Summary of dev.[redacted].app [Desktop version] Website Security Test

Provided "as is" without any warranty of any kind.

dev.[redacted].app was tested 3 times during the last 12 months.

Your final score:

Tested on:	Aug 11th, 2025 00:06:06 GMT+0
Server IP:	18.134.147.218
Reverse DNS:	ec2-18-134-147-218.eu-west-2.compute.amazonaws.com
Location:	London
Client:	Desktop version

A | B | C | F

F

Software Security Test	Compliance Test	Compliance Test	Content Security Policy Test
5 ISSUES FOUND	2 ISSUES FOUND	2 ISSUES FOUND	MISSING

Headers Security Test

5 ISSUES FOUND

Full Test Results: https://www.immuniweb.com/websec/dev[redacted]app/tmfwFZoS/

Web Server Security Test

HTTP RESPONSE

200 OK

HTTP VERSIONS

HTTP/1.0 HTTP/1.1 HTTP/2

NPN

N/A

ALPN

N/A

CONTENT ENCODING

None

SERVER SIGNATURE

Apache/2.4.6 CentOS OpenSSL/1.0.2k-fips PHP/7.0.33

WAF

No WAF detected

LOCATION

Massachusetts Institute of Technology

HTTP METHODS ENABLED

✔ GET ✔ POST ✔ HEAD ✔ OPTIONS ✔ DELETE ✔ PUT ✔ TRACE ✔ TRACK ✔ CUSTOM

Web Software Security Test

Web Software Found	Web Software Outdated	Web Software Vulnerabilities
8	7	16

Fingerprinted CMS & Vulnerabilities

No CMS were fingerprinted on the website.	Information

Fingerprinted CMS Components & Vulnerabilities

jQuery 3.3.1

The fingerprinted component version is outdated and vulnerable to publicly known vulnerabilities. Urgently update to the most recent version **3.7.1**.

CVSSv4.0 Score	CVE-ID	Vulnerability Type
6.9 Medium	CVE-2019-11358	CWE-1321 - Prototype pollution
5.1 Medium	CVE-2020-11022	CWE-79 - Cross-site scripting
2.1 Low	CVE-2020-11023	CWE-79 - Cross-site scripting

jQuery UI 1.12.1

The fingerprinted component version is outdated and vulnerable to publicly known vulnerabilities. Urgently update to the most recent version **1.14.1**.

CVSSv4.0 Score	CVE-ID	Vulnerability Type
5.1 Medium	CVE-2021-41182	CWE-79 - Cross-site scripting
5.1 Medium	CVE-2021-41184	CWE-79 - Cross-site scripting
5.1 Medium	CVE-2021-41183	CWE-79 - Cross-site scripting
2.1 Low	CVE-2022-31160	CWE-79 - Cross-site scripting

Bootstrap 3.3.7

The fingerprinted component version is outdated and vulnerable to publicly known vulnerabilities. Urgently update to the most recent version **5.3.7**.

CVSSv4.0 Score	CVE-ID	Vulnerability Type
5.1 Medium	CVE-2024-6485	CWE-79 - Cross-site scripting
5.1 Medium	CVE-2024-6484	CWE-79 - Cross-site scripting
5.1 Medium	CVE-2019-8331	CWE-79 - Cross-site scripting
5.1 Medium	CVE-2016-10735	CWE-79 - Cross-site scripting
5.1 Medium	CVE-2018-20677	CWE-79 - Cross-site scripting
5.1 Medium	CVE-2018-20676	CWE-79 - Cross-site scripting
5.1 Medium	CVE-2018-14040	CWE-79 - Cross-site scripting
5.1 Medium	CVE-2018-14042	CWE-79 - Cross-site scripting
5.1 Medium	CVE-2018-14041	CWE-79 - Cross-site scripting

Lit-element 4.1.1

The component is outdated. No known security vulnerabilities found.

Lit-html 3.2.1

The component is outdated. No known security vulnerabilities found.

Owlcarousel2 2.0.0-beta-1

The component is outdated. No known security vulnerabilities found. Update to the most recent version **2.3.4**.

Gmaps 0.4.8

The component is outdated. No known security vulnerabilities found. Update to the most recent version **0.4.25**.

Jquery-timepicker-addon 1.6.3

The fingerprinted component version is up2date, no security issues were found.

