ImmuniWeb® On-Demand

ImmuniWeb® On-Demand leverages our award-winning Machine Learning technology to accelerate and enhance web penetration testing. Every pentest is easily customizable and provided with a zero false-positives SLA. Unlimited patch verifications and 24/7 access to our security analysts are included into every project.

www.immuniweb.com

Gartner Cool Vendor™

IDC Innovator

AIFINTECH 100 2021

Quality. Simplicity. Speed.

Zero False-Positives SLA

Money-Back Guarantee for
a single false-positive

In-Depth Testing

Business logic testing, SANS Top 25,
PCI DSS & OWASP coverage

Actionable Reporting

Tailored remediation guidelines
and 24/7 access to analysts

Rapid Delivery SLA

Guaranteed execution schedule
and report delivery

DevSecOps Native

One-click WAF virtual patching,
SDLC & CI/CD integration

1 Customize and schedule pentest in a few clicks

2 Get your pentest report and re-test at no cost

3 Receive your pentest compliance certificate

Actionable Report. Simple Remediation.

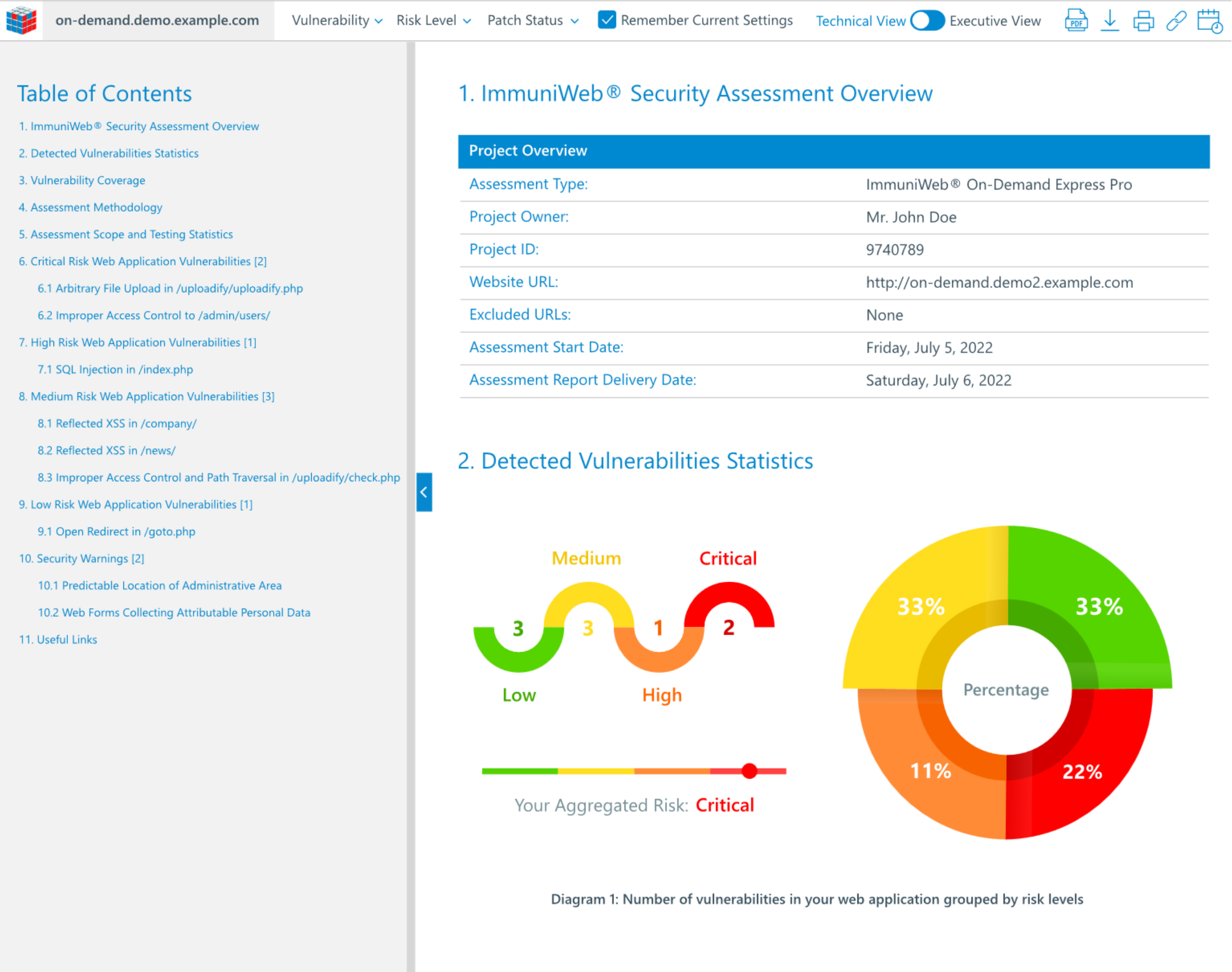


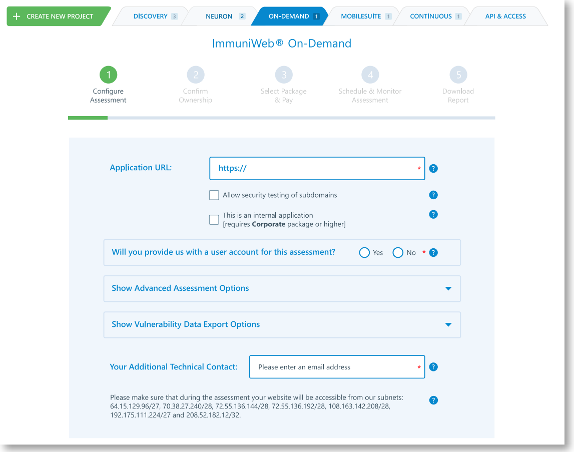
Table of Contents

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, July 5, 2022
Assessment Report Delivery Date:	Saturday, July 6, 2022

2. Detected Vulnerabilities Statistics

