

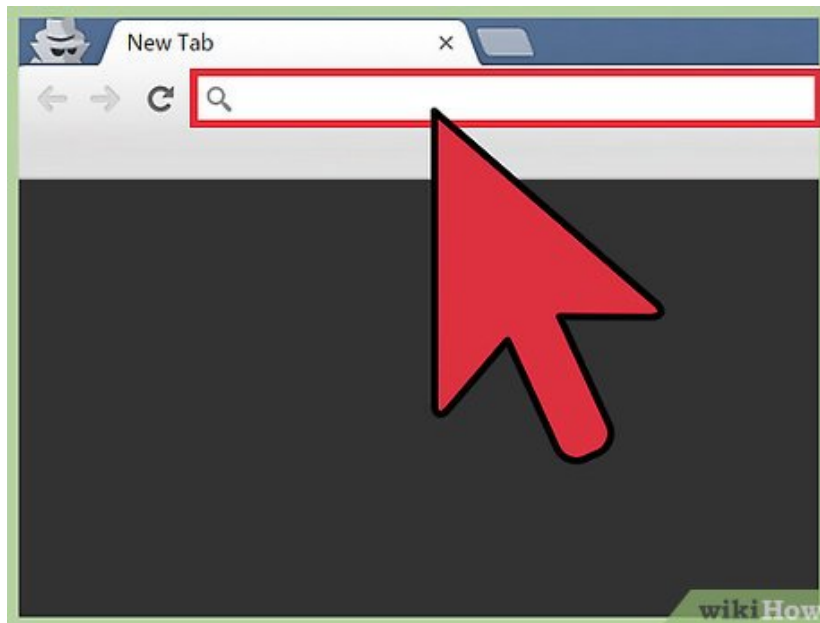
How to Hack a Database

The best way to make sure your database is secure from hackers is to think like a hacker. If you were a hacker, what sort of information would you be looking for? How would you try to get it? There are numerous types of databases and many...

Method 1 of 3:

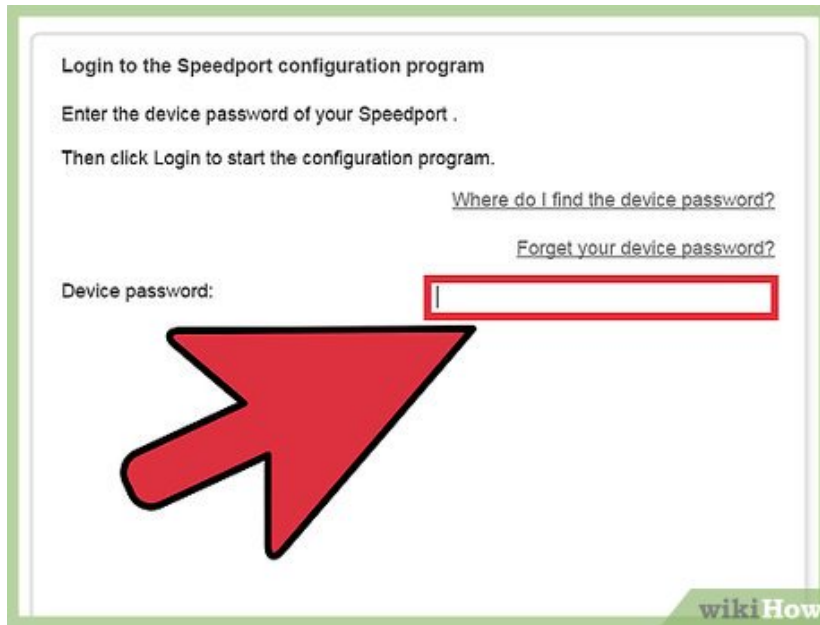
Using a SQL Injection

1.



