ImmuniWeb® On-Demand Express | Security Assessment Report

PDF is a short version of the dashboard. Full data and interactive features are available on the dashboard.

1. ImmuniWeb® Security Assessment Overview

Project Overview	
Assessment Type:	ImmuniWeb® On-Demand Express
Project Owner:	Mr. Zeke Gabrielse
Project ID:	1083794
Website URL:	https://app.keygen.sh
Additional Application URLs:	https://api.keygen.sh https://dist.keygen.sh https://keygen.sh
Excluded URLs:	None
Login:	demo+immuniweb@keygen.dev
Password:	U**********3
Login URL:	
Additional Information:	Docs: https://keygen.sh/docs/api/
Assessment Start Date:	Wednesday, June 30, 2021
Assessment Report Delivery Date:	Thursday, July 1, 2021

Suggested Next Steps

- Address the reported security warnings.
- Run free patch verification to ensure that all of the detected security issues are properly fixed.
- Perform another penetration test after the next major update of your web application (a larger ImmuniWeb package is recommended for the defined application scope).

2. Detected Vulnerabilities Statistics

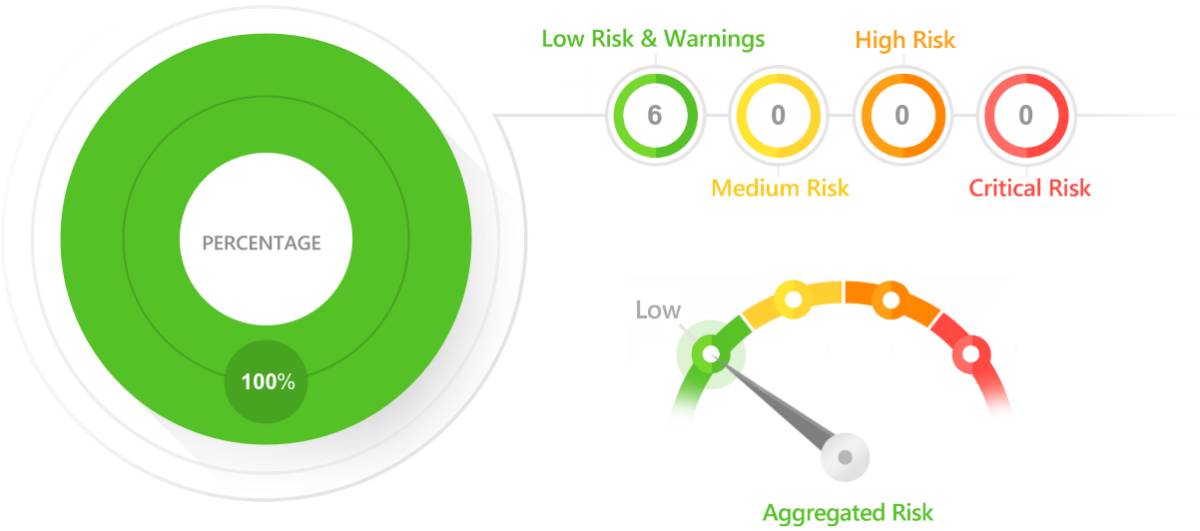

Diagram 1: Number of vulnerabilities in your web application grouped by risk levels

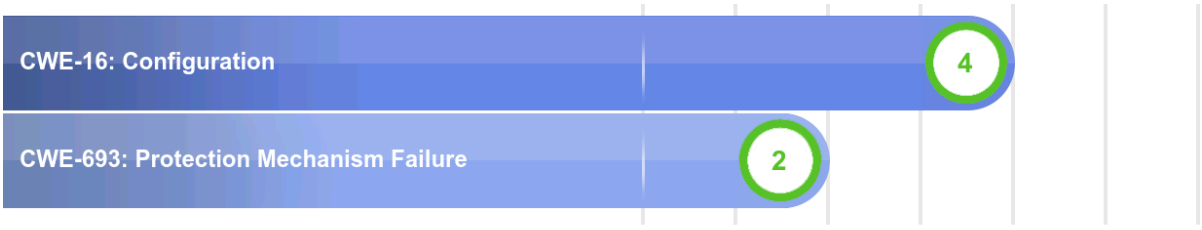

Diagram 2: Vulnerabilities and weaknesses in your web application grouped by the CWE classification

