SivaCore Security Audit

Site: http://host.docker.internal:5000

Generated on Thu, 22 Jan 2026 22:03:24

ZAP Version: 2.17.0

ZAP by Checkmarx

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	0
Low	2
Informational	2

Insights

Level	Reason	Site	Description	Statistic
Info	Informational	http://host.docker.internal:5000	Percentage of responses with status code 2xx	10 %
Info	Informational	http://host.docker.internal:5000	Percentage of responses with status code 4xx	89 %
Info	Informational	http://host.docker.internal:5000	Percentage of endpoints with content type application/json	11 %
Info	Informational	http://host.docker.internal:5000	Percentage of endpoints with content type application/problem+json	3 %
Info	Informational	http://host.docker.internal:5000	Percentage of endpoints with content type text/plain	15 %
Info	Informational	http://host.docker.internal:5000	Percentage of endpoints with method DELETE	7 %
Info	Informational	http://host.docker.internal:5000	Percentage of endpoints with method GET	45 %

Info	Informational	http://host.docker.internal:5000	Percentage of endpoints with method POST	35 %
Info	Informational	http://host.docker.internal:5000	Percentage of endpoints with method PUT	12 %
Info	Informational	http://host.docker.internal:5000	Count of total endpoints	133
Info	Informational	http://host.docker.internal:5000	Percentage of slow responses	1 %

Alerts

Name	Risk Level	Number of Instances
Cookie with SameSite Attribute None	Low	2
X-Content-Type-Options Header Missing	Low	1
Authentication Request Identified	Informational	5
Session Management Response Identified	Informational	2

Alert Detail

Low	Cookie with SameSite Attribute None
Description	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
URL	http://host.docker.internal:5000/User/passkey/authenticate/options
Node Name	http://host.docker.internal:5000/User/passkey/authenticate/options ()("John Doe")
Method	POST
Attack	
Evidence	Set-Cookie: .AspNetCore.Session
Other Info	
URL	http://host.docker.internal:5000/User/passkey/register/options
Node Name	http://host.docker.internal:5000/User/passkey/register/options ()("John Doe")
Method	POST
Attack	
Evidence	Set-Cookie: .AspNetCore.Session
Other Info	
Instances	2

Solution	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Reference	https://datatracker.ietf.org/doc/html/draft-ietf-httpbis-cookie-same-site
CWE Id	1275
WASC Id	13
Plugin Id	10054

Low	**X-Content-Type-Options Header Missing**
Description	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://host.docker.internal:5000/swagger/v1/swagger.json
Node Name	http://host.docker.internal:5000/swagger/v1/swagger.json
Method	GET
Attack	
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	1
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

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://host.docker.internal:5000/Address
Node Name	http://host.docker.internal:5000/Address ()({id,city,country,street,street2,zipCode,customer:{userId,user:{id,emailCipher,emailHash,pseudo,password,steamID,userData:{userId,user,gemCoins,descriptionGemCoins,descriptionGemCoinsFr,goldCoins,descriptionGoldCoins,descriptionGoldCoinsFr,silverCoins,descriptionSilverCoins,descriptionSilverCoinsFr,inventory,level,experience,experienceToNextLevel,maxMana,currentMana,maxHealth,currentHealth},isNewsletterSubscribed,isEmailVerified,isTwoFactorEnabled,twoFactorSecret,backupCodes,role,skins:[{id,name,imageUrl,...)
Method	POST
Attack	
Evidence	customer.user.password

Other Info	userParam=customer.user.backupCodes userValue=John Doe passwordParam=customer.user.password
URL	http://host.docker.internal:5000/Customer
Node Name	http://host.docker.internal:5000/Customer ()({userId,user:{id,emailCipher,emailHash,pseudo,password,steamID,userData:{userId,user,gemCoins,descriptionGemCoins,descriptionGemCoinsFr,goldCoins,descriptionGoldCoins,descriptionGoldCoinsFr,silverCoins,descriptionSilverCoins,descriptionSilverCoinsFr,inventory,level,experience,experienceToNextLevel,maxMana,currentMana,maxHealth,currentHealth},isNewsletterSubscribed,isEmailVerified,isTwoFactorEnabled,twoFactorSecret,backupCodes,role,skins:[{id,name,imageUrl,price,users:[]}],spells:[{id,name,description,pri...)
Method	POST
Attack	
Evidence	user.password
Other Info	userParam=user.backupCodes userValue=John Doe passwordParam=user.password
URL	http://host.docker.internal:5000/Invoice
Node Name	http://host.docker.internal:5000/Invoice ()({numInvoice,date,totalAmount,totalPriceHT,totalPriceTTC,totalTva,customerId,customer:{userId,user:{id,emailCipher,emailHash,pseudo,password,steamID,userData:{userId,user,gemCoins,descriptionGemCoins,descriptionGemCoinsFr,goldCoins,descriptionGoldCoins,descriptionGoldCoinsFr,silverCoins,descriptionSilverCoins,descriptionSilverCoinsFr,inventory,level,experience,experienceToNextLevel,maxMana,currentMana,maxHealth,currentHealth},isNewsletterSubscribed,isEmailVerified,isTwoFactorEnabled,twoFactorSecret,backup...)
Method	POST
Attack	
Evidence	customer.user.password
Other Info	userParam=customer.user.backupCodes userValue=John Doe passwordParam=customer.user.password
URL	http://host.docker.internal:5000/Order
Node Name	http://host.docker.internal:5000/Order ()({numOrder,customerId,customer:{userId,user:{id,emailCipher,emailHash,pseudo,password,steamID,userData:{userId,user,gemCoins,descriptionGemCoins,descriptionGemCoinsFr,goldCoins,descriptionGoldCoins,descriptionGoldCoinsFr,silverCoins,descriptionSilverCoins,descriptionSilverCoinsFr,inventory,level,experience,experienceToNextLevel,maxMana,currentMana,maxHealth,currentHealth},isNewsletterSubscribed,isEmailVerified,isTwoFactorEnabled,twoFactorSecret,backupCodes,role,skins:[{id,name,imageUrl,price,users:[]}],sp...)
Method	POST
Attack	
Evidence	customer.user.password
Other Info	userParam=customer.user.backupCodes userValue=John Doe passwordParam=customer.user.password
URL	http://host.docker.internal:5000/User/login
Node Name	http://host.docker.internal:5000/User/login ()({emailorPseudo,password,twoFactorCode})
Method	POST
Attack	
Evidence	password
Other Info	userParam=emailorPseudo userValue=John Doe passwordParam=password
Instances	5
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	Session Management Response Identified
Description	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
URL	http://host.docker.internal:5000/User/passkey/authenticate/options
Node Name	http://host.docker.internal:5000/User/passkey/authenticate/options ()("John Doe")
Method	POST
Attack	
Evidence	.AspNetCore.Session
Other Info	cookie:.AspNetCore.Session
URL	http://host.docker.internal:5000/User/passkey/register/options
Node Name	http://host.docker.internal:5000/User/passkey/register/options ()("John Doe")
Method	POST
Attack	
Evidence	.AspNetCore.Session
Other Info	cookie:.AspNetCore.Session
Instances	2
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/session-mgmt-id/
CWE Id	
WASC Id	
Plugin Id	10112