ZAP Scan for FCB CCPA UAT server

ZAP Scan for FCB CCPA UAT server

Sites: https://uat-ffc.msxi.com https://fcbccpa-uat.msxint.com

Generated on Sat, 22 Feb 2025 23:56:37

ZAP Version: 2.16.0

ZAP by Checkmarx

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	0
Low	1
Informational	2

Alerts

Name	Risk Level	Number of Instances
Strict-Transport-Security Multiple Header Entries (Non-compliant with Spec)	Low	1
Authentication Request Identified	Informational	1
Information Disclosure - Sensitive Information in URL	Informational	1

Alert Detail

Low	Strict-Transport-Security Multiple Header Entries (Non-compliant with Spec)
Description	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL).
URL	https://uat-ffc.msxi.com/DELETIONAPI/V1/DELETIONDATAREQUEST?token=eVpSMTlCOW4wdDA1N3pFeA==
Method	POST
Attack	
Evidence	

Other Info	
Instances	1
Solution	Ensure that only one component in your stack: code, web server, application server, load balancer, etc. is configured to set or add a HTTP Strict-Transport-Security (HSTS) header.
Reference	https://datatracker.ietf.org/doc/html/rfc6797#section-8.1
CWE Id	319
WASC Id	15
Plugin Id	10035

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	https://fcbccpa-uat.msxint.com/api/getMSXIKeyAPI?Apikey=aSNASDBNMASDNMA,SDXM%20zd,JMM,M,89300P3O22_JSDSADSD_12948I9134
Method	POST
Attack	
Evidence	password
Other Info	userParam=userId userValue=Apiuser passwordParam=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	**Information Disclosure - Sensitive Information in URL**
Description	The request appeared to contain sensitive information leaked in the URL. This can violate PCI and most organizational compliance policies. You can configure the list of strings for this check to add or remove values specific to your environment.
URL	https://uat-ffc.msxi.com/DELETIONAPI/V1/DELETIONDATAREQUEST?token=eVpSMTlCOW4wdDA1N3pFeA==
Method	POST
Attack	
Evidence	token
Other Info	The URL contains potentially sensitive information. The following string was found via the pattern: token token
Instances	1
Solution	Do not pass sensitive information in URIs.
Reference	
CWE Id	200
WASC Id	13
Plugin Id	10024