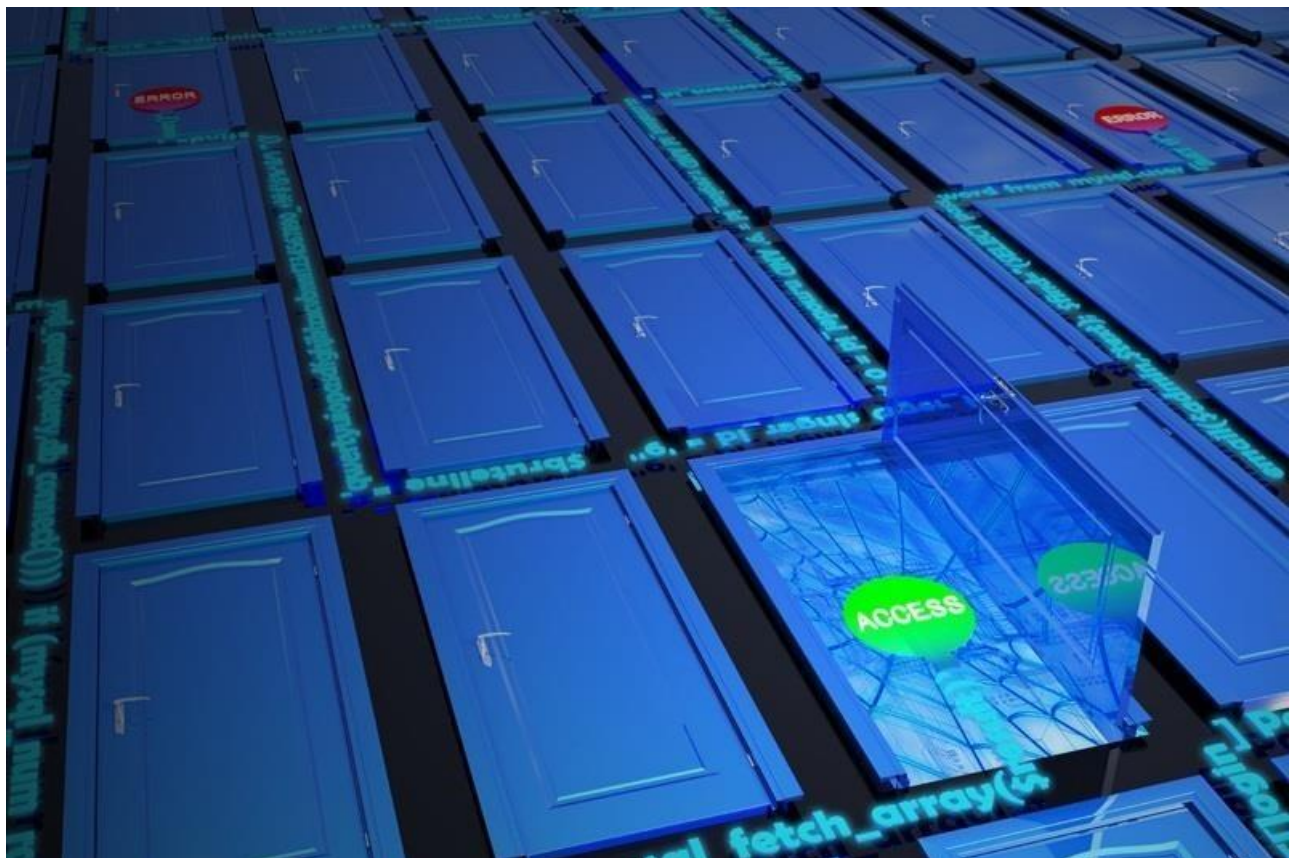


# How to Find Almost Every Known Vulnerability & Exploit Out There

Earlier, I wrote a guide on [finding operating system and application vulnerabilities](#) in Microsoft's own security bulletins/vulnerability database. In this tutorial, I will demonstrate another invaluable resource for finding vulnerabilities and exploits by using the [SecurityFocus](#) database.

