Lab 11.1: File Permissons
IN618 Security

May 11, 2015

Introduction

We've spent much of this semester learning about security vulnerabilities in code and how to avoid them. It doesn't matter how secure your code is, however, if you don't store your data correctly. In this lab you will see an example of an extremely common mistake made by web developers.

1 Setup

Using PuTTY, log into your account on `sec-student.sqrawler.com`. Create an instance of our vulnerable example with the following commands:

```
cd public_html
cp -R /home/tclark/public_html/permissions .
```

Experiment with the application by visiting `http://sec-student.sqrawler.com/~<your-username>/permissions` to get a sense for what it does.

2 Explore the vulnerability

The vulnerability in this application is fairly simple. There are only a few files where things can go wrong. Examine how the files are set up and see if you can recognise the problem before checking the reverse side of this lab handout.

3 Explanation of the vulnerability

We can see the vulernability by performing a file listing as follows:

```
ls -l ~/public_html/permissions
```

You will get output like this:

```
total 12
-rw-rw-r-- 1 tclark tclark 666 May 10 16:46 index.php
-rw-rw-r-- 1 tclark tclark 146 May 10 16:44 modifycss.php
-rwxrwxrwx 1 tclark tclark  67 May 10 16:49 style.css
```

The user/group names will be different when you run your command.

The problem is with the permissions on the file `style.css`. Anyone who can access the system has complete access to the file. In our case the problem is pretty innocuous, but if the file contained security-sensitive information this would be a big problem. Developers make this mistake *all the time*, because many of them don't properly grasp file ownership and permissions. In their efforts to get their applications to work they resort to setting their file permissions incorrectly.