SQL injection

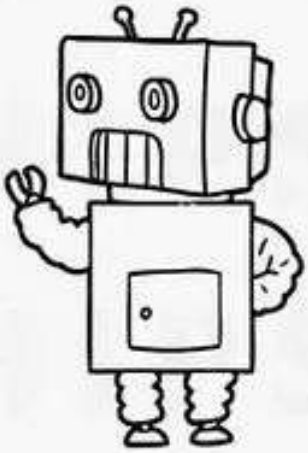
@codechips

Cody Dev

codechipsig@gmail.com

Lets say you have a Robot

Whose job is to buy things from the store and bring it to you



But it can't function by itself

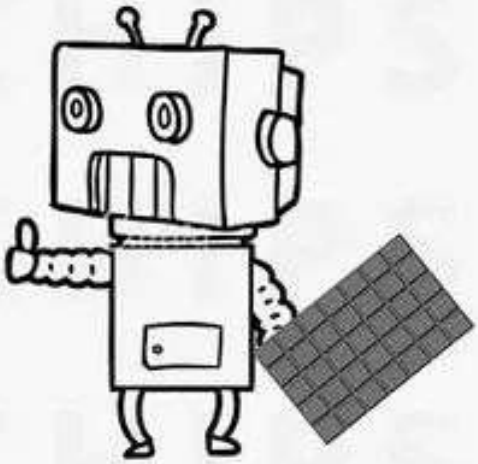
You need to pass commands along with values to make it do the work

command

Buy chocolates, Come home

value

1. Buy chocolates
2. come home

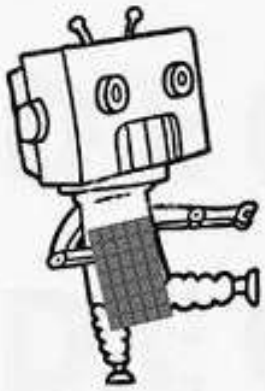


Great ,

But what if someone adds **unusual** values to the command ?

Buy chocolates and beat the shop owner ,

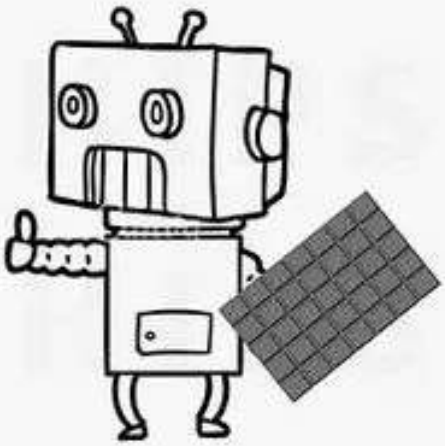
Come home



The reason this happened is,

The Robot cannot differentiate between instructions and data

1. Buy chocolates
2. Beat shop owner
3. Come home



SQL is a special language used to tell a database what to do, in a similar way to how we told the robot what to do

eg:

SQL query

```
SELECT * FROM login_details WHERE
username='username' AND password='password'
```

SQL injection is a web hacking technique by placing malicious code in SQL statements, via web page input

eg:

username : username

password : password' OR 1 = 1 --

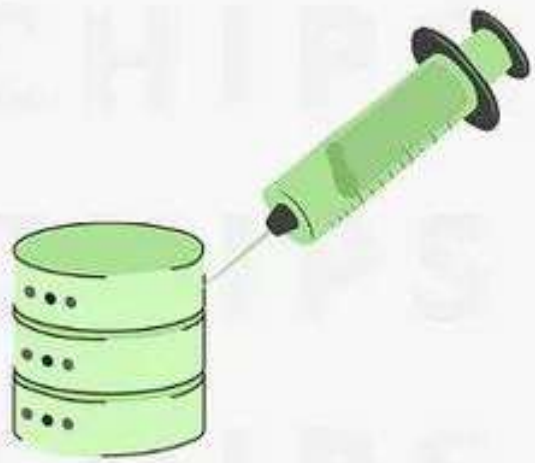
comments the rest of the query

```
SELECT * FROM login_details WHERE
username='username' AND password='password' OR 1 = 1 -- '
```

