

# Android Security & Exploitation



**Aditya Gupta (@adi1391)**

**Founder, Attify (<http://attify.com>)**

**[adi@attify.com](mailto:adi@attify.com)**

Certifications : <http://securitytube-training.com>

Pentester Academy : <http://PentesterAcademy.com>

# Client Side Injection

# SQLite Injection

- SQLite databases for storing application's data
- Storing sensitive information in databases
- Do you sanitize user input before applying SQL queries

# Sample Code

```
uname = (EditText) findViewById(R.id.username);  
pwd = (EditText) findViewById(R.id.password);
```

```
String getSQL = "SELECT * FROM " + tableName + " WHERE " + username  
+ " = '" + uname + "' AND " + password + " = '" + pwd + "'";
```

```
Cursor cursor = dataBase.rawQuery(getSQL , null);
```