SQL Injection

SQL Injection

- Application does not handle user input securely
- User provides input that changes behavior of SQL statement
  - Extract additional data beyond what is expected
  - Perform malicious modification operations on databases
    - Insert invalid tuples
    - Delete complete tables
- **SOLUTION: ALWAYS USE PREPARED STATEMENTS**

Python Application Code

- Insecure
  - def printerByType_insecure(_conn, _type):

```
        sql = """select model, price
                from Printer
                where type = '{}'""".format(_type)
```

- Secure (prepared)
  - def printerByType_secure(_conn, _type):

```
        sql = """select model, price
                from Printer
                where type = ?"""
        args = [_type]
```

Print the Full Table Content

- sql = """select model, price
  from Printer
  where type = **'{}'**""".format(_type)
- printerByType_insecure(conn, "laser")
- printerByType_insecure(conn, "laser**' OR '1'='1**")

Extract Attribute Values (Extra Tuples)

- sql = """select model, price

  from Printer

  where type = **'{}'**""".format(_type)
- printerByType_insecure(conn, "laser**' OR type LIKE \'%ink%**")
- printerByType_insecure(conn,

  """laser**' UNION**

  select model, price from PC --""")

Extract Attribute Names

- sql = """select model, price

  from Printer

  where type = **'{}'**""".format(_type)
- printerByType_insecure(conn, "laser**' AND color = true --**")
- printerByType_insecure(conn,

  """laser**' UNION**

  select name, sql from sqlite_master where type = 'table'--""")

Extract Table Names

- sql = """select model, price
  from Printer
  where type = **'{}'**""".format(_type)
- printerByType_insecure(conn,
  """laser**' AND 13 = (select count(*) from PC) --**""")
- printerByType_insecure(conn,
  """laser**' UNION**
  select name, tbl_name from sqlite_master where type = 'table'--""")

Perform Modification Operations

- sql = """select model, price
  from Printer
  where type = **'{}'**""".format(_type)
- execute(sql)
- printerByType_insecure(conn,
  """laser**'; insert into printer (price) values(300); --**""")
- **executescript(sql)**
- printerByType_**script**_insecure(conn,
  """laser**'; insert into printer (price) values(300); --**""")