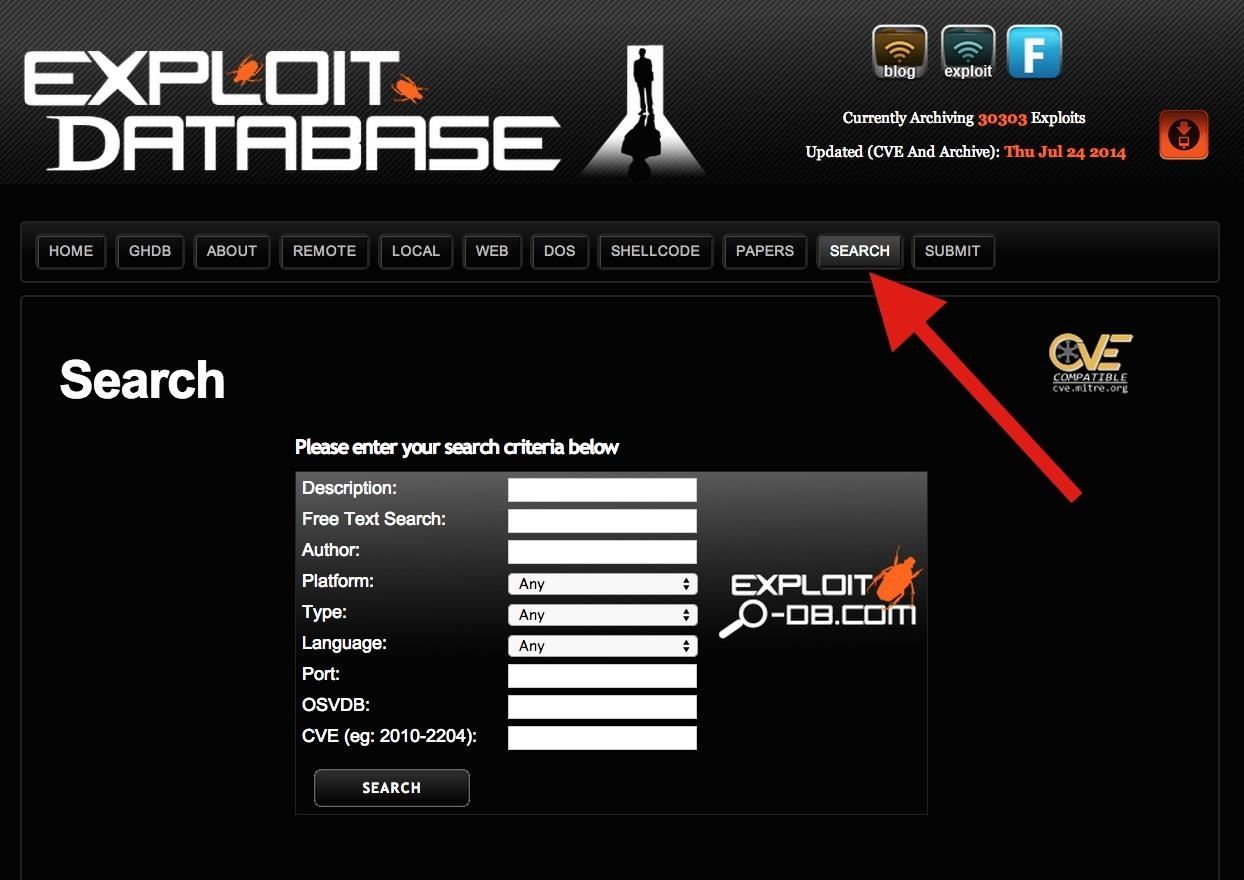
How to Find Exploits Using the Exploit Database in Kali

[](https://img.wonderhowto.com/img/original/30/10/63541799599573/0/635417995995733010.jpg)