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



ImmuniWeb® On-Demand

Application URL: https:// *

□ Allow security testing of subdomains

□ This is an internal application
[requires **Corporate** package or higher]

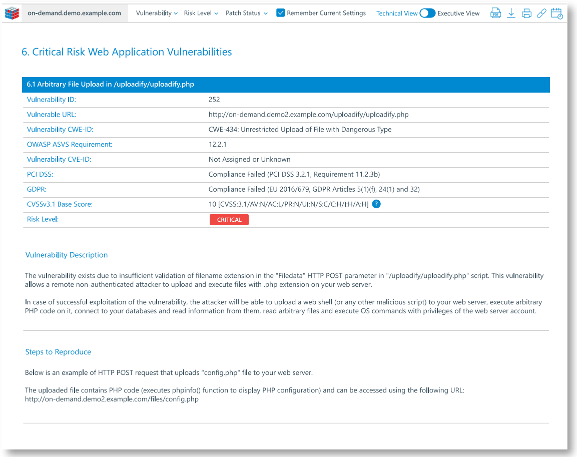
Will you provide us with a user account for this assessment? ○ Yes ○ No *

Show Advanced Assessment Options

Show Vulnerability Data Export Options

Your Additional Technical Contact: Please enter an email address *

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.



6. Critical Risk Web Application Vulnerabilities

6.1 Arbitrary File Upload in /uploadify/uploadify.php	
Vulnerability ID:	252
Vulnerable URL:	http://on-demand.demo2.example.com/uploadify/uploadify.php
Vulnerability CWE-ID:	CWE-434: Unrestricted Upload of File with Dangerous Type
OWASP ASVS Requirement:	12.2.1
Vulnerability CVE-ID:	Not Assigned or Unknown
PCI DSS:	Compliance Failed (PCI DSS 3.2.1, Requirement 11.2.3b)
GDPR:	Compliance Failed (EU 2016/679, GDPR Articles 5(1)(f), 24(1) and 32)
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 validation of filename extension in the "Filedata" HTTP POST parameter in "/uploadify/uploadify.php" script. This vulnerability allows a remote non-authenticated attacker to upload and execute files with .php extension on your web server.

