SQL Injection

Michael and Zach

Databases!

Users

id	username	password_hash	fullname
0	michael	asf-82w9sdlk4jt0s	Michael Ballantyne
1	zach	wdv8234vkzx082	Zachary Morin

```
select fullname, password_hash from users where username
like 'michael';
```

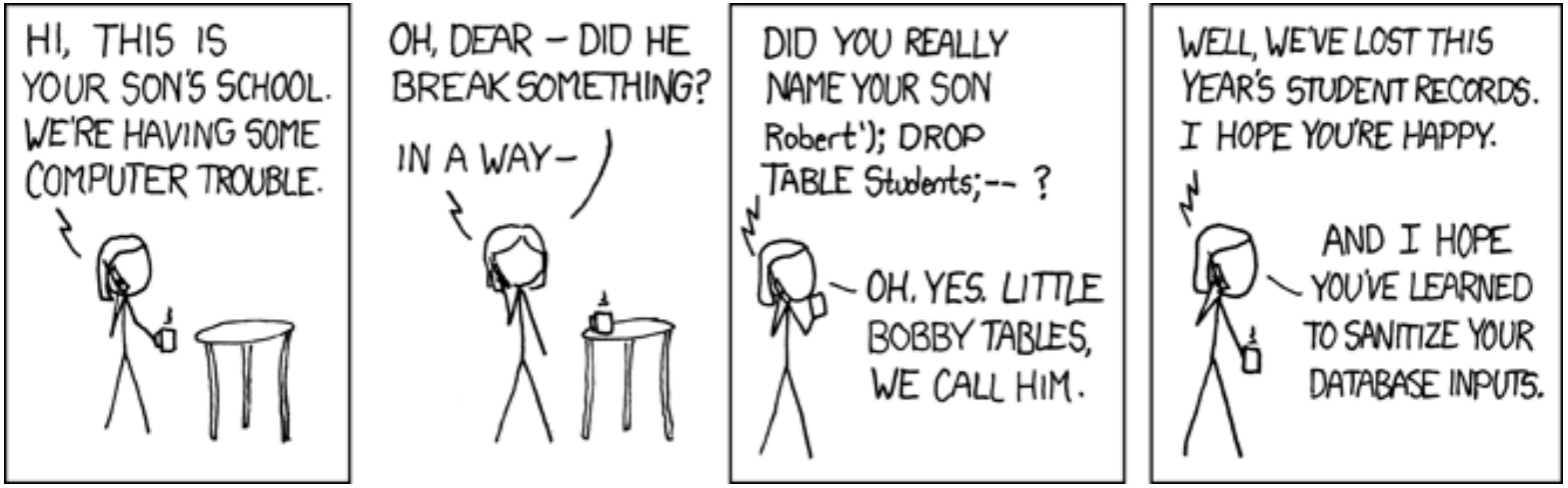
fullname	password_hash
Michael Ballantyne	asf-82w9sdlk4jt0s

Accessing Databases in Code

Never ever do this!

```
public boolean login(Form form) {
   Statement statement = mConnection.createStatement();
   String passwordHash = statement.execute("select hash
from users where name = '" + form.username + "';");
   ...
}
```

Why?



What are we looking for?

- SQL errors if we make the SQL malformed
- Different behavior of the application when we guess a table or database name correctly
- Pages that will produce a table of the results of our query

Avoiding SQL Injection

- Never concatenate user-entered data with your SQL statements! Always use your database driver's prepared statements feature, which automatically sanitizes parameters.

```
public boolean login(Form form) {
    PreparedStatement statement = mConnection.
prepareStatement("select hash from users where name =
?;");
   statement.setString(1, form.username);
    String passwordHash = statement.execute();
    ...
}
```

- Never let the behavior of your application reveal SQL exceptions

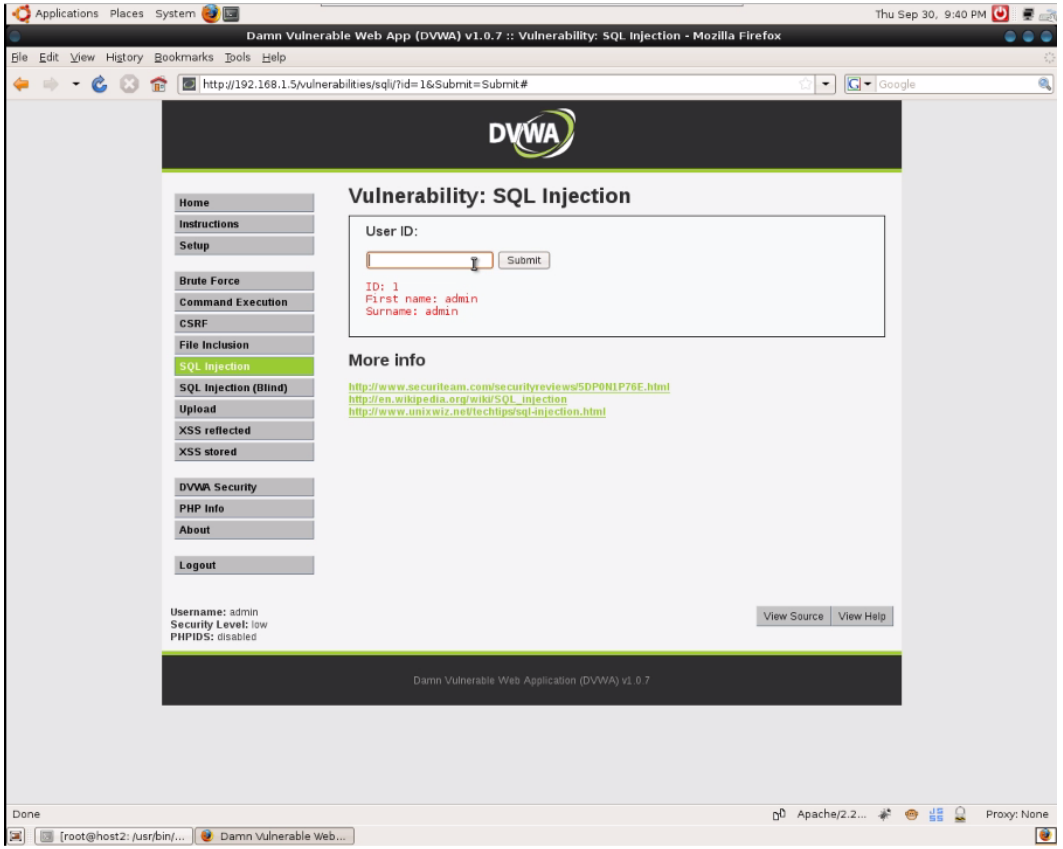
DVWA

Point Browser to 146.86.241.54:8081

Login: admin

Pass: password

SQL Injection Tab



Practice!

http://www.hackyeah.com/010/05/Hacwp-content/uploads/2kYeah-SQL-Injection.pdf