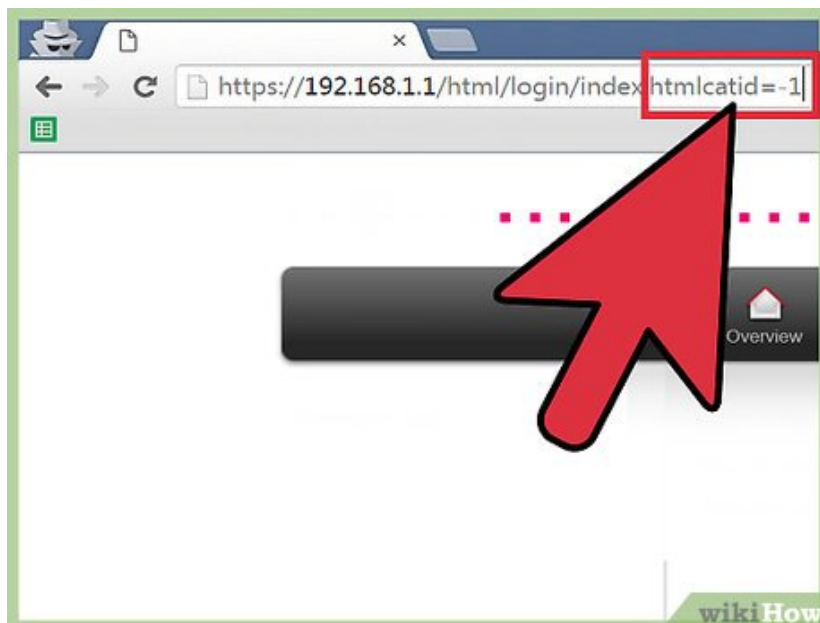
Find out if the database is vulnerable.^[1] You'll need to be handy with database statements to use this method. Open the database web interface login screen in your web browser and type a `'` (single quote) into the username field. Click 'Login.' If you see an error that says something like 'SQL Exception: quoted string not properly terminated' or 'invalid character,' the database is vulnerable to SQL injections.

2.

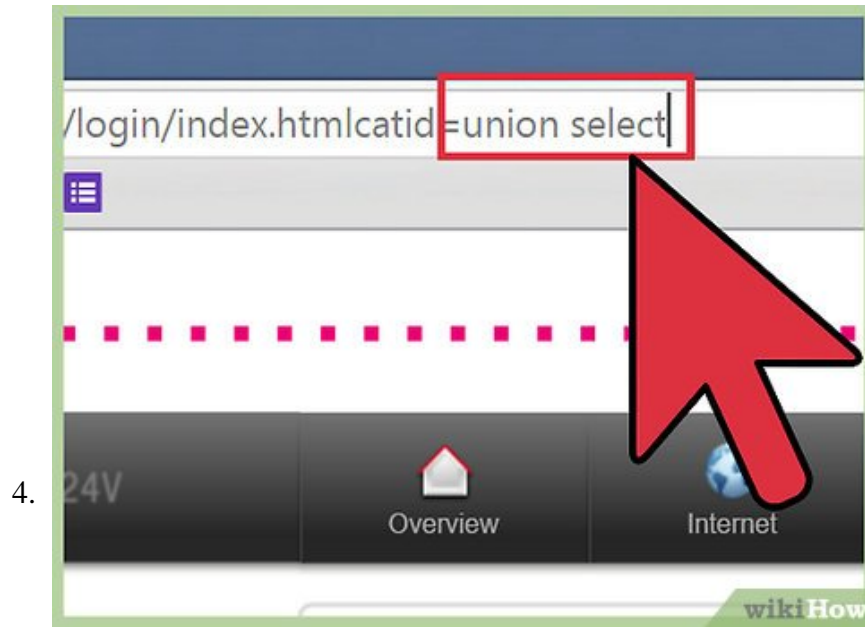


Find the amount of columns.^[2] Return to the login page for the database (or any other URL that ends in 'id=' or 'catid=') and click into the browser address box. After the URL, hit the space bar and type `order by 1`, then hit `Enter`. Increase the number to 2 and press `Enter`. Keep increasing until you get an error. The actual number of columns is the number you entered before the number that gave you the error.

3.



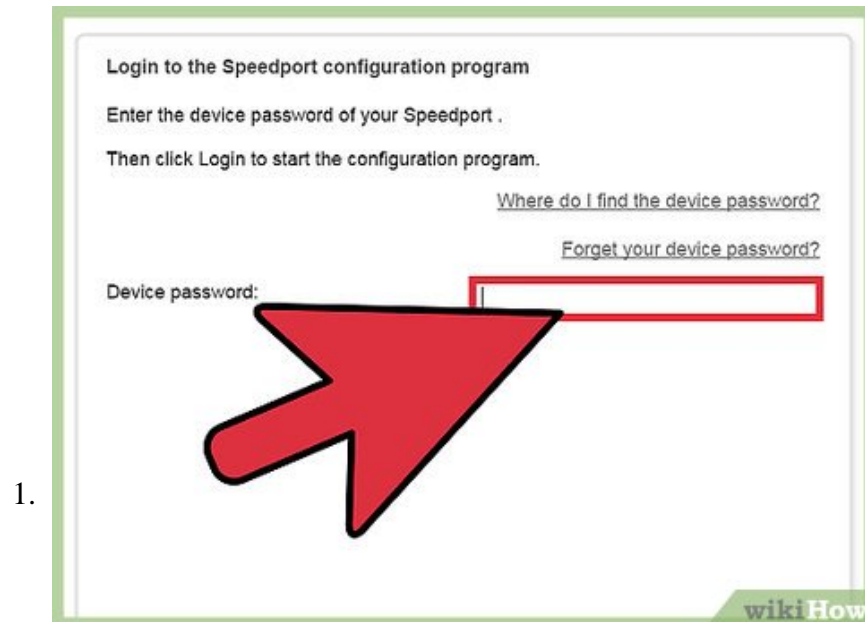
Find which columns accept queries. At the end of the URL in the address bar, change the `catid=1` or `id=1` to `catid=-1` or `id=-1`. Hit the space bar and type `union select 1,2,3,4,5,6` (if there are 6 columns). The numbers should count all the way up to the total amount of columns, and each should be separated by a comma. Press `Enter` and you'll see the numbers of each column that will accept a query.



