

January 3, 2025

Vulnerability Scan Report

Prepared By

HostedScan Security



hostedscan.com

Overview

1	Executive Summary	3
2	Vulnerabilities By Target	4
3	Active Web Application Vulnerabilities	6
4	Glossary	8

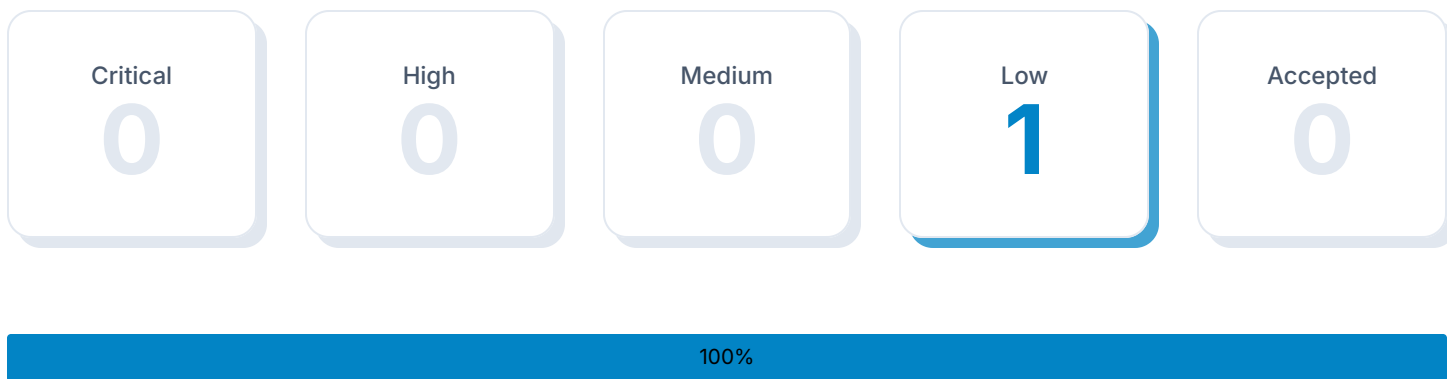


1 Executive Summary

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 Categories







1
Active Web Application Vulnerabilities

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.

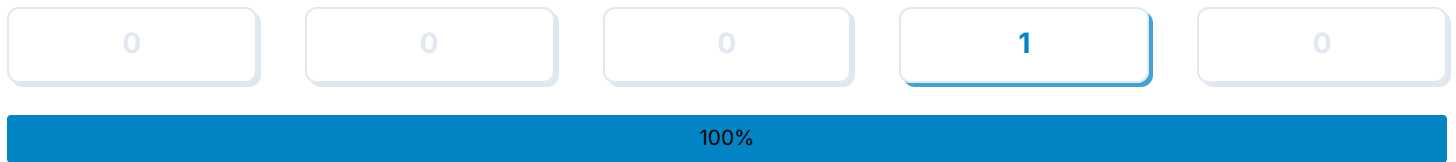
Target	 Critical	 High	 Medium	 Low	 Accepted
 files.liquidfiles.com	0	0	0	1	0

2.2 Target Breakdowns

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

files.liquidfiles.com

Total Risks



Active Web Application Vulnerabilities	Severity	First Detected	Last Detected
Private IP Disclosure	● Low	22 days ago	0 days ago

This low severity vulnerability exist on a default LiquidFiles system because it's not possible to get started if this gets hardened further. On a production system when a proper FQDN has been set, you can harden this further if you want. Please see: <https://docs.liquidfiles.com/security/hardening.html> for more information.

3 Active Web Application Vulnerabilities

The OWASP ZAP Active Web Application scan crawls the pages of a website or web application testing for vulnerabilities and configuration weaknesses. The active scan includes all of the passive scan tests and additionally makes requests and submits forms to actively test an application for more vulnerabilities. The active scan tests for vulnerabilities such as SQL injection, remote command execution, XSS, and more.

3.1 Total Vulnerabilities

Total number of vulnerabilities found by severity.



100%

3.2 Vulnerabilities Breakdown

Summary list of all detected vulnerabilities.

Title	Severity	Open	Accepted
Private IP Disclosure	● Low	1	0

This low severity vulnerability exist on a default LiquidFiles system because it's not possible to get started if this gets hardened further. On a production system when a proper FQDN has been set, you can harden this further if you want. Please see: <https://docs.liquidfiles.com/security/hardening.html> for more information.

3.3 Vulnerability Details

Detailed information about each potential vulnerability found by the scan.

Private IP Disclosure

SEVERITY	AFFECTED TARGETS	LAST DETECTED
Low	1 target	0 days ago

Description

A private IP (such as 10.x.x.x, 172.x.x.x, 192.168.x.x) or an Amazon EC2 private hostname (for example, ip-10-0-56-78) has been found in the HTTP response body. This information might be helpful for further attacks targeting internal systems.

Solution

Remove the private IP address from the HTTP response body. For comments, use JSP/ASP/PHP comment instead of HTML/JavaScript comment which can be seen by client browsers.

Instances (1 of 1)

uri: <https://files.liquidfiles.com/assets/application-9e0774fa0db171f1caf101828b9443018702955b8e56cc49db50ef72403bdf73.js>
method: GET
evidence: 10.1.2.3
otherinfo: 10.1.2.3

References

<https://tools.ietf.org/html/rfc1918>

Vulnerable Target	First Detected	Last Detected
files.liquidfiles.com	22 days ago	0 days ago

This low severity vulnerability exist on a default LiquidFiles system because it's not possible to get started if this gets hardened further.
On a production system when a proper FQDN has been set, you can harden this further if you want. Please see: <https://docs.liquidfiles.com/security/hardening.html> for more information.

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.

Active Web Application Vulnerabilities

The OWASP ZAP Active Web Application scan crawls the pages of a website or web application testing for vulnerabilities and configuration weaknesses. The active scan includes all of the passive scan tests and additionally makes requests and submits forms to actively test an application for more vulnerabilities. The active scan tests for vulnerabilities such as SQL injection, remote command execution, XSS, and more.

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.

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

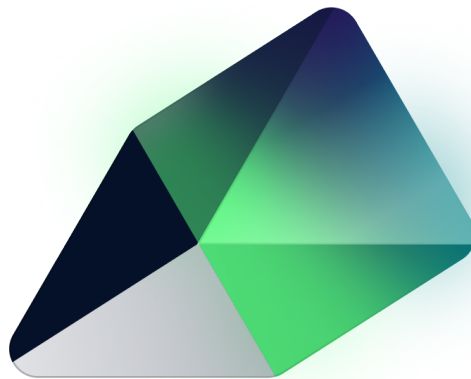
9.0 - 10.0 = Critical

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