

choose one: Received Received help from:
(or more) no help Collaborated with: _____

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

1. Go to <http://intranet.usna.edu/> and, in the "search" box near the upper right corner, enter as a search term: look<u>out</u>

The resulting webpage shows your search results, including echoing back your search term under the label "Results for:".

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

10/0/0/0

b. Is this page susceptible to an HTML injection attack? Justify your answer!

10/8/6/0

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

10/8/6/0

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!

10/8/6/0

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>

10/8/6/0

"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 only if you happen to be logged into your account at insecurebank.com at the time you open the email from Guy Bad.

5. Below is a link to a special SI110 message board. Some user has nuked the message board with some kind of injection attack. NOTE: type the URL by hand please!

http://rona.cs.usna.edu/~wcbrown/hw/msg/mb.html

10/0/0/0

a. The name of the user who attacked the message board is:

b. Describe exactly what one needs to do to discover for oneself the answer to part a.

10/8/6/0

6. There is an alternate message board at the URL:

<http://rona.cs.usna.edu/~wcbrown/esc/msg/mb.html>

10/8/6/0

This version of the message board uses a client-side script to escape < >'s in message posts. Find a way to post a message that renders as football despite this input sanitization. Describe below precisely what you did to make this happen!

Note: the board auto-wipes itself every 60 seconds, just in case someone inadvertently brings the message board down. Still, please don't attack this message board!

7. Take my word for this: In the SI110 message board, if a user is logged in so his "cookie" exists, the following expression evaluates to the username within the cookie:

```
document.cookie.split(/>=|;/)[1]
```

Given that, suppose a student with username **fepicail** posts the following on Dr. Brown's SI110 message board:

```
drbrown is
<script>
if (document.cookie != "" && document.cookie.split(/>=|;/)[1] != "drbrown")
{
  document.write("a real jerk");
}
else
{
  document.write("great");
}
</script>
```

a. What does someone who views the message board but is not logged in see posted?

5/3/2/0

b. What does someone who views the message board while logged in as **drbrown** see posted?

5/3/2/0

c. What does someone who views the message board while logged in as **thedude** see posted?

5/3/2/0

d. What does someone who views the message board while logged in as **fepicail** see posted?