# ImmuniWeb® Neuron

ImmuniWeb® Neuron unleashes the power of Machine Learning and AI to take traditional web vulnerability scanning to the next level. While detecting more vulnerabilities compared to traditional web scanners, every web vulnerability scan by Neuron is equipped with a contractual zero false-positives SLA.

**www.immuniweb.com**

Gartner
Cool Vendor ™

IDC 💡 Innovator

AI FINTECH 100 2021

# Premium Web Application Security Scanning

## Zero False-Positives SLA

Money-Back Guarantee for a single false positive

## AI-Driven Testing

Deep Learning engine detects sophisticated vulnerabilities

## Expert Assistance

Our security analysts will help your software developers

## Unlimited Scalability

Simultaneous web scanning of hundreds or thousands apps

## DevSecOps Native

Full automation of testing and CI/CD pipeline integrations

**1** Configure and start scanning

**2** Get 100% valid findings, zero false positives

**3** Schedule regular scans and alerts

# More Findings. No False Positives.

+ CREATE NEW PROJECT | DISCOVERY 3 | NEURON 2 | ON-DEMAND 1 | MOBILESUITE 1 | CONTINUOUS 1 | API & ACCESS

## Your ImmuniWeb® Neuron Projects

Neuron: Project #3138898

🔔 Notifications | 🌐 IP Ranges | Subscription Valid Until: July 1, 2023 | Targets Left: 44

| New 10 | 🔍 GDPR 12 | 🔧 PCI DSS 23 | ☰ |

🔍 Search and Filters | 🏷 Tags | ➕ Add Target | Import Targets | CI/CD Integrations

| ☐ | Target ⇕ | Availability ⇕ | Scan Status ⇕ | Vulnerabilities ⇕ | Actions ☰ |
|---|---|---|---|---|---|
| ☐ | https://www.example.com ✏ ✖ 🏷 🇺🇸 93.184.216.34 \| HTTP Code: 200 Authentication: HTTP | Available | Running Scan Started: June 07 2022, 10:25 CEST Next Scan: Unscheduled | 0 1 0 3 0 | ⏹ ⚙ 🕐 💬 🥧 🥧 ⬆ |
| ☐ | https://portal.example.com ✏ ✖ 🏷 🇺🇸 88.277.119.33 \| HTTP Code: 404 Authentication: None | Unavailable | Stopped Latest Scan: Never Next Scan: Unscheduled | 0 0 4 0 0 | ▶ ⚙ 🕐 💬 🥧 🥧 ⬆ |
| ☐ | https://pay.example.com ✏ ✖ 🏷 🇺🇸 103.180.278.22 \| HTTP Code: 200 Authentication: Web | Available | Running Scan Started: June 02 2022, 14:25 CEST Next Scan: Unscheduled | 1 2 3 0 3 | ⏹ ⚙ 🕐 💬 🥧 🥧 ⬆ |
| ☐ | http://dev.example.com ✏ ✖ 🏷 🇺🇸 191.14.678.20 \| HTTP Code: 403 Authentication: None | Banned | Stopped Latest Scan: June 12 2022, 04:05 CEST Next Scan: July 08 2022, 11:50 CEST | 3 7 4 0 2 | ▶ ⚙ 🕐 💬 🥧 🥧 ⬆ |
| ☐ | https://example.net/blog ✏ ✖ 🏷 🇺🇸 33.405.210.11 \| HTTP Code: 200 Authentication: None | Available | Scheduled Latest Scan: Never Next Scan: August 11 2022, 21:00 CEST | 0 0 0 0 0 | ⏹ ⚙ 🕐 💬 🥧 🥧 ⬆ |
| ☐ | https://sales.example.com ✏ ✖ 🏷 🇺🇸 201.224.16.13 \| HTTP Code: 200 Authentication: None | Error | Stopped Latest Scan: June 07 2022, 08:35 CEST Next Scan: July 08 2022, 21:20 CEST | 0 0 0 0 0 | ▶ ⚙ 🕐 💬 🥧 🥧 ⬆ |

