

**ImmuniWeb**<sup>®</sup>  
AI for Application Security

# Continuous Breach and Attack Simulation

Test your web infrastructure and applications continuously with real-life attacks from MITRE's ATT&CK matrix with [ImmuniWeb<sup>®</sup> Continuous](#) Breach and Attack Simulation



[www.immuniweb.com](http://www.immuniweb.com)

Copyright © 2024 ImmuniWeb SA

# Why Investing in Continuous Breach and Attack Simulation

88%

of companies now consider cybersecurity a critical business risk

Gartner

\$4.45M

is the average cost of a data breach in 2024, a 15% surge in just three years

IBM

100+

countries have laws imposing a personal liability on executives for a data breach

ImmuniWeb

Continuous Breach and Attack Simulation (BAS) offers a significant advantage over traditional security measures by mimicking real-world attacks, constantly testing an organization's defenses. Unlike point-in-time assessments, BAS provides a proactive and ongoing evaluation, identifying vulnerabilities as they emerge, such as through new software installations or configuration changes. Furthermore, BAS helps prioritize remediation efforts by highlighting the most critical vulnerabilities and their potential impact. This enables security teams to focus their resources on addressing the most pressing threats, optimizing their effectiveness in protecting sensitive data and systems.

# Continuous Breach and Attack Simulation with ImmuniWeb® Continuous

+ CREATE NEW PROJECT | Discovery 5 | Neuron 2 | Neuron Mobile 1 | On-Demand 1 | MobileSuite 2 | Continuous 1

demo.example.com | Subscription Valid Until July 1, 2024

Unpatched Vulnerabilities: 2 2 5 3 | Patched Vulnerabilities: 0 2 1 2 | SCA: 0 2 1 | API & User Access | User Manual

Unpatched Vulnerabilities | Archived Vulnerabilities | SCA | Statistics | Executive View | Vulnerability Notifications | Configuration

Below you can see recently detected vulnerabilities that are not patched yet

All Targets | Keyword Filter | 02/02/2024 - 11/08/2024 | Critical | High | Medium | Low | Warning | Export

0 new vulnerability or warning since your last login | Show only new or updated vulnerabilities since my last login

Vulnerability	CWE-ID	Detected	Status	Risk	Actions
<input type="checkbox"/> Blind SQL Injection in /e-shop/profile.php demo.example.com	SQL Injection CWE-89	25 Mar 2024	Unpatched	CRITICAL	<a href="#">Info</a> <a href="#">Print</a> <a href="#">Share</a>
<input type="checkbox"/> Improper Authentication in /sendmail/ demo.example.com	Improper Authentication CWE-287	23 Mar 2024	Unpatched	MEDIUM	<a href="#">Info</a> <a href="#">Print</a> <a href="#">Share</a>
<input type="checkbox"/> Path Traversal in /sendfile/ demo.example.com	Path Traversal CWE-22	12 Mar 2024	Unpatched	MEDIUM	<a href="#">Info</a> <a href="#">Print</a> <a href="#">Share</a>
<input type="checkbox"/> Information Exposure in /systemstate.php demo.example.com	Information Exposure CWE-200	25 Mar 2024	Unpatched	LOW	<a href="#">Info</a> <a href="#">Print</a> <a href="#">Share</a>
<input type="checkbox"/> Misconfigured Content Security Policy (CSP) demo.example.com	Security Warning	23 Mar 2024	Unpatched	WARNING	<a href="#">Info</a> <a href="#">Print</a> <a href="#">Share</a>
<input type="checkbox"/> Path Traversal in /version/files/ demo.example.com	Path Traversal CWE-22	12 Mar 2024	Unpatched	MEDIUM	<a href="#">Info</a> <a href="#">Print</a> <a href="#">Share</a>
<input type="checkbox"/> RCE via Server-Side Request Forgery (SSRF) in /items... demo.example.com	Server-Side Request Forgery CWE-918	25 Mar 2024	Unpatched	CRITICAL	<a href="#">Info</a> <a href="#">Print</a> <a href="#">Share</a>
<input type="checkbox"/> Misconfigured TLS Encryption demo.example.com	Security Warning	23 Mar 2024	Unpatched	WARNING	<a href="#">Info</a> <a href="#">Print</a> <a href="#">Share</a>
<input type="checkbox"/> Path Traversal in /sendfile/ demo.example.com	Path Traversal CWE-22	12 Mar 2024	Unpatched	MEDIUM	<a href="#">Info</a> <a href="#">Print</a> <a href="#">Share</a>

+ CREATE NEW PROJECT | Discovery 5 | Neuron 2 | Neuron Mobile 1 | On-Demand 1 | MobileSuite 2 | Continuous 1

## ImmuniWeb® Continuous

- 1 Configure Assessment
- 2 Confirm Ownership
- 3 Confirm Activation
- 4 Get Dashboard Access

Application URL:  ?

Project Name:  ?

Show Advanced Assessment Options

Show Vulnerability Data Export Options

Please make sure that during the assessment your website will be accessible from our subnets: 64.15.129.96/27, 70.38.27.240/28, 72.55.136.144/28, 72.55.136.192/28, 108.163.142.208/28, 192.175.111.224/27 and 208.52.182.12/32. ?

I have read, understood, and agreed to the Terms of Service & Privacy \*

[ImmuniWeb Continuous User Manual](#)

**Continue**

# Efficient. Simple. Cost-Effective.

We continuously monitor and test your web applications and APIs for security vulnerabilities, their exploitability and subsequent data exfiltration by using most relevant TTPs (tactics, techniques and procedures) from MITRE's ATT&CK matrix. Once a security flaw is confirmed, you will be immediately alerted by email, SMS or phone call.

For all customers of continuous breach and attack simulation, we offer a contractual zero false positives SLA and money-back guarantee: if there is a single false positive on your breach and attack simulation dashboard, you get the money back. Our award-winning technology and experienced security experts detect SANS Top 25 and OWASP Top 10 vulnerabilities, including the most sophisticated ones that may require chained, or otherwise untrivial, exploitation.





















Leverage our integrations with the leading WAF providers for instant virtual patching of the discovered vulnerabilities. Request to re-test any finding with one click. Ask our security analysts your questions about exploitation or remediation of the findings at no additional cost around the clock. Get a customizable live dashboard with the findings, download vulnerabilities in a PDF or XLS file, or use our DevSecOps integrations to export the continuous breach and attack simulation data into your bug tracker or SIEM.

# Trusted by 1,000+ Global Customers



# Looking for Something Else?

Explore 20 use cases we have for you

-  API Penetration Testing
-  Continuous Automated Red Teaming
-  Continuous Penetration Testing
-  Phishing Websites Takedown
-  API Security Scanning
-  Mobile Penetration Testing
-  Cyber Threat Intelligence
-  Red Teaming Exercise
-  Attack Surface Management
-  Mobile Security Scanning
-  Cybersecurity Compliance
-  Third-Party Risk Management
-  Cloud Penetration Testing
-  Network Security Assessment
-  Dark Web Monitoring
-  Web Penetration Testing
-  Cloud Security Posture Management
-  Continuous Breach and Attack Simulation
-  Digital Brand Protection
-  Web Security Scanning





[www.immuniweb.com](http://www.immuniweb.com)



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



One Platform. All Needs.