Checkmarx - Swagger Authorization

Enabling Swagger use via ‘implicit’ flow creates a Security Vulnerability

December, 2021

Table of Contents

CxSAST and CxReportingService contain a Security Vulnerability

CxSAST and CxReportingService use an OAuth2 Authentication scheme called ‘implicit’ flow to enable their Swagger use. This is a known and reported Security Vulnerability as the technique exposes the Token through the HTTP/HTTPS flow and allows an attacher to obtain and use the token outside of its’ authorized and intended container.

Browser tools (such as ‘HTTP-TRACKER’ [FireFox]) can be used to intercept the HTTP/HTTPS ‘request’ and ‘response’ flows and expose the application Token.

Use this link for background on the various flows: https://auth0.com/docs/authorization/flows/which-oauth-2-0-flow-should-i-use

Use this link for an alternative to ‘implicit’ flow for Swagger use: https://auth0.com/docs/authorization/flows/authorization-code-flow-with-proof-key-for-code-exchange-pkce

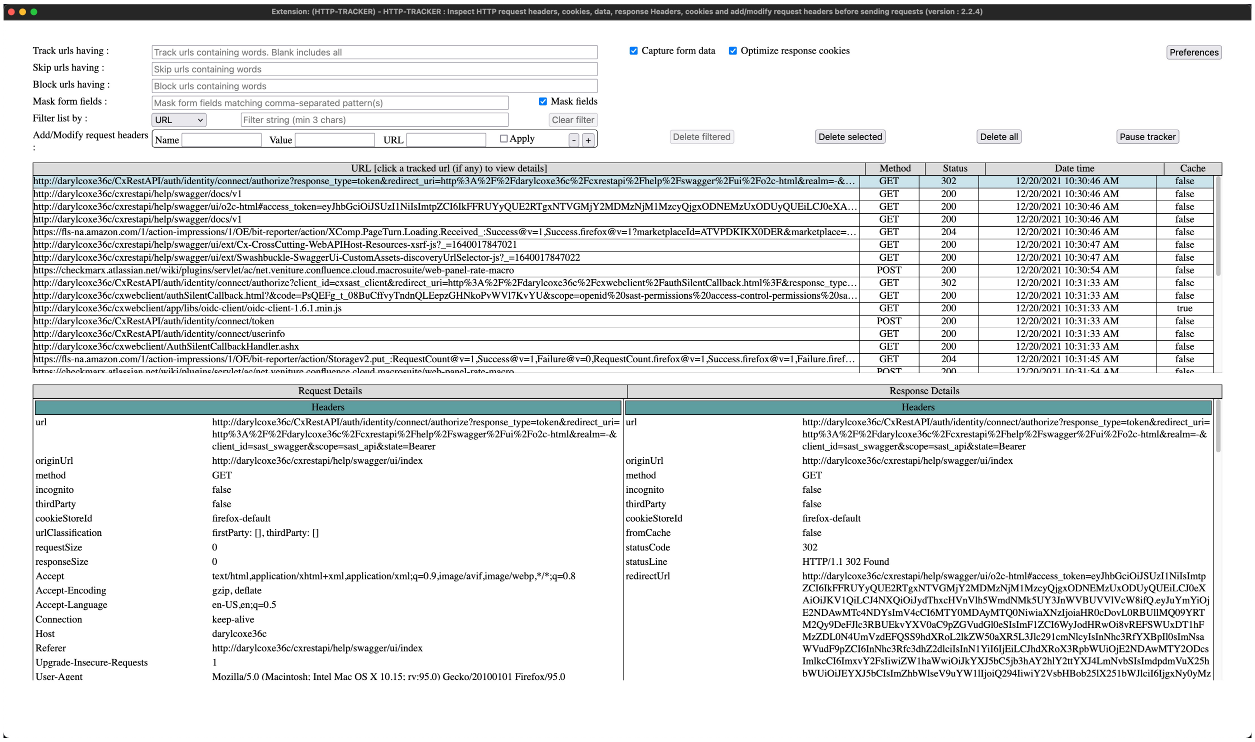
'Quick' Token stealing step(s)

{This example uses Firefox as the browser}

Step(s) to 'steal' an application Token:

1. Open the browser and go to the CxSAST 'login' page.
2. 'Login' to the CxSAST application.
3. Open a new browser tab and go to the appropriate CxReportingService Swagger page.
4. On the Swagger page, click on the 'Authorize' button.
5. Bring up the page with the HTTP-TRACKER extension.
6. In the HTTP-TRACKER page, delete ALL existing records.
7. Back on the Swagger page, select all authentications, click on 'Login'.
8. The HTTP-TRACKER extension will have intercepted the 'token' auth call, from the 302 response obtain the application token from the redirect URI in the headers.
9. Use the obtained token for the rest of the remaining token lifetime.