---

portal.example.com | Vulnerability | Risk Level | ☑ Remember current settings

### Table of Contents

1. Detected Vulnerability Statistics
2. Vulnerability Coverage
3. Scan Scope and Setting Statistics
4. Critical Risk Web Application Vulnerabilities [2]
   4.1 OS Command Injection in /ext/randomimage.php
   4.2 SQL Injection in /index.php
5. High Risk Web Application Vulnerabilities [1]
   5.1 Path Traversal in /upload/
6. Medium Risk Web Application Vulnerabilities [1]
   6.1 Reflected XSS in /company/
   6.2 Stored XSS in /shop/save.php
7. Low Risk Web Application Vulnerabilities [1]
   7.1 Directory Listing at /path/
   7.2 Information Disclosure at /option/stats.php
   7.3 Open Redirect in /goto.php
8. Security Warnings [3]
   8.1 Predictable Location of Administrative Area in /admin/
   8.2 Deprecated HTTP Header "X-XSS-Protection"
   8.3 Untrusted TLS Certificate
9. Useful Links

### 1. Detected Vulnerabilities Statistics

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

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

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

---

on-demand.demo.example.com | Vulnerability | Risk Level | Patch Status | ☑ Remember Current Settings | Technical View ⚪ Executive View

#### 4.1 OS Command Injection in /ext/randomimage.php

| Vulnerability ID: | 252 |
|---|---|
| Vulnerable URL: | http://portal.example.com/ext/randomimage.php |
| Vulnerability CWE-ID: | CWE-78: OS Command Injection |
| Vulnerability CVE-ID: | Not Assigned or Unknown |
| CVSSv3.1 Base Score: | 10 [CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H] |
| Risk Level: | CRITICAL |

**Vulnerability Description**

The vulnerability exists due to insufficient sanitization of user-supplied input data passed via the "imparams" HTTP GET parameter to "/ext/randomimage.php". A remote unauthenticated attacker can send a specially crafted HTTP request to the vulnerable script and execute arbitrary OS commands on the web server. In case of success, the web application, its web server and databases will be compromised.

**Vulnerability Exploitation**

URL:
http://portal.example.com/ext/randomimage.php?
uniqueKey=514&count=1&dynamic=1&recursive=0&imp1=ext/fileadmin/item_9877_413x217.jpg&imparams=|whoami%3Eimmuniweb.txt|

Raw HTTP Server Response:
HTTP/2.0 200 OK server: nginx content-type: text/html; charset=UTF-8 content-length: 8562 cache-control: no-cache x-frame-options: SAMEORIGIN x-xss-protection: 1; mode=block x-content-type-options: nosniff DEMO

**Vulnerability Remediation**

It is recommended to perform a holistic filtration of all user-supplied input before using it in the code. Moreover, using any user-supplied data in system commands shall be avoided. More information about OS Command Injection is available at the ImmuniWeb Knowledge Base: https://www.immuniweb.com/CWE-78

# CI/CD and DevSecOps Native

# Premium Web Security Scanning for Any Environment

## APIs & Web Services
Find security flaws in your microservices and APIs

## Single Page Apps
Detect vulnerabilities in SPA and Ajax apps

## Cloud-Native Apps
Test your full web stack at AWS, Azure or GCP

## Authenticated Scans
Manual authentication scripts, SSO & MFA scanning

## Open-Source Security
Discover security risks in open source you use

## SDLC Automation
Integrate fully automated scanning into your CI/CD pipeline

# Detect Everything. Stay Compliant.

## OWASP TOP 10

- ✓ **A1:** Broken Access Control
- ✓ **A2:** Cryptographic Failures
- ✓ **A3:** Injection
- ✓ **A4:** Insecure Design
- ✓ **A5:** Security Misconfiguration
- ✓ **A6:** Vulnerable and Outdated Components
- ✓ **A7:** Identification and Authentication Failures
- ✓ **A8:** Software and Data Integrity Failures
- ✓ **A9:** Security Logging and Monitoring Failures
- ✓ **A10:** Server-Side Request Forgery

