



Cloud Penetration Testing

Test your web applications, cloud-native apps or APIs hosted in AWS, Azure, GCP or other cloud service providers (CSP) with [ImmuniWeb® On-Demand](#) cloud penetration testing



www.immuniweb.com

Copyright © 2024 ImmuniWeb SA

Why Investing in Cloud Penetration Testing

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

Cloud Penetration Testing addresses security challenges by acting as a proactive shield for your cloud environment. This testing process mimics real-world attacks, uncovering vulnerabilities in your cloud infrastructure, applications, and services. Investing in Cloud Penetration Testing helps you leverage the benefits of the cloud while minimizing security risks, ultimately promoting a secure and trustworthy cloud environment.

Cloud Penetration Testing 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

Percentage: 33% (Low), 33% (Medium), 17% (High), 17% (Critical)

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.

Customize your cloud penetration testing scope and requirements, schedule the penetration testing date and get your cloud penetration test report. The cloud penetration testing is accessible around the clock 365 days a year.

Our cloud penetration testing is provided with a contractual zero SLA. If there false positive in your penetration testing report, you get the money back. Detect OWASP Top 10 and SANS Top 25 vulnerabilities, as well as OWASP API Top 10 weaknesses, CSP-specific security issues and misconfigurations. Uncover what can be done with cloud IMDS pivoting and privilege escalation attacks by exploiting excessive access permissions or default IAM policies in your cloud environment.





















Every cloud penetration test is provided with unlimited patch verification assessments so your cloud engineers can fix the security flaws and then validate, at no additional cost, that everything has been properly remediated. Download your cloud penetration test report from the interactive and user-friendly dashboard into a PDF file or just export the data directly into your SIEM via our DevSecOps and CI/CD integrations. Enjoy 24/7 access to our security analysts may you need any assistance during the cloud penetration test.

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.