ZAP by Checkmarx Scanning Report

Sites: http://localhost:8081 http://localhost:4200

Generated on Sal, 30 Eyl 2025 17:43:56

ZAP Version: 2.16.1

ZAP by Checkmarx

Summary of Alerts

Risk Seviyesi	Number of Alerts
Yükek	0
Orta	3
Düük	2
Bilgilendirme	2

Uyarlar

sim	Risk Seviyesi	Number of Instances
CSP: Failure to Define Directive with No Fallback	Orta	2
Content Security Policy (CSP) Header Not Set	Orta	4
Missing Anti-clickjacking Header	Orta	4
Application Error Disclosure	Düük	1
X-Content-Type-Options Header Missing	Düük	8
Bilginin Aça Çkmas - üpheli Yorumlar	Bilgilendirme	1
Modern Web Application	Bilgilendirme	4

Alert Detail

Orta	CSP: Failure to Define Directive with No Fallback
Açklama	The Content Security Policy fails to define one of the directives that has no fallback. Missing /excluding them is the same as allowing anything.
URL	http://localhost:4200/robots.txt
Yöntem	GET
Saldr	
Evidence	default-src 'none'
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	http://localhost:4200/sitemap.xml

Yöntem	GET
Saldr	
Evidence	default-src 'none'
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
Instances	2
Solution	Ensure that your web server, application server, load balancer, etc. is properly configured to set the Content-Security-Policy header.
Reference	https://www.w3.org/TR/CSP/ https://caniuse.com/#search=content+security+policy https://content-security-policy.com/ https://github.com/HtmlUnit/htmlunit-csp https://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variety_of_resources
CWE Id	693
WASC Id	15
Plugin Id	10055

Orta	**Content Security Policy (CSP) Header Not Set**
Açklama	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.
URL	http://localhost:4200/
Yöntem	GET
Saldr	
Evidence	
Other Info	
URL	http://localhost:4200/login
Yöntem	GET
Saldr	
Evidence	
Other Info	
URL	http://localhost:4200/register
Yöntem	GET
Saldr	
Evidence	
Other Info	
URL	http://localhost:4200/vulnerable-login
Yöntem	GET
Saldr	
Evidence	

Other Info	
Instances	4
Solution	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Reference	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/
CWE Id	693
WASC Id	15
Plugin Id	10038

Orta	**Missing Anti-clickjacking Header**
Açklama	The response does not protect against 'ClickJacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options.
URL	http://localhost:4200/
Yöntem	GET
Saldr	
Evidence	
Other Info	
URL	http://localhost:4200/login
Yöntem	GET
Saldr	
Evidence	
Other Info	
URL	http://localhost:4200/register
Yöntem	GET
Saldr	
Evidence	
Other Info	
URL	http://localhost:4200/vulnerable-login
Yöntem	GET
Saldr	
Evidence	
Other Info	
Instances	4
	Modern Web browsers support the Content-Security-Policy and X-Frame-Options HTTP headers. Ensure one of them is set on all web pages returned by your site/app.

Solution	If you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET) then you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed, you should use DENY. Alternatively consider implementing Content Security Policy's "frame-ancestors" directive.
Reference	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
CWE Id	1021
WASC Id	15
Plugin Id	10020

Düük	**Application Error Disclosure**
Açklama	This page contains an error/warning message that may disclose sensitive information like the location of the file that produced the unhandled exception. This information can be used to launch further attacks against the web application. The alert could be a false positive if the error message is found inside a documentation page.
URL	http://localhost:8081/api/vulnerable/login
Yöntem	GET
Saldr	
Evidence	HTTP/1.1 500
Other Info	
Instances	1
Solution	Review the source code of this page. Implement custom error pages. Consider implementing a mechanism to provide a unique error reference/identifier to the client (browser) while logging the details on the server side and not exposing them to the user.
Reference	
CWE Id	550
WASC Id	13
Plugin Id	90022

Düük	**X-Content-Type-Options Header Missing**
Açklama	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.
URL	http://localhost:4200/
Yöntem	GET
Saldr	
Evidence	
Other Info	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.
URL	http://localhost:4200/@vite/client
Yöntem	GET
Saldr	
Evidence	
Other Info	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.
URL	http://localhost:4200/favicon.ico
Yöntem	GET
Saldr	
Evidence	
Other Info	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.
URL	http://localhost:4200/login
Yöntem	GET
Saldr	
Evidence	
Other Info	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.
URL	http://localhost:4200/main.js
Yöntem	GET
Saldr	
Evidence	
Other Info	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.
URL	http://localhost:4200/register
Yöntem	GET
Saldr	
Evidence	
Other Info	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.
URL	http://localhost:4200/styles.css
Yöntem	GET
Saldr	
Evidence	
Other Info	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.
URL	http://localhost:4200/vulnerable-login
Yöntem	GET
Saldr	
Evidence	
Other Info	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.

Instances	8
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.
Reference	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
CWE Id	693
WASC Id	15
Plugin Id	10021

Bilgilendirme	**Bilginin Açа Çkmas - üpheli Yorumlar**
Açklama	The response appears to contain suspicious comments which may help an attacker.
URL	http://localhost:4200/main.js
Yöntem	GET
Saldr	
Evidence	User
Other Info	The following pattern was used: \bUSER\b and was detected in likely comment: "// User API", see evidence field for the suspicious comment/snippet.
Instances	1
Solution	Bir saldrgana yardmc olabilecek bilgileri döndüren tüm yorumlar kaldrn ve alttaki bavurulan problemleri düzeltin.
Reference	
CWE Id	615
WASC Id	13
Plugin Id	10027

Bilgilendirme	**Modern Web Application**
Açklama	The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
URL	http://localhost:4200/
Yöntem	GET
Saldr	
Evidence	<script type="module" src="/@vite/client"></script>
Other Info	No links have been found while there are scripts, which is an indication that this is a modern web application.
URL	http://localhost:4200/login
Yöntem	GET
Saldr	
Evidence	<script type="module" src="/@vite/client"></script>
Other Info	No links have been found while there are scripts, which is an indication that this is a modern web application.
URL	http://localhost:4200/register
Yöntem	GET

Saldr	
Evidence	<script type="module" src="/@vite/client"></script>
Other Info	No links have been found while there are scripts, which is an indication that this is a modern web application.
URL	http://localhost:4200/vulnerable-login
Yöntem	GET
Saldr	
Evidence	<script type="module" src="/@vite/client"></script>
Other Info	No links have been found while there are scripts, which is an indication that this is a modern web application.
Instances	4
Solution	This is an informational alert and so no changes are required.
Reference	
CWE Id	
WASC Id	
Plugin Id	10109