**Burp Suite Assignment**

By: Shabaz Badshah and Waleed Muhammad

Tuesday March 17, 2020

CSC427 - Information Security

**Prerequisite Information:**

* You will use the same VM from the Burp tutorial
* Make sure to set DVWA security to “low” before starting the assignment.
* For all questions below, please add any resources (links, etc.) you’ve used to them.

**Virtual Office Hours:**

* You can @Waleed or @Shabaz, or DM us directly on MS Teams
* You can ask your questions in the “Burp Tutorial and Assignments” channel on MS Teams

**Assignment Tasks:**

1. **You’ve run a scan on a client’s site, and the following report (same report.html as tutorial) is generated. Read the report and answer the following questions for vulnerability 2.3.**

a. Description of the vulnerability

b. The request/response object that can be used to exploit the vulnerability

c. How you can mitigate the vulnerability

1. **What do the following Burp tools do? Also give an example of a possible attack that you can run using a combination of at least 2 tools.**
   1. Intruder
   2. Repeater
   3. Proxy
   4. Target
   5. Comparer
2. **Now you’ll try and perform a stored XSS attack on DVWA using Burp. You’ll be performing the stored XSS attack on the following URL within DVWA.** [**http://localhost/vulnerabilities/xss\_s/**](http://localhost/vulnerabilities/xss_s/)**. Utilize Burp to create XSS payloads that can do the following. There’s some very good resources in the presentation** [**deck**](https://docs.google.com/presentation/d/14gnUzIn3L7aR7pusMBhW9HUGGGuj1wBSXZZKzu5e1BA/edit?usp=sharing)**.**
   1. Create an alert box that prints “Hello World”. Take a screenshot of the DVWA for submission (call it 1.jpg/png). Paste the script used below.
   2. Create another alert box that will print the cookie in the alert box. Paste the script used below. Take a screenshot of the DVWA for submission (call it 2.jpg/png)
      1. What is a type of attack that you could execute if you have a browser’s cookie?
   3. Change the colour of the text on the page to orange. Paste the script you used below. Take a screenshot of the DVWA for submission (call 3.jpg/png)
   4. Create a script that will redirect you to<http://www.cs.toronto.edu/~arnold/427/20s/> as soon as you click on the “XSS (Stored)” option in DVWA. Paste your script below.
      1. What is a stored XSS attack? Give an example of one, and a major hack that used it.

HINT: You may need to modify the message box element to accept more text than the default 50 characters if you’re manually testing.

* 1. You will see that when you load the page again, all of your previous scripts and responses are stored and executed.
     1. Why is this the case?
     2. How could a malicious user take advantage of this exploit?
     3. How would you resolve this issue?

**Files to submit:**

* answers.txt
* 1/2/3.jpg/png
* members.txt