April 5, 2025

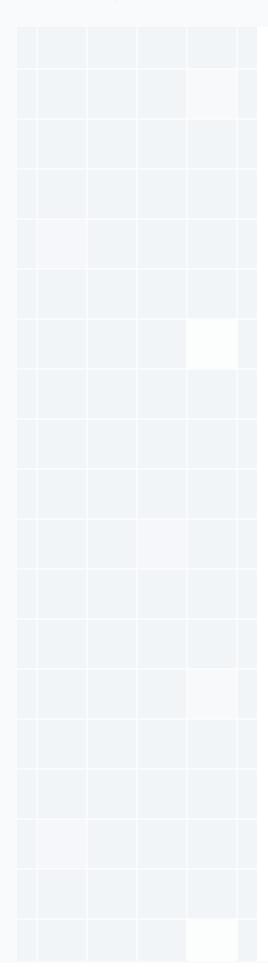
Vulnerability Scan Report

Prepared By

HostedScan Security



HostedScan Security Vulnerability Scan Report



Overview

1	Executive Summary	3
2	Vulnerabilities By Target	4
3	Active Web Application Vulnerabilities	7
4	Passive Web Application Vulnerabilities	8
5	SSL/TLS Security	12
6	Network Vulnerabilities	13
7	Open TCP Ports	15
8	Open UDP Ports	20
9	Glossary	21



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.

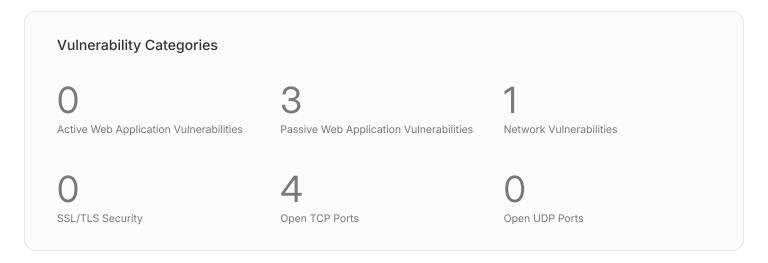
1.1 Total Vulnerabilities

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 2 targets scanned. Each target is a single URL, IP address, or fully qualified domain name (FQDN).



Vulnerability Scan Report

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.



https://lecube.cnc.cd

Total Risks 3 5 38% 63% Passive Web Application Vulnerabilities First Detected Last Detected Severity 0 days ago 0 days ago Content Security Policy (CSP) Header Not Set Medium Strict-Transport-Security Header Not Set 0 days ago 0 days ago Low 0 days ago 0 days ago X-Content-Type-Options Header Missing Low Network Vulnerabilities First Detected Last Detected Severity **TCP Timestamps Information Disclosure** Low 0 days ago 0 days ago cvss score: 2.6 Open TCP Ports Last Detected Severity First Detected Open TCP Port: 8080 Medium 0 days ago 0 days ago 0 days ago Open TCP Port: 8443 Medium 0 days ago Open TCP Port: 80 0 days ago Low 0 days ago Open TCP Port: 443 0 days ago Low 0 days ago



http://presence.cnc.cd

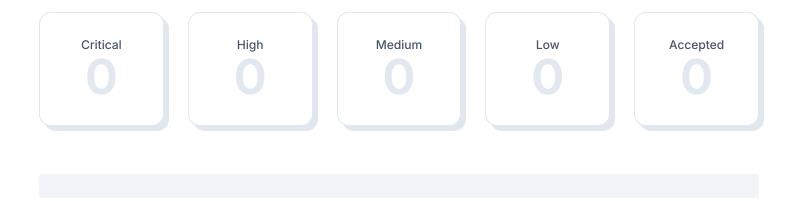
Total Risks						
0						
		No vulr	nerabilities	s found.		

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.



3.2 Vulnerabilities Breakdown

Summary list of all detected vulnerabilities.

Title	Severity	Open	Accepted
No vulnerabilities detected			

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
Content Security Policy (CSP) Header Not Set	Medium	1	0
Strict-Transport-Security Header Not Set	Low	1	0
X-Content-Type-Options Header Missing	Low	1	0

4.3 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: https://lecube.cnc.cd/ 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
https://lecube.cnc.cd	0 days ago	0 days ago



Strict-Transport-Security Header Not Set

SEVERITY

AFFECTED TARGETS

LAST DETECTED

Low

1 target

0 days ago

Description

HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

Solution

Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.