***Author & Credits:***

*Occupytheweb*

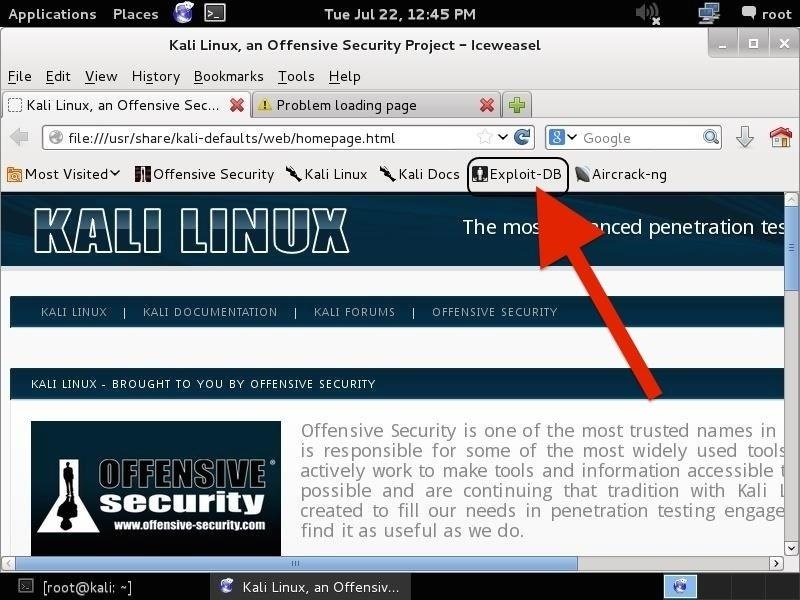
*https://creator.wonderhowto.com/occupythewebotw/*

When we are looking for ways to hack a system, we need a specific exploit to take advantage of a certain vulnerability in the operating system, service, or application. Remember, exploitation is very specific, there is no one silver bullet that will allow you to exploit all systems. You need to find an exploit that will specifically take advantage of a vulnerability in the system that you are attacking. That is where the [**Exploit Database**](http://www.exploit-db.com/) can be so incredibly useful.

EDB is a project of [Offensive Security](http://www.offensive-security.com/), the same folks who developed [BackTrack](../../../../docs/Technology/Hacking/ExploitDatabase/BackTrack.pdf) and [Kali Linux](../../../../docs/Technology/Hacking/ExploitDatabase/Kali.pdf), which includes exploits categorized by platform, type, language, port, etc. to help you find the exploit that will work in your particular circumstance. Then, if you feel it will work on your target, you can simply copy and paste it into Kali for your attack.

Step 1 Fire up Kali & Open a Browser

Let's start by firing up Kali and opening a browser, such as Iceweasel, the default browser in Kali (EDB can be reached from any browser, in any operating system). If we use the default browser in Kali, we can see that there is a built-in shortcut to the "Exploit-DB" in the browser shortcut bar, as seen below.



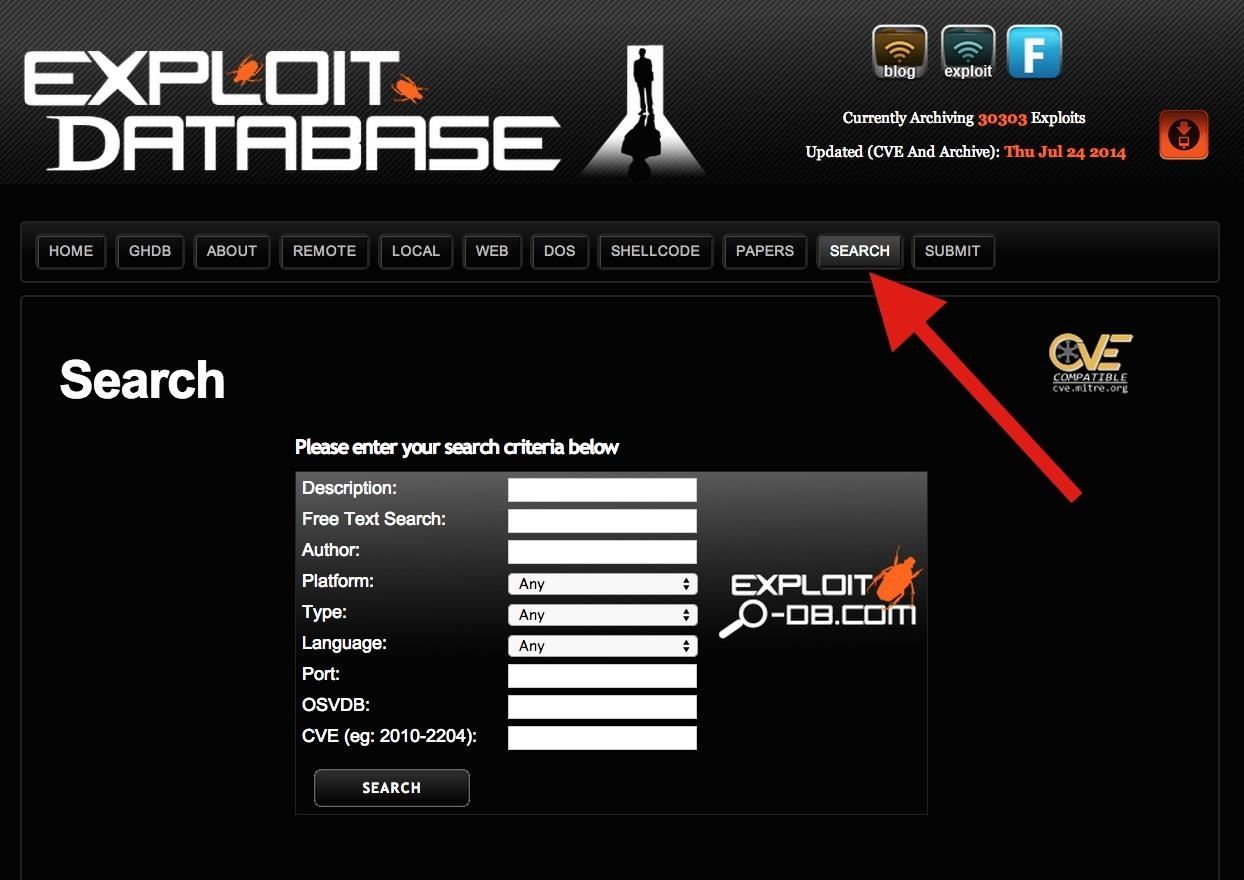
When we click on it, it takes us to the Exploit Database, as seen below.



