Technical Security Report

Target Information

URL
http://weew.com/

Web Server
Microsoft-HTTPAPI/2.0

IP Address
209.98.55.153

Security Alerts

Content Security Policy (CSP) Header Not Set

Risk: Medium

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.

Method: GET

Confidence: High

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

Affected URLs and Technologies

http://weew.com/sitemap.xml
http://weew.com/robots.txt
http://weew.com/

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

Risk: Low

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.

Method: GET

Confidence: High

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

Affected URLs and Technologies

http://weew.com/sitemap.xml
http://weew.com/robots.txt
http://weew.com/