

Objective--Badge Manipulation (Part 2)

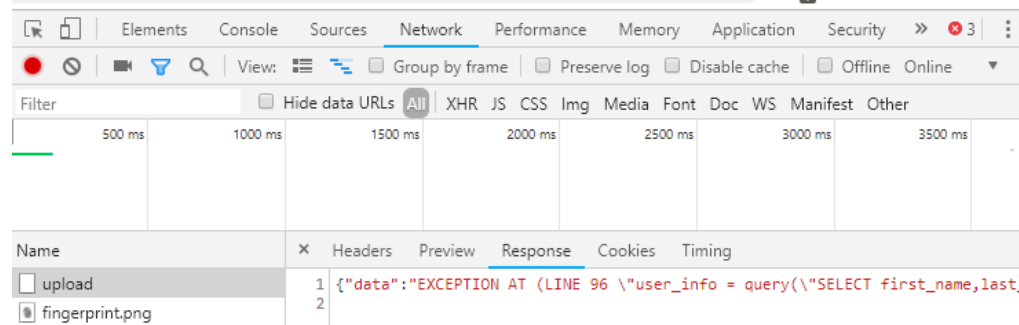
Solution (so far)

This query will generate the error we need.

```
aaa' OR 1=1
```

The entire error is:

```
"data": "EXCEPTION AT (LINE 96 \"user_info = query(\"SELECT first_name,last_name,enabled FROM employees WHERE authorized = 1 AND uid = '{}\" LIMIT 1\".format(uid))\"): (1064, u\"You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near '\" LIMIT 1' at line 1\")\", \"request\": false}
```



If you strip away the error message text, you have this:

```
SELECT first_name,last_name,enabled FROM employees WHERE authorized = 1 AND uid = '{} ' LIMIT 1
```

To proceed with the SQLI, you need to answer some questions.

Hand In

- 1) What does the application expect the query to return? (Hint: It is not "TRUE" or "FALSE")
- 2) Where will your input appear in the query? This is important because you can't modify what was there before you, only your entry point and the text after that.
- 3) If you wipe out everything after your input, will there be any unterminated quotes, parentheses, or the like?

- 4) You want to get rid of everything after the place where your code will go. Look at the type of database (see the error) and then determine what the comment symbol is. If you end your injection with a comment symbol, the rest of the query will be commented out.