**PROG8190**

**Computer and Application Security \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Assignment #2 – SQL Injection – due at the date/time specified in eConestoga**

**Marks: / 25**

**Weight: 5%**

*This is an individual assignment. Do your own work and do not share your work with others. Sharing work is an Academic Offense and is subject to a penalty. Be aware that all source code and other documentation is automatically checked by eConestoga upon submission.*

The purpose of this assignment is to demonstrate a SQL Injection attack on a vulnerable web app (Mutillidae).

Task 1

To setup Mutillidae:

Install it locally on your computer under the XAMPP\htdocs folder. Download Mutillidae from [here](https://github.com/webpwnized/mutillidae). To run it locally, go to <http://127.0.0.1/mutillidae>

Then, go into OWASP 2017 | A1 – Injection (SQL) | SQLi Extract Data | User Info (SQL) as shown:

Graphical user interface, text, application

Description automatically generated

Next, register for a new account by clicking on the “Please register here” link:

Graphical user interface, Word

Description automatically generated

As for the “Username”, provide your Conestoga College account – this should be the characters to the left of the “@” sign in your CC email address – for instance, if your email address is [astudent1234@conestogac.on.ca](mailto:astudent1234@conestogac.on.ca), then use the “astudent1234” portion only for your username.

As for the “Password”, provide your first name as your password.

Provide your own Signature that is at least fifteen (15) characters long (including spaces).

Graphical user interface

Description automatically generated

Graphical user interface, application

Description automatically generated

Ensure that your account gets created:



After the account gets created, login using your credentials:

Graphical user interface

Description automatically generated

After creating your account, enter your username and password and then click on “View Account Details”

Graphical user interface, application, Word

Description automatically generated

Provide a screenshot showing your username, password and signature. **[5 Marks]**

Task 2

Next, using an apostrophe (‘), break the query by inserting it in the “Name” field only and then clicking on “View Account Details”. Provide a screenshot of this outcome. **[3 Marks]**

Task 3

From the previous Task, you should be able to see what SQL query was being executed. Provide a screenshot of the query as well as a screenshot of the name of the table that the query is referencing. **[2 Marks]**

Task 4

Using only the Username field and the name of the table from the previous task, perform a SQL Injection attack that will show ALL of the user accounts from the table. Provide the exact input that was used along with screenshots of the screens that results. Highlight your specific account in the result. **[5 Marks]**

**Hint:** you may want to use either of the following queries in the Name field only (there is a blank space at the end of each query):

‘ OR 1=1 –-

‘ UNION select \* from accounts --

Task 5

For this part of the exercise, go into OWASP 2017 | A1 – Injection (SQL) | SQLi – Bypass Authentication | Login:

Graphical user interface, text, application

Description automatically generated

Now, login using only your username along with an apostrophe (i.e. ‘) and capture a screenshot.

Using {your\_username}’-- (there is one space at the end of this line and do not include the {}’s) in the username, attempt to login to the web app. Take a screenshot of what you see next. **[5 Marks]**

Task 6

Reflections – provide your reflections in this section with regards to this exercise, namely:

* What worked well for you
* What didn’t work well and how you resolved the issue(s)
* What is one thing that you were able to learn or accomplish through this Assignment that you did not know prior to starting.
* What can be done to prevent such attacks from occurring? **[5 Marks]**

**Submissions:**

eConestoga submission –

A single MS Word document named:

**FirstName\_LastName\_StudentID\_Assignment2.docx**

Where FirstName, LastName and StudentID (seven-digit student ID) are your particulars.

that contains:

* 1. Assignment Title Page with your name, student ID, “Assignment #2” in the title and date
  2. Answers to the above questions, along with accompanying screen shots
  3. References

Late penalties will apply for any/all submissions submitted past the due date.

A -10% penalty will be applied for any files that are zipped up or not using the correct naming format.

As this is a technical report, proper spelling and grammar will also be required and marks may be lost for reports that have poor spelling and / or grammar. A more detailed marking scheme is shown in the Rubric associated with the Assignment Folder in eConestoga.