Damn Vulnerable Web Application (DVWA)

SQL INJECTION

Description:

The server is vulnerable to SQL injection which occurs when an attacker insert malicious SQL statements to data-driven applications. SQL injection help attackers to spoof identity, unauthorised access to user data, tamper with existing data, destroy the data or make it unavailable, allow the complete disclosure of all data on the system and even become the administrator of database server. An SQL injection vulnerability may attack any website or web application using an SQL database.

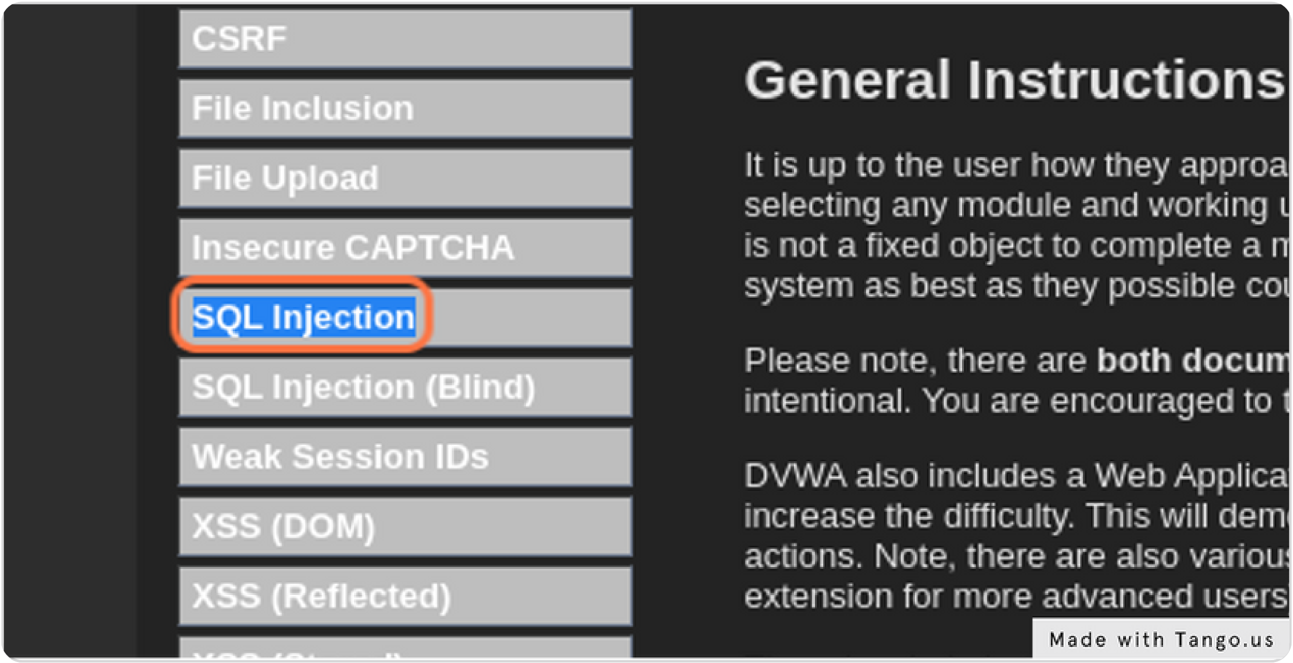
Solution :

Proper sanitation of database
Do not create SQL statements that include outside data
Use parameterised SQL calls

Occurrence

STEP 1

Click on SQL Injection



General Instructions

It is up to the user how they approa selecting any module and working u is not a fixed object to complete a m system as best as they possible cou

