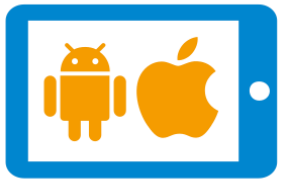
ImmuniWeb® MobileSuite



www.immuniweb.com

ImmuniWeb outperformed IBM Watson for Cybersecurity and won in the "Best Usage of Machine Learning and AI" Category

SC 2018 awards EUROPE Winner
Best Usage of Machine Learning and AI

Mobile Penetration Testing Made Simple

Zero False-Positive SLA

Money-Back Guarantee for
a single false-positive

Rapid Delivery SLA

Guaranteed schedule of execution
and report delivery

In-Depth Testing

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

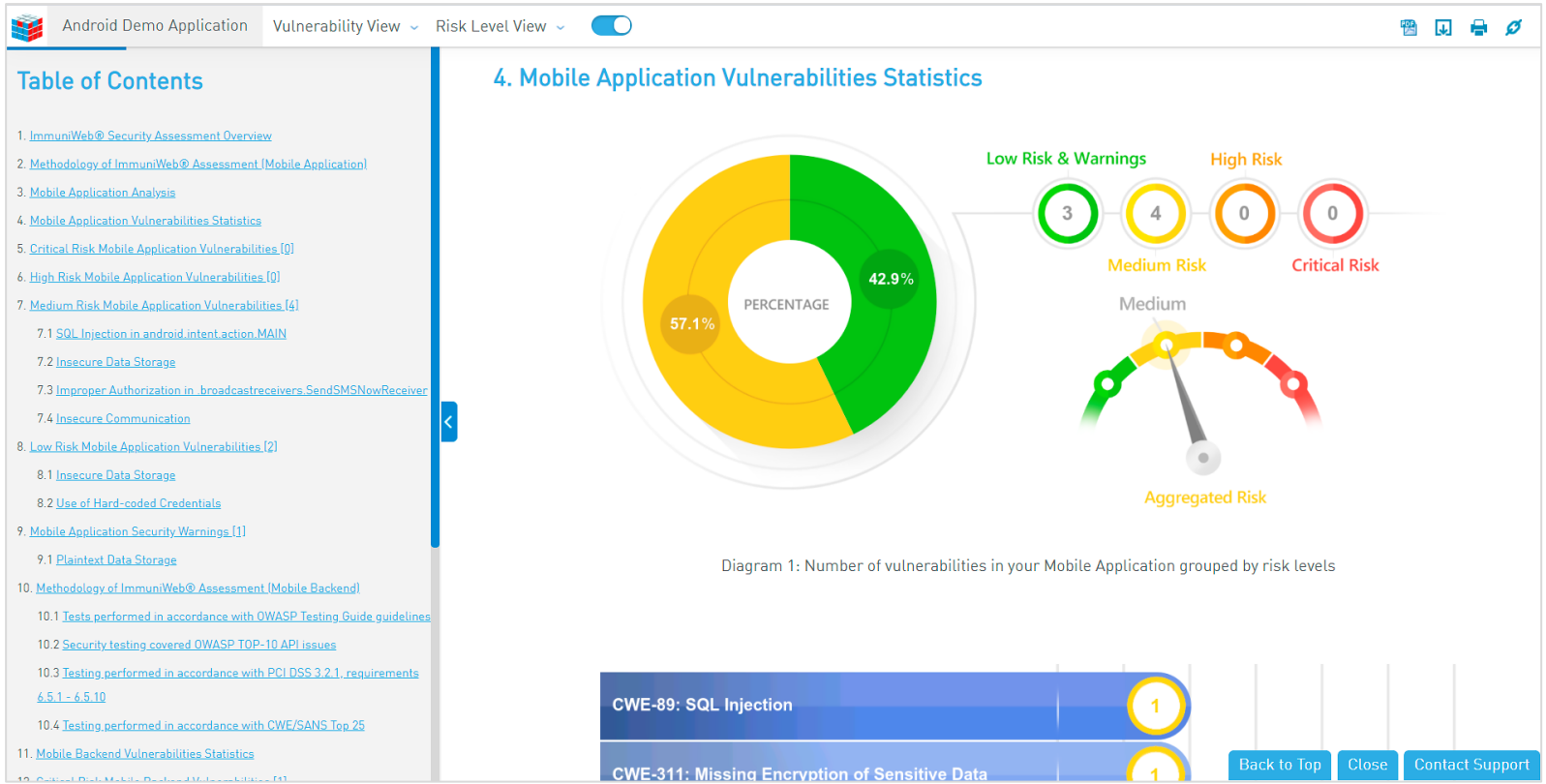
Actionable Reporting

Tailored remediation guidelines
and 24/7 support

DevSecOps Tailored

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

Best Vulnerability Coverage. Actionable Report. Simple Remediation.



