October 7, 2025

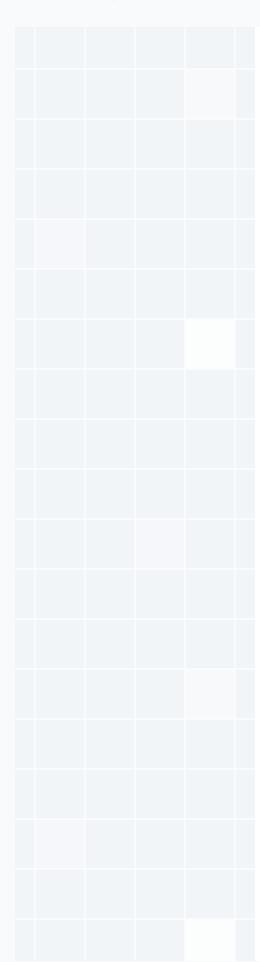
Vulnerability Scan Report

Prepared By

HostedScan Security



HostedScan Security Vulnerability Scan Report



Overview

1	Executive Summary	3
2	Trends	4
3	Vulnerabilities By Target	5
4	Passive Web Application Vulnerabilities	7
5	Glossary	11



1 Executive Summary

Vulnerability scans were conducted on select servers, networks, websites, and applications. This report contains the discovered potential vulnerabilities from these scans. Vulnerabilities have been classified by severity. Higher severity indicates a greater risk of a data breach, loss of integrity, or availability of the targets.

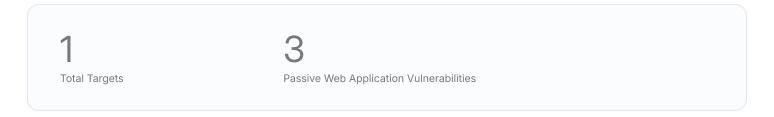
1.1 Total Vulnerabilities

Below are the total number of vulnerabilities found by severity. Critical vulnerabilities are the most severe and should be evaluated first. An accepted vulnerability is one which has been manually reviewed and classified as acceptable to not fix at this time, such as a false positive detection or an intentional part of the system's architecture.



1.2 Report Coverage

This report includes findings for **1 target** scanned. Each target is a single URL, IP address, or fully qualified domain name (FQDN).

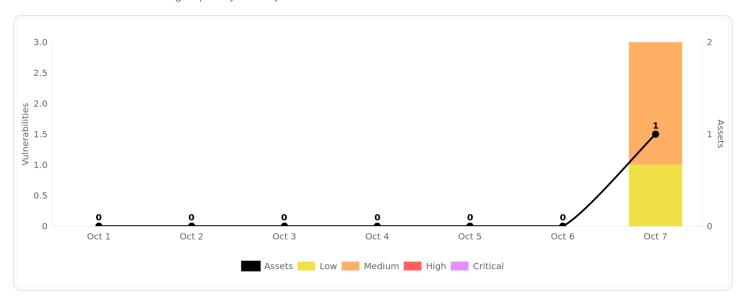


Vulnerability Scan Report

2 Trends

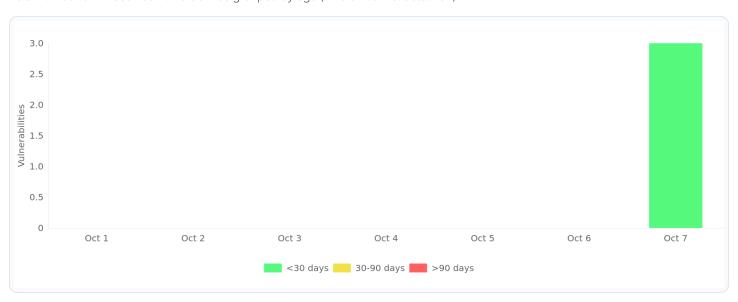
2.1 Open Risks

Total number of vulnerabilities grouped by severity level.



2.2 Exposure Window

Total number of unresolved vulnerabilities grouped by age (time since first detection).



Vulnerability Scan Report

3 Vulnerabilities By Target

This section contains the vulnerability findings for each scanned target. Prioritization should be given to the targets with the highest severity vulnerabilities. However, it is important to take into account the purpose of each system and consider the potential impact a breach or an outage would have for the particular target.

3.1 Targets Summary (1)

The number of potential vulnerabilities found for each target by severity.



3.2 Target Breakdowns

Details for the potential vulnerabilities found for each target by scan type.



https://taisen.pages.dev

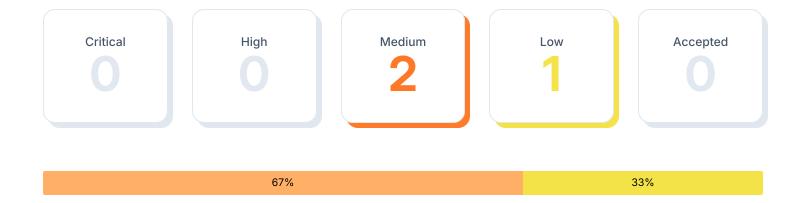
Total Risks 2 33% 67% Passive Web Application Vulnerabilities First Detected Last Detected Severity 0 days ago 0 days ago **Cross-Domain Misconfiguration** Medium 0 days ago Content Security Policy (CSP) Header Not Set Medium 0 days ago Cross-Domain JavaScript Source File 0 days ago 0 days ago Low Inclusion

4 Passive Web Application Vulnerabilities

The OWASP ZAP Passive Web Application scan crawls the pages of a website or web application. The passive scan inspects each page as well as the requests and responses sent between the server. The passive scan checks for vulnerabilities such as cross-domain misconfigurations, insecure cookies, vulnerable Javascript dependencies, and more.