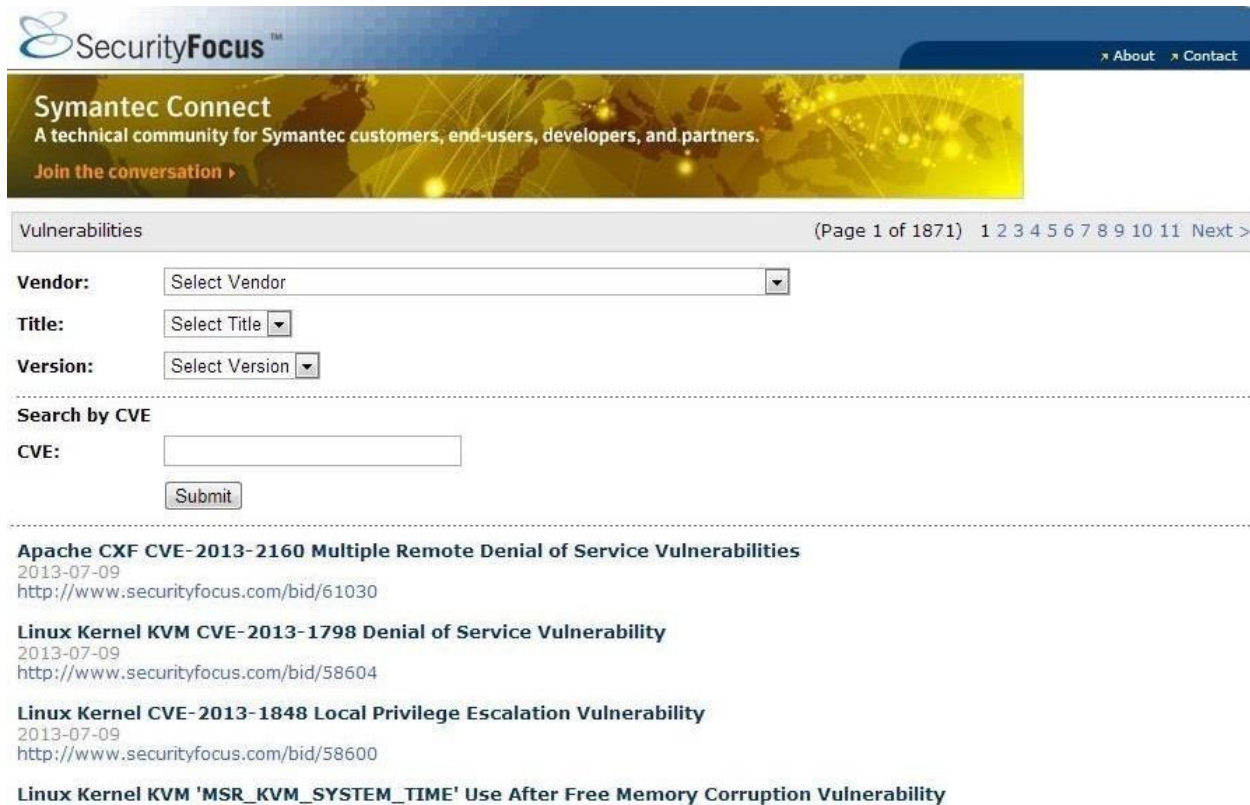
Most often, when we're trying to hack a system, the vulnerabilities and exploits that will work on the target are not going to be simply handed to us, like I have done in these tutorials. We need to do a bit of research to find what will work on a particular target system. After running [reconnaissance on the system](#), we can determine what operating system is running, what ports are open, and what services are running. From there, we need to decide upon the best strategy to compromise the system without being detected. That's not always going to be obvious or simple.



We most likely will have to do a little research first to find the proper vulnerability on the target system and then find an exploit to take advantage of it. In this tutorial, we'll look at one of the most complete and helpful resources in finding vulnerabilities and exploits.

## Step 1 Navigate to SecurityFocus

Let's start by navigating to [www.securityfocus.com](http://www.securityfocus.com). It should look like this.



The screenshot shows the SecurityFocus website interface. At the top is the SecurityFocus logo and navigation links for 'About' and 'Contact'. Below this is a yellow banner for 'Symantec Connect' with the text 'A technical community for Symantec customers, end-users, developers, and partners.' and a 'Join the conversation' link. The main content area is titled 'Vulnerabilities' and includes a pagination bar showing '(Page 1 of 1871)' and a series of numbers from 1 to 11, followed by 'Next >'. Below the pagination bar are search filters: 'Vendor:' with a 'Select Vendor' dropdown, 'Title:' with a 'Select Title' dropdown, and 'Version:' with a 'Select Version' dropdown. A section titled 'Search by CVE' contains a 'CVE:' text input field and a 'Submit' button. Below the search filters is a list of vulnerabilities, each with a title, date, and URL. The first entry is 'Apache CXF CVE-2013-2160 Multiple Remote Denial of Service Vulnerabilities' dated 2013-07-09 with URL 'http://www.securityfocus.com/bid/61030'. The second entry is 'Linux Kernel KVM CVE-2013-1798 Denial of Service Vulnerability' dated 2013-07-09 with URL 'http://www.securityfocus.com/bid/58604'. The third entry is 'Linux Kernel CVE-2013-1848 Local Privilege Escalation Vulnerability' dated 2013-07-09 with URL 'http://www.securityfocus.com/bid/58600'. The fourth entry is 'Linux Kernel KVM 'MSR\_KVM\_SYSTEM\_TIME' Use After Free Memory Corruption Vulnerability'.