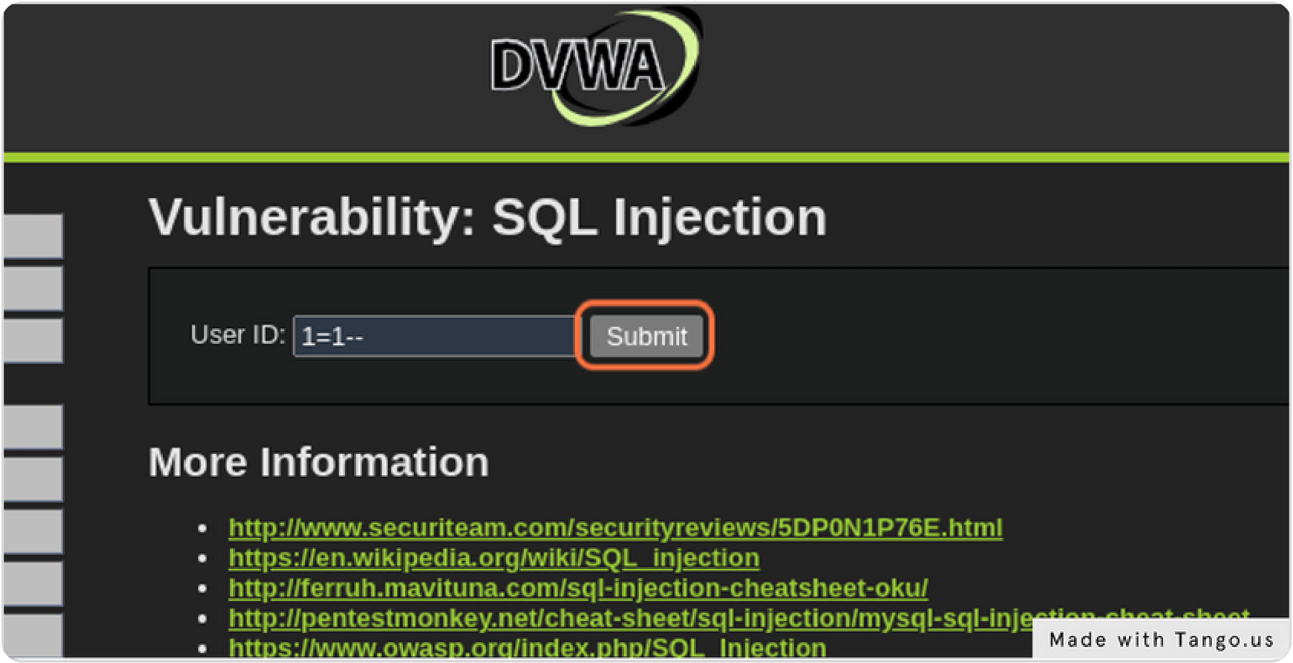
Please note, there are **both docum** intentional. You are encouraged to t

DVWA also includes a Web Applica increase the difficulty. This will dem actions. Note, there are also various extension for more advanced users