4.1 Total Vulnerabilities

Total number of vulnerabilities found by severity.



4.2 Vulnerabilities Breakdown

Summary list of all detected vulnerabilities.

Title	Severity	Open	Accepted
Cross-Domain Misconfiguration	Medium	1	0
Content Security Policy (CSP) Header Not Set	Medium	1	0
Cross-Domain JavaScript Source File Inclusion	Low	1	0

4.3 Vulnerability Details

Detailed information about each potential vulnerability found by the scan.



Cross-Domain Misconfiguration

SEVERITY

AFFECTED TARGETS

LAST DETECTED

Medium

1 target

0 days ago

Description

Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.

Solution

Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance).

Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.

Instances (1 of 46)

uri: https://taisen.pages.dev/

method: GET

evidence: Access-Control-Allow-Origin: *

otherinfo: The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.

References

https://vulncat.fortify.com/en/detail?category=HTML5&subcategory=Overly%20Permissive%20CORS%20Policy

Vulnerable Target	First Detected	Last Detected
https://taisen.pages.dev	0 days ago	0 days ago



Content Security Policy (CSP) Header Not Set

SEVERITY

AFFECTED TARGETS

LAST DETECTED

Medium

1 target

0 days ago

Description

Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

Solution

Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.

Instances (1 of 26)

uri: https://taisen.pages.dev/ method: GET

References

https://developer.mozilla.org/en-US/docs/Web/HTTP/Guides/CSP

https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html

https://www.w3.org/TR/CSP/

https://w3c.github.io/webappsec-csp/

https://web.dev/articles/csp

https://caniuse.com/#feat=contentsecuritypolicy

https://content-security-policy.com/

Vulnerable Target	First Detected	Last Detected
https://taisen.pages.dev	0 days ago	0 days ago



Cross-Domain JavaScript Source File Inclusion

SEVERITY

AFFECTED TARGETS

LAST DETECTED

Low

1 target

0 days ago

Description

The page includes one or more script files from a third-party domain.

Solution

Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.

Instances (1 of 4)

uri: https://taisen.pages.dev/

method: GET

param: https://cse.google.com/cse.js?cx=178f66b21f928448b

evidence: <script async src="https://cse.google.com/cse.js?cx=178f66b21f928448b"></script>

Vulnerable Target	First Detected	Last Detected
https://taisen.pages.dev	0 days ago	0 days ago

Glossary Vulnerability Scan Report

5 Glossary

Accepted Vulnerability

An accepted vulnerability is one which has been manually reviewed and classified as acceptable to not fix at this time, such as a false positive scan result or an intentional part of the system's architecture.

Fully Qualified Domain Name (FQDN)

A fully qualified domain name is a complete domain name for a specific website or service on the internet. This includes not only the website or service name, but also the top-level domain name, such as .com, .org, .net, etc. For example, 'www.example.com' is an FQDN.

Passive Web Application Vulnerabilities

The OWASP ZAP Passive Web Application scan crawls the pages of a website or web application. The passive scan inspects each page as well as the requests and responses sent between the server. The passive scan checks for vulnerabilities such as cross-domain misconfigurations, insecure cookies, vulnerable Javascript dependencies, and more.

Vulnerability

A weakness in the computational logic (e.g., code) found in software and hardware components that, when exploited, results in a negative impact to confidentiality, integrity, or availability. Mitigation of the vulnerabilities in this context typically involves coding changes, but could also include specification changes or even specification deprecations (e.g., removal of affected protocols or functionality in their entirety).

Target

A target represents target is a single URL, IP address, or fully qualified domain name (FQDN) that was scanned.

Severity

Severity represents the estimated impact potential of a particular vulnerability. Severity is divided into 5 categories: Critical, High, Medium, Low and Accepted.

CVSS Score

The CVSS 3.0 score is a global standard for evaluating vulnerabilities with a 0 to 10 scale. CVSS maps to threat levels:

0.1 - 3.9 = Low

4.0 - 6.9 = Medium

7.0 - 8.9 = High

9.0 - 10.0 = Critical

EPSS Score

The EPSS score is the estimated probability that a given vulnerability will be exploited in the wild within the next 30 days, on a 0% to 100% scale.

This report was prepared using

HostedScan Security ®

For more information, visit hostedscan.com

Founded in Seattle, Washington in 2019, HostedScan, LLC. is dedicated to making continuous vulnerability scanning and risk management much more easily accessible to more businesses.



HostedScan, LLC.

2212 Queen Anne Ave N Suite #521 Seattle, WA 98109

Terms & Policies hello@hostedscan.com