Cross Site Scripting: Introduction
IN618 Security

Introduction

I discussed this paper with an industry security consultant who told me that *cross site scripting* (XSS) was the most important topic we would cover this semester. This is because mistakes leading to XSS vulnerabilities are easily and frequently made, and because they are easily exploited.

Examine a vulnerable system

Go to the web site at `http://xss.foo.org.nz` and try out the web pages there. View the HTML source and do anything else you want to do to explore the site.

Note that the results you see vary considerably depending on the browser you use, so you may want to try things in a variety of browsers.

1. Do you see any potential vulnerabilities here? Document your suspicions below:

2. Now enter `http://xss.foo.org.nz/pg2.php?secure=<script>alert('pwned')</script>`. What happens? Why?

3. Can you think of any other ways to exploit this? Try some and document this below.

4. Now go to `http://xss.foo.org.nz/trouble.html`. Follow the link and see what happens. Explain what you observe below.

5. Source code for this example is in the `week03` directory on GitHub. Inspect the source and be prepared to discuss it.