Vulnerability Assessment & Exploitation Report (PTES)

During the Application Vulnerability Analysis phase of the PTES methodology, a SQL Injection vulnerability was identified in the DVWA application at the endpoint /vulnerabilities/sqli/. The vulnerable id parameter failed to properly validate and sanitize user input, allowing malicious SQL queries to be executed against the backend database.

Using the automated tool **sqlmap**, the vulnerability was successfully exploited under a low-security configuration. The assessment confirmed the ability to enumerate databases, identify tables and columns, and dump sensitive data from the dvwa.users table. This demonstrates a full compromise of database confidentiality and highlights the potential for further attacks such as authentication bypass or data manipulation.

The impact of this vulnerability is **High**, as an attacker could access sensitive user credentials, escalate privileges, or leverage the database for lateral movement. The exploitation required no authentication beyond a valid session cookie, increasing the overall risk.

Remediation actions include implementing prepared statements, enforcing strict input validation, and applying the principle of least privilege to database accounts. Following remediation, a comprehensive rescan is strongly recommended to ensure the vulnerability has been effectively mitigated and no related injection points remain.