1 = 1 is always true

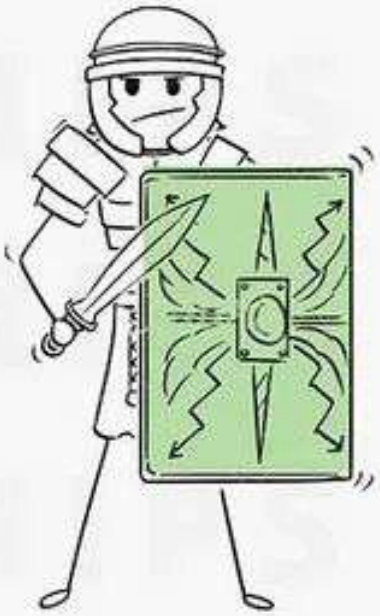
This will make the hacker login to the website throught SQL injection

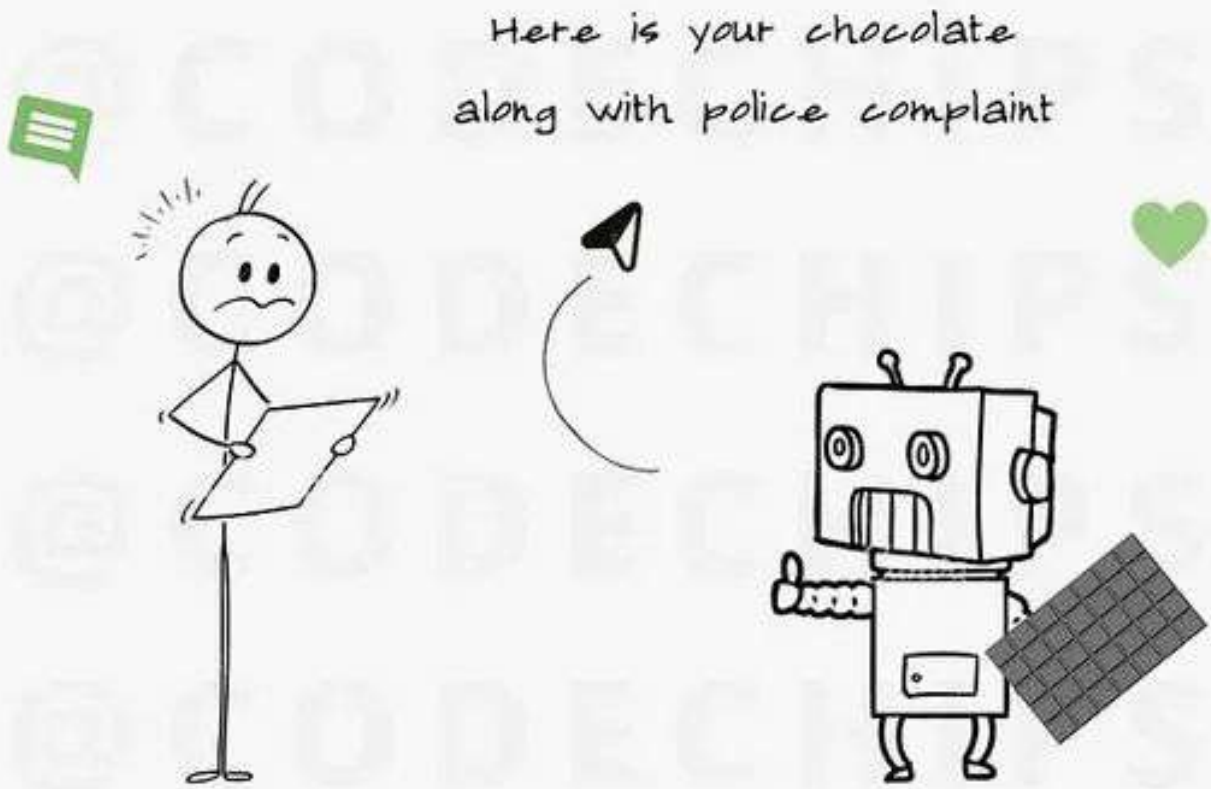
A successful **SQL injection exploit** can read sensitive data from the database, modify database data (viz., insert, update, or delete), etc.



Prevention ?

- Input validation
- Parametrized queries
- Stored procedures
- Escaping
- Avoiding administrative privileges
- Web application firewall




Here is your chocolate
along with police complaint