Inject SQL statements into the column. For example, if you want to know the current user and want to put the injection in column 2, erase everything after the id=1 in the URL and hit the space bar. Then, type `union select 1,concat(user()),3,4,5,6--`. Hit `Enter` and you will see the name of the current database user on the screen. Use any SQL statements you'd like to return information, such as lists of usernames and passwords to crack.

Method 2 of 3:

Cracking the Database Root Password



Try logging in as root with the default password. Some databases don't have a root (admin) password by default, so you may be able to get in leaving the password field empty. Some others have default

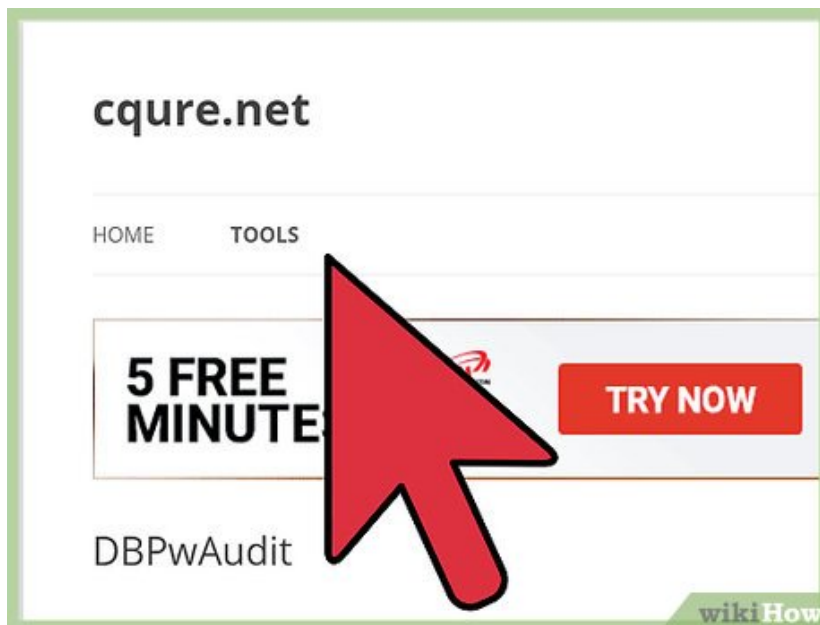
passwords that can be found easily by searching database tech support forums.



2.

Try common passwords. If the admin secured the account with a password (a likely situation), try common username/password combinations. Some hackers publicly post lists of passwords they've cracked while using auditing tools. Try some different username and password combinations.

1. A reputable site with collected password lists is <https://github.com/danielmiessler/SecLists/tree/master/Passwords>.
2. Trying passwords by hand can be time-consuming, but there's no harm in giving it a shot before breaking out the big guns.



3.

Use a password auditing tool.^[3] You can use a variety of tools to try thousands of dictionary words and letter/number/symbol combinations by brute force until the password is cracked.

1. Tools like DBPwAudit (for Oracle, MySQL, MS-SQL and DB2) and Access Passview (for MS Access) are popular password auditing tools that can be run against most databases.^[4] You can also

- search Google for newer password auditing tools specifically for your database. For instance, a search for password audit tool oracle db if you're hacking an Oracle database.
2. If you have an account on the server that hosts the database, you can run a hash cracker like John the Ripper against the database's password file. The location of the hash file is different depending on the database.^[5]
 3. Only download from sites that you can trust. Research tools extensively before using them.

