CMPE279 : Security
Assignments 3 & 4

In these assignments, you will be attacking a vulnerable web application using a variety of techniques. The web application we will be using is called "DVWA" – *Damn Vulnerable Web App*. This web application is intentionally poorly-written and can be exploited in a number of ways.

You may work in teams of up to 2 people if you want.

Install DWVA in your VM (http://dvwa.co.uk). There are several different ways to install DVWA, you can read on the site how to do it. The easiest way is likely to run DVWA as a "Live CD" – this way you don't need to install anything at all. There is also a .zip file that contains the code, but that requires you to install some prerequisites in your VM.

DVWA has quite a large number of writeups and videos that explain how to exploit its various weaknesses. Feel free to search for the answers to these assignments and follow along with whatever solution works. The goal of the assignments is to understand how vulnerable web applications can be compromised by attackers.

Assignment 3

Set DVWA's script security to "Low" and perform the following exploits (you can Google how this is done for the exact syntax):

- Perform a SQL injection attack and retrieve the list of users in the user database
- Perform a reflected XSS attack (payload is your choice; I'd recommend just popping up a JavaScript alert)

Submit answers to the following questions before the due date:

- Describe the SQLi attack you used, how did you cause the user table to be dumped? What was the input string you used?
- If you switch the security level in DVWA to "Medium", does the SQLi attack still work?
- Describe the reflected XSS attack you used, how did it work?
- If you switch the security level in DVWA to "Medium", does the XSS attack still work?

Due – 13 May 2020 before midnight

Assignment 4

Perform **either** a CSRF attack **or** a stored XSS attack against DVWA. The payload is your choice.

Submit answers to the following questions before the due date:

- Describe the attack you used. How did it work?
- Does your attack work in "Medium" security level?
- Set the security mode to "Low" and examine the code that is vulnerable, and then set the security mode to "High" and reexamine the same code. What changed? How do the changes prevent the attack from succeeding?

Due – 13 May 2020 before midnight