We can see that the SecurityFocus database has some handy tools for searching for vulnerabilities. It will allow us to search by vendor, by title of the software and by the version. Finally, it will allow us to search by CVE, which is the Common Vulnerability and Exploit number. These numbers are assigned by Mitre Corporation, who is funded by the National Cyber Security Division of the U.S. Homeland Security.

## Step 2 Searching for Vulnerabilities

The CVE database includes nearly every vulnerability that has been found in the wild or discovered by security researchers, even if the software publisher doesn't want it known or hasn't patched it yet.

For instance, Adobe has had a very bad run in recent years with poorly designed software that's full of security vulnerabilities. These include such ubiquitous software as Adobe Reader, Adobe Flash, etc. Since nearly every client-side computer system has Adobe Flash or Reader installed on it, let's take a look at the known vulnerabilities to these applications.

Let's look at Adobe Flash. Simply select Adobe in the pull-down menu of vendors and then select Flash Player from the pull-down in the title window. Finally, click on the submit button and the system will return pages of Adobe Flash Player vulnerabilities.

info

discussion

exploit

solution

references

---

### Adobe Flash Player APSB13-17 Multiple Remote Code Execution Vulnerabilities

Bugtraq ID: 61038

Class: Unknown

CVE: CVE-2013-3344  
CVE-2013-3345  
CVE-2013-3347

Remote: Yes

Local: No

Published: Jul 09 2013 12:00AM

Updated: Jul 09 2013 12:00AM

Credit: Mateusz Jurczyk, Gynvael Coldwind and Fermin Serna of the Google Security Team, Vulnazoid via HP's Zero Day Initiative

Vulnerable: Adobe Flash Player for Android 11.1.102.59  
Adobe Flash Player 10.1.53 .64  
Adobe Flash Player 10.1.51 .66  
Adobe Flash Player 10.0.45 2  
Adobe Flash Player 10.0.45 2  
Adobe Flash Player 10.0.45 2  
Adobe Flash Player 10.0.32 18  
Adobe Flash Player 10.0.22 .87  
Adobe Flash Player 10.0.15 .3  
Adobe Flash Player 10.0.12 .36  
Adobe Flash Player 10.0.12 .35  
Adobe Flash Player 11.2.202.235  
Adobe Flash Player 11.2.202.233  
Adobe Flash Player 11.2.202.229  
Adobe Flash Player 11.2.202.228  
Adobe Flash Player 11.2.202.228

The very first vulnerability to appear is **Adobe Flash Player APSB13-17 Multiple Remote Code Execution Vulnerabilities**. This is a brand new vulnerability just published July 9, 2013. Woohoo!

Even better, it allows for "remote code execution," or in other words, it will allow for the installation of a listener/rootkit on the system running Flash Player. If we scroll down, we see that this vulnerability is included in the Android Flash Player 11.1.102.59 and nearly every version of Adobe Flash Player right up to 11.2.202.235. Since the current version of

Adobe Flash Player is 11.8, this would mean that unless the user has updated their Flash Player very recently, this vulnerability exists on their system.

## Step 3 Finding Exploits

Now that we've found a vulnerability that virtually every PC will have, the next step is to find an exploit. A vulnerability is simply a weakness or hole in the system that *can* be exploited, it does not necessarily mean it *has* been exploited. Developing an exploit requires some advanced coding skills, but is not beyond the capability of a talented, aspiring hacker.

To find the exploit for this vulnerability, we simply need to click on the **EXPLOIT** tab at the top of the page. This will open that tab and reveal any and all exploits that have been developed for that vulnerability. When we do that for this brand new vulnerability, we can see that no one has yet developed the exploit.



So....all my newbie hackers, here is your opportunity to make your name and develop an exploit for this brand new vulnerability!

## Step 4 More Adobe Flash Vulnerabilities

We can see that SecurityFocus has over four pages of vulnerabilities for Adobe Flash alone. This doesn't count all the other Adobe products that are almost as flawed as Flash Player. Do you have any question in your mind now why Apple banned Flash Player from its iOS?

Let's take a look at some of the other Flash Player vulnerabilities. If we scroll down a bit, we come to a vulnerability called **Adobe Flash Player CVE-2012-0754**. That one sounds interesting, let's click on it.

	info	discussion	exploit	solution	references
<b>Adobe Flash Player CVE-2012-0754 Remote Memory Corruption Vulnerability</b>					
Bugtraq ID:	52034				
Class:	Unknown				
CVE:	CVE-2012-0754				
Remote:	Yes				
Local:	No				
Published:	Feb 15 2012 12:00AM				
Updated:	Jun 20 2013 09:40AM				
Credit:	Alexander Gavrun through TippingPoint's Zero Day Initiative				
Vulnerable:	SuSE SUSE Linux Enterprise Desktop 11 SP1 for SP2				

We can see that it was published just last year ago in February 2012 and was updated just last June 2013. If we look down a bit, we can see all the browsers and operating systems that are vulnerable when running Flash Player.

