Vulnerability Scanner to detect SQL Injection Attacks

Astha Sharma

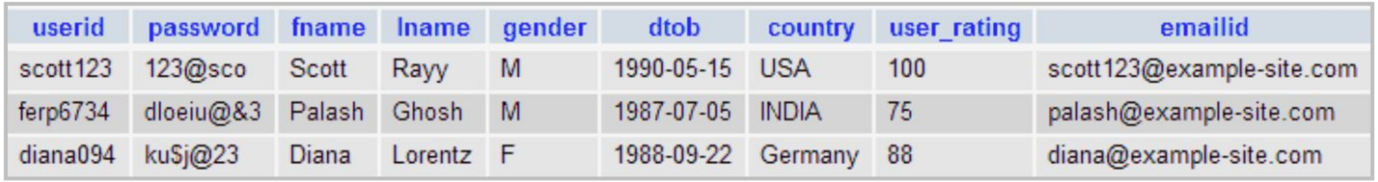
SQL Injection?

- A query used by hackers to steal the information from the database.

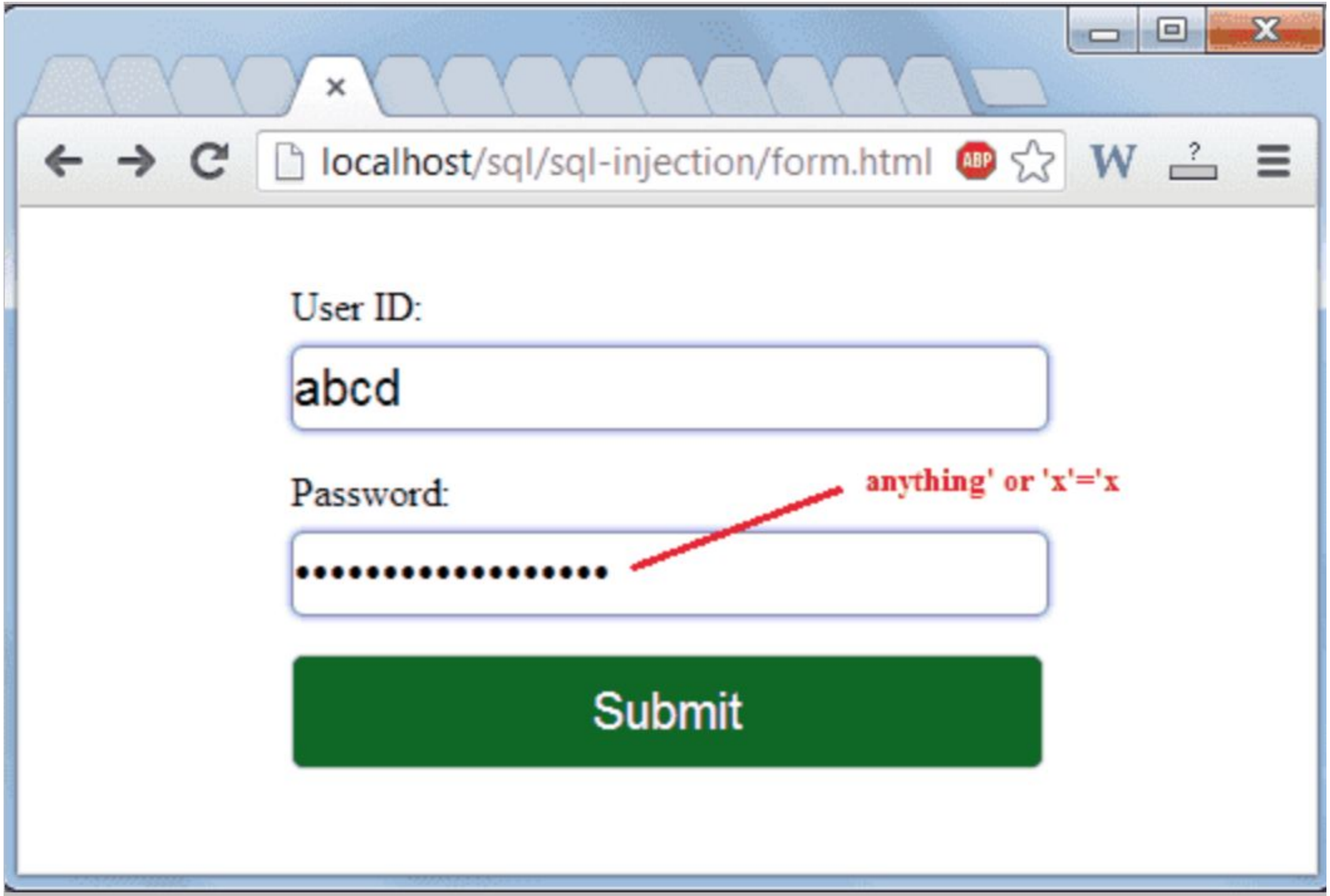
- It is a command of SQL which directly attacks on the database

