

请求

Raw 二进制 十六进制

GET /[redacted]38518848/download_url HTTP/1.1

Host: [redacted]

Connection: [redacted]

sec-ch-ua: "Google Chrome";v="107", "Chromium";v="107", "Not=A?Brand";v="24"

X-Version: 2.36.0

X-Signature: deb8f8795c68e8741b39226c71f7159a162bfb64

sec-ch-ua-mobile: ?0

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.0.0 Safari/537.36

Accept: application/json, text/plain, */*

X-Timestamp: 1682344440

X-Request-Id: 385f58582-5f8b-f08b-3052-bf1ea43b289

sec-ch-ua-platform: "Windows"

Origin: [redacted]

Sec-Fetch-Site: same-site

Sec-Fetch-Mode: cors

Sec-Fetch-Dest: empty

Referer: [redacted]

Accept-Encoding: [redacted]

Accept-Language: zh-CN;q=0.9

网络

响应

Raw 二进制 十六进制

X-Requested-With: XMLHttpRequest

Authorization: [redacted]

Content-Type: application/json; charset=UTF-8

X-Request-Id: 385f58582-5f8b-f08b-3052-bf1ea43b289

X-Signature: deb8f8795c68e8741b39226c71f7159a162bfb64

X-Expire-In: 2591918

Access-Control-Allow-Methods: GET,POST,OPTIONS,DELETE,PUT,PUT

Access-Control-Allow-Origin: https://wx.zsxq.com

Access-Control-Expose-Headers: X-Expire-In

Cache-Control: no-store, no-cache, must-revalidate

Date: Mon, 24 Apr 2023 13:54:22 GMT

Expires: Thu, 19 Nov 1981 08:52:00 GMT

Pragma: no-cache

Server: openresty

Vary: Accept-Encoding,Origin

X-Frame-Options: SAMEORIGIN

Connection: close

Content-Length: 209

AjE [redacted] WT X

网络

找一下接口信息 找到一处接口泄露

[https://api-\[redacted\]1552818888442/files?count=9](https://api-[redacted]1552818888442/files?count=9)

[https://api-\[redacted\]1552818888442/files?count=9](https://api-[redacted]1552818888442/files?count=9)

一、详细说明： ↵

知识星球 星主为了防止某些人白嫖会设置三天新人权限，直到三天之后才可以查看星球全部主题。这个漏洞可以绕过三天新人权限越权下载所有文件完成白嫖↵

三天权限证明↵



二、漏洞证明： ↵

我们在下载文件的时候开启抓包 通过查看数据包发现下载哪个文件主要由这串数字控制↵