If you are not using Iceweasel and its built-in shortcut, you can navigate to Exploit-DB by typing [**www.exploit-db.com**](http://www.exploit-db.com) in the URL bar.

Step 2 Search the Exploit Database

If we look at the top menu bar in the Exploit Database website, second from the right is a menu item called "Search". When we click on it, it enables us to search the database of exploits and returns a search function screen similar to the screenshot below.

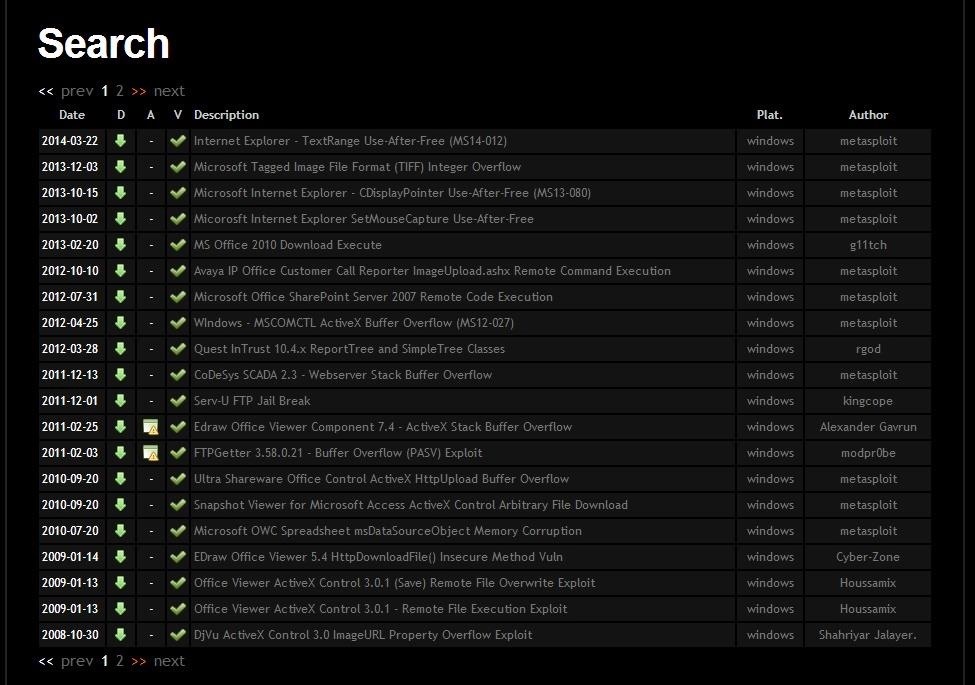
[](https://img.wonderhowto.com/img/original/30/10/63541799599573/0/635417995995733010.jpg)

