Secure Programming Techniques — exam 08.06.2018

1. What problem can a web browser cause to the user if it has a mistake of ignoring Content-Security-Policy header?

2. How should a decompression program sanitize the file names of included files?

3. Find all potential vulnerabilities in this C snippet:

```
/* return 0123456789ABCDEF ASCII character */
char hex_char(char c) {
return '0' + c + ('A' - '0') * (c > 9);
}

int input_and_url_encode(void) {
    char input[500], encoded[1000];
    int i, j;

    scanf("%s", input);
    if (strlen(input) > 500) {
        return 0;
    }
    for (i = 0, j = 0; i < strlen(input); ++i) {
        encoded[j++] = '%';
        encoded[j++] = hex_char((input[i] >> 4) & 15);
        encoded[j++] = hex_char(input[i] & 15);
    }
    encoded[j] = 0; /* Null-terminate C string */
    return 1;
}
```

4. Find all potential vulnerabilities in this Ruby function:

```
def saveto(pattern, contents)
  filename = `ls -t #{pattern} | head -n 1`
  raise if File.stat(filename).symlink?
  File.open(filename, 'w') do |file|
    file.write contents
  end
end
```

5. Find all potential vulnerabilities in this JSP snippet:

```
<%
 String user = request.getParameter("user");
 user = user.replace ('<','&lt;');
 user = user.replace ('>','&gt;');
 Statement statement = conn.createStatement();
 ResultSet users = stmt.executeQuery(
   "select * from users where name="+user);
 String hobby = "unknown";
 if (users != null) {
  users.next();
  hobby = users.getString("hobby");
 }
%>

Hello, <%= user %>! Your hobby is <%= hobby %>.
```

Send response by e-mail to mroos@ut.ee no later than 14.00. You can answer either in English or in Estonian.