulnerabilities and Exposures (CVE) Compatible
- ✓ Common Weakness Enumeration (CWE) Compatible
- ✓ Common Vulnerability Scoring System (CVSS v4)



ImmuniWeb® MobileSuite Deliverables

Penetration Testing

- ✓ Full Customization of Testing
- ✓ Mobile App Penetration Testing:
 - SANS Top 25 Full Coverage
 - PCI DSS 6.2.4 Full Coverage
 - OWASP Mobile Top 10 Full Coverage
 - Authenticated Testing (MFA/SSO)
 - Business Logic Testing
- ✓ Mobile Backend Penetration Testing:
 - SANS Top 25 Full Coverage
 - PCI DSS 6.2.4 Full Coverage
 - OWASP Top 10 Full Coverage
 - OWASP Top 10 API Full Coverage
 - Authenticated Testing (MFA/SSO)
 - Business Logic Testing
- ✓ Mobile Application Privacy Review
- ✓ Software Composition Analysis
- ✓ Open Source Software Security Ratings
- ✓ Rapid Delivery SLA Money back

Reporting

- ✓ Threat-Aware Risk Scoring
- ✓ MITRE ATT&CK® Matrix Mapping
- ✓ Step-by-Step Instructions to Reproduce
- ✓ Web, PDF, JSON, XML and CSV Formats
- ✓ Tailored Remediation Guidelines
- ✓ PCI DSS and GDPR Compliances
- ✓ CVE and CWE Mapping
- ✓ CVSSv4 Scoring
- ✓ OWASP MASVS Mapping
- ✓ Zero False-Positives SLA Money back

Remediation

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



ImmuniWeb® MobileSuite Packages

Mobile Application Penetration Testing

ImmuniWeb® MobileSuite	Ultimate	Corporate Pro	Corporate	Express Pro
Threat-Led Penetration Testing	✓			
AI-Powered Security Testing	✓	✓	✓	✓
OWASP MASVS Testing Level	L1, L2, R	L1, L2, R	L1, L2	L1
OWASP ASVS Testing Level	Level 3	Level 3	Level 2	Level 1
Manual Penetration Testing	10 days	5 days	5 days	3 days
Report Writing	2 days	8 hours	8 hours	4 hours
Unlimited Retesting	✓	✓	✓	✓
Penetration Test Certificate	✓	✓	✓	
Network Security Assessment	✓	✓		
Testing on Physical Device	✓	✓		
Resilience Mechanism Bypass	✓	✓		

How
To
Buy?



Instant Online Purchase

- ✓ All Product Benefits
- ✓ Instant Online Payment
- ✓ Instant Start 24/7/365
- ✓ Zero Paperwork
- ✓ 100% Online

Buy Now



or



Guided Purchase

- ✓ All Product Benefits
- ✓ Volume Discounts
- ✓ Custom Packaging
- ✓ Custom Contract
- ✓ Personal Manager

Talk to Sales

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 I 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 your 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 known 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 can I get a letter of compliance after completing penetration test?

A For cybersecurity compliance services, ImmuniWeb collaborates with external law firms that can provide you with a letter of compliance signed by lawyers. [Learn more.](#)

Q Where will my data reside?

A By default, your data resides on ImmuniWeb's servers in Switzerland and Canada: both countries have an adequacy decision by [the European Commission \(EC\) for the EU GDPR](#) compliance purposes. Upon request, your data can be stored in another jurisdiction of your preference for an extra cost. Your data can be securely deleted at any time upon your request. No public cloud providers are used to store your data.

Q Do you offer special pricing for government, academia and non-profit organizations?

A Yes, we do offer advantageous pricing for government, academia and non-profit organizations. Please reach out to our [sales team](#) to see whether your organization qualifies.

Why Choosing ImmuniWeb® AI Platform

Because You Deserve the Very Best



Reduce Complexity

All-in-one platform for 20 synergized use cases

[Learn More](#)



Optimize Costs

All-in-one model & AI automation reduce costs by up to 90%

[Learn More](#)



Validate Compliance

Letter of conformity from law firm confirming your compliance

[Learn More](#)



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

DevSecOps and CI/CD Integrations



[See All 50 Integrations](#)

Trusted by 1,000+ Global Customers

“

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



“

*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.*



“

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.



“

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

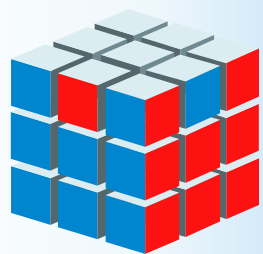


Partnerships with the Industry Leaders



[See Partners Directory](#)

1 Platform



ImmuniWeb®
AI Platform

6 SaaS Products



ImmuniWeb®
Discovery



ImmuniWeb®
Neuron



ImmuniWeb®
Neuron Mobile



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 Automated
Red Teaming



Continuous Breach and
Attack Simulation



Continuous Penetration
Testing



Continuous Threat
Exposure Management



Cyber Threat
Intelligence



Dark Web
Monitoring



Mobile Penetration
Testing



Mobile Security
Scanning



Network Security
Assessment



Penetration
Testing-as-a-Service



Phishing Websites
Takedown



Third-Party Risk
Management



Threat-Led
Penetration Testing



Web Penetration
Testing



Web Security
Scanning

50 CI/CD Integrations



See All...

Contacts

Headquarters

 Geneva, Switzerland

+41 22 560 6800

Quai de l'Île 13
Geneva, CH-1204
Switzerland



Sales inquiries: sales@immuniweb.com
Press inquiries: press@immuniweb.com
General inquiries: info@immuniweb.com

www.immuniweb.com

Join our **58,361** subscribers:



Newsletter

Regional Offices

 London

+44 20 4534 7678

4/4a Bloomsbury Square
Greater London WC1A 2RP
United Kingdom

 Washington, D.C.

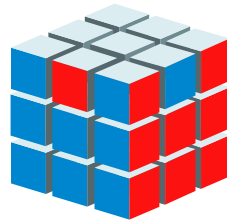
+1 720 605 9147

1500 K Street, 2nd Floor
Washington, D.C. 20005
United States

 Dubai

+971 04 291 2320

8th Floor, Sheikh Rashid Tower
DWTC, Sheikh Zayed Rd
United Arab Emirates



ImmuniWeb®
AI for Application Security

www.immuniweb.com



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

SCawards
EUROPE
Winner

One Platform. All Needs.