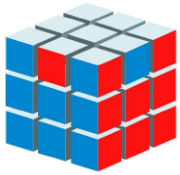


ImmuniWeb® Continuous

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

Continuous Penetration Testing Made Simple

Zero False-Positive SLA

Money-Back Guarantee for
a single false-positive

24/7 Just in Time Testing

Once your code is changed, our
experts will promptly test it

In-Depth Testing

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

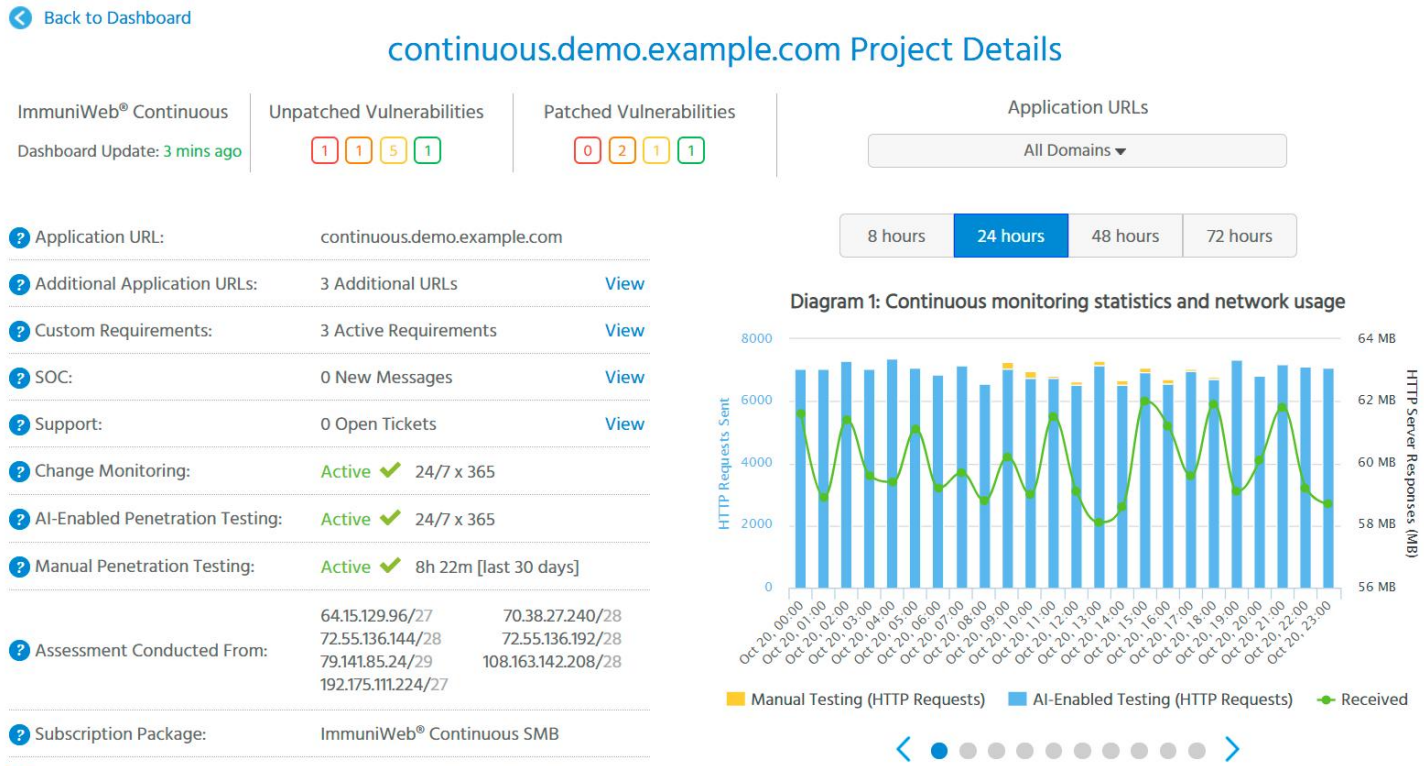
Actionable Reporting

Tailored remediation guidelines
and 24/7 support

DevSecOps Tailored

One-click WAF virtual patching,
SDLC & CI/CD integration

Best Vulnerability Coverage. Actionable Report. Simple Remediation.



1 Configure, schedule and start online

2 Have new or updated code tested instantly

3 Get 24/7 alerts by our security analysts

Continuous Penetration Testing for Any Need

Internal & External Web Apps

Virtual Appliance technology for internal applications testing

APIs and Web Services

Comprehensive coverage of API & Web Services (REST/SOAP)

Internal & External Web Apps

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

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 Web Security Testing Guide (WSTG)
- 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

Most Comprehensive Continuous Penetration Testing

In Every ImmuniWeb Continuous Package

24/7 Penetration Testing

- ✔ Rapid Detection of New Code
- ✔ Rapid Detection of Updated Code
- ✔ Continuous Penetration Testing
  - SANS Top 25 Full Coverage
  - OWASP Top 10 Full Coverage
  - PCI DSS 6.5.1-6.5.11 Full Coverage
  - AI Augments Human Testing and Analysis
  - Machine Learning Accelerates Testing
  - Authenticated Testing (2FA / SSO)
  - REST/SOAP API Testing
  - Business Logic Testing
- ✔ Full Customization of Testing

24/7 Reporting

- ✔ Instant SMS Alerts
- ✔ Instant Email Alerts
- ✔ Threat-Aware Risk Scoring
- ✔ Step-by-Step Instruction to Reproduce
- ✔ Web, PDF, JSON, XML and CSV Formats
- ✔ PCI DSS and GDPR Compliances
- ✔ CVE, CWE and CVSSv3.1 Scores
- ✔ Zero False-Positive SLA Money back

24/7 Remediation

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

ImmuniWeb® Continuous Packages

One package per business application with **unlimited** URLs	Corporate Pro	Corporate	Express Pro	Express
AI-Automated Penetration Testing	24/7	24/7	24/7	24/7
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	✔			
Unbeatable value for money	$5,495 / month	$3,495 / month	$1,495 / month	$995 / month

ImmuniWeb® Continuous Packages

1 Configure Your Test

Enter the URL(s) of 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 subscription starting date, add users, customize alerts and you are done!

Corporate Pro

Corporate Pro package is best suited for business-critical applications of large size that require sophisticated business logic testing under multiple user roles and interacting with different APIs. Multifunctional e-banking or complicated CRM systems fit well this package, as well as applications based on web solutions from SAP, Oracle or Microsoft.

Corporate

Corporate package is best suited for business applications with several user roles, diverse dynamic functionality and APIs. Medium-sized e-banking or payment processing systems also fit well into this package.

Express Pro

Express Pro package is best suited for medium-sized websites and small e-commerce applications with several APIs. It also fits to audit a small part of a larger web application. Websites running standardized e-commerce systems such as Magento match well the package.

Express

Express package is best suited for uncomplicated websites, for example, a presentational website with some dynamic functionality. It also fits to audit a small part of a larger web application. Business websites running WordPress or Drupal with a few third-party plugins match well the package.

Web application may be any HTTP/S application from corporate website to CRM or e-banking.
The application may be hosted on several (sub)domains and have unlimited number of URLs, Web Services and 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. Furthermore, you have a 24/7 online access to our security experts to easily communicate any new or adjusted testing requirements or request specific testing.

Q How are we better than traditional web 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. Moreover, we provide a just-in-time (24/7) penetration testing by instantly testing all new or updated code without leaving your applications untested during two separate penetration tests for example.

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. On top of this, you can instantly remediate the detected vulnerabilities with a virtual patching and request re-testing in just one click.

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