Assignment 6: Attack!

1 Problem

You are to find an exploitable security vulnerability in a free software project, demonstrate that the vulnerability is real, provide a patch and finally issue a security advisory.

You are allowed to work on this project in groups of two. Furthermore, you should document (!) the steps of your security analysis. In case that you fail to find a vulnerability, your report can be used to demonstrate that you were just unlucky (but working hard and systematic in your approach). In this case, your report will be graded instead of the security advisory.

2 Approach

The suggested approach for finding vulnerabilities is to use the `coverity` static analysis tool on less-popular free software projects and to investigate the reported bugs. However, any other method that results in success is also welcome.

Look for C and C++ free software projects on `freshmeat.net`. You should not select too popular projects (top 100) or projects nobody cares about (not in top 10000 by popularity). Also applications that are generally installed SUID or run by root only are unlikely to be good targets. Network applications and libraries and in particular applications and libraries that parse *untrusted* input data (text, graphics, audio, video) are likely to be good targets. A specially crafted image or OpenOffice document causing koffice (import filter!) to execute arbitrary code would be a picture-perfect exploit.

In order to use `coverity`, you must be able to compile the software. If the Linux lab machines fail to satisfy the dependencies, feel free to request any Debian package to be installed on the system(s).

3 Implementation

You are to implement a simple program that demonstrates the vulnerability.

Furthermore, you should provide a patch that addresses the security problem.

4 Submission

You must submit the security advisory in ASCII to your subversion repository to the directory `courses/comp3704/s2007/$USER/p6/`. Your advisory should include a reference to the original sources.

Also submit the patch (generated with `diff`) and the exploit code. Do not include generated files.