

## Regarding the JWT Zap Scanner

9 messages

yaakov beckerman <beckermanyaakov@gmail.com> To: preetkaran20@gmail.com <preetkaran20@gmail.com> Tue, 4 Jan, 2022 at 10:03 pm

Hi there

I'm trying to create a vulnerable API which includes JWT vulnerabilities. Unfortunately I haven't been able to trigger a JWT alert no matter what I try. Do you know what sort of request would trigger one?

Karan Preet <preetkaran20@gmail.com> To: yaakov beckerman <beckermanyaakov@gmail.com> Tue, 4 Jan, 2022 at 10:32 pm

Hi Yaakov,

It is tough to help without much context however here are a few things:

1. Have you installed JWT addon from Marketplace?

2. Is your JWT signed by RSA? if so you need to configure RSA Key, Please look at https://github.com/SasanLabs/owaspzap-jwt-addon#scanner-configuration for more details.

3. Are you using an Active scanner or fuzzer?

4. Can you please send me the JWT token so that I can look more into it?

One simple way to generate the vulnerable JWT token is using HMac based token with a key from https://github.com/ SasanLabs/owasp-zap-iwt-addon/blob/master/src/main/resources/weakKeys/wallarm\_jwt\_hmac\_secrets\_list location.

Please let me know if you still have any questions, I will try to help you.

thanks, Karan [Quoted text hidden]

yaakov beckerman <beckermanyaakov@gmail.com> To: Karan Preet <preetkaran20@gmail.com>

Tue, 4 Jan, 2022 at 10:50 pm

Tue, 4 Jan, 2022 at 11:46 pm

Hi, thanks for your quick response.

1) I've installed the JWT addon

2) I only want to test the server side aspect of the JWT scanner (I'm creating a vulnerable NodeJS server) 3) I'm using the Active Scanner

4) The JWT is - eyJhbGciOiJIUzI1NiIsInR5cCl6lkpXVCJ9.eyJzdWliOilxMjM0NTY3ODkwliwibm FtZSI6lkpvaG4gRG9lliwiaWF0ljoxNTE2MjM5MDlyfQ.SflKxwRJSMeKKF2QT4fwpMeJf36P0k6yJV\_adQssw5c It's the default token that's created with jwt.io and uses HS256.

I've already tried changing the attack strength/alert threshold but I can't get any alerts to be triggered. Do you know what response the server should return in order for the JWT scanner to alert that there's a vulnerability. I don't care if it's the most contrived example.

Thanks Yaakov [Quoted text hidden]

Karan Preet <preetkaran20@gmail.com> To: yaakov beckerman <beckermanyaakov@gmail.com> thanks for sharing the JWT token. Actually, for validating the JWT token, the addon sends the same request with manipulated tokens and it expects that the target application returns the same status code and response body, then only it considers that the application is vulnerable.

Does your application send the same response for the same request with just manipulated headers? Have a look at code: https://github.com/SasanLabs/owasp-zap-jwt-addon/blob/cb0b85efa9c291e3a5eeb35b755e7f bc35c4f2bc/src/main/java/org/zaproxy/zap/extension/jwt/JWTActiveScanRule.java#L192-L196

Also if you are writing vulnerable code then have a look at https://github.com/SasanLabs/VulnerableApp/tree/ master/src/main/java/org/sasanlabs/service/vulnerability/jwt code which i created to test JWT scanner.

thanks, Karan

[Quoted text hidden]

yaakov beckerman <beckermanyaakov@gmail.com> To: Karan Preet <preetkaran20@gmail.com>

Hi,

The issue that I'm encountering is that the JWT scanner isn't actually sending requests. When I look at the active scanner progress, it shows that the JWT scanner made 0 requests. Is there some sort of pre-condition for the JWT scanner to attempt some requests? For example, does the header with the token have to be in a specific format? [Quoted text hidden]

## Karan Preet <preetkaran20@gmail.com> To: yaakov beckerman <beckermanyaakov@gmail.com>

Hi Yaakov,

Oh ok, I don't think there is any except that the token is valid. code: https://github.com/SasanLabs/owasp-zap-jwt-addon/ blob/cb0b85efa9c291e3a5eeb35b755e7fbc35c4f2bc/src/main/java/org/zaproxy/zap/extension/jwt/ JWTActiveScanRule.java#L79-L81

