ENEE457 – Computer Systems Security
Project 2 Rubric

The project has been divided into 2 parts:

(1) *Cross-Site Request Forgery (CSRF) Attack Lab* – tasks 1 to 4
(2) *Cross-Site Scripting (XSS) Attack Lab* – tasks 1 to 6.

Note: Make sure to document your responses in a separate (.doc or .pdf) file, with details and screenshots of each task.

Task #	Description	Points
	Cross-Site Request Forgery (CSRF) Attack Lab (55 points)	
1	Inspect one http **GET** request package and one http **POST** request package. Identify the parameters used in these requests, if any.	5
2	I. While being logged in as Samy, find the *GUID* of both Samy and Alice (3) II. Find the *http get request* for adding a friend (3) III. Create the malicious html file and upload it on Samy's attack website (7) IV. Demonstrate the CSRF attack (with all the steps) that forces Alice to become friends with Samy (7)	20
3	I. Describe how the html file, javascript and post request relate together in the context of the "Samy is my Hero" attack (5) II. Demonstrate the attack. (10) III. Answer Questions 1 & 2 (5)	20
4	I. Successfully turn on the token validation countermeasure (2) II. Show what will happen (3) III. Answer the question (5)	10
	Cross-Site Scripting (XSS) Attack Lab (45 points)	
1	Create a script in Boby's profile such that when Alice visits Boby's profile, it shows an alert	6
2	Create a script in Boby's profile such that when Alice visits Boby's profile, it shows Alice's cookies	2
3	Show how to retrieve Alice's cookie	7
4	I. Write the script so that Samy gets added to Alice's friend list (10) II. Answer Questions 1 & 2 (4)	14
5	I. Successful edit of Alice's profile from Samy' profile (6) II. Answer Question 3 (2)	8
6	Write a self-propagate XSS Worm using DOM and demonstrate it working by a series of screenshots	8
	TOTAL POINTS:	100