Let's use this search function to find some recent Windows exploits (we are always looking for new Windows exploits, aren't we?). In the search function window, we can enter any of the following information;

* Description
* Free Text Search
* Author
* Platform (this is the operating system)
* Type
* Language
* Port
* OSVDB (the Open Source [Vulnerability](https://www.youtube.com/watch?v=K78YOmbuT48) Database)
* CVE ([Common Vulnerability and Exploits](../../../../docs/Technology/Hacking/ExploitDatabase/SecurityFocus.pdf))

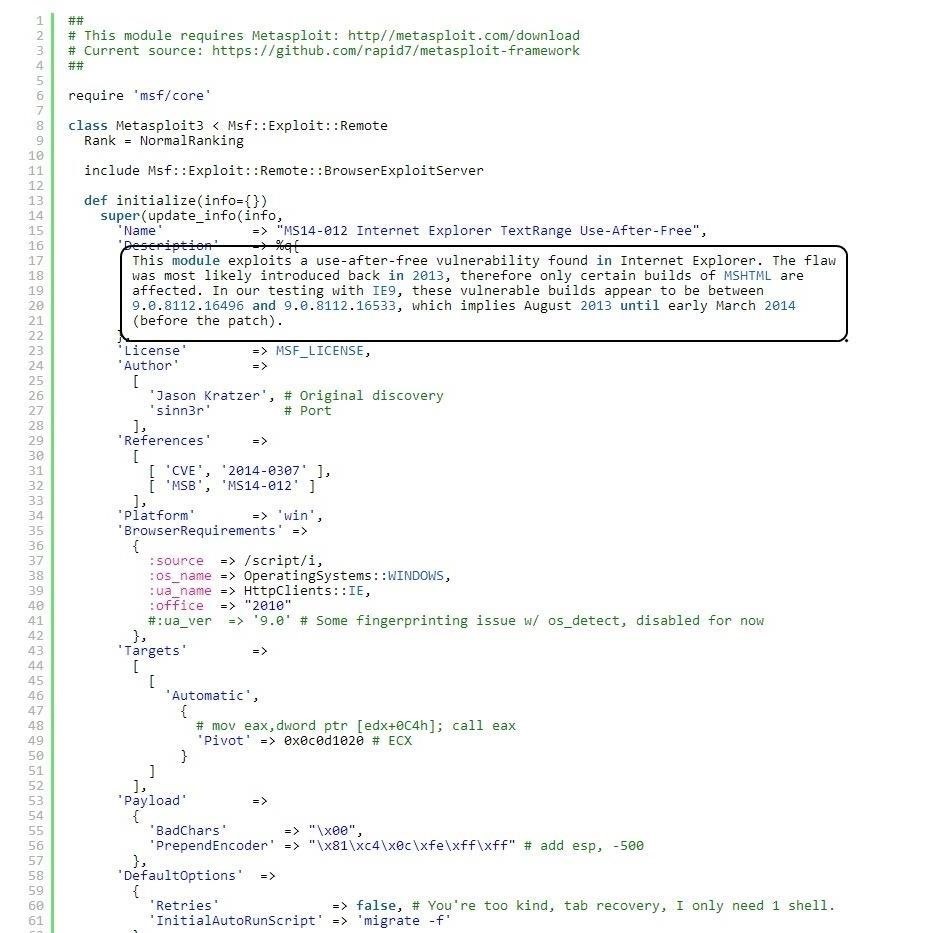
The last two fields can be used if you are specifically looking for an exploit that takes advantage of a known, numbered vulnerability in either of those databases.

In the Platform field, enter "Windows", in the Type field, enter "remote", and in the Free Text Search box, enter "Office". When we do so, the Exploit Database returns a list and a link to all of the exploits that meet those criteria. Of course, you can put in whatever criteria you are searching for. I am only using these as an example.



Step 3 Open an Exploit

From the search results page, we can click on any of the two pages of search results and it will take us to the particular exploit. I clicked on the very first exploit in the list "Internet Explorer TextRange Use-After Free (MS14\_012)". When I do so, I am brought to a screen that displays the exploit code like that below. I have circled the description in the code of the exploit.