Instances (1 of 15)

uri: https://lecube.cnc.cd/

method: GET

References

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

https://owasp.org/www-community/Security_Headers

https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security

https://caniuse.com/stricttransportsecurity

https://datatracker.ietf.org/doc/html/rfc6797

Vulnerable Target	First Detected	Last Detected
https://lecube.cnc.cd	0 days ago	0 days ago



X-Content-Type-Options Header Missing

SEVERITY

AFFECTED TARGETS

LAST DETECTED

Low

1 target

0 days ago

Description

The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.

Solution

Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.

If possible, ensure that the end user uses a standards-compliant and modern web browser that does not perform MIME-sniffing at all, or that can be directed by the web application/web server to not perform MIME-sniffing.

Instances (1 of 11)

uri: https://lecube.cnc.cd/cdn-cgi/challenge-platform/h/g/orchestrate/chl_page/v1?ray=92b2592f1be80c80

method: GET

param: x-content-type-options

otherinfo: This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.

References

https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85) https://owasp.org/www-community/Security_Headers

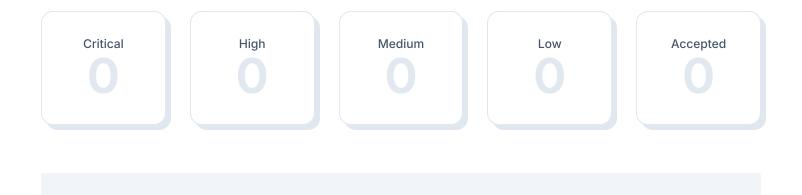
Vulnerable Target	First Detected	Last Detected
https://lecube.cnc.cd	0 days ago	0 days ago

5 SSL/TLS Security

The SSLyze security scan tests for misconfigured SSL/TLS certificates, expired certificates, weak ciphers, and SSL/TLS vulnerabilities such as Heartbleed.

5.1 Total Vulnerabilities

Total number of vulnerabilities found by severity.



5.2 Vulnerabilities Breakdown

Summary list of all detected vulnerabilities.



6 Network Vulnerabilities

The OpenVAS network vulnerability scan tests servers and internet connected devices for over 150,000 vulnerabilities. OpenVAS uses the Common Vulnerability Scoring System (CVSS) to quantify the severity of findings. 0.0 is the lowest severity and 10.0 is the highest.

Lite Scan

Free accounts use the lite network scan which is limited to the 10 most common ports and excludes brute force tests.

6.1 Total Vulnerabilities

Total number of vulnerabilities found by severity.



100%

6.2 Vulnerabilities Breakdown

Summary list of all detected vulnerabilities.



6.3 Vulnerability Details

Detailed information about each potential vulnerability found by the scan.



TCP Timestamps Information Disclosure

SEVERITY

AFFECTED TARGETS

LAST DETECTED

CVSS SCORE

Low

1 target

0 days ago

2.6

Description

The remote host implements TCP timestamps and therefore allows to compute the uptime.

The remote host implements TCP timestamps, as defined by RFC1323/RFC7323.

A side effect of this feature is that the uptime of the remote host can sometimes be computed.

Solution

To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps

References

https://datatracker.ietf.org/doc/html/rfc1323

https://datatracker.ietf.org/doc/html/rfc7323

https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/download/details.aspx?id=9152

https://www.fortiguard.com/psirt/FG-IR-16-090

Vulnerable Target	First Detected	Last Detected
https://lecube.cnc.cd	0 days ago	0 days ago

7 Open TCP Ports

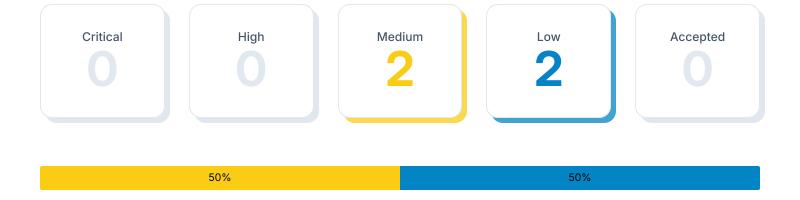
The NMAP TCP port scan discovers open TCP ports with a complete scan of ports 0 to 65535.

Lite Scan

Free accounts use the lite port scan which is limited to the top 100 most common ports.

