Homework 6 – Client Side Injection

Lab Information

Due Date:

Homework 6 Dropbox Deadline

Objectives/Goal:

In this homework we will be investigating part one of client side injection attacks. I encourage you to try this out manually and follow it up by using tools such as XSSHunter. The environment which you are entering is also hostile so be aware and use private browsing as needed.

Deliverables:

- Images and descriptions of the XSS issues.
- Provide your weaponized XSS and graph of friends obtained
- Show evidence that you abused the hidden functionality to change passwords

Table of Contents:

Activity 1: A life in the day of a tester

Today we're working with our Hooli friends to identify some nasty little bugs that are targeting their clients. They have their ArmBook social network that is designed for security and ease of use. You did such a good job previously that they have designed a new version of the site with some of your suggestions incorporated. You can access the new ArmBook at http://csec380-core.csec.rit.edu:86. As a member of the staff, you also have access to the Hooli Guestbook at http://csec380-core.csec.rit.edu:5006 (Note the 6).

Step 1: Just a quick reflection on life

You know all about basic cross-site scripting. The kind that takes advantage of the victim's faith in the domain. In this sense, it's very similar to the CSRF vulnerability you found earlier. Today you need to demonstrate to your client basic XSS. He wants to see BOTH variants so he can decide which is more dangerous. Take a look at the NEWER ARMBOOK (http://csec380-core.csec.rit.edu:86). See if you can spot the problem.

Exploit reflected XSS and take a screenshot where you triggering an alert box. Provide a short description of where the issue was found. (Same document as step 2)

Step 2: If the glove persists you must affix

Now that you've figured out the basics, it's time to get a little bit more rowdy. Demonstrate the other form of XSS. Make sure he knows that it is working. Do not break the site, or there will be downtime for the customer and he might fire you (deduct points), make sure to test locally first!

Exploit persistent XSS and take a screenshot where you triggering an alert box. Provide a short description of where the issue was found. (Same document as step 1)

Activity 2: An insect by any other name

Sure we had our classic Hooli employee convinced that XSS existed in their site, but they don't see it as a big problem. Your goal is going to be to show them just how dangerous this attack can be on a highly interactive site. Do not break the site, or you may be fired again!

Step 1: creepy crawler

Your goal is to show them that you can use XSS to spread through their site. Your end goal is to get at minimum 4 people to be infected. Track your worm's propagation over time and provide a graphical representation of when people friended you. Because I know you all, the model should account for new friends UNTIL AT LEAST the day this assignment is due. If you are sure you completed the assignment but no one is logging on, reach out to the professor. **Your code must have gone through minification and obfuscated in at least 3 other ways.**

Provide your unobfuscated and obfuscated code. Also, provide a graph of people who friended you.

Activity 3: The holiest of holies

Sure, most sites are have some hidden functionality. The Armbook site is probably not an exception. Those jerks have been mistreating you ever since you got here. What you need to do is show them who is boss! Find their hidden controls and show them who's boss. But be careful not to break the site, if you break it they'll know it's you. (Hint: you may need to leverage the Hooli guestbook)

Step 1: Finish Him!

See if you can use the information to disclose what the password of the sites most prominent user (Andy Culler). Once you have found the password, post it for the world to see on your wall and change it! That'll be sure to make them lose faith in the site!

Provide a screenshot of the hidden functionality, include Andy's current password in the photo

Signoffs

Activity 1.1 – Provide pictures and writeup for XSS locations (10%)

Activity 2.1 – Provide the code that allows you to friend people and graphics demonstrating the trend. (45%)

Activity 3.1 – Show that you know Andy's password and have changed it to something more fitting. (45%)