

Hand in a stapled, printed copy with your answers.

Homework: /SI110/The Cyber Battlefield/Web-HTML Injection Attacks, XSS

1. Go to amazon.com and enter as a search term: `foot<u>ball</u>`

The resulting webpage shows your search results, above which is echoed back your search term, in quotes.

a. What do you see echoed back as your search term?

b. Did you successfully inject HTML?
Justify your answer!

Circle one: Yes No

2. Circle the correct word "client" or "server" in each underlined section below so that the text is accurate:

A "cookie" is a small piece of data stored on the harddrive of the web

client / server. For a given site, the client / server asks the

client / server to store the cookie, and to then send it when any

"GET" requests are made by the client / server for files at the site.

3. When I enter the URL amazon.com in a browser on my laptop, the page I get always says "Welcome Dr. Brown" at the top. Cookies make that possible. I recently entered the same URL in a browser on a computer at the library, but the resulting page did not say "Welcome Dr. Brown". Explain why!

4. Suppose you have an account at insecurebank.com. Someone named Guy Bad sends you an email that tricks you into pointing your browser at the URL:

`http://insecurebank.com/transfer.cgi?amount=1000.00&toAcct=780023`

Transfer.cgi is a server-side script that transfers money between accounts. Explain why \$1000.00 will be transferred from your account to account 780023 if you happen to be logged into your account at www.insecurebank.com at the time you opened the email from Guy Bad.

SI110 Introduction to Cyber Security AY12S
Technical Foundations

Name: _____

Alpha _____

Hand in a stapled, printed copy with your answers.

5. Assume that your instructor and your entire section are logged in to your instructor's SI110 Message Board. Midn Bad posts the following to the message board, then everyone refreshes their browser.

```
<script type="text/javascript">document.write(document.cookie)</script>
```

What's the difference between:

- what you will see when you look at the Message Board in the browser on your laptop
- what will be shown on the Message Board pulled up on the instructor's browser, projected onto the screen in front of the class?

6. A website like the message board can protect itself from injection attacks by "escaping" characters like `<`, `>` and `&` that have special meaning in html, i.e. replacing them with equivalents like `<` which displays as `<`, but doesn't get interpreted as starting a tag. What does a page like our message board lose by doing this? I.e. what's the downside?