

**Bearbeiter:** Gideon Schwarz mail@gideon-schwarz.de

**Datum:** 12.6.04

**Toolname:** Flawfinder

**Herkunft:** Open Source / Autor David Wheeler

**Zielsprachen:** C / C++

**Plattform:** Linux

**Lizenzstatus:** General Public License (GPL) Version 2

**Kurzbeschreibung der Funktionalität:**

Flawfinder durchsucht Quelltexte nach Befehlen, die zu einem Sicherheitsloch führen kann und gibt Warnung aus. Die Ausgabe ist sehr detailliert und gibt Zeile, Art und Grund des Sicherheitslochs aus. Allerdings wird nur nach bestimmten Befehlen und Bezeichnungen gesucht, so dass Warnungen ausgegeben werden zu Befehlen, die absolut sicher sind.

**Erfahrungen im Umgang:**

- Installation: RPM - Paket
- Stabilität : keine Stabilitätsprobleme
- Performanz: Sehr schnell
- Handhabbarkeit: Einfach, obwohl Konsolen Programm
- Einarbeitungsaufwand: keinen
- Oberfläche: ASCII
- Sonstiges:

**Quellen:** <http://www.dwheeler.com/flawfinder>

**Toolname: Rats**

**Herkunft:** Open Source /Secure Software Inc

**Zielsprachen:** C/C++, Perl, PHP, Python

**Plattform:** Windows/Linux

**Lizenzstatus:** General Public License (GPL) Version 2

**Kurzbeschreibung der Funktionalität:**

Rats durchsucht Quelltexte nach Befehlen, die zu einem Sicherheitsloch führen kann und gibt Warnung aus. Die Ausgabe ist sehr detailliert und gibt Zeile, Art und Grund des Sicherheitslochs aus. Allerdings wird nur nach bestimmten Befehlen und Bezeichnungen gesucht, so dass Warnungen ausgegeben werden zu Befehlen, die absolut sicher sind.

**Erfahrungen im Umgang:**

- Installation:       Linux: entpacken Makefile ausführen  
                          Windows: entzippen und starten
- Stabilität : Keine Stabilitätsprobleme
- Performanz: sehr schnell
- Handhabbarkeit: einfach, obwohl Konsolenprogramm
- Einarbeitungsaufwand: keinen
- Oberfläche: ASCII
- Sonstiges: findet nicht jeden Fehler und findet „keine“ Fehler

**Quellen:** [http://www.securesw.com/download\\_rats.htm](http://www.securesw.com/download_rats.htm)

**Toolname: PSCAN**

**Herkunft:** Open Source / Autor Alan Dekok

**Zielsprachen: C**

**Plattform: Linux**

**Lizenzstatus: kein**

**Kurzbeschreibung der Funktionalität:**

Auch PSCAN durchsucht den Quelltext, allerdings sucht PSCAN nach Lücken für eine Format String Attacke. Man hat auch die Möglichkeit eigene Definitionen anzugeben nach denen gesucht werden soll.

**Erfahrungen im Umgang:**

- Installation: benötigt Lex und/oder Yacc; dann entpacken und Makefile ausführen
- Stabilität : Keine Stabilitätsprobleme
- Performanz: sehr schnell
- Handhabbarkeit: einfach, obwohl Konsolenprogramm
- Einarbeitungsaufwand: keinen
- Oberfläche: ASCII
- Sonstiges:

**Quellen:** <http://www.striker.ottawa.on.ca/~aland/pscan/>

**Toolname: Bfbtester**

**Herkunft:** Open Source / Autor Mike Heffner

**Zielsprachen: C/C++**

**Plattform: Linux**

**Lizenzstatus: General Public License (GPL)**

**Kurzbeschreibung der Funktionalität:**

Bfbtester testet, anders als die vorherigen Tools, den Binärcode eines Programms, indem es das Programm aufruft mit allen möglichen und unterschiedlich Großen Argumente als Eingabe. Dabei beobachtet Bfbtester das Programm auf Verhalten und gibt die Beobachtung als Eingabe aus. Man erhält eine sehr große Ausgabe für ein kleines Programm und kann keine genauen Rückschlüsse auf einen Fehler machen.

**Erfahrungen im Umgang:**

- Installation: Entpacken und Makefile ausführen
- Stabilität : keine Stabilitätsprobleme, soll aber bei der Ausführung viel Speicher benötigen
- Performanz: im Vergleich mit den anderen Tool sehr langsam
- Handhabbarkeit: einfach, obwohl Konsolen Programm
- Einarbeitungsaufwand: geringer
- Oberfläche: ASCII

- Sonstiges: Meiner Meinung nach nicht sehr hilfreich!

**Quellen:** <http://bfbtester.sourceforge.net/>