Secure Programming Techniques — exam 07.06.2013

1. Describe different attacks to learn other users’ session ID in web applications (as many as you can but at least 3).

2. What measures would you implement to solve the following races:
   - Two threads accessing the same shared array
   - Two processes creating temporary files in same directory

3. Find all potential vulnerabilities in this C function:

```c
int url_encode_and_validate(void) {
    char input[100], encoded[200];
    int ret = 0;
    int i, j;

    gets(input);
    if (strlen(input) > 100) {
        return 0;
    }
    j = 0;
    for (i=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;
    if (validate(encoded)) ret = 1;
    return ret;
}
```

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 shell script:

```
#!/bin/sh
# remove files with name pattern matching regexp

[ x$1 = x ] && { echo -n "Enter directory: "; read dir } || dir=$1
[ x$2 = x ] && { echo -n "Enter pattern: "; read pat } || pat=$1

find $dir > /tmp/listing
cmd='rm `grep "$pat" /tmp/listing`'

echo "Running command $cmd"; eval $cmd

rm /tmp/listing
```

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