SQL INJECTION

INTRODUCTION

SQL injection (SQLi) is a web security vulnerability that generally allows an attacker talk dirrectly with the database and to view data that they are not normally able to retrieve.

TOOLS TO IDENTIFY SQL INJECTION

wpoison **/** sqlmap **/** wapiti **/** w3af **/** paros **/** sqid

SQL INJECTION TYPES

ERROR Ask the DB a quetion and lock for an respound
UNION Add a querry to the commands and see if she will run the cmd
BLIND Asking true/false from DB like 1=1 **|** 1+1=1

SQL CODE

Select **X** from **Y** ;
X Colums
Y TABLE

Create table Y (name datatype) ;
Insert into Y (A, B, C) ;
Values (A, B, C) ;

INPUT BOX NON-STRING

Querry : Where ID=X (wich is a number) and paswd= ' '
Bypass : ID = X or 1 = 1 --

INPUT BOX STRING

Querry : Where ID=NAME (wich is a string) and paswd= ' '
Bypass : ID = NAME or 1 = 1 --

URL INJECTION

URL : /login?profileID=VICTIM&paswd=XXXX
ATTACK : /login?profileID=NAMEor1=1

So we gaved her an ID but we also gaved her OR 1=1 wich is true