SIGMA Report

Date: 15-12-2022

Time: 17:02:52

Vulnerability Scanning :

Web Application Vulnerability Scanners are automated tools that scan web applications, normally from the outside, to look for security vulnerabilities such as Cross-site scripting, SQL Injection, Command Injection, Path Traversal and insecure server configuration.

Vulnerabilities Section :

1) Headers and Cookies:

Content-Security-Policy

Severity	Best Practice
Description	Content-Security-Policy 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.
Impact	If CSP is implemented to your website, u will have an extra layer of security and prevent XSS attack. By not implementing CSP, your website will be vulnerable to XSS attack.
Remediation	Enable CSP on your website by sending the Content-Security-Policy in HTTP response headers that instruct the browser to apply the policies you specified.

Referrer-Policy

Severity	Best Practice
Description	Referrer-Policy is a security header designed to prevent cross-domain Referer leakage.
Impact	Referer header is a request header that indicates the site which the traffic originated from. If there is no adequate prevention in place, the URL itself, and even sensitive information contained in the URL will be leaked to the cross-site. The lack of Referrer-Policy header might affect privacy of the users and site's itself
Remediation	In a response header: Referrer-Policy: no-referrer | same-origin | origin | strict-origin | no-origin-when-downgrading In a META tag <meta name="Referrer-Policy" value="no-referrer | same-origin"/> In an element attribute or

Cookie Not Marked as Secure

Severity	Low
Description	A cookie not marked as secure, and transmitted over HTTPS. This means the cookie could potentially be stolen by an attacker who can successfully intercept and decrypt the traffic, or following a successful man-in-the-middle attack.
Impact	This cookie will be transmitted over a HTTP connection, therefore if this cookie is important, an attacker might intercept it and hijack a victim'session. If the attacker can carry out a man-in-the-middle attack, he/she can force the victim to make an HTTP request to steal the cookie.
Remediation	Mark all cookies used within the application as secure.

Cookie Not Marked as HttpOnly

Severity	Low
Description	HTTPOnly cookies cannot be read by client-side scripts, therefore marking a cookie as HTTPOnly can provide an additional layer of protection against cross-site scripting attacks
Impact	During a cross-site scripting attack, an attacker might easily access cookies and hijack the victim's session.
Remediation	Mark the cookie as HTTPOnly. This will be an extra layer of defense against XSS. However this is not a silver bullet and will not protect the system against cross-site scripting attacks. An attacker can use a tool such as XSS Tunnel to bypass HTTPOnly protection.

X-Frame Options

Severity	Low
Description	The X-Frame-Options HTTP header field indicates a policy that specifies whether the browser should render the transmitted resource within a frame or an iframe.
Impact	Missing X-Frame-Options header means that this website could be at risk of a clickjacking attack.
Remediation	Set the X-Frame header with on of two values : 1) SAMEORIGIN-only websites located in the same domain can embed the returned page in an iframe. 2) DENY - embedding in an iframe is not allowed.

X-Content-Type-Options

Severity	Low
Description	The X-Content-Type-Options header is used to protect against MIME sniffing vulnerabilities. These vulnerabilities can occur when a website allows users to upload content to a website.
Impact	Execute MIME sniffing attacks to obtain technical information and craft new attack vectors.
Remediation	Configure your web server to include an (X-Content-Type-Options) header with a value of (nosniff)

X-XSS-Protection

Severity	Medium
Description	X-XSS-Protection response header is a feature of Internet Explorer, Chrome and Safari that stops pages from loading when they detect reflected cross-site scripting (XSS) attacks.

Impact	Increase the chance of exploiting a stored XSS.
Remediation	Add the X-XSS-Protection header with a value of "1; mode= block" Enables XSS filtering. Rather than sanitizing the page, the browser will prevent rendering of the page if an attack is detected.

HTTP Strict Transport Security (HSTS)

Severity	Medium
Description	The HTTP Strict Transport Security header informs the browser that it should never load a site using HTTP and should automatically convert all attempts to access the site using HTTP to HTTPS requests instead.
Impact	Could allow the attackers to fool the browser into expiring HSTS entries and allowing insecure HTTP connections.
Remediation	Set the Strict-Transport-Security header and a max-age of at least 31536000 in all server responses so that the browser should remember that a site is only to be accessed using HTTPS.

Cache-Control

Severity	Critical
Description	Cache-control is an HTTP header used to specify browser caching policies in both client requests and server responses. Policies include how a resource is cached, where its cached and its maximum age before expiring.
Impact	If the server did not return or returned an invalid "Cache-Control" header, which means the page contains sensitive information, (password, credit card, personal data, and so on) could be stored and then exposed to unauthorized individuals.
Remediation	Configure your web server to include a ‘ Cache-Control ’ header with the value ‘no-store’ .