3. Vulnerability Coverage

During the security assessment, your web application was tested for the following weaknesses and vulnerabilities:

4. Assessment Methodology

During the security assessment, your web application was tested following the OWASP Web Security Testing Guide (WSTG) guidelines:

- ✔ Information Gathering (OTG-INFO)

Information Gathering	Test Name	Manual Testing	AI-enhanced Automated Testing
OTG-INFO-001	Conduct Search Engine Discovery and Reconnaissance for Information Leakage	Yes	Yes
OTG-INFO-002	Fingerprint Web Server	No	Yes
OTG-INFO-003	Review Webserver Metafiles for Information Leakage	Yes	No
OTG-INFO-004	Enumerate Applications on Webserver	No	Yes
OTG-INFO-005	Review Webpage Comments and Metadata for Information Leakage	Yes	Yes
OTG-INFO-006	Identify application entry points	Yes	No
OTG-INFO-007	Map execution paths through application	No	Yes
OTG-INFO-008	Fingerprint Web Application Framework	Yes	Yes
OTG-INFO-009	Fingerprint Web Application	Yes	Yes
OTG-INFO-010	Map Application Architecture	No	Yes

- ✔ Configuration and Deploy Management Testing (OTG-CONFIG)
- ✔ Identity Management Testing (OTG-IDENT)
- ✔ Authentication Testing (OTG-AUTHN)
- ✔ Authorization Testing (OTG-AUTHZ)
- ✔ Session Management Testing (OTG-SESS)
- ✔ Data Validation Testing (OTG-INPVAL)
- ✔ Error Handling (OTG-ERR)
- ✔ Cryptography (OTG-CRYPST)
- ✔ Business Logic Testing (OTG-BUSLOGIC)
- ✔ Client Side Testing (OTG-CLIENT)

5. Assessment Scope and Testing Statistics

app.keygen.sh	
Outgoing Traffic	270.9 MB sent
Incoming Traffic	13.5 GB received
HTTP Requests	8,535,231 sent
Dynamic URLs	671 found, 671 tested
HTTP Parameters	7 found, 7 tested
Cookies	3 found, 3 tested
Vulnerabilities	0 vulnerabilities 2 warnings
dist.keygen.sh	
Outgoing Traffic	1.6 MB sent
Incoming Traffic	117.5 MB received
HTTP Requests	1,181,607 sent
Dynamic URLs	2 found, 2 tested
HTTP Parameters	2 found, 2 tested
Cookies	0 found, 0 tested
Vulnerabilities	0 vulnerabilities 1 warning
api.keygen.sh	
Outgoing Traffic	20.4 MB sent
Incoming Traffic	76.2 MB received
HTTP Requests	229,891 sent
Dynamic URLs	22 found, 22 tested
HTTP Parameters	12 found, 12 tested
Cookies	0 found, 0 tested
Vulnerabilities	0 vulnerabilities 1 warning
keygen.sh	
Outgoing Traffic	29.3 MB sent
Incoming Traffic	2.5 GB received
HTTP Requests	111,006 sent
Dynamic URLs	89 found, 89 tested
HTTP Parameters	9 found, 9 tested
Cookies	0 found, 0 tested
Vulnerabilities	0 vulnerabilities 2 warnings

6. Critical Risk Web Application Vulnerabilities

ImmuniWeb® security assessment did not detect any critical-risk security vulnerabilities in your web application.

7. High Risk Web Application Vulnerabilities

ImmuniWeb® security assessment did not detect any high-risk security vulnerabilities in your web application.

8. Medium Risk Web Application Vulnerabilities

ImmuniWeb® security assessment did not detect any medium-risk security vulnerabilities in your web application.

