ImmuniWeb® On-Demand

Compliance-Ready Web Application Penetration Testing

ImmuniWeb® On-Demand leverages our award-winning Machine Learning technology to accelerate and enhance web 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

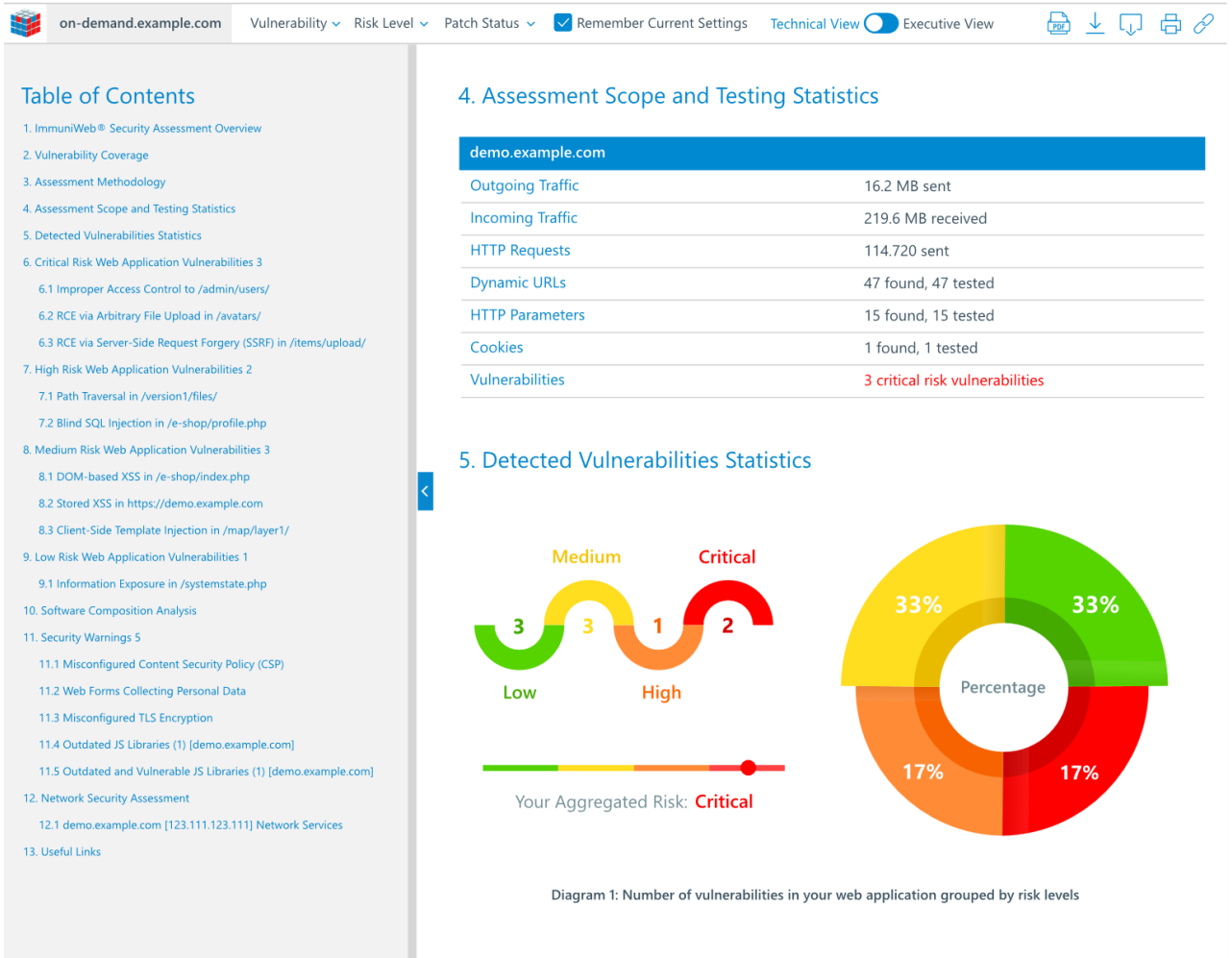
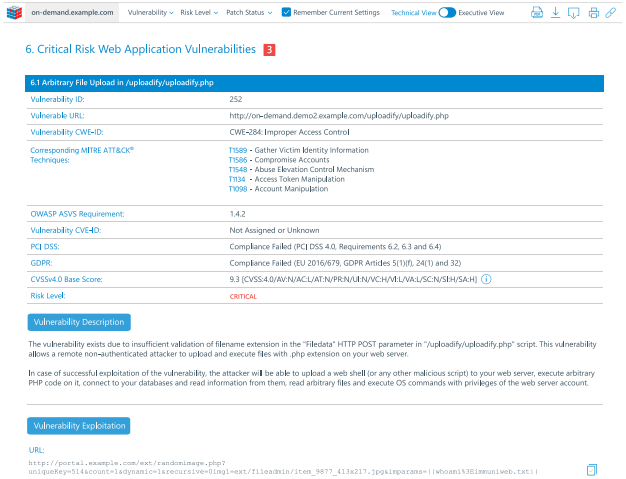
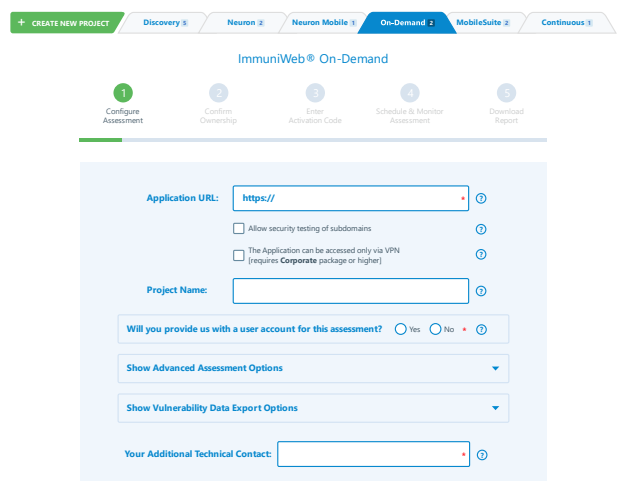


