SQL Injection was found in the **/onhs/admin/password-recovery.php** page of the **Online Nurse Hiring System Project, Allows remote attackers to execute arbitrary SQL command to get unauthorized database access via** the **mobileno** parameter in a POST HTTP request.

Official Website Project URL:
https://phpgurukul.com/?sdm_process_download=1&download_id=17826

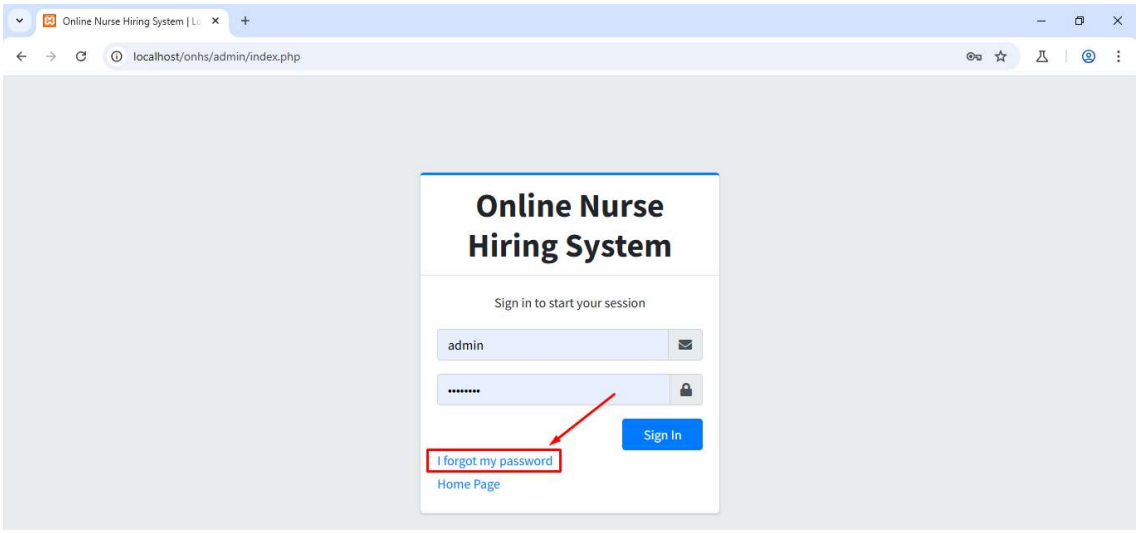
Affected Product Name

Online Nurse Hiring System

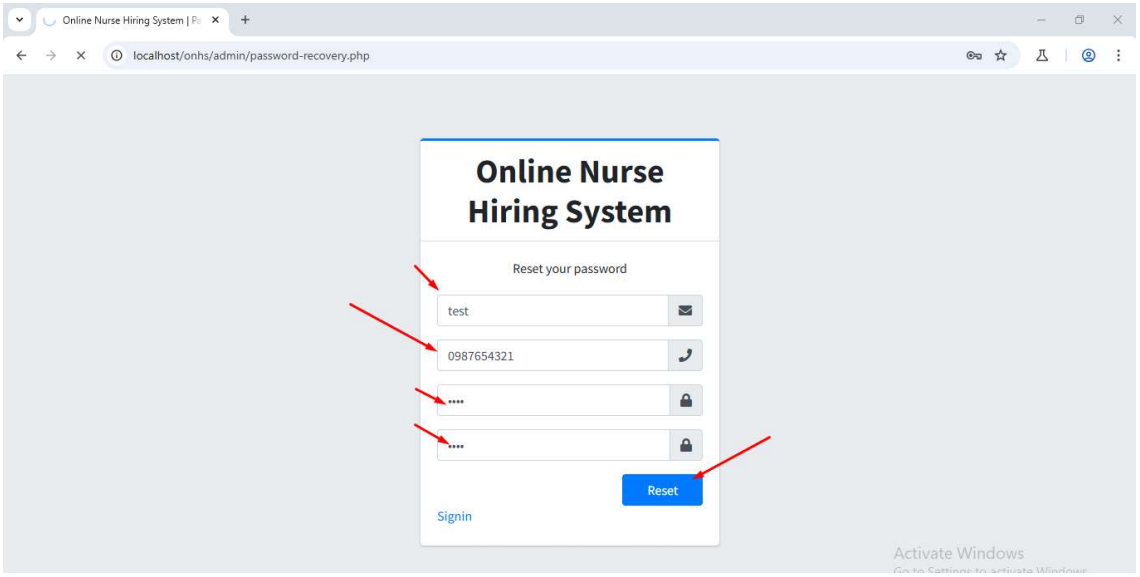
Affected End Point	**/onhs/admin/password-recovery.php**
Affected Parameter	**mobileno**
Method	POST
Type	Time based blind
Version	**V1.0**

Step to Reproduce:

Step 1: Visit to **Admin login** page then click on **forget password**



Step 2: Fill the form then click on **Reset** option

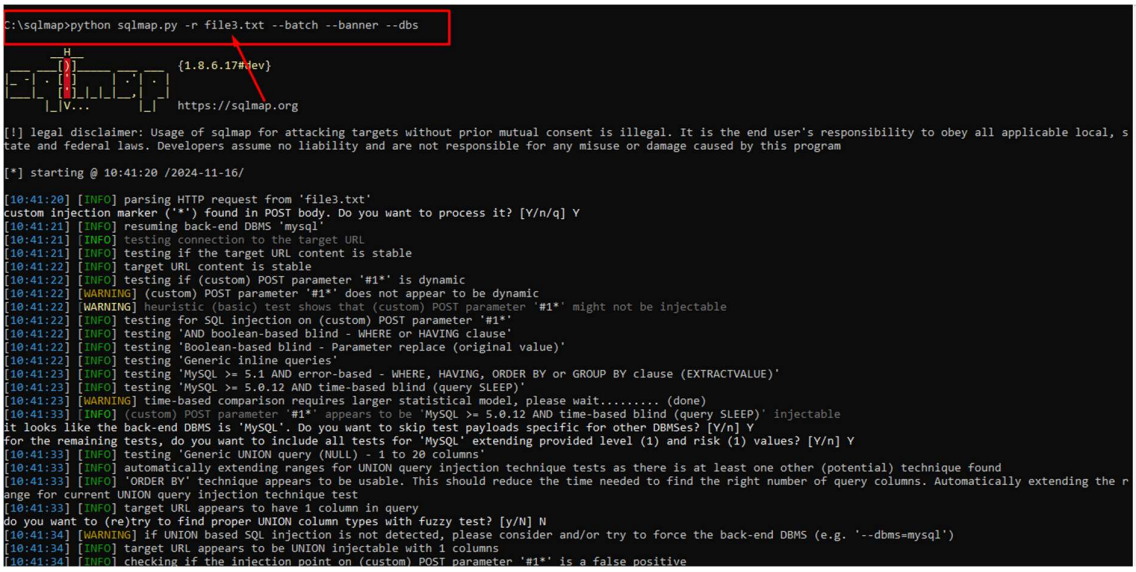


Step 3: Intercept the request through burpsuite and add * on mobileno Copy the request in **text** file and **save**

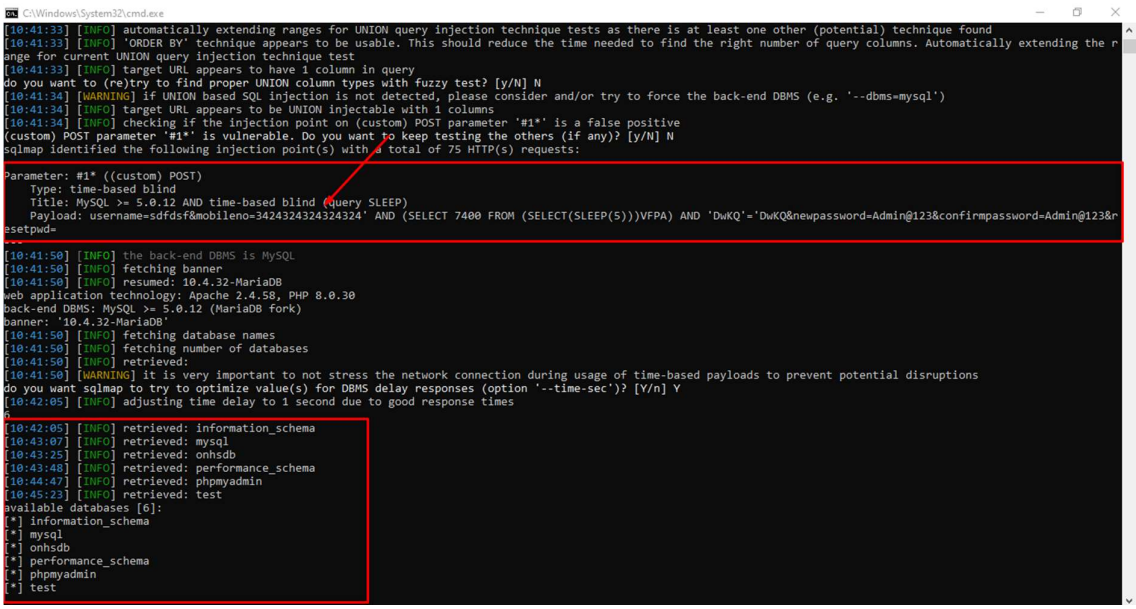
Note: we added * for checking specific point like: mobileno

Step 4: Now run the **sqlmap** command against request **saved** in file

python sqlmap.py -r file2.txt --batch --banner --dbs



Attacker is able to fetch **Database** which is listed below



Affected Point: mobileno

Mitigation:

https://portswigger.net/web-security/sql-injection#how-to-prevent-sql-injection