9. Low Risk Web Application Vulnerabilities

ImmuniWeb® security assessment did not detect any low-risk security vulnerabilities in your web application.

10. Security Warnings

api.keygen.sh

10.1 Detected Insecure SSL/TLS Implementation in api.keygen.sh	
Vulnerability CWE-ID:	CWE-16: Configuration
OWASP ASVS Requirement:	14.1.3
Description: Your web server is configured to support TLSv1.0 protocol with known security weaknesses. A remote attacker with ability to intercept traffic can perform a Man-in-the-Middle (MitM) attack.	
Remediation: The following TLS protocols are considered secure: TLSv1.2 or TLSv1.3. Please, refer to the detailed TLS test results: https://www.immuniweb.com/ssl/?test=api.keygen.sh	

app.keygen.sh

10.2 Detected Insecure SSL/TLS Implementation in app.keygen.sh	
Vulnerability CWE-ID:	CWE-16: Configuration
OWASP ASVS Requirement:	14.1.3
Description: Your web server is configured to support TLSv1.0 protocol with known security weaknesses. A remote attacker with ability to intercept traffic can perform a Man-in-the-Middle (MitM) attack.	
Remediation: The following TLS protocols are considered secure: TLSv1.2 or TLSv1.3. Please, refer to the detailed TLS test results: https://www.immuniweb.com/ssl/?test=app.keygen.sh	

dist.keygen.sh

10.3 Detected Insecure SSL/TLS Implementation in dist.keygen.sh	
Vulnerability CWE-ID:	CWE-16: Configuration
OWASP ASVS Requirement:	14.1.3
Description: Your web server is configured to support TLSv1.0 protocol with known security weaknesses. A remote attacker with ability to intercept traffic can perform a Man-in-the-Middle (MitM) attack.	
Remediation: The following TLS protocols are considered secure: TLSv1.2 or TLSv1.3. Please, refer to the detailed TLS test results:	

https://www.immuniweb.com/ssl/?test=dist.keygen.sh

keygen.sh

10.4 Detected Insecure SSL/TLS Implementation in keygen.sh	
Vulnerability CWE-ID:	CWE-16: Configuration
OWASP ASVS Requirement:	14.1.3

Description:

Your web server is configured to support TLSv1.0 protocol with known security weaknesses. A remote attacker with ability to intercept traffic can perform a Man-in-the-Middle (MitM) attack.

Remediation:

The following TLS protocols are considered secure: TLSv1.2 or TLSv1.3.

Please, refer to the detailed TLS test results:

https://www.immuniweb.com/ssl/?test=keygen.sh

app.keygen.sh

10.5 Insecure Value for the Content-Security-Policy Header in app.keygen.sh	
Vulnerability CWE-ID:	CWE-693: Protection Mechanism Failure
OWASP ASVS Requirement:	14.1.3

Description:

Your web server configuration lacks the recommended configuration for the Content-Security-Policy header:

- The header was not sent by the server.

Remediation:

Configure your server to enable the Content-Security-Policy HTTP header.

keygen.sh

10.6 Insecure Value for the Content-Security-Policy Header in keygen.sh	
Vulnerability CWE-ID:	CWE-693: Protection Mechanism Failure
OWASP ASVS Requirement:	14.1.3

Description:

Your web server configuration lacks the recommended configuration for the Content-Security-Policy header:

- The header was not sent by the server.

Remediation:

Configure your server to enable the Content-Security-Policy HTTP header.

11. Useful Links

- Customer Support
  https://portal.immuniweb.com/client/support/
- Compliance and Data Protection Regulations
  https://www.immuniweb.com/compliance/
- OWASP Top 10 Vulnerabilities
  https://www.immuniweb.com/owasp-top-10/
- CWE Vulnerability Glossary
  https://www.immuniweb.com/vulnerability/
- Common Vulnerabilities and Exposures (CVE)
  http://cve.mitre.org
- Common Weakness Enumeration (CWE)
  http://cwe.mitre.org
- Terms of Service and Privacy
  https://portal.immuniweb.com/client/ToS