

ImmuniWeb[®]
AI for Application Security



Red Teaming Exercise

Conduct highly customizable Red Teaming exercises with [ImmuniWeb[®] On-Demand](#) web application penetration testing offering



www.immuniweb.com

Copyright © 2024 ImmuniWeb SA

Why Investing in Red Teaming Exercise

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

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® On-Demand

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

Table of Contents

- 1. ImmuniWeb® Security Assessment Overview
- 2. Detected Vulnerabilities Statistics
- 3. Vulnerability Coverage
- 4. Assessment Methodology
- 5. Assessment Scope and Testing Statistics
- 6. Critical Risk Web Application Vulnerabilities [2]
 - 6.1 Arbitrary File Upload in /uploadify/uploadify.php
 - 6.2 Improper Access Control to /admin/users/
- 7. High Risk Web Application Vulnerabilities [1]
 - 7.1 SQL Injection in /index.php
- 8. Medium Risk Web Application Vulnerabilities [3]
 - 8.1 Reflected XSS in /company/
 - 8.2 Reflected XSS in /news/
 - 8.3 Improper Access Control and Path Traversal in /uploadify/check.php
- 9. Low Risk Web Application Vulnerabilities [1]
 - 9.1 Open Redirect in /goto.php
- 10. Security Warnings [2]
 - 10.1 Predictable Location of Administrative Area
 - 10.2 Web Forms Collecting Attributable Personal Data
- 11. Useful Links

1. ImmuniWeb® Security Assessment Overview

Project Overview	
Assessment Type:	ImmuniWeb® On-Demand Express Pro
Project Owner:	Mr. John Doe
Project ID:	9740789
Website URL:	http://on-demand.demo2.example.com
Excluded URLs:	None
Assessment Start Date:	Friday, Feb 5, 2024
Assessment Report Delivery Date:	Saturday, Feb 6, 2024

2. Detected Vulnerabilities Statistics

Low: 3, Medium: 3, High: 1, Critical: 2

Risk Level	Count	Percentage
Low	3	33%
Medium	3	33%
High	1	17%
Critical	2	17%

Your Aggregated Risk: **Critical**

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

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

ImmuniWeb® On-Demand API & User Access

- 1 Configure Assessment
- 2 Confirm Ownership
- 3 Select Package & Pay
- 4 Schedule & Monitor Assessment
- 5 Download Report

Application URL: ?

Allow security testing of subdomains ?

This is an internal application (requires **Corporate** package or higher) ?

Project Name: ?

Will you provide us with a user account for this assessment? Yes No * ?

Show Advanced Assessment Options

Show Vulnerability Data Export Options

Your Additional Technical Contact: ?

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



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



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



One Platform. All Needs.