Diagram 1: Number of vulnerabilities in your web application grouped by risk levels





Web Application Penetration Testing That Covers Everything

Internal & External Web Apps

Virtual Appliance technology for internal applications testing

APIs and Web Services

API (REST/SOAP/GraphQL) security & privacy testing

Cloud Security Testing

Exploitation of cloud-specific flaws in your cloud-hosted apps & APIs

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® matrix

IAM Testing

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

Compliance-Ready Web 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 Web Security Testing Guide (WSTG)
- ✔ NIST SP 800-115 Technical Guide to Information Security Testing and Assessment
- ✔ PCI DSS Information Supplement: Penetration Testing Guidance
- ✔ MITRE ATT&CK® Matrix for 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 Top 10
- ✔ OWASP Top 10 API

Reporting Standards

- ✔ 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 v4)

ImmuniWeb® On-Demand Deliverables

Penetration Testing

- Full Customization of Testing
- Web Application Penetration Testing
  - SANS Top 25 Full Coverage
  - OWASP Top 10 Full Coverage
  - OWASP Top 10 API Full Coverage
  - PCI DSS 6.2.4 Requirement Full Coverage
  - Authenticated Testing (MFA / SSO)
  - REST/SOAP/GraphQL API Testing
  - Business Logic Testing
- Software Composition Analysis
- Network Security Assessment
- Web Application Privacy Review
- 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 ASVS Mapping
- Zero False-Positives SLA Money back

Remediation

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

ImmuniWeb® On-Demand Packages

Threat-Led Penetration Testing

ImmuniWeb® On-Demand	Ultimate	Corporate Pro	Corporate	Express Pro
Threat-Led Penetration Testing	✔			
AI-Powered Security Testing	✔	✔	✔	✔
OWASP ASVS Testing Level	Level 3	Level 3	Level 2	Level 1
Manual Penetration Testing	10 days	5 days	3 days	1 day
Report Writing	2 days	8 hours	4 hours	2 hours
Unlimited Retesting	✔	✔	✔	✔
Penetration Test Certificate	✔	✔	✔	
Network Security Assessment	✔	✔		
Internal Web Application Testing	✔	✔		

How To Buy?

Instant Online Purchase

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

Buy Now

VISA · mastercard · AMERICAN EXPRESS · PayPal · maestro · JCB · UnionPay 银联 · BANK TRANSFER

or

Guided Purchase

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

Talk to Sales

Frequently Asked Questions

Q How many URLs and domains can I include into one package?

A There is no hard limit on the number of URLs or domains per package. All targets should, however, belong to the same business application. For example, an e-commerce platform may be located across several (sub)domains, APIs or third-party managed web services. They can normally all be included into one package. If you also wish to test your e-banking system, you will need a second package.

Q How can I customize my testing and reporting requirements?

A At the first step of project creation, you can easily configure special requirements for penetration testing or reporting. For example, you can select authenticated (White Box) testing with 2FA/SSO, exclude testing for some specific vulnerabilities (e.g. self-XSS) or areas of the web application, request to spend more time on cloud pivoting or container escaping if your web application is hosted in a cloud environment. All pentesting reports by default contain PCI DSS and GDPR sections.

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 web application for all know web application vulnerabilities and attack vectors. Please reach out to us for a quote tailored for your specific needs and scope.

