

ELECS425F

Computer and Network Security

SQL injection

Outline – SQL Injection

- What is an SQL Injection vulnerability
- An example of SQL Injection
- An analysis of how it works
- How the attacker views the situation
- Input validation
- More attack vectors
- More remediation
- Avoiding SQL Injection



What is an SQL Injection vulnerability?

- It is a software defect
- It results in a security vulnerability
- One of the possible attack types is an SQL Injection



SQL

- SQL is “Structured Query Language”
- SQL is a standard language for accessing and manipulating databases.
 - execute queries against a database
 - retrieve data from a database
 - insert records in a database
 - update records in a database
 - delete records from a database
 - create new databases
 - create new tables in a database
 - create stored procedures in a database
 - create views in a database
 - set permissions on tables, procedures, and views
 - ...

Example

- We have a database

CustomerID	CustomerName	ContactName	Address	City	PostalCode	Country
1	Alfreds Futterkiste	Maria Anders	Obere Str. 57	Berlin	12209	Germany
2	Ana Trujillo Emparedados y helados	Ana Trujillo	Avda. de la Constitución 2222	México D.F.	05021	Mexico
3	Antonio Moreno Taquería	Antonio Moreno	Mataderos 2312	México D.F.	05023	Mexico
4	Around the Horn	Thomas Hardy	120 Hanover Sq.	London	WA1 1DP	UK
5	Berglunds snabbköp	Christina Berglund	Berguvsvägen 8	Luleå	S-958 22	Sweden



Example 1

- I want to get the information of customer whose customerID is 1.

SQL Statement:

```
SELECT * FROM Customers  
WHERE CustomerID=1;
```

Edit the SQL Statement, and click "Run SQL" to see the result.

Run SQL »

Result:

Number of Records: 1

CustomerID	CustomerName	ContactName	Address	City	PostalCode	Country
1	Alfreds Futterkiste	Maria Anders	Obere Str. 57	Berlin	12209	Germany



Example 1

- How to get all info in this database?
- You can try here
- https://www.w3schools.com/sql/trysql.asp?filename=trysql_select_where

Example 1

- A typical usage of such select statement to look up a value
- Enter Customer ID

Input = 1

```
SELECT * FROM Customers  
WHERE CustomerID=1;
```

- what's the input value?

Example 1

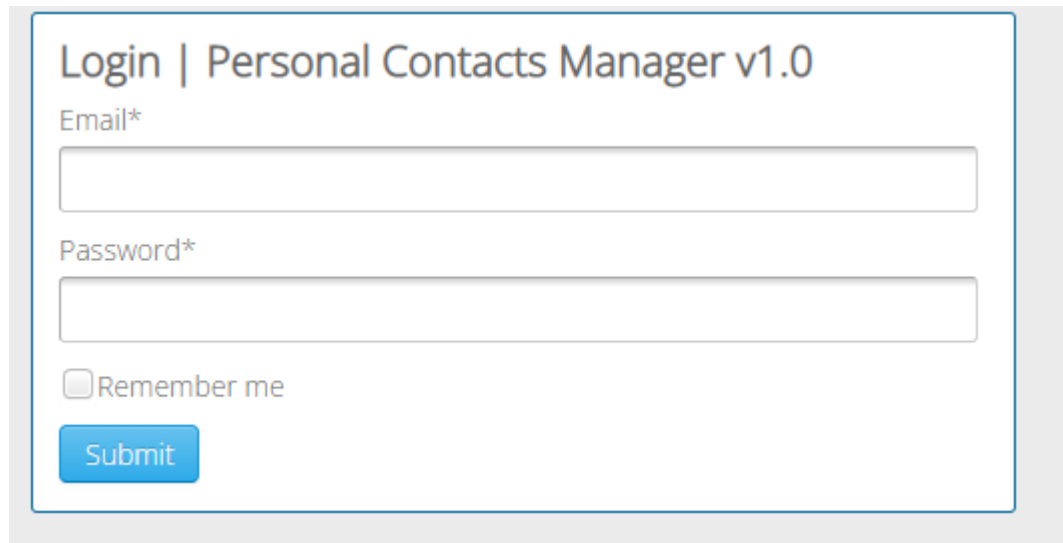
- Try this one:

```
SELECT * FROM Customers  
WHERE CustomerID= '1' or '1=1';
```

- Why it works?
- '1=1' always true

Example 2

- How to login a web page?



Login | Personal Contacts Manager v1.0

Email*

Password*

☐ Remember me

Submit

```
SELECT * FROM users WHERE email = '$email' AND password = md5('$password');
```

- <http://www.techpanda.org/index.php>

Example 2

```
SELECT * FROM users WHERE email = '$email' AND password = md5('$password');
```

Supplied values { xxx@xxx.xxx

xxx') OR 1 = 1 --]

```
SELECT * FROM users WHERE email = 'xxx@xxx.xxx' AND password = md5('xxx') OR 1 = 1 -- ]');
```

```
SELECT * FROM users WHERE FALSE AND FALSE OR TRUE
```

```
SELECT * FROM users WHERE FALSE OR TRUE
```

```
SELECT * FROM users WHERE TRUE
```

Here,

- The statement intelligently assumes md5 encryption is used
- Completes the single quote and closing bracket
- Appends a condition to the statement that will always be true

Try it:

<http://www.techpanda.org/index.php>

Example 3

- How to delete a table?
- SQL:

Syntax

```
DROP TABLE table_name;
```

- Try:
- https://www.w3schools.com/sql/trysql.asp?filename=trysql_drop_table

Example 3

- How to delete a table by using input?

Example

```
txtUserId = getRequestString("UserId");  
txtSQL = "SELECT * FROM Users WHERE UserId = " + txtUserId;
```

And the following input:

User id:

The valid SQL statement would look like this:

Result

```
SELECT * FROM Users WHERE UserId = 105; DROP TABLE Suppliers;
```

https://www.w3schools.com/sql/sql_injection.asp

What's the cause of SQL injection?

- Build a SQL command string with user input is dangerous