GDPR Compliance Test

If the website processes or stores personal data of the EU residents, the following requirements of EU GDPR may apply:

PRIVACY POLICY

Privacy Policy was found on the website.	Good configuration

WEBSITE SECURITY

Website CMS or its components are outdated and contain publicly known security vulnerabilities.	Misconfiguration or weakness

TLS ENCRYPTION

HTTPS encryption is present on the web server.	Good configuration

COOKIE PROTECTION

Cookies with personal or tracking information are sent without Secure flag.	Misconfiguration or weakness

COOKIE DISCLAIMER

Third-party cookies or cookies with tracking information are sent, cookie disclaimer was found on the website.	Good configuration

PCI DSS Compliance Test

If the website falls into a CDE (Cardholder Data Environment) scope, the following Requirements of PCI DSS may apply:

REQUIREMENT 6.2

Website CMS or its components seem to be outdated. Check for available updates.	Misconfiguration or weakness

REQUIREMENT 6.5

Fingerprinted website CMS or its components contain publicly known vulnerabilities (Ref. PCI DSS 6.5.1-6.5.10).	Misconfiguration or weakness

REQUIREMENT 6.6

No WAF was detected on the website. Implement a WAF to protect the website against common web attacks.	Misconfiguration or weakness

HTTP Headers Security

Some HTTP headers related to security and privacy are missing or misconfigured.	Misconfiguration or weakness

MISSING REQUIRED HTTP HEADERS

Strict-Transport-Security (HSTS) | X-Frame-Options | X-Content-Type-Options

MISSING OPTIONAL HTTP HEADERS

Access-Control-Allow-Origin | Permissions-Policy

SERVER

The web server discloses its version, potentially facilitating further attacks against it.	Misconfiguration or weakness

Server

Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.0.33

X-POWERED-BY

The web server discloses its version, potentially facilitating further attacks against it.	Misconfiguration or weakness

X-Powered-By

X-Powered-By: PHP/7.0.33

CACHE-CONTROL

The header is properly set.	Good configuration

Cache-Control

Cache-Control: no-cache, no-store, must-revalidate

Content Security Policy Test

CONTENT-SECURITY-POLICY (CSP)

The header was not sent by the server.	Misconfiguration or weakness

CONTENT-SECURITY-POLICY-REPORT-ONLY

The header was not sent by the server.	Information

Cookies Privacy and Security Analysis

Some cookies have missing secure flags or attributes.	Misconfiguration or weakness

COOKIE: SESSION

The cookie is missing Secure, HttpOnly and SameSite flag. Make sure it does not store sensitive information.	Misconfiguration or weakness

Raw HTTP Header

Set-Cookie: session=2qtucnabi6fsmv206v7ht4j3b2; path=/

Directives

Name	Value	Description
path	/	Sets the path of the application where the cookie should be sent.

Need More? Upgrade to ImmuniWeb® AI Platform

Get remediation advice and ensure compliance with ImmuniWeb AI Platform:

FREE DEMO

ASK A QUESTION

Full Test Results: https://www.immuniweb.com/websec/dev.[redacted]pp/tmfwFZoS/

External Content Privacy and Security Analysis

SUBRESOURCE INTEGRITY

Subresource Integrity (SRI) is a security feature that allows browsers to verify that fetched resources (scripts and stylesheets) are delivered without unexpected alterations. The integrity of third-party resources is ensured by validating their cryptographic hashes.

SRI is correctly implemented for 0 out of 6 third-party JavaScripts and CSS files. Ensure that SRI is applied to all external JavaScripts and CSS files for complete security.	Information

EXTERNAL CONTENT

External web content (e.g. images, video, CSS or JavaScript) can improve website loading time. However, the external content can also put privacy of website visitors at risk given that some information about them is transmitted to the third parties operating the external resources, sometimes even without proper HTTPS encryption or user consent.

External HTTP Requests	Failed HTTP Requests
10	0

fonts.googleapis.com

https://fonts.googleapis.com/css?family=Roboto:100,300,400,500,700,900&subset=cyrillic,cyrillic-ext,greek,greek-ext,latin-ext,vietnamese	SRI

maps.google.com

https://maps.google.com/maps-api-v3/api/js/61/14/common.js	SRI
https://maps.google.com/maps-api-v3/api/js/61/14/places_impl.js	SRI
https://maps.google.com/maps-api-v3/api/js/61/14/controls.js	SRI

Full Test Results: https://www.immuniweb.com/websec/dev[redacted]app/tmfwFZoS/

https://maps.google.com/maps-api-v3/api/js/61/14/util.js SRI

https://maps.google.com/maps/api/js?key=AIzaSyAdPeaa1WEf9Ff8JisMuRaNgmDYQbzhOY8&sessiontoken=9a39bd2c-1d90-40b4-babc-9943bbfd4980&libraries=places,geometry SRI

maps.googleapis.com

https://maps.googleapis.com/maps/api/mapsjs/gen_204?csp_test=true

fonts.gstatic.com

https://fonts.gstatic.com/s/roboto/v48/KFO7CnqEu92Fr1ME7kSn66aGLdTylUAMa3yUBA.woff2

maps.gstatic.com

https://maps.gstatic.com/mapfiles/api-3/images/powered-by-google-on-white3.png

https://maps.gstatic.com/mapfiles/api-3/images/autocomplete-icons.png

The End of Report

Upgrade from Free Community Edition to ImmuniWeb® AI Platform