## OWASP TOP 10 API

- ✓ **API1:** Broken Object Level Authorization
- ✓ **API2:** Broken User Authentication
- ✓ **API3:** Excessive Data Exposure
- ✓ **API4:** Lack of Resources & Rate Limiting
- ✓ **API5:** Broken Function Level Authorization
- ✓ **API6:** Mass Assignment
- ✓ **API7:** Security Misconfiguration
- ✓ **API8:** Injection
- ✓ **API9:** Improper Assets Management
- ✓ **API10:** Insufficient Logging & Monitoring

# ImmuniWeb® Neuron Setup and Deliverables

**1** Configure and start scanning →
**2** Get 100% valid findings, zero false positives →
**3** Schedule regular scans and alerts

## Web Security Scanning

- ✓ Scan Customization
- ✓ Authenticated Scans
- ✓ Web Security Scanning:
  - AI-Based Fuzzing
  - OWASP Top 10 Vulnerabilities
  - OWASP API Top 10 Vulnerabilities
  - Insecure HTTP Headers
  - SSL/TLS Weaknesses
- ✓ Known Web Vulnerabilities Scanning:
  - WordPress & 400+ Other Popular CMSs
  - 150,000+ CMS Plugins & Themes
  - 12,000+ JavaScript Libraries
  - 10,000+ Known CVE-IDs
- ✓ Turnkey CI/CD Automation

## Reporting

- ✓ Zero False-Positives SLA **Money back**
- ✓ Risk-Based Prioritization of Findings
- ✓ Simple Instructions to Reproduce Findings
- ✓ Web, PDF, JSON, XML and CSV Reports
- ✓ Friendly Remediation Guidelines
- ✓ Screenshots and Raw HTTP Data
- ✓ Consolidated View of All Scans
- ✓ CVE and CWE Mapping
- ✓ CVSSv3.1 Scoring

## Remediation

- ✓ Access to Our Security Analysts
- ✓ Seamless DevSecOps Integration
- ✓ RBAC Scan Management Dashboard
- ✓ Unlimited Dashboard Users
- ✓ Simple Scan Scheduling
- ✓ Recurrent Scans
- ✓ Email Alerts

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 you support authenticated scanning?

**A** Yes, we support all modern types of authentication scanning for cloud-based and on-premise web applications and APIs.

**Q** Can I integrate Neuron into my CI/CD pipeline?

**A** Yes, you can integrate Neuron with majority of on-premise and cloud-based CI/CD pipelines. You can also use our API to automatically manage scans.

**Q** How often can I scan my web applications?

**A** Neuron is a subscription-based service. While your subscription is active, you can scan your website unlimited amount of times.

**Q** How are you different from other web security scanners?

**A** ImmuniWeb® Neuron leverages our award-winning Machine Learning technology to intelligently automate sophisticated tests and checks that usually require human labor. Eventually, you may expect more vulnerabilities to be detected compared to traditional web security scanners, as well as more sophisticated vulnerabilities to be found.

**Q** Can ImmuniWeb Neuron replace penetration testing?

**A** No, the current state of AI and Machine Learning technologies is still far from being capable to fully replace human intelligence. For penetration testing needs, we have a dedicated offering that includes expert manual testing. Of note, many laws and regulations require mandatory penetration testing that you cannot substitute with vulnerability scanning.

# 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

amazon

G

PivotalTracker

Bugzilla

ROHDE & SCHWARZ

JET BRAINS

# 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



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.

**GDPR**
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
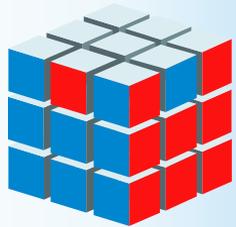
- ImmuniWeb® Discovery
- ImmuniWeb® Neuron
- ImmuniWeb® On-Demand
- ImmuniWeb® MobileSuite
- ImmuniWeb® Continuous
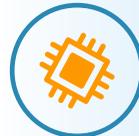
# 20 Use Cases

- 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
- Phishing Websites Takedown
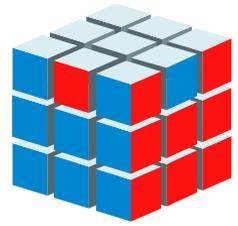- Red Teaming Exercise
- Software Composition Analysis
- Third-Party Risk Management
- Web Penetration Testing
- Web Security Scanning

# 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.