1. Configure, schedule and start online
2. Enjoy 24/7 access to our security analysts
3. Get remediation report and schedule re-test

Mobile Penetration Test for Any Need

Ultimate Mobile App Testing

Static, dynamic and interactive security testing with SCA

Backend Security Testing

Manual security testing of Web Services and APIs

Intelligent Behavioral Analysis

Machine learning technology enhanced with manual security testing

Black & White Box

Authenticated (including 2FA/MFA) or Black Box testing

Attack Simulation

Threat-aware testing scenarios and attack vectors upon request

Advanced Reconnaissance

Expert analysis of threats at Dark Web and Public Code repositories

Proven Methodology and Global Standards

- OWASP Mobile Security Testing Guide (MSTG)
- NIST SP 800-115 Technical Guide to Information Security Testing and Assessment
- PCI DSS Information Supplement: Penetration Testing Guidance
- FedRAMP Penetration Test Guidance
- ISACA's How to Audit GDPR

- Common Vulnerabilities and Exposures (CVE) Compatible
- Common Weakness Enumeration (CWE) Compatible
- Common Vulnerability Scoring System (CVSSv3.1)

SANS Top 25 Full Coverage

- ✔ CWE-22: Path Traversal
- ✔ CWE-89: SQL Injection
- ✔ CWE-78: Command injection
- ✔ CWE-89: Blind SQL Injection
- ✔ CWE-90: LDAP Injection
- ✔ CWE-79: Reflected XSS
- ✔ CWE-91: XML Injection
- ✔ CWE-79: DOM-Based XSS
- ✔ CWE-93: CRLF Injection
- ✔ CWE-94: Code Injection
- ✔ CWE-113: HTTP Response splitting
- ✔ CWE-94: AJAX Injection
- ✔ CWE-200: Information Exposure
- ✔ CWE-94: JSON Injection
- ✔ CWE-255: Credentials Management
- ✔ CWE-97: SSI injection
- ✔ CWE-284: Improper Access Control
- ✔ CWE-98: Remote/Local PHP File Inclusion
- ✔ CWE-287: Authentication Bypass
- ✔ CWE-345: Insufficient Verification of Data Authenticity
- ✔ CWE-352: Cross-site request forgery (CSRF)
- ✔ CWE-384: Session Fixation
- ✔ CWE-400: Resource Exhaustion
- ✔ CWE-434: Arbitrary File Upload
- ✔ CWE-502: Deserialization of Untrusted Data
- ✔ CWE-521: Weak Password Requirements
- ✔ CWE-601: Open Redirect
- ✔ CWE-611: Improper Restriction of XML External Entity Reference
- ✔ CWE-613: Insufficient Session Expiration
- ✔ CWE-643: XPath Injection
- ✔ CWE-804: Guessable CAPTCHA
- ✔ CWE-799: Improper Control of Interaction Frequency
- ✔ CWE-918: Server-Side Request Forgery (SSRF)
- ✔ CWE-942: Overly permissive Cross-domain Whitelist

PCI DSS and OWASP Top 10 Full Coverage

- Injection Flaws
- Many other "High" Risk Vulnerabilities
- Buffer Overflows
- Cross-Site Scripting (XSS)
- Insecure Cryptographic Storage
- Improper Access Control
- Insecure Communications
- Cross-Site Request Forgery (CSRF)
- Improper Error Handling
- Broken Authentication and Session Management

PCI Security Standards Council™

- A1: Injection
- A6: Security Misconfiguration
- A2: Broken Authentication
- A7: Cross-Site Scripting (XSS)
- A3: Sensitive Data Exposure
- A8: Insecure Deserialization
- A4: XML External Entities (XXE)
- A9: Using Components with Known Vulnerabilities
- A5: Broken Access Control
- A10: Insufficient Logging & Monitoring

OWASP Open Web Application Security Project

- M1: Improper Platform Usage
- M2: Insecure Data Storage
- M3: Insecure Communication
- M4: Insecure Authentication
- M5: Insufficient Cryptography
- M6: Insecure Authorization
- M7: Client Code Quality
- M8: Code Tampering
- M9: Reverse Engineering
- M10: Extraneous Functionality

OWASP Mobile Security Project

Most Comprehensive Mobile Penetration Testing

In Every ImmuniWeb MobileSuite Package:

Penetration Testing

- ✔ Mobile App Penetration Testing
  - Mobile App Audit
  - Mobile Endpoints Audit
  - SANS Top 25 Full Coverage
  - OWASP Top 10 Full Coverage
  - OWASP Mobile Top 10 Full Coverage
  - PCI DSS 6.5.1-6.5.11 Full Coverage
  - AI Augments Human Testing and Analysis
  - Machine Learning Accelerates Testing
- ✔ Full Customization of Testing
- ✔ Rapid Delivery SLA Money back