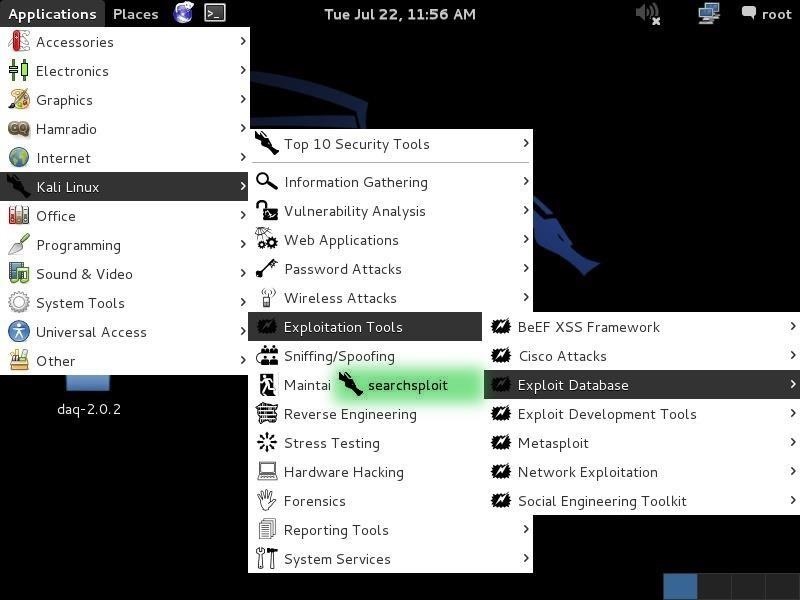


This exploit works against Internet Explorer that was built between August 2013 and March 2014. If you want to use it, you can simply copy and paste this text file and put it into the exploit directory in [Metasploit](../../../../docs/Technology/Hacking/ExploitDatabase/Metasploit.pdf) (if you are using an up-to-date version of Metasploit, it is already included). This is a good example of how specific an exploit can be.

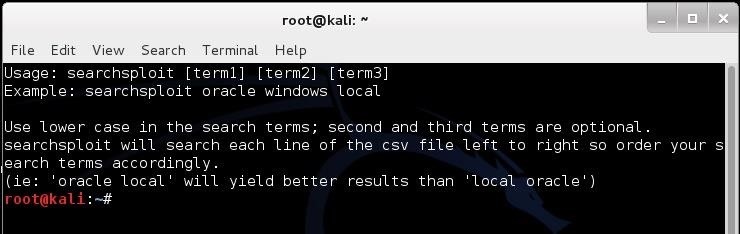
Step 4 Open up Searchsploit

Kali, having also been developed by Offensive Security, has built into it a local database of exploits based on the same Exploit Database. We can access it by going to

Applications -> Kali Linux -> Exploitation Tools -> Exploit Database and clicking on **searchsploit** as shown below.



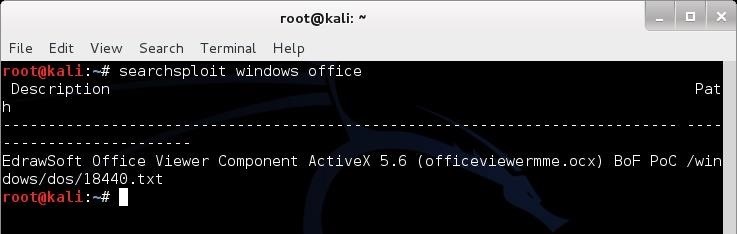
It will open a screen like that below that details the basic syntax on how to use searchsploit. Note that it explains that you must use lowercase search terms and that it searches a CSV (comma separated values) file from left to right, so search term order matters.



Step 5 Search the Exploit Database with Searchsploit

Now that we have opened a terminal for searchsploit, we can now use this tool to search our local copy of the Exploit Database. As you might expect, our local copy of the exploit database is much faster to search, but does NOT have all the updates that the online database does. Despite this, unless we looking for the very latest exploits, the local database works fast and is effective.

One other note on its use. As the information is organized in CSV files, searches locally often will yield results slightly differently than the online database. In the screenshot below, I searched for "Windows" and "Office" and only received a single result, unlike what I received when I used the online database.



Exploit Database is an excellent repository for exploits and other hacks that we might need, including new Google hacks, white papers on security and hacking, denial of service (DOS) attacks, and shellcode that you can use out the box or tailor for your unique attack.