Q Can you test my applications in Microsoft Azure, AWS or GCP?

A Yes, we can test your web applications, cloud-native apps, microservices or APIs hosted in AWS, Azure, GCP and any other public cloud service providers. Aside from detecting OWASP Top 10, OWASP API Top 10 and SANS Top 25 vulnerabilities, we also detect cloud-specific misconfigurations and try cloud pivoting and privilege escalation attacks by exploiting excessive access permissions, IMDS flaws or default IAM policies in your cloud environment.

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

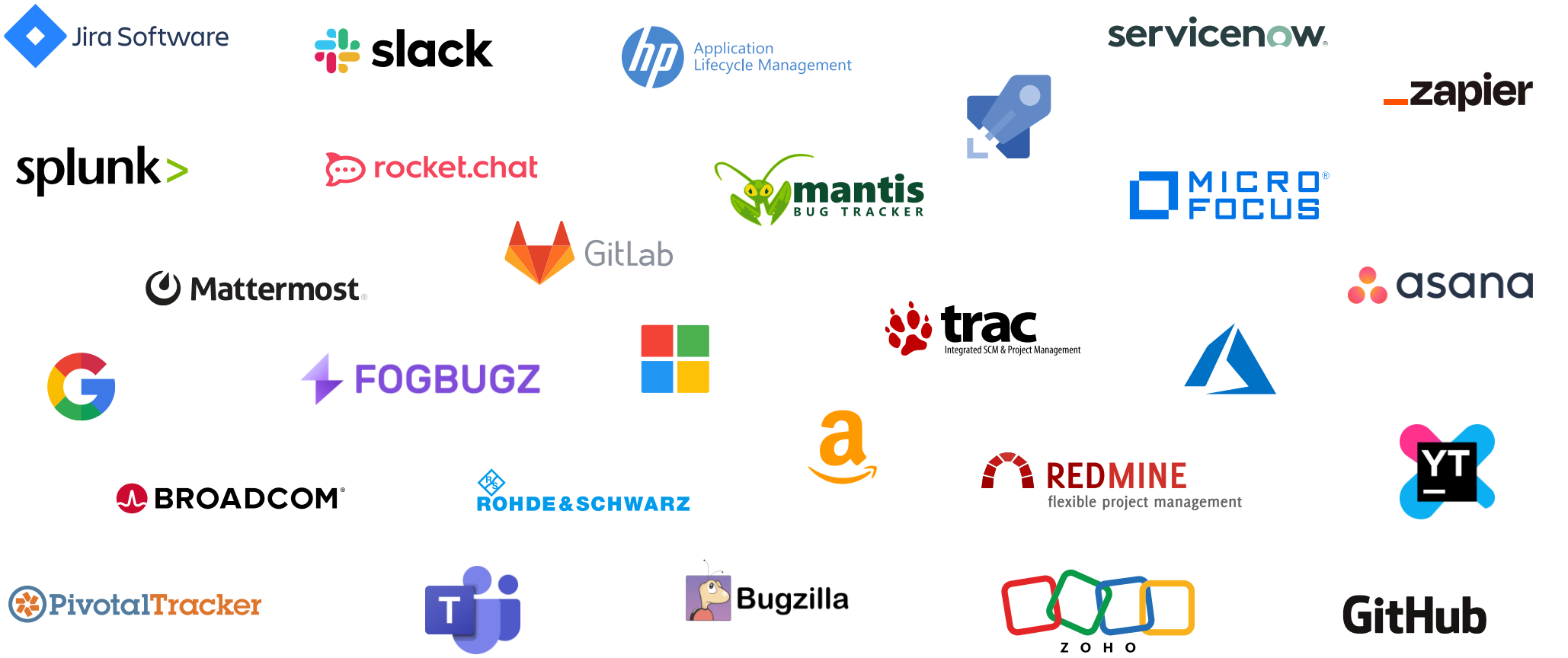
Letter of conformity from law firm confirming your compliance

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

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

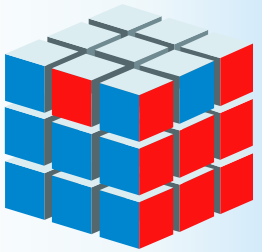
ImmuniWeb is an efficient and very easy-to-use solution that combines automatic and human tests. The results are complete, straightforward and easy to understand. It's an essential tool for the development of the new digital activities

next bank
CRÉDIT AGRICOLE

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'Ile 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.

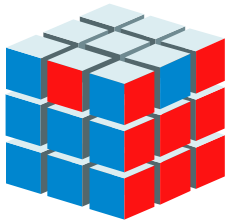
+1 720 605 9147

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

CREST ACCREDITED

SYSTEM CERTIFICATION ISO 9001 SGS

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 EUROPE Winner

One Platform. All Needs.