

June 10, 2024

Vulnerability Scan Report

prepared by
HostedScan Security



Overview

1 Executive Summary	3
2 Vulnerabilities By Target	4
3 Passive Web Application Vulnerabilities	6
4 Glossary	10

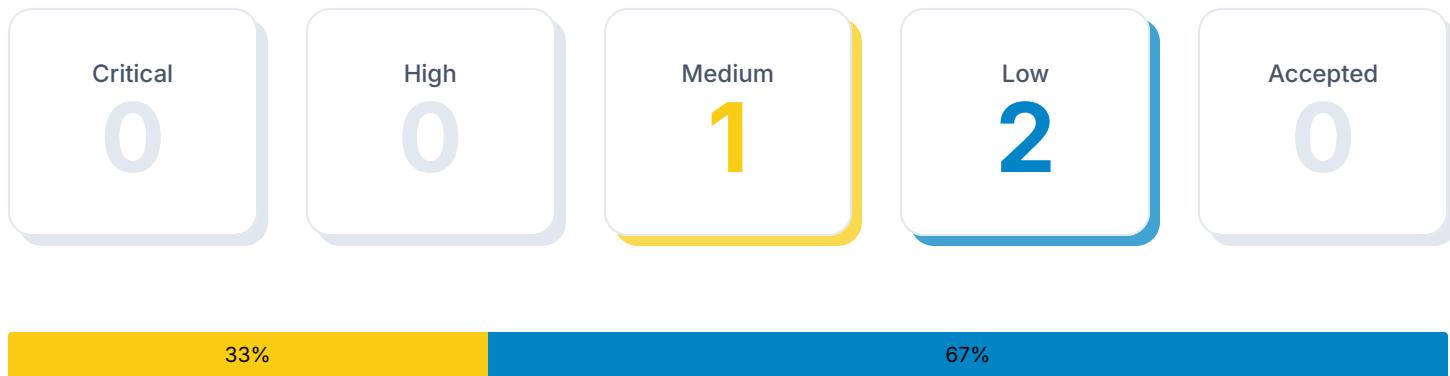


1 Executive Summary

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.

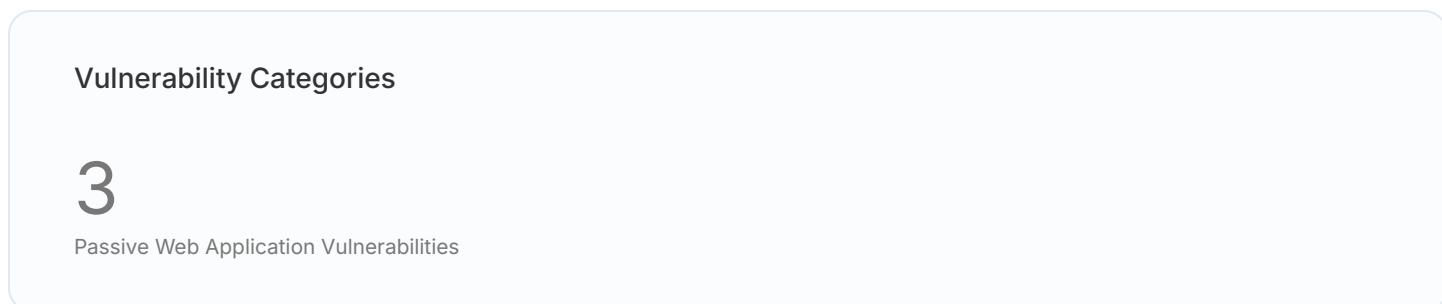
1.1 Total Vulnerabilities

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).

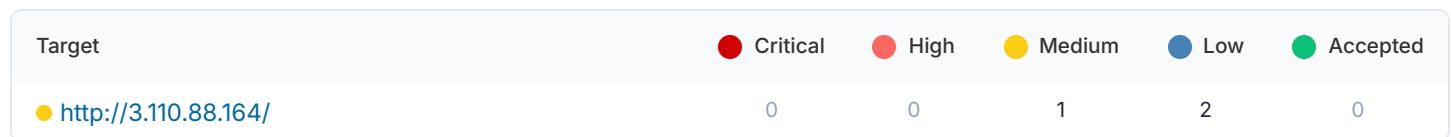


2 Vulnerabilities By Target

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.