Example - HTTP-TRACKER 302 Response:



Extension: (HTTP-TRACKER) - HTTP-TRACKER : Inspect HTTP request headers, cookies, data, response Headers, cookies and add/modify request headers before sending requests (version : 2.2.4)

Track urls having : Track urls containing words. Blank includes all
Skip urls having : Skip urls containing words
Block urls having : Block urls containing words
Mask form fields : Mask form fields matching comma-separated pattern(s)
Filter list by : URL
Filter string (min 3 chars)
Clear filter
Add/Modify request headers : Name Value URL
Delete filtered
Delete selected
Delete all
Pause tracker
Preferences

☑ Capture form data ☑ Optimize response cookies

☑ Mask fields

□ Apply

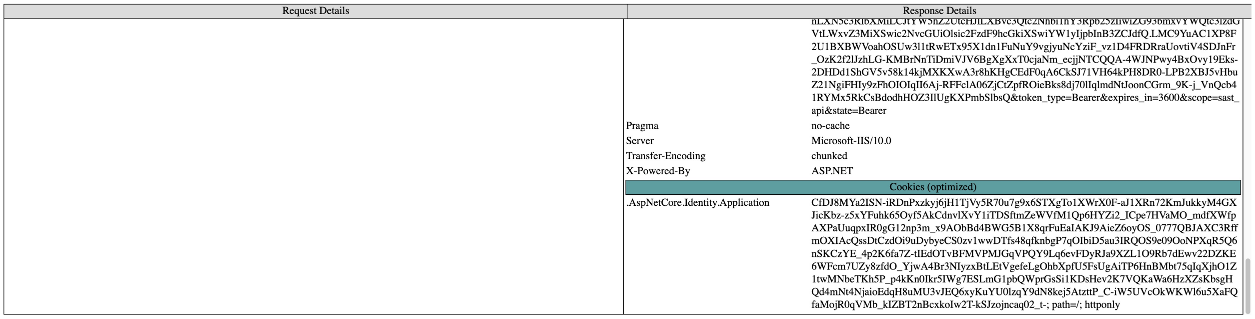
URL [click a tracked url (if any) to view details]	Method	Status	Date time	Cache
http://darylcoxe36c/CxRestAPI/auth/identity/connect/authorize?response_type=token&redirect_uri=http%3A%2F%2Fdarylcoxe36c%2Fcxrestapi%2Fhelp%2Fswagger%2Fui%2Fo2c-html&realm=-&…	GET	302	12/20/2021 10:30:46 AM	false
http://darylcoxe36c/cxrestapi/help/swagger/docs/v1	GET	200	12/20/2021 10:30:46 AM	false
http://darylcoxe36c/cxrestapi/help/swagger/ui/o2c-html#access_token=eyJhbGciOiJSUzI1NiIsImtpZCI6IkFFRUYyQUE2RTgxNTVGMjY2MDMzNjM1MzcyQjgxODNEMzUxODUyQUEiLCJ0eXA…	GET	200	12/20/2021 10:30:46 AM	false
http://darylcoxe36c/cxrestapi/help/swagger/docs/v1	GET	200	12/20/2021 10:30:46 AM	false
https://fls-na.amazon.com/1/action-impressions/1/OE/bit-reporter/action/XComp.PageTurn.Loading.Received_:Success@v=1,Success.firefox@v=1?marketplaceId=ATVPDKIKX0DER&marketplace=…	GET	204	12/20/2021 10:30:46 AM	false
http://darylcoxe36c/cxrestapi/help/swagger/ui/ext/Cx-CrossCutting-WebAPIHost-Resources-xsrf-js?_=1640017847021	GET	200	12/20/2021 10:30:47 AM	false
http://darylcoxe36c/cxrestapi/help/swagger/ui/ext/Swashbuckle-SwaggerUi-CustomAssets-discoveryUrlSelector-js?_=1640017847022	GET	200	12/20/2021 10:30:47 AM	false
https://checkmarx.atlassian.net/wiki/plugins/servlet/ac/net.veniture.confluence.cloud.macrosuite/web-panel-rate-macro	POST	200	12/20/2021 10:30:54 AM	false
http://darylcoxe36c/CxRestAPI/auth/identity/connect/authorize?client_id=cxsast_client&redirect_uri=http%3A%2F%2Fdarylcoxe36c%2Fcxwebclient%2FauthSilentCallback.html%3F&response_type…	GET	302	12/20/2021 10:31:33 AM	false
http://darylcoxe36c/cxwebclient/authSilentCallback.html?&code=PsQEFg_t_08BuCffvyTndnQLEepzGHNkoPvWVl7KvYU&scope=openid%20sast-permissions%20access-control-permissions%20sa…	GET	200	12/20/2021 10:31:33 AM	false
http://darylcoxe36c/cxwebclient/app/libs/oidc-client/oidc-client-1.6.1.min.js	GET	200	12/20/2021 10:31:33 AM	true
http://darylcoxe36c/CxRestAPI/auth/identity/connect/token	POST	200	12/20/2021 10:31:33 AM	false
http://darylcoxe36c/CxRestAPI/auth/identity/connect/userinfo	GET	200	12/20/2021 10:31:33 AM	false
http://darylcoxe36c/cxwebclient/AuthSilentCallbackHandler.ashx	GET	200	12/20/2021 10:31:33 AM	false
https://fls-na.amazon.com/1/action-impressions/1/OE/bit-reporter/action/Storagev2.put_:RequestCount@v=1,Success@v=1,Failure@v=0,RequestCount.firefox@v=1,Success.firefox@v=1,Failure.firef…	GET	204	12/20/2021 10:31:45 AM	false
https://checkmarx.atlassian.net/wiki/plugins/servlet/ac/net.veniture.confluence.cloud.macrosuite/web-panel-rate-macro	POST	200	12/20/2021 10:31:54 AM	false