Made with Tango.us

STEP 2

Click on Submit



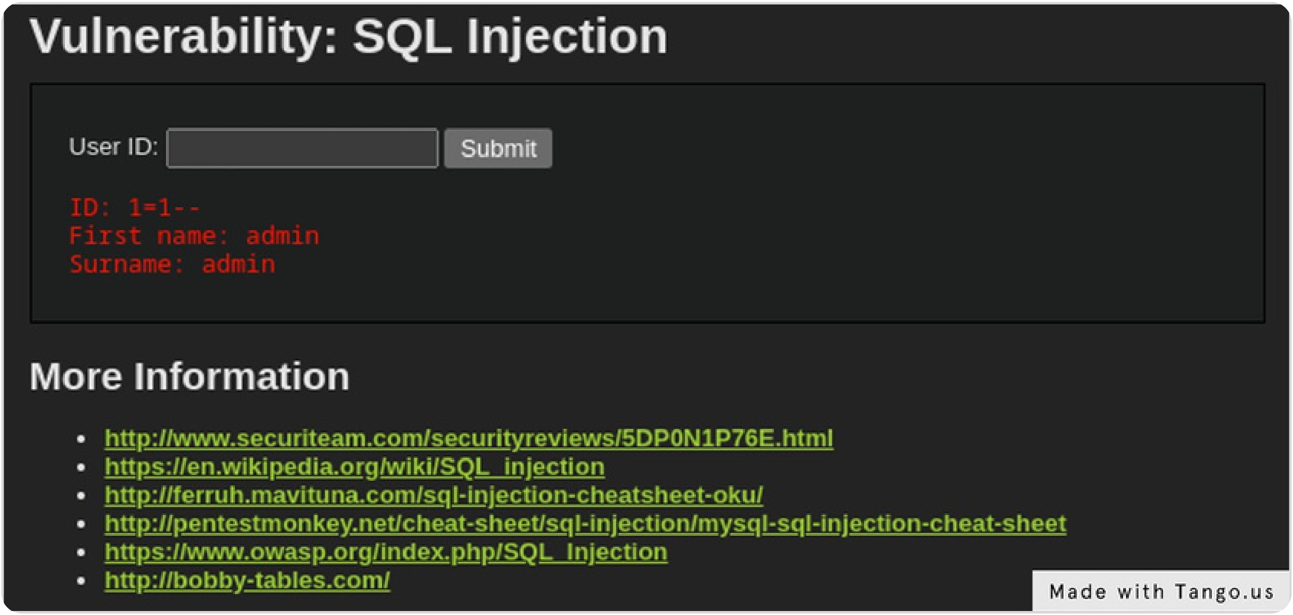
Vulnerability: SQL Injection

User ID: 1=1--

More Information

- http://www.securiteam.com/securityreviews/5DP0N1P76E.html
- https://en.wikipedia.org/wiki/SQL_injection
- http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/
- http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet
- https://www.owasp.org/index.php/SQL_Injection