## One question, does your original request contains valid JWT token? [Quoted text hidden]

## **yaakov beckerman** <beckermanyaakov@gmail.com> To: Karan Preet preetkaran20@gmail.com>

Here is my exact flow.	
1) Create a request manually in the requester tool which contains the	he JWT token I sent you
<pre>GET http://localhost:3003/api/v1/stats/logs HTTP/1.1 Host: localhost:3003 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:92.0) Gecko/20100101 Firefox/92.0 Pragma: no-cache Cache-Control: no-cache Authorization: Bearer eyJhbGci0iJIUzI1NiIsInR5cCI6IkpXVCJ9. eyJzdWI10iIxMjM0NTY30DkwIiwibmFtZ5I6IkpvaG4gRG9lIiwiaWF0IjoxNTE2MjM5MDIyfQ. SflKxwRJSMeKKF2QT4fwpMeJf36P0k6yJV_adQssw5c Content-Length: 0 </pre>	HTTP/1.1 200 OK X-Powered-By: Express Access-Control-Allow-Origin: * Content-Type: application/json; charset utf-8 Content-Length: 20 ETag: W/"14-VX693CeUFaY21xsj05kbqUc4auo Date: Tue, 04 Jan 2022 18:23:19 GMT Connection: keep-alive Keep-Alive: timeout=5
	[{"ip": "127.0.0.1"}]

Tue, 4 Jan, 2022 at 11:49 pm

Wed, 5 Jan, 2022 at 12:02 am

Wed, 5 Jan, 2022 at 12:10 am

	Active Scan			
Scope Input Vectors Custo	om Vectors Technology Policy	Filter Seque	ence	
<ul> <li>Policy</li> <li>Client Browser</li> <li>Information Gathering</li> <li>Injection</li> <li>Miscellaneous</li> <li>Server Security</li> </ul>	Policy       Default Polic         Policy:       Default Polic         Default Alert Threshold:       Medium          Default Attack Strength:       Insane          Apply       Default          Apply       Default          Threshold To       All         Apply       Default          Strength To       All         Client Browser       Information Gathering         Injection       Miscellaneous         Server Security       Server Security	(Default thresh (MUCH more a VRules VRules	Attacks) Go Go reshold Ilt C Ilt C Ilt C Ilt C	Strength Default Default Default Default Default
	Active Scan om Vectors Technology Policy	Start Scan Filter Sequ	Reset	Cancel
<ul> <li>Policy Client Browser Information Gathering Injection Miscellaneous Server Security</li> </ul>	Miscellaneous Test Name ^ An example active scan rule which Bypassing 403 Example Active Scan Rule: Denial o External Redirect Generic Padding Oracle GET for POST HTTP Only Site HTTPS Content Available via HTTP JWT Scan Rule Log4Shell (CVE-2021-44228) Script Active Scan Rules Session Fixation SOAP Action Spoofing SOAP XML Injection Web Cache Deception	Default	Strength Default Default Default Default Default Default Default Default Default Default Default Default Default Default Default Default Default	Quality Alpha Alpha Alpha Release Beta Beta Beta Alpha Alpha Release Beta Alpha Alpha Alpha Alpha
	·	Start Scan	Reset	Cancel

3) When I look at the progress report, I see that the JWT scanner didn't send out any requests.

۹ 🗙	Miscellaneous			
<ul> <li>Policy</li> <li>Client Browser</li> </ul>	Test Name $\wedge$	Threshold	Strength	Quality
Information Gathering Injection Miscellaneous Server Security	An example active scan rule which Bypassing 403 Example Active Scan Rule: Denial o External Redirect Generic Padding Oracle GET for POST HTTP Only Site HTTPS Content Available via HTTP JWT Scan Rule Log4Shell (CVE-2021-44228) Script Active Scan Rules Session Fixation SOAP Action Spoofing SOAP XML Injection Web Cache Deception	Default	Default Default Default Default Default Default Default Default Default Default Default Default Default Default Default Default	Alpha Alpha Alpha Release Beta Beta Beta Alpha Release Beta Alpha Alpha Alpha

I also manually verified that the response is exactly the same no matter what JWT is sent (as long as a JWT is actually sent) [Quoted text hidden]

Karan Preet <preetkaran20@gmail.com> To: yaakov beckerman <beckermanyaakov@gmail.com>

Hi Yaakov,

Can we connect over a call? https://meet.google.com/tmf-rodz-nnb

thanks, Karan [Quoted text hidden]

**Karan Preet** <preetkaran20@gmail.com> To: yaakov beckerman <br/> <br/>beckermanyaakov@gmail.com>

Sorry, https://meet.google.com/khz-zhdb-cam one.

thanks, Karan [Quoted text hidden] Wed, 5 Jan, 2022 at 12:15 am

Wed, 5 Jan, 2022 at 12:16 am