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

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

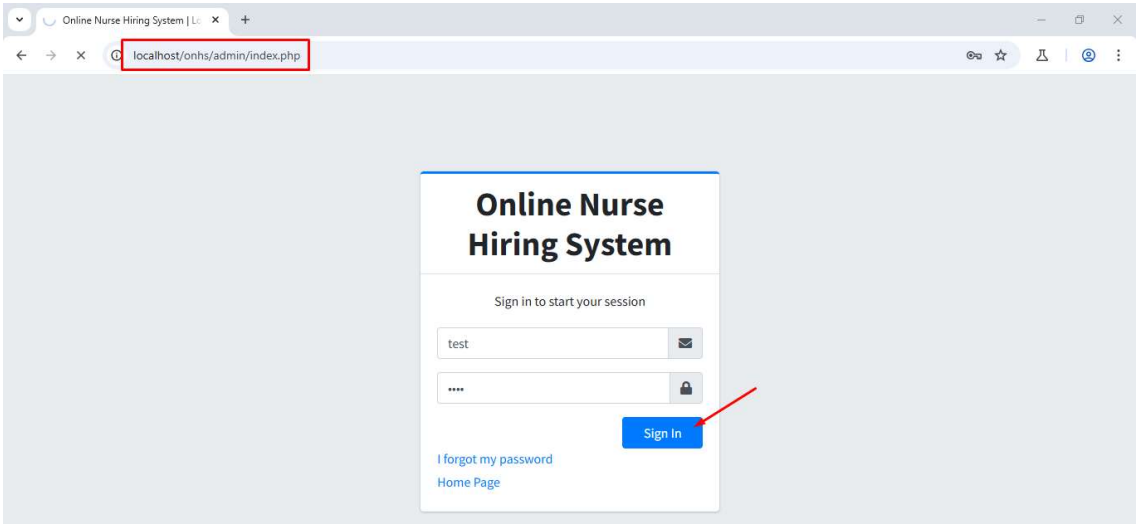
Affected Product Name

Online Nurse Hiring System

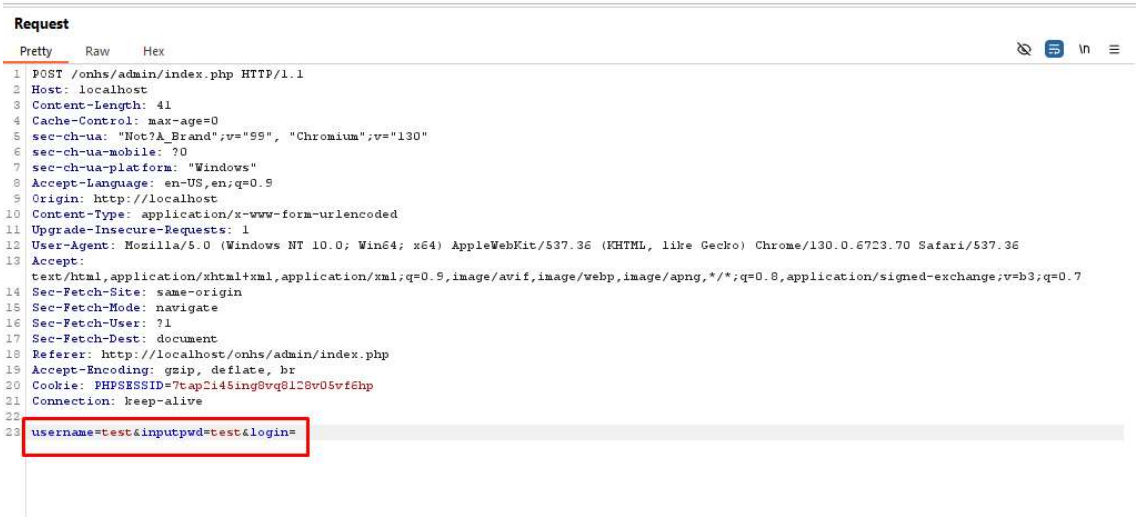
Affected End Point	**/onhs/admin/index.php**
Affected Parameter	**username**
Method	POST
Type	Boolean, Time based and UNION based
Version	**V1.0**

Step to Reproduce:

Step 1: Visit to **Admin login** page and enable burpsuite intercept and give **username** and **password** values with test then **click** on **Sign In**

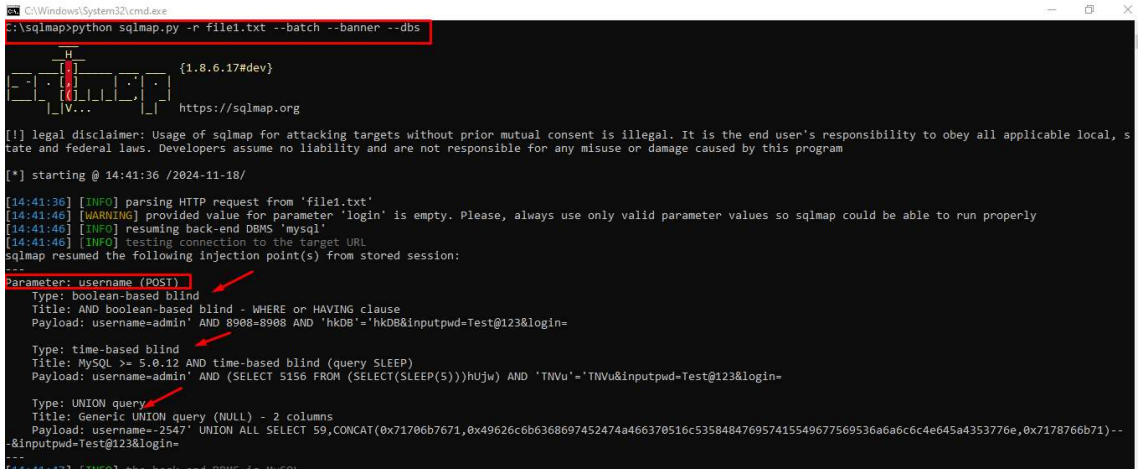


Step 2: Copy the request in **text** file and **save**

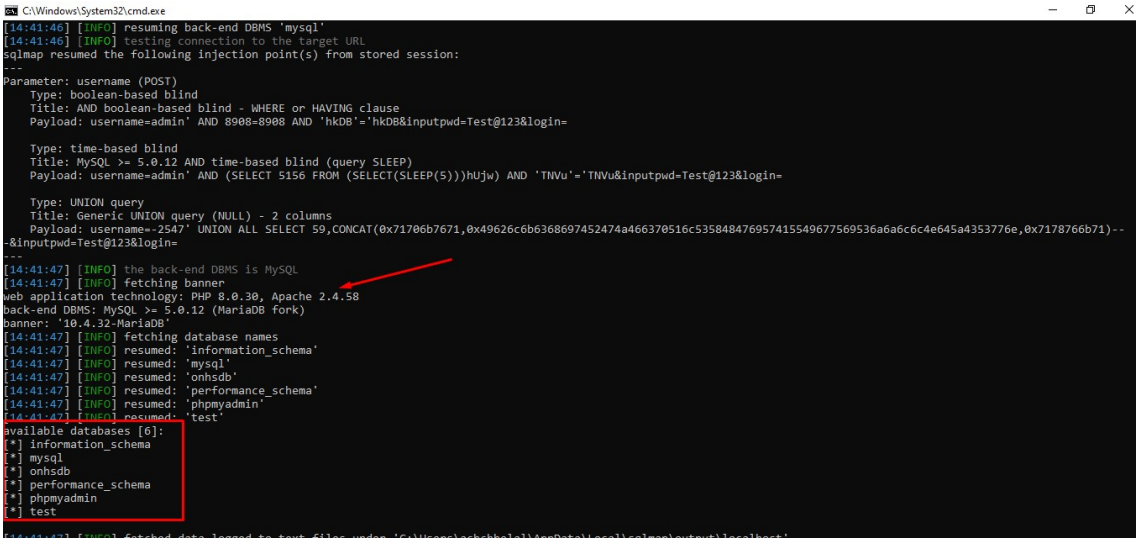


Step 3: Now run the **sqlmap** command against request **saved** in file

python sqlmap.py -r file1.txt --batch --banner --dbs



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



Affected Point: username

Mitigation:

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