Made with Tango.us



Vulnerability: SQL Injection

```
ID: 1=1--
First name: admin
Surname: admin
```

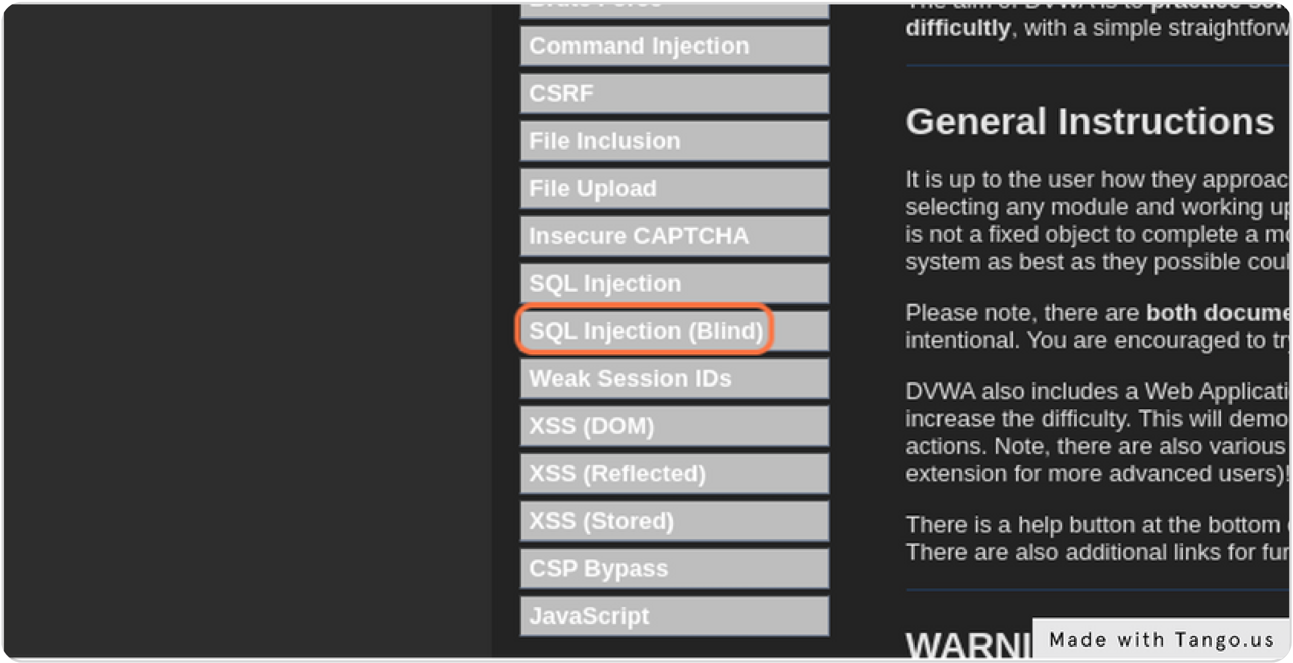
More Information

- http://www.securiteam.com/securityreviews/5DP0N1P76E.html
- https://en.wikipedia.org/wiki/SQL_injection
- http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/
- http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet
- https://www.owasp.org/index.php/SQL_Injection
- http://bobby-tables.com/

SQL Blind Injection

STEP 1

Click on SQL Injection (Blind)



difficultly, with a simple straightforw

General Instructions

It is up to the user how they approac selecting any module and working u is not a fixed object to complete a m system as best as they possible cou

Please note, there are **both docume** intentional. You are encouraged to tr

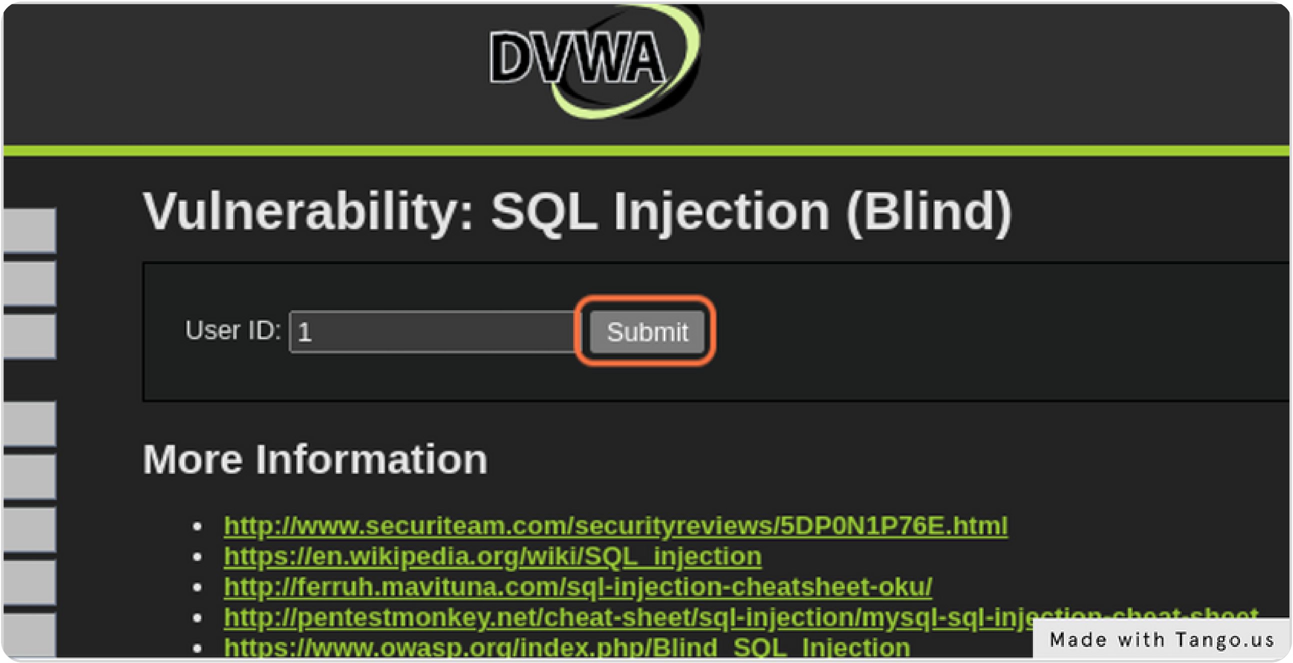
DVWA also includes a Web Applicati increase the difficulty. This will demo actions. Note, there are also various extension for more advanced users)!