Request Details

Headers	
url	http://darylcoxe36c/CxRestAPI/auth/identity/connect/authorize?response_type=token&redirect_uri=http%3A%2F%2Fdarylcoxe36c%2Fcxrestapi%2Fhelp%2Fswagger%2Fui%2Fo2c-html&realm=-&client_id=sast_swagger&scope=sast_api&state=Bearer
originUrl	http://darylcoxe36c/cxrestapi/help/swagger/ui/index
method	GET
incognito	false
thirdParty	false
cookieStoreId	firefox-default
urlClassification	firstParty: [], thirdParty: []
requestSize	0
responseSize	0
Accept	text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Encoding	gzip, deflate
Accept-Language	en-US,en;q=0.5
Connection	keep-alive
Host	darylcoxe36c
Referer	http://darylcoxe36c/cxrestapi/help/swagger/ui/index
Upgrade-Insecure-Requests	1
User-Agent	Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:95.0) Gecko/20100101 Firefox/95.0

Response Details

Headers	
url	http://darylcoxe36c/CxRestAPI/auth/identity/connect/authorize?response_type=token&redirect_uri=http%3A%2F%2Fdarylcoxe36c%2Fcxrestapi%2Fhelp%2Fswagger%2Fui%2Fo2c-html&realm=-&client_id=sast_swagger&scope=sast_api&state=Bearer
originUrl	http://darylcoxe36c/cxrestapi/help/swagger/ui/index
method	GET
incognito	false
thirdParty	false
cookieStoreId	firefox-default
fromCache	false
statusCode	302
statusLine	HTTP/1.1 302 Found
redirectUrl	http://darylcoxe36c/cxrestapi/help/swagger/ui/o2c-html#access_token=eyJhbGciOiJSUzI1NiIsImtpZCI6IkFFRUYyQUE2RTgxNTVGMjY2MDMzNjM1MzcyQjgxODNEMzUxODUyQUEiLCJ0eXAiOiJKV1QiLCJ4NXQiOiJydThxcHVnVlh5WmdNMk5UY3JnWVBUVVlVcW8ifQ.eyJuYmYiOjE2NDAwMTc4NDYsImV4cCI6MTY0MDAyMTQ0NiwiaXNzIjoiaHR0cDovL0RBUllMQ09YRTM2Qy9DeFJlc3RBUEkvYXV0aC9pZGVudGl0eSIsImF1ZCI6WyJodHRwOi8vREFSWUxDT1hFMzZDL0N4UmVzdEFQSS9hdXRoL2lkZW50aXR5L3Jlc291cmNlcyIsInNhc3RfYXBpIl0sImNsaWVudF9pZCI6InNhc3Rfc3dhZ2dlciIsInN1YiI6IjEiLCJhdXRoX3RpbWUiOjE2NDAwMTY2ODcsImlkcCI6ImxvY2FsIiwiZW1haWwiOiJkYXJ5bC5jb3hAY2hlY2ttYXJ4LmNvbSIsImdpdmVuX25hbWUiOiJEYXJ5bCIsImZhbWlseV9uYW1lIjoiQ294IiwiY2VsbHBob25lX251bWJlciI6IjgxNy0yMz



