```
==================================================
XSS Lab Description:
https://seedsecuritylabs.org/Labs_16.04/PDF/Web_XSS_Elgg_new.pdf
==================================================
SETUP
  + Start Apache server
  $ sudo service apache2 start
  + Open Firefox --> Http Live Header (Second icon (from right side) in Firefox url bar)
  + Log in as Alice: alice -- seedalice

==================================================
TURN-IN TASKS
==================================================
+ TASK 01: Display an Alert Window
  + Go to Alice's "Edit profile" (in right panels)
  + Test for a field that is vulnerable to XSS
    Hint: "<script>alert('XSS')</script>"

+ TASK 02: Display Session Cookie
  + Display Alice's session cookie
    Hint: Inject your script in the form of "<script>alert(....)</script>"

+ TASK 03: Stealing Session Cookie from the Victim's Machine
  + Our victim would be Admin.
  + Log out Alice. Log in as Admin: admin -- seedelgg
  + Open a new terminal and enter
    $ nc -l 5555 -v
    (This will serve as the attacker's remote terminal)
  + Visit Alice's profile.
  + The Admin's session cookie should show in the attacker's terminal

+ TASK 04: Becoming the Victim's Friend
  + Sammy is a malicious user.
  + She wants to add anyone who visits her page to her friendlist without their notice.
  + From Sammy's page, try to make a friend request and observe the http header(s)
  + Write a javascritp to do this following the manual's template.

TASK 05: Modifying the Victim's profile
  + Follow the lab descriptions.
```