

# Website Security Scan Report

Generated on: 2024-12-11 18:57:46

## Crawling Information

Crawled URL
http://vulnweb.com/acunetix-logo.png
http://vulnweb.com/sitemap.xml
http://vulnweb.com/robots.txt
http://vulnweb.com/

## Scan Information

Target URL	http://vulnweb.com/	
Attack Type	Command Injection	
Scan Started At	2024-12-11 18:57:46	
Scan Duration	30.51 seconds	

## Vulnerabilities Found

High Severity	0	
Medium Severity	4	
Low Severity	6	

## Vulnerability Details

URL	Risk	Description
http://vulnweb.com/	Medium	The response does not protect against 'ClickJacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options.

<a href="http://vulnweb.com/acunetix-logo.png">http://vulnweb.com/acunetix-logo.png</a>	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.
<a href="http://vulnweb.com/robots.txt">http://vulnweb.com/robots.txt</a>	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.
<a href="http://vulnweb.com/sitemap.xml">http://vulnweb.com/sitemap.xml</a>	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.
<a href="http://vulnweb.com/acunetix-logo.png">http://vulnweb.com/acunetix-logo.png</a>	Low	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.
<a href="http://vulnweb.com/robots.txt">http://vulnweb.com/robots.txt</a>	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.

http://vulnweb.com/sitemap.xml	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.
http://vulnweb.com/	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.
http://vulnweb.com/	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.
http://vulnweb.com/	Low	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.