New issue

rawchen/sims has a Unauthorized Arbitrary File Delete Vulnerability #2

Open

yingxiujie opened 3 weeks ago Owner

[Title]
rawchen/sims has a Unauthorized Arbitrary File Delete Vulnerability

[PRODUCT]
sims

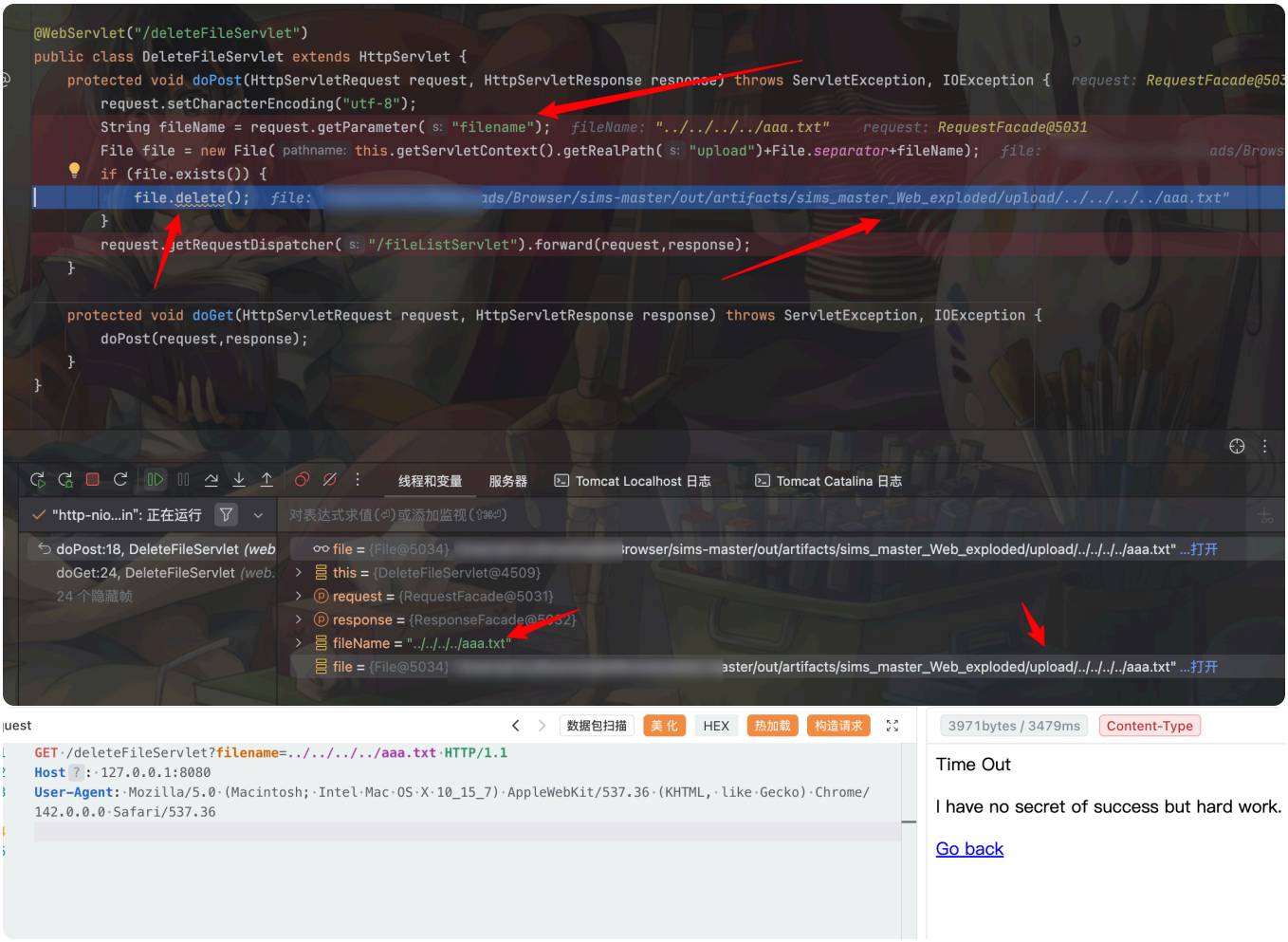
[TYPE]
Unauthorized Arbitrary File Delete Vulnerability

[DESCRIPTION]
Rawchen/sims has an unauthorized arbitrary file download vulnerability. This vulnerability is due to the deletionFileServlet routing of sims-master/src/web/servlet/file/DeleteFileServlet.java without permission management, and the file name entered by the user is not filtered, causing the attacker to delete server-critical files without permission, which may lead to system paralysis, data loss or even complete service failure.

ANALYZE：

First of all, analyze the permissions of the project. No permission verification was found for the DeleteFileServlet route, so you can directly access the DeleteFileServlet route under sims-master/src/web/servlet/file/DeleteFileServlet.java:

Enter the DeleteFileServlet route, which obtains the filename parameters entered by the user, and does not filter the parameters in any way, but directly splices the directory to delete the file content, resulting in unauthorized arbitrary file deletion vulnerabilities:



POC：

```
GET /downloadServlet?filename=../aaaa.txt HTTP/1.1
Host: 127.0.0.1:8080
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like G
```


Metadata

Assignees

No one assigned

Labels

No labels

Projects

No projects

Milestone

No milestone

Relationships

None yet

Development

No branches or pull requests

Participants