PCS Lab 3: Cross-site Scripting Instructions

Instructions

Read and follow the SEED lab instructions below, and answer the questions in the next page.

SEED Lab Instruction on XSS:
http://www.cis.syr.edu/~wedu/seed/Labs_16.04/Web/Web_XSS_Elgg/Web_XSS_Elgg.pdf

Some useful materials:

- Background Info: http://www.cis.syr.edu/~wedu/seed/Labs_16.04/Web/Web_XSS_Elgg/
- OWASP page: https://www.owasp.org/index.php/Cross-site_Scripting_(XSS)
- Google XSS Game Area: http://xss-game.appspot.com/

Submission

Due: April 3, 11:00 PM (EST)

Late submissions are accepted with 50% grading penalty within 24 hours of the due.
Submissions that are late for more than 24 hours will NOT be accepted.

Please submit your solution in PDF or image on https://www.gradescope.com/courses/38640.
Please choose the right page for your answer to every question.

Questions

Question 1: Please provide the names and NetIDs of your collaborator (up to 2). If you finished the lab alone, write None.
Collaboration Policy

1. **You can optionally form study groups consisting of up to 3 people per group (including yourself).**
2. **Everybody should write individually by themselves, and submit the lab reports separately. DO NOT copy each other's lab reports, or show your lab reports to anyone other than the course staff, or read other students' lab reports.**

Question 2.

2.1 Please describe your observations of "Task 1: Posting a Malicious Message to Display an Alert Window", including necessary screenshots.
2.2 In the example in Task 1, why were you able to request and execute example.com/myscripts.js despite the Same-Origin Policy?

Question 3: Please describe your observations of "Task 2: Posting a Malicious Message to Display Cookies", including necessary screenshots.

Question 4.

4.1 Please describe your observations of "Task 3: Stealing Cookies from the Victim's Machine", including necessary screenshots.
4.2 Why could the victim's cookies be sent to another server in Task 3 despite the Same-Origin Policy?
4.3 Would you be able to steal the victim's Cookies of another website (e.g. bankofamerica.com) which is also stored in the victim's browser when the victim is visiting www.xsslabelgg.com? Why?

Question 5.

5.1 Please paste the code you use as "About me" in Task 4
5.2 Please describe your observations of "Task 4: Becoming the Victim's Friend", including necessary screenshots.
5.3 What is the purpose of ①and ② in Task 4, why are they needed?
5.4 If the Elgg application only provides the Editor mode for the "About Me" field, i.e., you cannot switch to the Text mode, can you still launch a successful attack? Why?

Question 6.

6.1 Please paste the code you use as "About me" in Task 5

6.2 Please describe your observations "Task 5: Modifying the Victim's Profile", including necessary screenshots.

6.3 : Why do we need Line ①? Remove this line, and repeat your attack. Report and **explain** your observation

Question 7.

7.1 Please paste the code you use as "About me" in Task 6

7.2 Please describe your observations of "Task 6: Writing a Self-Propagating XSS Worm", including necessary screenshots.

Question 8: Please describe your observations of "Task 7: Countermeasures", and use one or two sentences to explain why encoding the special characters avoids XSS attack, including necessary screenshots.