**Assignment 2: Web Application Security**

**NOTE: ALL ASSIGNMENTS/ASSESSMENTS FOR THIS COURSE ARE INDIVIDUAL IN NATURE. EACH STUDENT MUST COMPLETE THE WORK FOR THE ASSIGNMENTS BY HIS-/HER-SELF**

**Submission: Upload your assignment submission in a file called *assign2Web.zip* (details below) to BrightSpace by the due date. Late submissions cannot be accepted!**

**Problem: Perform CSRF, XSS and DOM exploits on a provided Java Web application, and then harden that application to stop your exploits from working on it**

You are being given two Java Web applications called **MessagesExploits** and **MessagesExploitsStealData**. This first application is a simple message board system, allowing users to log in, and then post, read and delete messages. The messages are stored in a provided MySQL database called **messages1**. The second application is an “evil” application only used to steal data from the other one.

Your tasks for this assignment are to:

1. Run and examine the functionality of the provided **MessagesExploits** and

**MessagesExploitsStealData** applications

1. Familiarize yourself with the source code for the applications (and the associated database) to understand how they work
2. Develop CSRF exploits that can be used to trick a user into posting and deleting messages invalidly in **MessagesExploits**
3. Develop XSS exploits that can be used to steal data such as usernames and passwords, and session ID’s, showing them via the **MessagesExploitsStealData** application
4. Develop DOM-based exploits (e.g. via HTML injection in the **MessagesExploits** application) that interfere with the valid operation of the **MessagesExploits** application, i.e. fooling a user into sending their login username and password to the evil application, pretending that another user

posted a message that they didn’t actually post, or denial of service in the **MessagesExploits**

application

1. Finally, you must change the **MessagesExploits** application code using ***nonce values*** and appropriate ***input validation*** to harden it against the exploits you have found (so that they no longer work on it)

The **MessagesExploitsStealData** project contains servlets that can be used to display stolen data sent to it from the **MessagesExploits** project (the stolen data is shown in the *NetBeans console output window* via ***System.out.println*** statements).

**Assignment Requirements**

You must develop and document separate exploits against the application to do each of the following things:

# CSRF:

* + cause a logged-in user to invalidly post a new message
  + cause a logged-in user to invalidly delete a message

# XSS:

* + steal a user’s login username and password
  + steal usernames and session ID values via cookies

# DOM (HTML injection):

* + Fake a message posting from another user
  + Denial of service (so that users cannot interact with the application as designed, i.e. they can’t read, post and delete messages in **MessagesExploits** when they log in)

Write up the exploits you developed *in detail* in the provided ***Microsoft Word*** file called **Assign2.docx** and include this document with your submission (details below). Include details of the type of exploit, and how it works. You must give step-by-step instructions on how to perform/repeat each exploit.2

You must also submit a copy of the revised NetBeans project containing your hardened version of the **MessagesExploits** application. This version of the application must not allow the exploits you found to work against it. This project *must* be loadable and runnable in NetBeans!

**Submission Requirements**

You must upload a file called **assign2Web.zip** (in ***Zip*** format only, please) to BrightSpace. This zip file must contain two things:

1. A copy of your **Assign2.docx** file
2. A copy of the revised **MessagesExploits** NetBeans project (loadable and runnable in NetBeans)3