ZAP Scanning Report

Site: http://localhost:8080

Generated on terça, 6 jun. 2023 22:52:17

ZAP Version: 2.12.0

Summary of Alerts

Risk Level	Number of Alerts
Alto	0
Médio	4
Baixo	2
Informational	2

Alertas

Name	Risk Level	Number of Instances
CSP: Wildcard Directive	Médio	9
CSP: script-src unsafe-eval	Médio	9
CSP: script-src unsafe-inline	Médio	9
CSP: style-src unsafe-inline	Médio	9
Application Error Disclosure	Baixo	2
Information Disclosure - Debug Error Messages	Baixo	2
Authentication Request Identified	Informational	1
Modern Web Application	Informational	9

Alert Detail

Médio	CSP: Wildcard Directive
Description	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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:8080
Método	GET
Atacar	
Evidence	default-src 'self'; frame-src 'self' data:; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://storage.googleapis.com; style-src 'self' 'unsafe-inline'; img-src 'self' data:; font-src 'self' data:
URL	http://localhost:8080/
Método	GET

Atacar	
Evidence	default-src 'self'; frame-src 'self' data:; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://storage.googleapis.com; style-src 'self' 'unsafe-inline'; img-src 'self' data:; font-src 'self' data:
URL	http://localhost:8080/api/account/reset-password/finish
Método	GET
Atacar	
Evidence	default-src 'self'; frame-src 'self' data:; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://storage.googleapis.com; style-src 'self' 'unsafe-inline'; img-src 'self' data:; font-src 'self' data:
URL	http://localhost:8080/api/account/reset-password/init
Método	GET
Atacar	
Evidence	default-src 'self'; frame-src 'self' data:; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://storage.googleapis.com; style-src 'self' 'unsafe-inline'; img-src 'self' data:; font-src 'self' data:
URL	http://localhost:8080/content/
Método	GET
Atacar	
Evidence	default-src 'self'; frame-src 'self' data:; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://storage.googleapis.com; style-src 'self' 'unsafe-inline'; img-src 'self' data:; font-src 'self' data:
URL	http://localhost:8080/content/css/
Método	GET
Atacar	
Evidence	default-src 'self'; frame-src 'self' data:; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://storage.googleapis.com; style-src 'self' 'unsafe-inline'; img-src 'self' data:; font-src 'self' data:
URL	http://localhost:8080/content/images/
Método	GET
Atacar	
Evidence	default-src 'self'; frame-src 'self' data:; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://storage.googleapis.com; style-src 'self' 'unsafe-inline'; img-src 'self' data:; font-src 'self' data:
URL	http://localhost:8080/login
Método	GET
Atacar	
Evidence	default-src 'self'; frame-src 'self' data:; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://storage.googleapis.com; style-src 'self' 'unsafe-inline'; img-src 'self' data:; font-src 'self' data:
URL	http://localhost:8080/mvnw
Método	GET
Atacar	
Evidence	default-src 'self'; frame-src 'self' data:; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://storage.googleapis.com; style-src 'self' 'unsafe-inline'; img-src 'self' data:; font-src 'self' data:
Instances	9

Solution	Ensure that your web server, application server, load balancer, etc. is properly configured to set the Content-Security-Policy header.
Reference	http://www.w3.org/TR/CSP2/ http://www.w3.org/TR/CSP/ http://caniuse.com/#search=content+security+policy http://content-security-policy.com/ https://github.com/shapesecurity/salvation 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

Médio	CSP: script-src unsafe-eval
Description	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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:8080
Método	GET
Atacar	
Evidence	default-src 'self'; frame-src 'self' data:; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://storage.googleapis.com; style-src 'self' 'unsafe-inline'; img-src 'self' data:; font-src 'self' data:
URL	http://localhost:8080/
Método	GET
Atacar	
Evidence	default-src 'self'; frame-src 'self' data:; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://storage.googleapis.com; style-src 'self' 'unsafe-inline'; img-src 'self' data:; font-src 'self' data:
URL	http://localhost:8080/api/account/reset-password/finish
Método	GET
Atacar	
Evidence	default-src 'self'; frame-src 'self' data:; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://storage.googleapis.com; style-src 'self' 'unsafe-inline'; img-src 'self' data:; font-src 'self' data:
URL	http://localhost:8080/api/account/reset-password/init
Método	GET
Atacar	
Evidence	default-src 'self'; frame-src 'self' data:; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://storage.googleapis.com; style-src 'self' 'unsafe-inline'; img-src 'self' data:; font-src 'self' data:
URL	http://localhost:8080/content/
Método	GET
Atacar	
Evidence	default-src 'self'; frame-src 'self' data:; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://storage.googleapis.com; style-src 'self' 'unsafe-inline'; img-src 'self' data:; font-src 'self' data:

URL	http://localhost:8080/content/css/
Método	GET
Atacar	
Evidence	default-src 'self'; frame-src 'self' data:; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://storage.googleapis.com; style-src 'self' 'unsafe-inline'; img-src 'self' data:; font-src 'self' data:
URL	http://localhost:8080/content/images/
Método	GET
Atacar	
Evidence	default-src 'self'; frame-src 'self' data:; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://storage.googleapis.com; style-src 'self' 'unsafe-inline'; img-src 'self' data:; font-src 'self' data:
URL	http://localhost:8080/login
Método	GET
Atacar	
Evidence	default-src 'self'; frame-src 'self' data:; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://storage.googleapis.com; style-src 'self' 'unsafe-inline'; img-src 'self' data:; font-src 'self' data:
URL	http://localhost:8080/mvnw
Método	GET
Atacar	
Evidence	default-src 'self'; frame-src 'self' data:; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://storage.googleapis.com; style-src 'self' 'unsafe-inline'; img-src 'self' data:; font-src 'self' data:
Instances	9
Solution	Ensure that your web server, application server, load balancer, etc. is properly configured to set the Content-Security-Policy header.
Reference	http://www.w3.org/TR/CSP2/ http://www.w3.org/TR/CSP/ http://caniuse.com/#search=content+security+policy http://content-security-policy.com/ https://github.com/shapesecurity/salvation 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

Médio	**CSP: script-src unsafe-inline**
Description	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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:8080
Método	GET
Atacar	
Evidence	default-src 'self'; frame-src 'self' data:; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://storage.googleapis.com; style-src 'self' 'unsafe-inline'; img-src 'self' data:; font-src

	'self' data:
URL	http://localhost:8080/
Método	GET
Atacar	
Evidence	default-src 'self'; frame-src 'self' data:; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://storage.googleapis.com; style-src 'self' 'unsafe-inline'; img-src 'self' data:; font-src 'self' data:
URL	http://localhost:8080/api/account/reset-password/finish
Método	GET
Atacar	
Evidence	default-src 'self'; frame-src 'self' data:; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://storage.googleapis.com; style-src 'self' 'unsafe-inline'; img-src 'self' data:; font-src 'self' data:
URL	http://localhost:8080/api/account/reset-password/init
Método	GET
Atacar	
Evidence	default-src 'self'; frame-src 'self' data:; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://storage.googleapis.com; style-src 'self' 'unsafe-inline'; img-src 'self' data:; font-src 'self' data:
URL	http://localhost:8080/content/
Método	GET
Atacar	
Evidence	default-src 'self'; frame-src 'self' data:; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://storage.googleapis.com; style-src 'self' 'unsafe-inline'; img-src 'self' data:; font-src 'self' data:
URL	http://localhost:8080/content/css/
Método	GET
Atacar	
Evidence	default-src 'self'; frame-src 'self' data:; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://storage.googleapis.com; style-src 'self' 'unsafe-inline'; img-src 'self' data:; font-src 'self' data:
URL	http://localhost:8080/content/images/
Método	GET
Atacar	
Evidence	default-src 'self'; frame-src 'self' data:; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://storage.googleapis.com; style-src 'self' 'unsafe-inline'; img-src 'self' data:; font-src 'self' data:
URL	http://localhost:8080/login
Método	GET
Atacar	
Evidence	default-src 'self'; frame-src 'self' data:; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://storage.googleapis.com; style-src 'self' 'unsafe-inline'; img-src 'self' data:; font-src 'self' data:
URL	http://localhost:8080/mvnw
Método	GET
Atacar	
Evidence	default-src 'self'; frame-src 'self' data:; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://storage.googleapis.com; style-src 'self' 'unsafe-inline'; img-src 'self' data:; font-src

	'self' data:
Instances	9
Solution	Ensure that your web server, application server, load balancer, etc. is properly configured to set the Content-Security-Policy header.
Reference	http://www.w3.org/TR/CSP2/ http://www.w3.org/TR/CSP/ http://caniuse.com/#search=content+security+policy http://content-security-policy.com/ https://github.com/shapesecurity/salvation 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

Médio	**CSP: style-src unsafe-inline**
Description	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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:8080
Método	GET
Atacar	
Evidence	default-src 'self'; frame-src 'self' data:; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://storage.googleapis.com; style-src 'self' 'unsafe-inline'; img-src 'self' data:; font-src 'self' data:
URL	http://localhost:8080/
Método	GET
Atacar	
Evidence	default-src 'self'; frame-src 'self' data:; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://storage.googleapis.com; style-src 'self' 'unsafe-inline'; img-src 'self' data:; font-src 'self' data:
URL	http://localhost:8080/api/account/reset-password/finish
Método	GET
Atacar	
Evidence	default-src 'self'; frame-src 'self' data:; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://storage.googleapis.com; style-src 'self' 'unsafe-inline'; img-src 'self' data:; font-src 'self' data:
URL	http://localhost:8080/api/account/reset-password/init
Método	GET
Atacar	
Evidence	default-src 'self'; frame-src 'self' data:; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://storage.googleapis.com; style-src 'self' 'unsafe-inline'; img-src 'self' data:; font-src 'self' data:
URL	http://localhost:8080/content/
Método	GET
Atacar	
	default-src 'self'; frame-src 'self' data:; script-src 'self' 'unsafe-inline' 'unsafe-eval'

