Secure Programming Techniques — exam 27.06.2013

1. What are the security-related disadvantages of GET HTTP queries compared to POST queries?

2. If I want to make a setuid awk script, what options do I have?

3. Find all potential vulnerabilities in this C function:

   ```c
   void parse (char *input)
   {
       char buf[100], buf2[8], *array;
       int val;

       strncpy(buf, input, strlen(input));
       scanf("%d:%s", val, buf2);
       if (val > 15) return;
       array = malloc (val* sizeof(buf2));
       fill_array(array,buf2); // do the maths
   }
   ```

4. Find all potential vulnerabilities in this PHP snippet:

   ```php
   <?php
   if(loggedIn() && isset($_REQUEST['do'], $_REQUEST['email']) &&
   $_REQUEST['do'] == 'Email') {
       $sql = "UPDATE users SET email='" . $_REQUEST['email'] . ";
                WHERE username='" . currentUser() . ";";
       mysql_query($sql) || die($sql);
       echo "Email changed to " . $_REQUEST['email'];
   }
   ?>
   ```

5. Find all potential vulnerabilities in this JSP snippet:

   ```jsp
   <% String title = request.getParameter("title");
    // regexp replace
    title = title.replace('<script>','<div>');
    title = title.replace('<object>','<div>');
    title = title.replace('<applet>','<div>');
    title = title.replace('<embed>','<div>'); %>
   <p>Title <b>'<%= title %>'</b> added to your shopping cart.</p>
   ```

Send response by e-mail to mroos@ut.ee no later than 12.00. You can answer either in English or in Estonian.