2) Open Ports:

Port 80

Protocol	TCP
Service	HTTP,HTTPS
Description	HTTP and HTTPS are the hottest protocols on the internet, so they are often targeted by attackers. HTTP sends data over port 80 while HTTPS uses port 443. HTTP operates at application layer, while HTTPS operates at transport layer.
Impact	Vulnerable to cross-site scripting, SQL injections, cross-site request forgeries and DDoS attacks.

Port 443

Protocol	TCP
Service	HTTP,HTTPS
Description	HTTP and HTTPS are the hottest protocols on the internet, so they are often targeted by attackers. HTTP sends data over port 80 while HTTPS uses port 443. HTTP operates at application layer, while HTTPS operates at transport layer.
Impact	Vulnerable to cross-site scripting, SQL injections, cross-site request forgeries and DDoS attacks.

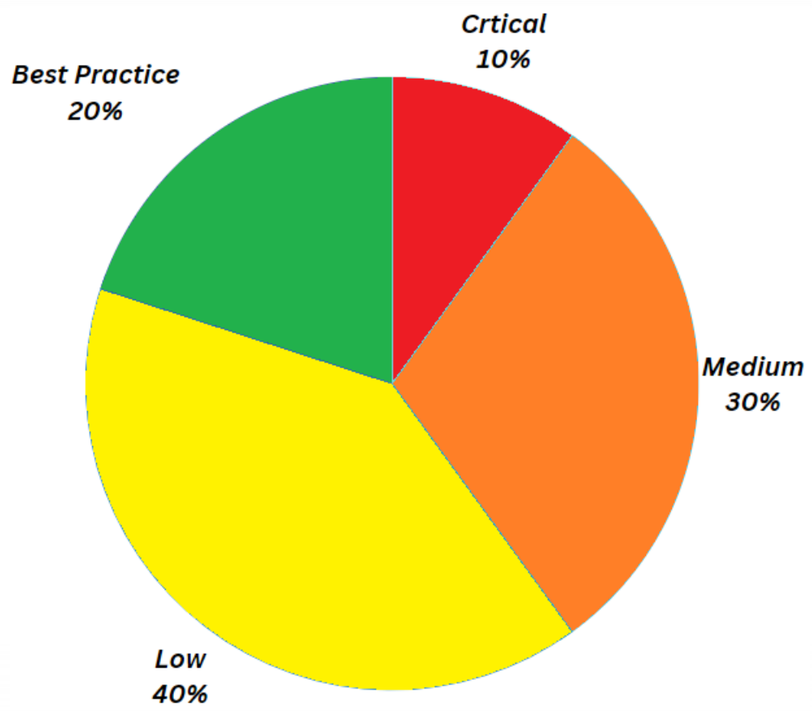
Port 8080

Protocol	TCP
Service	HTTP,HTTPS
Description	HTTP and HTTPS are the hottest protocols on the internet, so they are often targeted by attackers. HTTP sends data over port 80 while HTTPS uses port 443. HTTP operates at application layer, while HTTPS operates at transport layer.
Impact	Vulnerable to cross-site scripting, SQL injections, cross-site request forgeries and DDoS attacks.

Port 8443

Protocol	TCP
Service	HTTP,HTTPS
Description	HTTP and HTTPS are the hottest protocols on the internet, so they are often targeted by attackers. HTTP sends data over port 80 while HTTPS uses port 443. HTTP operates at application layer, while HTTPS operates at transport layer.
Impact	Vulnerable to cross-site scripting, SQL injections, cross-site request forgeries and DDoS attacks.

3) Report Details:



This PieChart is talking about percentage of Vulnerability and Headers Severities .To help you better decide which vulnerabilities should be fixed first, we classified the severities into 4 categories : Critical, Medium, Low, Best practice.

1) Critical Severity : The headers or vulnerabilities marked as Critical Severity can allow attackers to execute code on the web application or application server, or access sensitive data.

2) Medium Severity : The headers or vulnerabilities marked as Medium Severity usually arise because of errors and deficiencies in the application configuration. By exploiting these security issues, malicious attackers can access sensitive information on the application or server.

3) Low Severity : The headers or vulnerabilities marked as Low Severity are usually not critical, but they can still be exploited by attackers to access sensitive information on the application or server.

4) Best Practice : The headers or vulnerabilities marked as Best Practice are not critical, but they can still be exploited by attackers to access sensitive information on the application or server.

4) Conclusion:

The report is generated based on the results of the vulnerability scanning process on **tryhackme.com**. The report includes information about the headers, cookies and open ports that were detected during the scan. The report also includes information about the severity of the vulnerabilities, the impact of the vulnerabilities on the web application and how to remediate them.

The scanning process found **9** vulnerabilities (headers and cookies) and **4** open ports. In order to remediate them, you need to check the vulnerabilities in the report and then use the information to remediate the vulnerabilities.

For more information about vulnerabilities, you can visit the following links:

www.invicti.com

www.cvedetails.com