The **find** command has an operator that makes finding your vulnerable files easy. The **-perm** operator is usually followed by a three- or four-digit set of permissions, such as the example shown here:

find /usr/bin -perm 777

This example searches for any object in the **/usr/bin** directory and all subdirectories that has the exact permissions of rwxrwxrwx. This is fine, but it doesn’t help find security risks caused by the SUID and SGID bits. This next command does, however:

find / -perm -4000

At first glance, this might look as if we’re searching for all files that have the SUID bits and then blank permissions from that point on. It really searches the entire system for all files that have the SUID bit set, regardless of the other permissions.

You should install the system and then run a **find** command that reports any file that has an SUID bit set, like so:

find / -perm -4000 -ls

Redirect this output to a file and keep that file on a disk or in some safe place off the system (like on a USB drive). Every so often (especially after installing new software or when you think your system has been exploited), you should run the same **find** command and then compare the results to the original with the **diff** command, such as:

[**Click here to view code image**](ch10_images.html#p303pro01a)

diff /root/latestfindperm /mnt/usb/findperm.orig

Investigate any differences!