7.1 Total Vulnerabilities

Total number of vulnerabilities found by severity.



7.2 Vulnerabilities Breakdown

Summary list of all detected vulnerabilities.

Title	Severity	Open	Accepted
Open TCP Port: 8080	Medium	1	0
Open TCP Port: 8443	Medium	1	0
Open TCP Port: 80	Low	1	0
Open TCP Port: 443	Low	1	0

7.3 Vulnerability Details

Detailed information about each potential vulnerability found by the scan.



Open TCP Port: 8080

SEVERITY

AFFECTED TARGETS

LAST DETECTED

Medium

1 target

0 days ago

Description

An open port may be an expected configuration. For example, web servers use port 80 to serve websites over http and port 443 to serve websites over https. For a list of commonly used ports see https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers.

An unexpected open port could give unintended access to applications, data, and private networks. Open ports can also be dangerous when expected services are out of date and exploited through security vulnerabilities.

Vulnerable Target	First Detected	Last Detected
https://lecube.cnc.cd	0 days ago	0 days ago



Open TCP Port: 8443

SEVERITY

AFFECTED TARGETS

LAST DETECTED

Medium

1 target

0 days ago

Description

An open port may be an expected configuration. For example, web servers use port 80 to serve websites over http and port 443 to serve websites over https. For a list of commonly used ports see https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers.

An unexpected open port could give unintended access to applications, data, and private networks. Open ports can also be dangerous when expected services are out of date and exploited through security vulnerabilities.

Vulnerable Target	First Detected	Last Detected
https://lecube.cnc.cd	0 days ago	0 days ago



Open TCP Port: 80

SEVERITY

AFFECTED TARGETS

LAST DETECTED

Low

1 target

0 days ago

Description

An open port may be an expected configuration. For example, web servers use port 80 to serve websites over http and port 443 to serve websites over https. For a list of commonly used ports see https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers.

An unexpected open port could give unintended access to applications, data, and private networks. Open ports can also be dangerous when expected services are out of date and exploited through security vulnerabilities.

Vulnerable Target	First Detected	Last Detected
https://lecube.cnc.cd	0 days ago	0 days ago



Open TCP Port: 443

SEVERITY

AFFECTED TARGETS

LAST DETECTED

Low

1 target

0 days ago

Description

An open port may be an expected configuration. For example, web servers use port 80 to serve websites over http and port 443 to serve websites over https. For a list of commonly used ports see https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers.

An unexpected open port could give unintended access to applications, data, and private networks. Open ports can also be dangerous when expected services are out of date and exploited through security vulnerabilities.

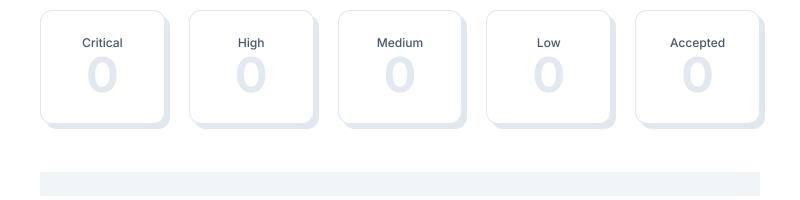
Vulnerable Target	First Detected	Last Detected
https://lecube.cnc.cd	0 days ago	0 days ago

8 Open UDP Ports

The NMAP UDP port scan discovers open ports of common UDP services

8.1 Total Vulnerabilities

Total number of vulnerabilities found by severity.



8.2 Vulnerabilities Breakdown

Summary list of all detected vulnerabilities.

Title	Severity	Open Accepted
No vulnerabilities detected		

Glossary Vulnerability Scan Report

9 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.

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.

Network Vulnerabilities

The OpenVAS network vulnerability scan tests servers and internet connected devices for over 150,000 vulnerabilities. OpenVAS uses the Common Vulnerability Scoring System (CVSS) to quantify the severity of findings. 0.0 is the lowest severity and 10.0 is the highest.

Open TCP Ports

The NMAP TCP port scan discovers open TCP ports with a complete scan of ports 0 to 65535.

Open UDP Ports

The NMAP UDP port scan discovers open ports of common UDP services

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).

SSL/TLS Security

The SSLyze security scan tests for misconfigured SSL/TLS certificates, expired certificates, weak ciphers, and SSL/TLS vulnerabilities such as Heartbleed.

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 = Low4.0 - 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