Quiz 28: Security

Name: ______________________________

CSCI 110 Section 1

Friday, November 18, 2016

1) Is the following web application code vulnerable to an XSS attack? If so, how should it be fixed? [30 points]

```
import cgi

# Assume page_header and page_footer are defined here

class MainPage(webapp.RequestHandler):

  def render_string(self, s):
    self.response.out.write(s)

  def get(self):
    self.response.headers.add_header("X-XSS-Protection", "0")

    if not self.request.get('query'):
      # Show main search page
      self.render_string(page_header + main_page_markup + page_footer)
    else:
      query = self.request.get('query', '[empty]')

      # Our search engine broke, we found no results :-(
      message = ("Sorry, no results were found for <b>"
         + cgi.escape(query) + "</b>.")
      message += " <a href='?'>Try again</a>."

      # Display the results page
      self.render_string(page_header + message + page_footer)

    return
```

2) Is the following web application code vulnerable to SQL injection? If so, how should it be fixed? [30 points]

```
// Get the 'var' parameter out of the POST request
$var = $_POST['var'];

// Use the value of that parameter in an SQL query
mysql_query("SELECT * FROM sometable WHERE id = $var");
```

3) In 6 words or fewer, describe what the following function does. [40 points]

```
int mystery(int a[]) {
    int aVal = -1;
    int aCount = -1;

    for (int i = 0; i < a.length; ++i) {
        int count = 0;
        for (int j = 0; j < a.length; ++j) {
            if (a[j] == a[i]) ++count;
        }
        if (count > aCount) {
            aCount = count;
            aVal = a[i];
        }
    }

    return aVal;
}
```