In case of successful exploitation of the vulnerability, the attacker will be able to upload a web shell (or any other malicious script) to your web server, execute arbitrary PHP code on it, connect to your databases and read information from them, read arbitrary files and execute OS commands with privileges of the web server account.

Steps to Reproduce

Below is an example of HTTP POST request that uploads "config.php" file to your web server.

The uploaded file contains PHP code (executes phpinfo() function to display PHP configuration) and can be accessed using the following URL:
http://on-demand.demo2.example.com/files/config.php

Web Application Penetration Test for Any Need

Internal & External Web Apps

Virtual Appliance technology for internal applications testing

Cloud Security Testing

Check if attackers can pivot to other systems in your cloud

APIs and Web Services

API (REST/SOAP/GraphQL) security & privacy testing

Black & White Box

Authenticated (including MFA/MFA) or Black Box testing

Open Source Security

Software Composition Analysis (SCA) tests for 20,000+ known CVE-IDs

Red Teaming

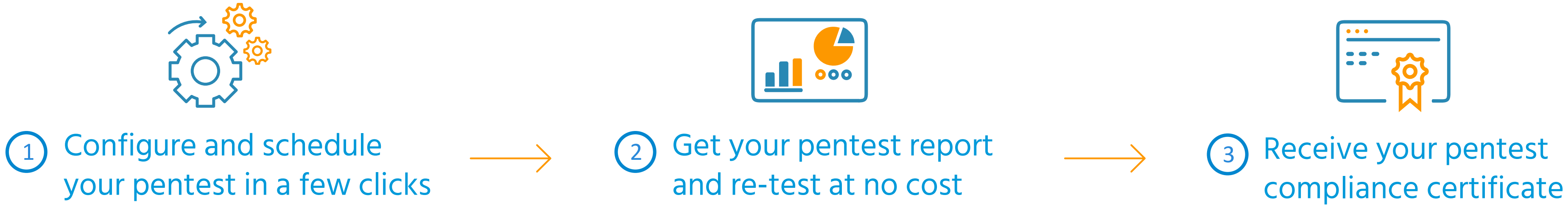
Breach and attack simulation per MITRE ATT&CK® Enterprise

Proven Methodology and Global Standards

- OWASP Web Security Testing Guide (WSTG)
- NIST SP 800-115 Technical Guide to Information Security Testing & Assessment
- PCI DSS Information Supplement: Penetration Testing Guidance
- MITRE ATT&CK® Matrix for Enterprise
- FedRAMP Penetration Test Guidance
- ISACA’s How to Audit GDPR

- OWASP Application Security Verification Standard (ASVS v4.0.2) Mapping
- Common Vulnerabilities and Exposures (CVE) Compatible
- Common Weakness Enumeration (CWE) Compatible
- Common Vulnerability Scoring System (CVSS v3.1)

ImmuniWeb® On-Demand Setup and Packages



1 Configure and schedule your pentest in a few clicks →

2 Get your pentest report and re-test at no cost →

3 Receive your pentest compliance certificate

ImmuniWeb® On-Demand	Corporate Pro	Corporate	Express Pro	Express
AI-Enabled Vulnerability Scanning	✓	✓	✓	✓
OWASP ASVS Testing	Level 3	Level 2	Level 1	Level 1
Manual Penetration Testing	5 days	3 days	1 day	1/2 day
Report Writing	8 hours	4 hours	2 hours	1 hour

Corporate Pro

Designed for one web application of large size and complexity, located on multiple subdomains or having several user roles.

Corporate

Designed for one web application of medium size and complexity, located on multiple subdomains or having a couple of user roles.

Express Pro

Designed for one web application of small size and complexity, located on one or two subdomains and having one user role.

Express

Designed for one web application of a very small size and complexity, located on one subdomain and having one simple user role.