Evidence	https://storage.googleapis.com; style-src 'self' 'unsafe-inline'; img-src 'self' data:; font-src 'self' data:
URL	http://localhost:8080/content/css/
Método	GET
Atacar	
Evidence	default-src 'self'; frame-src 'self' data:; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://storage.googleapis.com; style-src 'self' 'unsafe-inline'; img-src 'self' data:; font-src 'self' data:
URL	http://localhost:8080/content/images/
Método	GET
Atacar	
Evidence	default-src 'self'; frame-src 'self' data:; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://storage.googleapis.com; style-src 'self' 'unsafe-inline'; img-src 'self' data:; font-src 'self' data:
URL	http://localhost:8080/login
Método	GET
Atacar	
Evidence	default-src 'self'; frame-src 'self' data:; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://storage.googleapis.com; style-src 'self' 'unsafe-inline'; img-src 'self' data:; font-src 'self' data:
URL	http://localhost:8080/mvnw
Método	GET
Atacar	
Evidence	default-src 'self'; frame-src 'self' data:; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://storage.googleapis.com; style-src 'self' 'unsafe-inline'; img-src 'self' data:; font-src 'self' data:
Instances	9
Solution	Ensure that your web server, application server, load balancer, etc. is properly configured to set the Content-Security-Policy header.
Reference	http://www.w3.org/TR/CSP2/ http://www.w3.org/TR/CSP/ http://caniuse.com/#search=content+security+policy http://content-security-policy.com/ https://github.com/shapesecurity/salvation 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

Baixo	**Application Error Disclosure**
Description	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:8080/api/activate?key=key
Método	GET
Atacar	
Evidence	HTTP/1.1 500 Internal Server Error
URL	http://localhost:8080/api/account/reset-password/finish

Método	POST
Atacar	
Evidence	HTTP/1.1 500 Internal Server Error
Instances	2
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	200
WASC Id	13
Plugin Id	90022

Baixo	**Information Disclosure - Debug Error Messages**
Description	The response appeared to contain common error messages returned by platforms such as ASP.NET, and Web-servers such as IIS and Apache. You can configure the list of common debug messages.
URL	http://localhost:8080/api/activate?key=key
Método	GET
Atacar	
Evidence	Internal Server Error
URL	http://localhost:8080/api/account/reset-password/finish
Método	POST
Atacar	
Evidence	Internal Server Error
Instances	2
Solution	Disable debugging messages before pushing to production.
Reference	
CWE Id	200
WASC Id	13
Plugin Id	10023

Informational	**Authentication Request Identified**
Description	The given request has been identified as an authentication request. The 'Other Info' field contains a set of key=value lines which identify any relevant fields. If the request is in a context which has an Authentication Method set to "Auto-Detect" then this rule will change the authentication to match the request identified.
URL	http://localhost:8080/api/authenticate
Método	POST
Atacar	
Evidence	password
Instances	1
Solution	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Reference	https://www.zaproxy.org/docs/desktop/addons/authentication-helper/auth-req-id/
CWE Id	
WASC Id	
Plugin Id	10111

Informational	Modern Web Application
Description	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:8080
Método	GET
Atacar	
Evidence	<noscript> <h1>You must enable JavaScript to view this page.</h1> </noscript>
URL	http://localhost:8080/
Método	GET
Atacar	
Evidence	<noscript> <h1>You must enable JavaScript to view this page.</h1> </noscript>
URL	http://localhost:8080/api/account/reset-password/finish
Método	GET
Atacar	
Evidence	<noscript> <h1>You must enable JavaScript to view this page.</h1> </noscript>
URL	http://localhost:8080/api/account/reset-password/init
Método	GET
Atacar	
Evidence	<noscript> <h1>You must enable JavaScript to view this page.</h1> </noscript>
URL	http://localhost:8080/content/
Método	GET
Atacar	
Evidence	<noscript> <h1>You must enable JavaScript to view this page.</h1> </noscript>
URL	http://localhost:8080/content/css/
Método	GET
Atacar	
Evidence	<noscript> <h1>You must enable JavaScript to view this page.</h1> </noscript>
URL	http://localhost:8080/content/images/
Método	GET
Atacar	
Evidence	<noscript> <h1>You must enable JavaScript to view this page.</h1> </noscript>
URL	http://localhost:8080/login
Método	GET
Atacar	
Evidence	<noscript> <h1>You must enable JavaScript to view this page.</h1> </noscript>
URL	http://localhost:8080/mvnw
Método	GET
Atacar	
Evidence	<noscript> <h1>You must enable JavaScript to view this page.</h1> </noscript>
Instances	9
Solution	This is an informational alert and so no changes are required.

Reference	
CWE Id	
WASC Id	
Plugin Id	10109