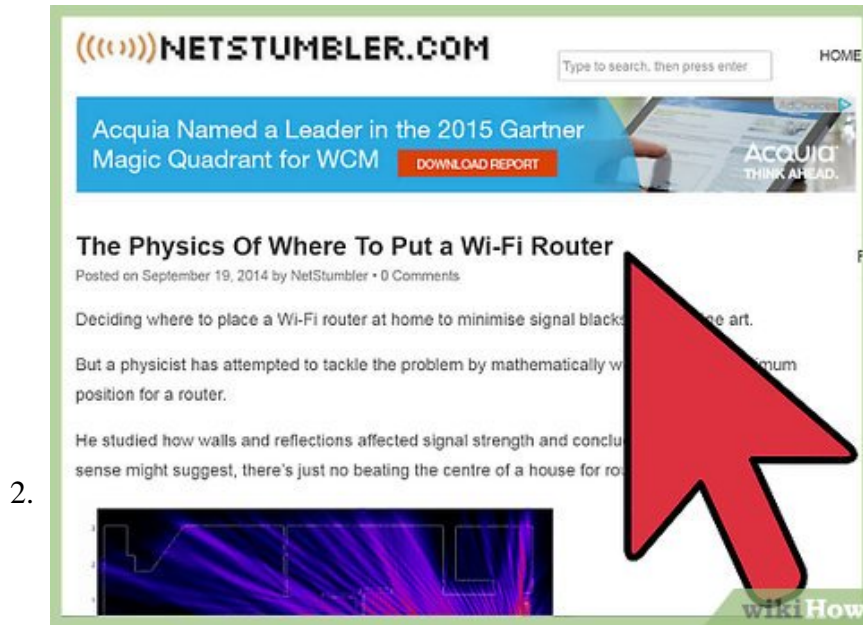
Method 3 of 3:

Running Database Exploits

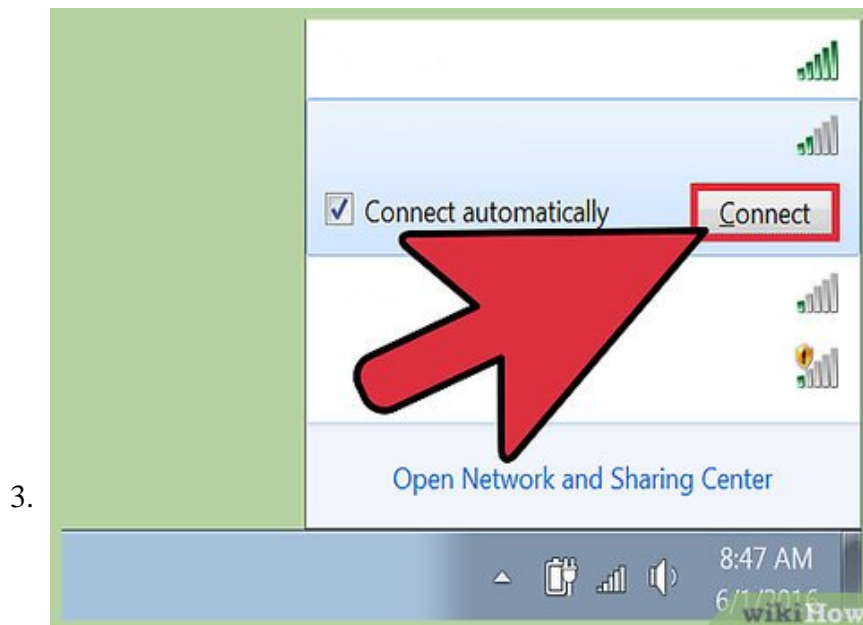


Find an exploit to run.^[6] Sectools.org has been cataloging security tools (including exploits) for over ten years. Their tools are reputable and used by system administrators all over the world for security testing. Browse their 'Exploitation' database (or find another trustworthy site) to find tools or text files that help you exploit security holes in databases.

1. Another site with exploits is www.exploit-db.com. Go to their website and click the Search link, then search for the type of database you want to hack (for example, 'oracle'). Type the Captcha code in the provided square and search.
2. Be sure you research all exploits you plan to try so you know what to do in case of potential issues.



Find a vulnerable network by wardriving.^[7] Wardriving is driving (or biking, or walking) around an area while running a network scanning tool (like NetStumbler or Kismet) in pursuit of an unsecured network. Wardriving is technically legal. Doing something illegal from a network you find while wardriving is not.



Use the database exploit from the vulnerable network. If you're doing something you're not supposed to be doing, it's probably not a good idea to do it from your own network. Connect wirelessly to one of the open networks you found while wardriving and run the exploit you've researched and chosen.

You finished reading the article "**How to Hack a Database**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.

