1.Reporting

I used the tool called draw.io to create a network diagram.

1.1 Findings:

SQL injection was identified in the ID parameter of the SQli module. Malicious input allowed unauthorized database queries and data exposure.

Reflected XSS was found in the name parameter of the XSS (Reflected) module. Unsensitized input was reflected in the response, enabling script execution in the browser.

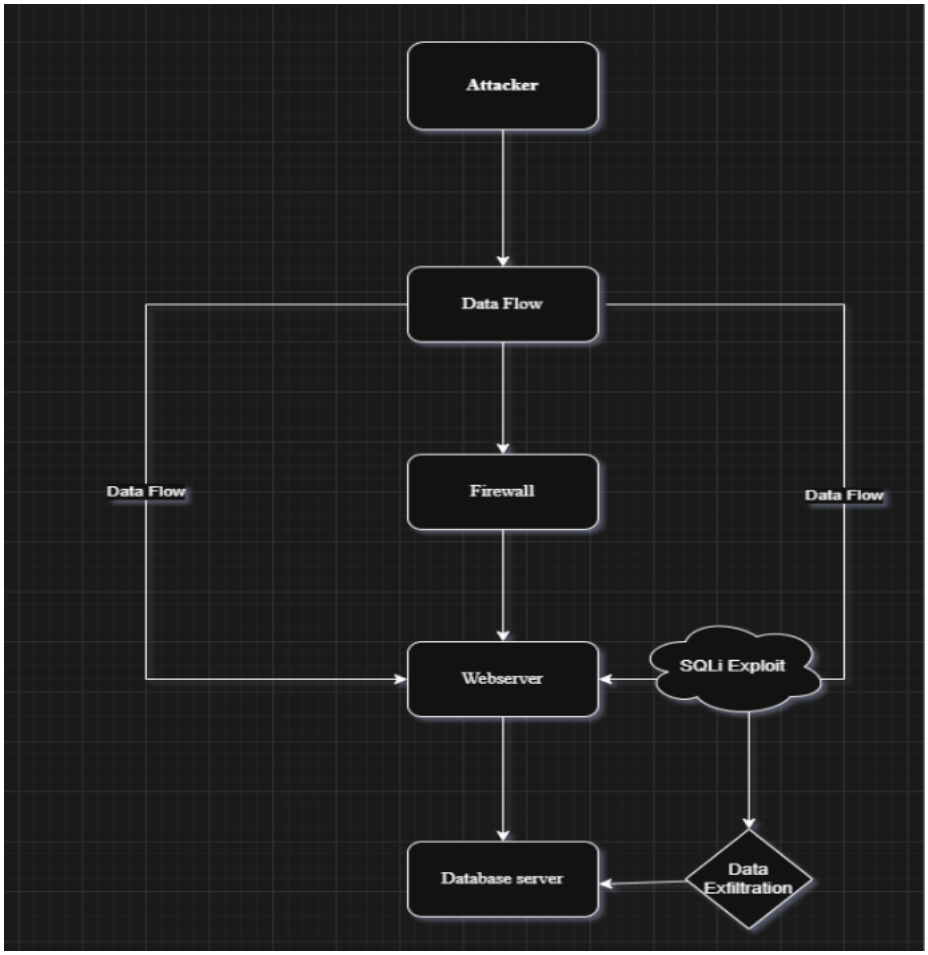
1.2 Remediation Plan:

- Upgrade DVWA to hardened version for training or isolate it from production networks.
- Conduct regular code reviews and automated security scans.
- Implement strict input validation and parameterized queries to prevent SQL injection.
-

ID	VULNERABILITY	CVSS SCORE	REMEDIATION
1	SQL injection	9.1	Input validation
2	XSS Reflected	7.5	Output Encoding & Sanitization

1.3 Network Diagram

I have created a network diagram based on finding the vulnerabilities as SQL injection and XSS Reflected.


Attacker
Data Flow
Firewall
Data Flow
Data Flow
Webserver
SQLi Exploit
Database server
Data Exfiltration