Now, if we click on the Exploit tab, we can see that an exploit is available and we can get it through clicking on the link.

	info	discussion	exploit	solution	references
<b>Adobe Flash Player CVE-2012-0754 Remote Memory Corruption Vulnerability</b>					
The following exploit is available:					
<ul style="list-style-type: none"> <li>• <a href="#">/data/vulnerabilities/exploits/52034.rb</a></li> </ul>					

## Step 5 Finding the Exploit for Use in Metasploit

Finally, we can go to [BackTrack](#) and open [Metasploit](#). There we can search for this exploit search for this exploit.

- **msf> search adobe flash mp4**

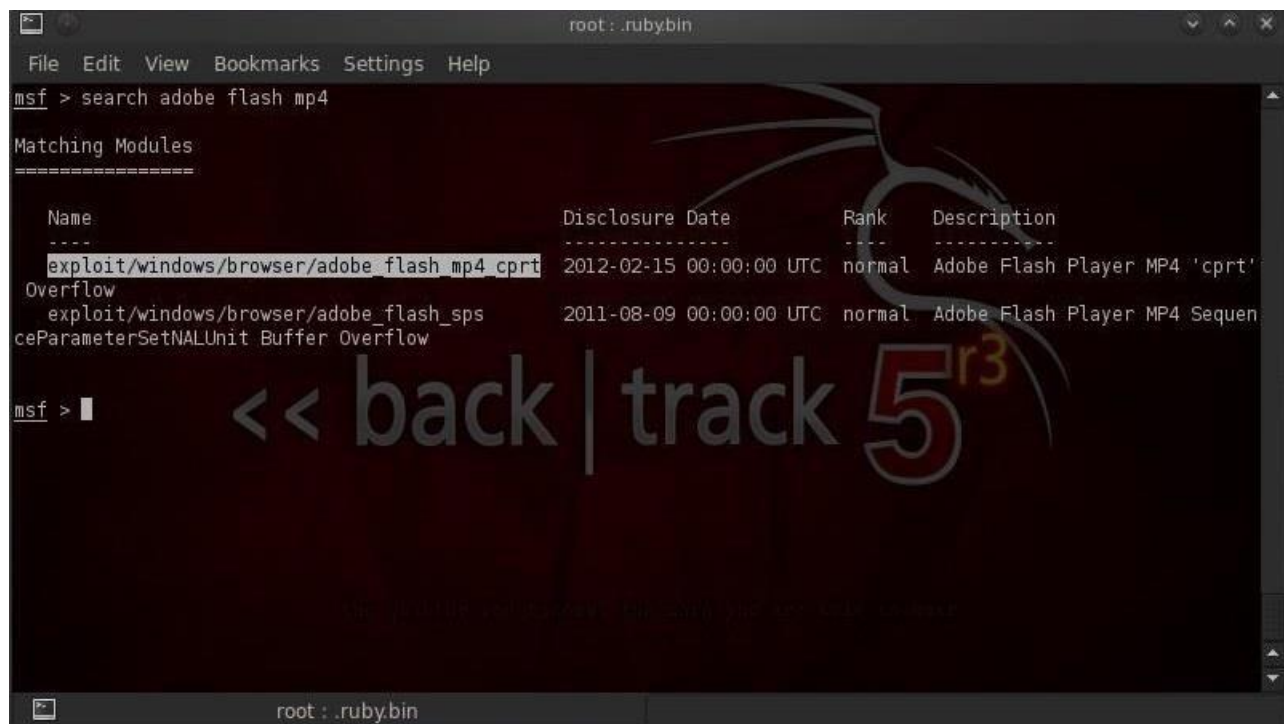


```
root: .rubybin
File Edit View Bookmarks Settings Help
msf > search adobe flash mp4

Matching Modules
=====

  Name                                           Disclosure Date   Rank   Description
  ----                                           -
  exploit/windows/browser/adobe_flash_mp4_cpri  2012-02-15 00:00:00 UTC normal Adobe Flash Player MP4 'cpri'
  Overflow
  exploit/windows/browser/adobe_flash_sps       2011-08-09 00:00:00 UTC normal Adobe Flash Player MP4 Sequen
  ceParameterSetNALUnit Buffer Overflow

msf > |
```



We can see that Metasploit has incorporated this exploit into its latest version and updates and is ready for us to use to own nearly any system (XP, Vista, and Windows 7 SP1) running Adobe Flash!