Reporting

- ✔ Threat-Aware Risk Scoring
- ✔ Step-by-Step Instruction to Reproduce
- ✔ Web Interface, PDF and XML Formats
- ✔ Tailored Remediation Guidelines
- ✔ PCI DSS and GDPR Compliances
- ✔ CVE, CWE and CVSSv3.1 Scores
- ✔ Zero False-Positive SLA Money back

Remediation

- ✔ Unlimited Patch Verifications
- ✔ 24/7 Access to Our Security Analysts
- ✔ DevSecOps & CI/CD Tools Integration
- ✔ One-Click Virtual Patching via WAF (backend)
- ✔ Multirole RBAC Dashboard

ImmuniWeb® MobileSuite Packages

One package per mobile app Includes backend testing	Corporate Pro	Corporate	Express Pro	Express
AI-Automated Penetration Testing	5 days	3 days	1 day	1 day
Enhancement with Manual Testing	3+ experts	2+ experts	1+ experts	1 expert
WAF Testing and Bypass	✔	✔	✔	✔
Zero False Positives SLA	✔	✔	✔	✔
Unlimited Patch Verification Scans	✔	✔	✔	✔
Dark and Deep Web Reconnaissance	✔	✔	✔	
Code Repositories Reconnaissance	✔	✔		
Root or Jailbreak Detection Bypass	✔			
Emulator Detection Bypass	✔			
Certificate Pinning Bypass	✔			
Code Obfuscation Bypass	✔			
Unbeatable value for money	$9,995	$7,495	$4,495	$1,495

ImmuniWeb® MobileSuite Packages

1 Configure Your Test

Upload your application, indicate any special testing, scoping or reporting requirements

2 Select the Best Package

Pick up a package or get a free consultation from our security analysts to select one

3 Schedule and Start

Select the dates of the penetration test and report delivery, and you are done!

Corporate Pro

Corporate Pro package is best suited for business-critical apps handling sensitive data of your clients, such as e-banking or e-payments apps with 15 or more systems in the mobile backend (e.g. web services, APIs, etc) and/or using active defense mechanisms.

Corporate

Corporate package is best suited for business-critical apps handling sensitive data of your clients, such as e-banking or e-payments apps with 15 or more systems in the mobile backend (e.g. web services, APIs, etc).

Express Pro

Express Pro package is best suited for business applications that process data of your clients or partners, such as online booking, basic e-commerce or document processing apps with up to 10 systems in the mobile backend (e.g. web services, APIs, etc).

Express

Express package is best suited for small mobile apps, such as games or news apps with up to 5 systems in the mobile backend (e.g. web services, APIs, etc).

Includes penetration test of the mobile app and its endpoints (e.g. Web Services of APIs).

Frequently Asked Questions

Q How can I customize testing to meet my specific needs?

A At the first step of online project creation, you can easily configure any special requirements for testing or reporting. For example, you can select testing with 2FA authentication, or exclude any specific vulnerabilities (e.g. self-XSS) from being reported, or contrariwise spend more time on authentication bypass attacks in a specific part of the application.

Q How are we better than traditional mobile penetration testing?

A We use our award-winning AI and Deep Learning ANN technology to intensify, augment and accelerate human testing thereby making application penetration testing scalable and cost-efficient. We deliver faster results, better vulnerability coverage and unbeatable pricing compared to traditional penetration testing services powered solely by a human.

Q How do you outperform automated vulnerability scanning?

A We perform in-depth security testing including business logic analysis and testing, and comprehensive coverage of SANS Top 25 vulnerabilities using globally renown penetration testing methodologies. Moreover, we provide all our customers with a zero false-positives SLA corroborated with money-back guarantee for a single false positive.

DevSecOps, CI/CD and WAF Integrations

Developers Environment

Web Application Firewalls

And Much More:

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

Gartner peer insights™

4.8 out of 5

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

ImmuniWeb® AI Platform in a Nutshell

1

Illuminate Your Attack Surface to Prioritize Testing

ImmuniWeb® Discovery

Dark Web & Attack Surface Monitoring

AI-Enabled | Automated | 24/7

2

Run Risk-Based Security Testing and Remediation

ImmuniWeb® On-Demand

Web Application Penetration Testing

AI-Enabled | Manual | One-Time

ImmuniWeb® MobileSuite

Mobile Penetration Testing

AI-Enabled | Manual | One-Time

3

Ensure Continuous Security Monitoring

ImmuniWeb® Continuous

Continuous Penetration Testing

AI-Enabled | Manual | 24/7

www.immuniweb.com