```
================================================
CSRF Lab Description
http://www.cis.syr.edu/~wedu/seed/Labs_16.04/Web/Web_CSRF_Elgg/Web_CSRF_Elgg.pdf
================================================

SETUP
1. Start the Apache server:
   $ sudo service apache2 start

2. Attacker’s website
   +  URL: http://www.csrflabattacker.com
   +  Folder: /var/www/CSRF/Attacker/

   Victim website (Elgg)
   +  URL: http://www.csrflabelgg.com
   +  Folder: /var/www/CSRF/Elg

   Credentials: Admin:    admin -- seedelgg
                Alice:    alice -- seedalice
                Boby:     boby -- seedboby
                Charlie:  charlie -- seedcharlie
                Samy:     samy -- seedsamy

3. Open "HTTP Headers Live" add-on

4. Login to alice's account. Modify her account and observe the trafic in "HTTP
Headers Live"

================================================
 TURN-IN TASKS
================================================
+ TASK 02: CSRF Attack using GET Request
  + Modify the attacker's code "index.html" (at /var/www/CSRF/Attacker) under root
account (password: seedubuntu).
    Note: Make sure you use the given template.
  + Lauch the attacker's page (http://www.csrflabattacker.com/)  while Alice's still
logging in. Hit the button.

+ TASK 03: CSRF Attack using POST Request
  + Make sure you answer Questions 1 and 2 in the lab description

+ TASK 04: Implementing a countermeasure for Elgg
  + Follow lab descriptions
```