Secure Programming Techniques exam 06.06.2017

1. Example historic web counter used architecture like that:

   - Apache web server
   - CGI application setuid to a real user
   - compiled C wrapper executing a
   - shell script for the logic
   - storing data file in the users home directory.

   What are the most probable vulnerability classes in this architecture?

2. How would you solve the following races:

   - Two processes of the same user accessing a file
   - Multiple processes of mutually untrusted users accessing a file

3. Find all potential vulnerabilities in this C function:

```
int prompt_and_save(char *question, unsigned char *data, int len) {
    unsigned char filename[32];
    int fd;

    printf(question);
    scanf("%s", filename);
    if (strlen(filename) > 32) {
        return 0;
    }
    unlink(filename); /* remove old file */
    fd = open(filename, O_WRONLY | O_CREAT, 0666);
    write(fd, data, len);
    close(fd);
    return 1;
}
```

4. Find all potential vulnerabilities in this PHP snippet:

```
<?php
if (isset($_REQUEST['theme']) {
    $file = fopen("/var/www/themes/".$_REQUEST['theme'], "r");
    fpassthru($file);
    fclose($file);
    $cmd="UPDATE themestats SET hits=hits+1 WHERE theme='".
        $_REQUEST['theme']."'");
    mysql_query($cmd) || die($cmd);
}
if (isset($_REQUEST['user']) {
    echo "Welcome, ".$_REQUEST['user'];
}
?>
```

5. What possible vulnerabilities could the following URL exploit? Find at least 4:

```
http://a.com/a.php/b.html?sessid=10203040506070809&user=`id`&
 pass=.&name=x'%20union%20select%20'z&message=%3ci%4dg+s%52c
 %3d%22j%61v%61S%43r%69pt%3a%61l%65rt(%27%2c%27)%3b%22%3e
```

Send response by e-mail to mroos@ut.ee no later than 16.00. You can answer either in English or in Estonian.