Vulnerabilities Report

1. Content Security Policy (CSP) Header Not Set

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.

Tags:

OWASP_2021_A05

SYSTEMIC

CWE-693

OWASP_2017_A06

Risk: Medium

URL: http://192.168.56.101/WebGoat/attack

Method: GET

2. Weak Authentication Method

Description: HTTP basic or digest authentication has been used over an unsecured connection. The credentials can be read and then reused by someone with access to the network.

Tags:

OWASP_2021_A01

OWASP_2021_A02

CWE-326

WSTG-v42-ATHN-01

OWASP_2017_A02

OWASP_2017_A03

Risk: Medium

URL: http://192.168.56.101/WebGoat/attack

Method: GET

3. Server Leaks Version Information via "Server" HTTP Response Header Field

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.

Tags:

OWASP_2021_A05

SYSTEMIC

OWASP_2017_A06

WSTG-v42-INFO-02

CWE-497

Risk: Low

URL: http://192.168.56.101/WebGoat/attack

Method: GET

4. ZAP is Out of Date

Description: The version of ZAP you are using to test your app is out of date and is no longer being updated. The risk level is set based on how out of date your ZAP version is.

Tags:

CWE-1104

Risk: Low

URL: http://192.168.56.101/WebGoat/attack

Method: GET