



# **Red Teaming Exercise**

Conduct highly customizable Red Teaming exercises with <u>ImmuniWeb<sup>®</sup> On-Demand</u> web application penetration testing offering







#### www.immuniweb.com

Copyright © 2024 ImmuniWeb SA

### Why Investing in Red Teaming Exercise



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

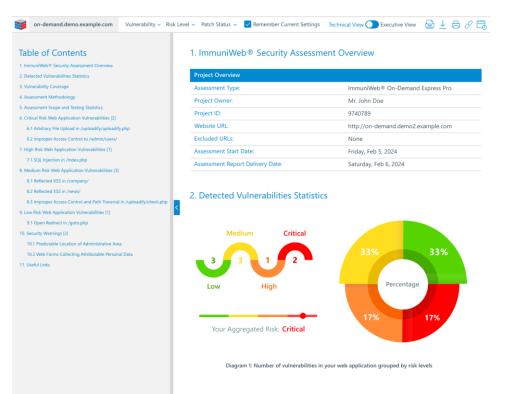
## 100+

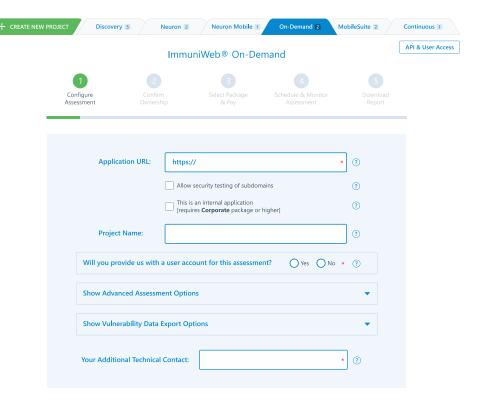
countries have laws imposing a personal liability on executives for a data breach

ImmuniWeb

Unlike penetration testing, which focuses on broader testing approach, Red Teaming Exercise takes on specific attack scenarios and areas, mimicking the tactics of real attackers. This can reveal unexpected vulnerabilities in your security posture, including weaknesses in policies, procedures, and human behavior. Red Teaming goes beyond identifying vulnerabilities. It tests your organization's ability to detect, contain, and respond to a simulated attack. This allows you to identify gaps in your incident response plan and make necessary improvements before a real attack occurs.

### Red Teaming Exercise with ImmuniWeb<sup>®</sup> On-Demand





### Efficient. Simple. Cost-Effective.

The Red Teaming exercise is tailored for your cybersecurity strategy and company- or industry-specific cyber threat landscape. When creating your Red Teaming project, just indicate the attack scenarios, specific cyber threats or known cyber threat actors whose specific behavior or intrusion tactics you wish to simulate. You may attach a detailed scenario or just briefly indicate key attack vectors and methods you wish us to launch against your web systems. The Red Teaming exercise is available around the clock 365 days a year.

Our cybersecurity analysts and experienced penetration testers will carefully go through the attack plan and get back to you in case of questions or suggestions on how to expand it. The Red Teaming report will elaborate the hacking tactics, techniques and procedures (TTP) and the obtained results equipped with a threat-aware risk scoring and detailed remediation guidelines for your software developers and DevOps engineers. May you have any questions or need assistance, our team remain at your disposal 24/7 during the Red Teaming exercise at no additional cost.

The Red Teaming exercise is provided with a contractual zero false positives SLA and is equipped with unlimited patch verification assessments, so your software developers can verify that all security flaws have been properly fixed. The Red Teaming exercise report is available on a user-friendly dashboard, can be downloaded as a PDF file, or simply exported into your SIEM or other internal systems thanks to our turnkey DevSecOps integrations. One-click virtual patching is also available for the leading WAF vendors.

Trusted by 1,000+ Global Customers





Paytweak

haymarket®







## Looking for Something Else?

Explore 20 use cases we have for you



**API** Penetration Testing



**API Security** Scanning



**Attack Surface** Management



**Cloud Penetration** Testing



**Cloud Security Posture** Management



20

</>>

Ģ

**Continuous Automated** 



**Mobile Security** Scanning







Cyber Threat 000

Intelligence



Compliance



**Digital Brand** Protection





2	Third-Party Risk
J	Management

gement

Web Penetration  $\langle \rangle$ Testing





#### www.immuniweb.com



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



One Platform. All Needs.