Request Details

Response Details

	nLXN5c3RlbXMiLCJtYW5hZ2UtcHJlLXBvc3Qtc2Nhbi1hY3Rpb25zIiwiZG93bmxvYWQtc3lzdGVtLWxvZ3MiXSwic2NvcGUiOlsic2FzdF9hcGkiXSwiYW1yIjpbInB3ZCJdfQ.LMC9YuAC1XP8F2U1BXBWVoahOSUw3l1tRwETx95X1dn1FuNuY9vgjyuNcYziF_vz1D4FRDRraUovtiV4SDJnFr_OzK2f2lJzhLG-KMBrNnTiDmiVJV6BgXgXxT0cjaNm_ecjjNTCQQA-4WJNPwy4BxOvy19Eks-2DHDd1ShGV5v58k14kjMXKXwA3r8hKHgCEdF0qA6CkSJ71VH64kPH8DR0-LPB2XBJ5vHbuZ21NgiFHIy9zFhOIOIqII6Aj-RFFclA06ZjCtZpfROieBks8dj70lIqlmdNtJoonCGrm_9K-j_VnQcb41RYMx5RkCsBdodhHOZ3IlUgKXPmbSlbsQ&token_type=Bearer&expires_in=3600&scope=sast_api&state=Bearer
Pragma	no-cache
Server	Microsoft-IIS/10.0
Transfer-Encoding	chunked
X-Powered-By	ASP.NET

Cookies (optimized)	
.AspNetCore.Identity.Application	CfDJ8MYa2ISN-iRDnPxzkyj6jH1TjVy5R70u7g9x6STXgTo1XWrX0F-aJ1XRn72KmJukkyM4GXJicKbz-z5xYFuhk65Oyf5AkCdnvlXvY1iTDSftmZeWVfM1Qp6HYZi2_ICpe7HVaMO_mdfXWfpAXPaUuqpxIR0gG12np3m_x9AObBd4BWG5B1X8qrFuEaIAKJ9AieZ6oyOS_0777QBJAXC3RffmOXIAcQssDtCzdOi9uDybyeCS0zv1wwDTfs48qfknbgP7qOIbiD5au3IRQOS9e09OoNPXqR5Q6nSKCzYE_4p2K6fa7Z-tIEdOTvBFMVPMJGqVPQY9Lq6evFDyRJa9XZL1O9Rb7dEwv22DZKE6WFcm7UZy8zfdO_YjwA4Br3NIyzxBtLEtVgefeLgOhbXpfU5FsUgAiTP6HnBMbt75qIqXjhO1Z1twMNbeTKh5P_p4kKn0Ikr5IWg7ESLmG1pbQWprGsSi1KDsHev2K7VQKaWa6HzXZsKbsgHQd4mNt4NjaioEdqH8uMU3vJEQ6xyKuYU0lzqY9dN8kej5AtzttP_C-iW5UVcOkWKWl6u5XaFQfaMojR0qVMb_kIZBT2nBcxkoIw2T-kSJzojncaq02_t-; path=/; httponly

Remediation Suggestion

Replace the OAuth2 Authentication ‘implicit’ flow with the Authorization Code Flow with PKCE (Proof Key for Code Exchange).

Use this link for an overview of Auth Code flow with PKCE: https://auth0.com/docs/authorization/flows/authorization-code-flow-with-proof-key-for-code-exchange-pkce

Use this link for a ‘Single Page App’ QuickStart: https://auth0.com/docs/quickstart/spa