Example:

```
$uid = $_POST['uid'];$pid = $_POST['passid'];$SQL = "select * from user_details where userid =
'$uid' and password = '$pid' "; $result = mySQL_query($SQL);
```



userid	password	fname	lname	gender	dtob	country	user_rating	emailid
scott123	123@sco	Scott	Rayy	M	1990-05-15	USA	100	scott123@example-site.com
ferp6734	dloeiu@&3	Palash	Ghosh	M	1987-07-05	INDIA	75	palash@example-site.com
diana094	ku$j@23	Diana	Lorentz	F	1988-09-22	Germany	88	diana@example-site.com



localhost/sql/sql-injection/form.html

User ID:

abcd

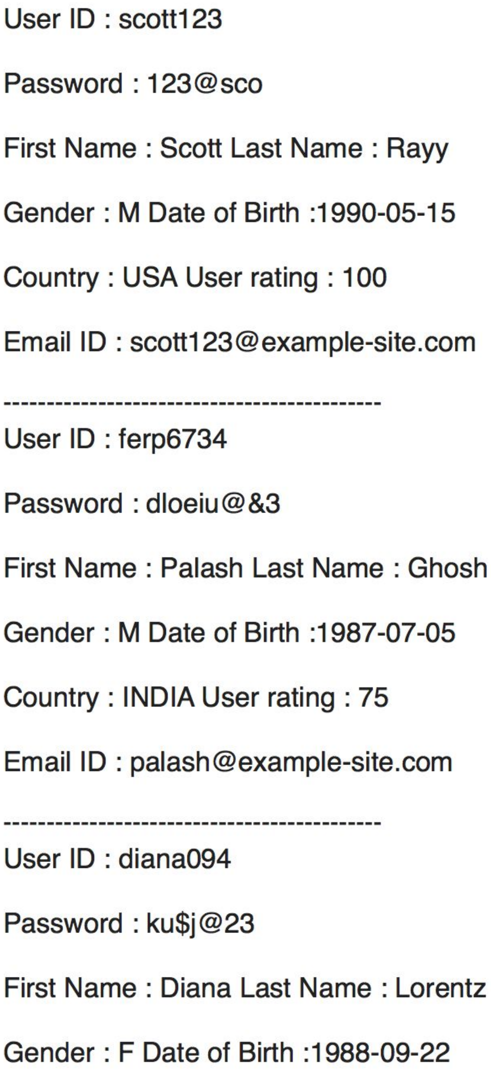
Password:

•••••••••••••••••

anything' or 'x'='x

```
$SQL = "select * from user_details where userid = 'abcd' and password =
'anything' or 'x'='x' ";
```

the WHERE clause is true for every row, therefore the query will return all records.



```
User ID : scott123

Password : 123@sco

First Name : Scott Last Name : Rayy

Gender : M Date of Birth :1990-05-15

Country : USA User rating : 100

Email ID : scott123@example-site.com

--------------------------------------------
User ID : ferp6734

Password : dloeiu@&3

First Name : Palash Last Name : Ghosh

Gender : M Date of Birth :1987-07-05

Country : INDIA User rating : 75

Email ID : palash@example-site.com

--------------------------------------------
User ID : diana094

Password : ku$j@23

First Name : Diana Last Name : Lorentz

Gender : F Date of Birth :1988-09-22
```

Motivation

- SQL injection attacks (SQLIAs) - a serious security threat to Web applications allowing attackers to obtain unrestricted access to the underlying databases and potentially sensitive information present in them.

- Maximum of the current approaches addressing SQLIAs, either fail to address the full scope of the problem or have limitations in their use and adoption

Project Outline

- List out different types of SQL injection attacks.
- Detect and prevent the potential attacks.
- Maybe, make a comparison of created tool with existing ones.

Citations

- Zoran Djuric. A Black Box testing tool for detecting SQL Injection Vulnerabilities. *IEEE Second International Conference of Informatics and Applications, pp. 216 - 221, 2013.*

- H. Shahriar, and M. Zulkernine. Automatic Testing of Program Security Vulnerabilities, 33rd Annual IEEE International Computer Software and Applications Conference, pp. 550 - 555, 2009.

- Hossain Shahriar and Mohammad Zulkernine. 33rd Annual IEEE International Computer Software and Applications Conference. 2009

- S. W. Boyd and A. D. Keromytis. SQLrand: Preventing SQL Injection Attacks. In *Proceedings of the 2nd Applied Cryptography and Network Security (ACNS) Conference*, pages 292–302, June 2004.

Thank You