ImmuniWeb® On-Demand Setup and Packages

Penetration Testing

- ✓ OSINT Search of Stolen Credentials
- ✓ Web Application Penetration Testing
  - SANS Top 25 Full Coverage
  - OWASP Top 10 Full Coverage
  - PCI DSS 6.5.1-6.5.10 Full Coverage
  - AI Augments Human Testing and Analysis
  - Machine Learning Accelerates Testing
  - Authenticated Testing (MFA / SSO)
  - REST/SOAP/GraphQL API Testing
  - Business Logic Testing
- ✓ Full Customization of Testing
- ✓ Rapid Delivery SLA Money back
- ✓ Privacy Review

Reporting

- ✓ Threat-Aware Risk Scoring
- ✓ Step-by-Step Instruction to Reproduce
- ✓ Web, PDF, JSON, XML and CSV Formats
- ✓ Tailored Remediation Guidelines
- ✓ PCI DSS and GDPR Compliances
- ✓ CVE, CWE and CVSS Scores
- ✓ OWASP ASVS Mapping
- ✓ Zero False-Positives SLA Money back

Remediation

- ✓ Unlimited Patch Verifications
- ✓ One-Click Virtual Patching via WAF
- ✓ 24/7 Access to Our Security Analysts
- ✓ DevSecOps & CI/CD Tools Integration
- ✓ Multirole RBAC Dashboard with 2FA
- ✓ Penetration Test Certificate

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 How many URLs and domains can I include into one package?

A There is no hard limit on the number of URLs or domains per package. All targets should, however, belong to the same business application. For example, an e-commerce platform may be located across several (sub)domains, APIs or third-party managed web services. They can normally all be included into one package. If you also wish to test your e-banking system, you will need a second package.

Q How can I customize my testing and reporting requirements?

A At the first step of project creation, you can easily configure special requirements for penetration testing or reporting. For example, you can select authenticated (White Box) testing with 2FA/SSO, exclude testing for some specific vulnerabilities (e.g. self-XSS) or areas of the web application, request to spend more time on cloud pivoting or container escaping if your web application is hosted in a cloud environment. All pentesting reports by default contain PCI DSS and GDPR sections.

Q What is the difference between the packages?

A Packages (from right to left) include gradually more human time and other resources that will be allocated for the penetration test. Generally, the bigger your scope is, the bigger package you need to comprehensively test your web application for all know web application vulnerabilities and attack vectors. Please reach out to us for a quote tailored for your specific needs and scope.

Q Can you test my applications in Microsoft Azure, AWS or GCP?

A Yes, we can test your web applications, cloud-native apps, microservices or APIs hosted in AWS, Azure, GCP and any other public cloud service providers. Aside from detecting OWASP Top 10, OWASP API Top 10 and SANS Top 25 vulnerabilities, we also detect cloud-specific misconfigurations and try cloud pivoting and privilege escalation attacks by exploiting excessive access permissions, IMDS flaws or default IAM policies in your cloud environment.

Q How are you different from other penetration testing companies?

A ImmuniWeb® On-Demand leverages our award-winning Machine Learning technology for acceleration and intelligent automation of laborious and time-consuming testing tasks and processes, eventually saving a considerable amount of human time on our side. Eventually, compared to traditional penetration testing, you may expect to get your penetration testing report much faster and to get higher vulnerability detection rate, as our security experts will spend their valuable time to meticulously reverse engineer your application and try the most sophisticated attack vectors instead of wasting time on routine or automatable security checks.

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

JET BRAINS

PivotalTracker

Bugzilla

ROHDE&SCHWARZ

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

pwc

softwareONE®

BDO

imperva

FORTINET®

ITU

Qualys

f5®

GLOBAL CYBER ALLIANCE™

Barracuda®

CyberPeace Institute

[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.

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

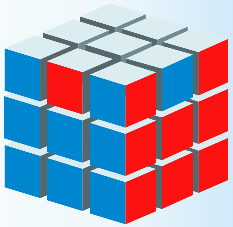
Brazil LGPD

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.