There is a help button at the bottom There are also additional links for fu

WARNI

STEP 2

Click on Submit



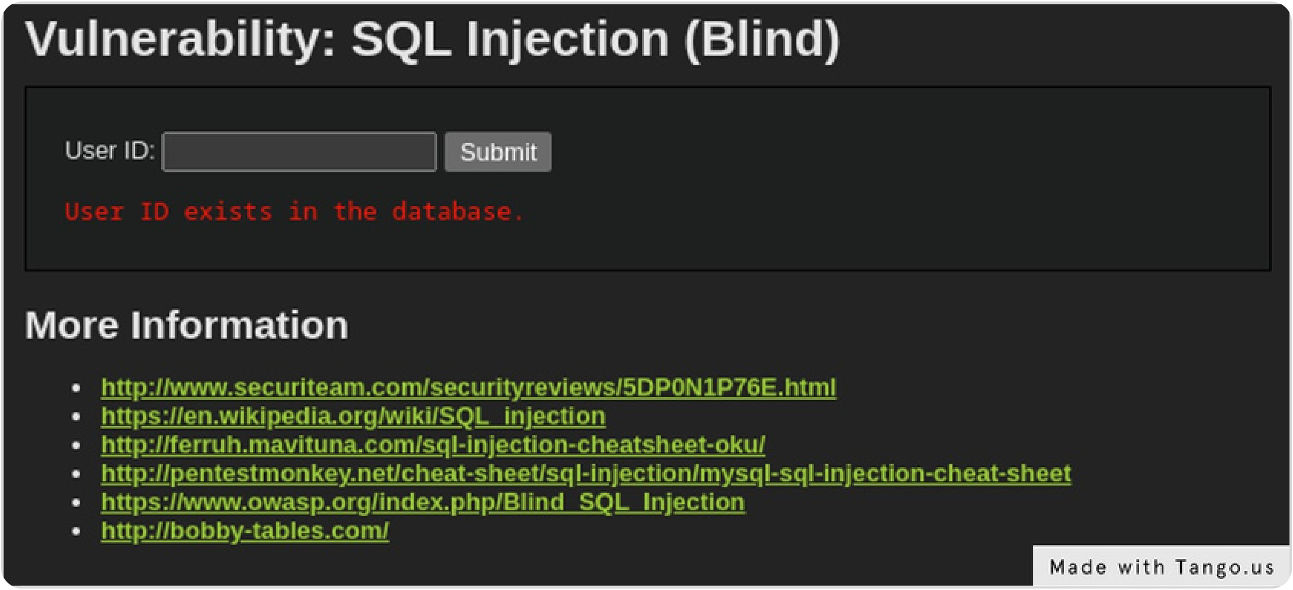
Vulnerability: SQL Injection (Blind)

User ID: 1

More Information

- http://www.securiteam.com/securityreviews/5DP0N1P76E.html
- https://en.wikipedia.org/wiki/SQL_injection
- http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/
- http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet
- https://www.owasp.org/index.php/Blind_SQL_Injection

STEP 3



Vulnerability: SQL Injection (Blind)

```
User ID exists in the database.
```

More Information

- http://www.securiteam.com/securityreviews/5DP0N1P76E.html
- https://en.wikipedia.org/wiki/SQL_injection
- http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/
- http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet
- https://www.owasp.org/index.php/Blind_SQL_Injection
- http://bobby-tables.com/