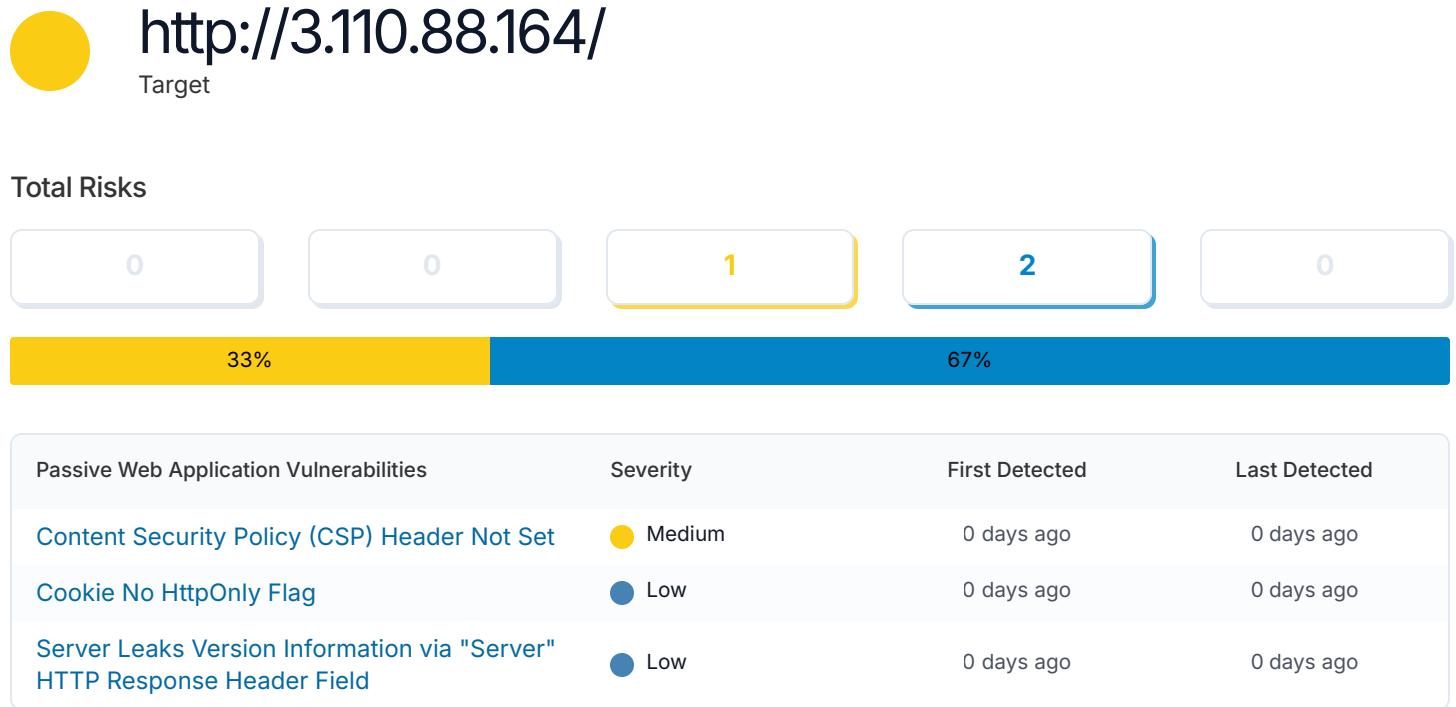
2.1 Targets Summary

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



2.2 Target Breakdowns

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

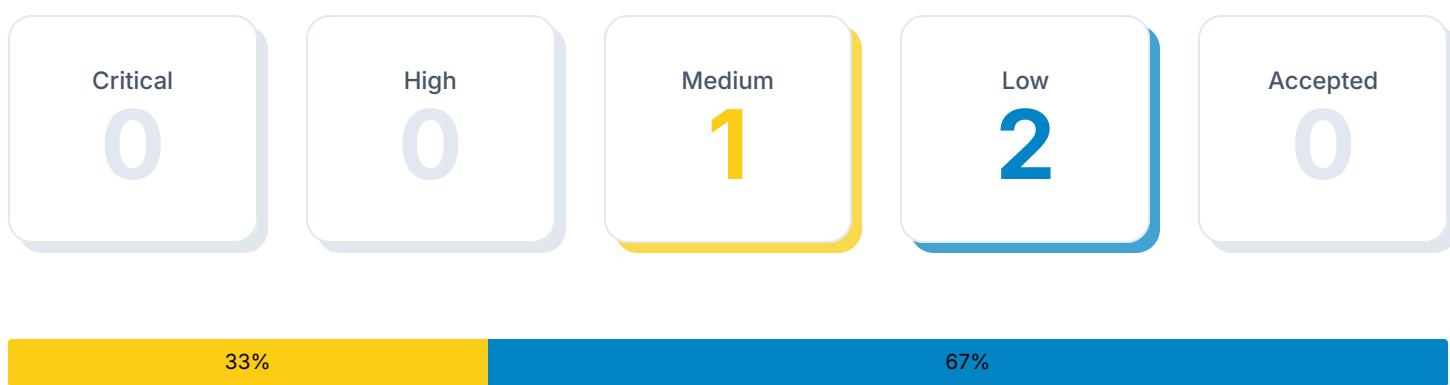


3 Passive Web Application Vulnerabilities

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.

3.1 Total Vulnerabilities

Total number of vulnerabilities found by severity.



3.2 Vulnerabilities Breakdown

Summary list of all detected vulnerabilities.

Title	Severity	Open	Accepted
Content Security Policy (CSP) Header Not Set	Medium	1	0
Cookie No HttpOnly Flag	Low	1	0
Server Leaks Version Information via "Server" HTTP Response Header Field	Low	1	0

3.3 Vulnerability Details

Detailed information about each potential vulnerability found by the scan.

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 4)

uri: <http://3.110.88.164/>
method: GET

References

https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy
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
http://3.110.88.164/	0 days ago	0 days ago

Cookie No HttpOnly Flag

SEVERITY	AFFECTED TARGETS	LAST DETECTED
Low	1 target	0 days ago

Description

A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.

Solution

Ensure that the HttpOnly flag is set for all cookies.

Instances (1 of 1)

uri: <http://3.110.88.164/login/>
method: GET
param: csrf token
evidence: Set-Cookie: csrf token

References

<https://owasp.org/www-community/HttpOnly>

Vulnerable Target	First Detected	Last Detected
http://3.110.88.164/	0 days ago	0 days ago

|||| Server Leaks Version Information via "Server" HTTP Response Header Field

SEVERITY	AFFECTED TARGETS	LAST DETECTED
Low	1 target	0 days ago

Description

The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.

Solution

Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.

Instances (1 of 4)

uri: <http://3.110.88.164/>

method: GET

evidence: WSGIServer/0.2 CPython/3.12.3

References

<https://httpd.apache.org/docs/current/mod/core.html#servertokens>

[https://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552\(v=pandp.10\)](https://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10))

<https://www.troyhunt.com/shhh-dont-let-your-response-headers/>

Vulnerable Target	First Detected	Last Detected
http://3.110.88.164/	0 days ago	0 days ago

4 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

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