University of Maryland
CMSC414 — Computer and Network Security
Professor Jonathan Katz

Project 4

Due by May 3, 11:59 PM

This project will introduce you to XSS and CSRF attacks. You will be using Labs 9 and 10 from here:

`http://www.cis.syr.edu/~wedu/seed/all_labs.html`.

To run those labs you will need to download the SeedUbuntu VM from here:

`http://www.cis.syr.edu/~wedu/seed/lab_env.html`.

A user manual (which also includes passwords) can be downloaded at the same URL. The lab writeups provide fairly extensive documentation for getting started.

Please submit the following to the TAs by email:

- Lab 9:

  1. Tasks 1 and 2: These are just for practice, and there is no need to submit anything for these tasks.
  2. Task 3 **(25 points)**: Submit a file `admin-cookie.txt` that contains exactly the result printed by your TCP server after implementing this attack and then loading the post containing the malicious code while logged in as the admin.
  3. Task 4 **(25 points)**: Submit java code `fakepost.java` that, when run, posts the message "I am the admin" on behalf of the admin (without being logged in as the admin).
  4. Task 5 **(10 points)**: Submit a file `worm1.txt` containing JavaScript code that, when injected and later viewed by any user who is currently logged in, ends up posting the message "I authorized this message" on behalf of that user.
  5. Task 6 **(10 points)**: Submit a file `worm2.txt` containing JavaScript code that, when injected and viewed by any user who is currently logged in, ends up posting a message *that includes a copy of the worm itself* on behalf of that user.

  (Note that Tasks 5 and 6 are probably the most difficult ones of the entire homework.)

- Lab 10:

  1. Task 1 **(15 points)**: Submit a file `csrf1.html` that, when viewed by any user who is currently logged in, posts the message "I authorized this message" on behalf of that user.
  2. Task 2 **(15 points)**: Submit a file `csrf2.html` that, when viewed by user Ted who is currently logged in, changes Ted's signature to "I have been pwned".