# How to Hack a Database

*Test your database security with this easy-to-follow guide*

**Written by Nicole Levine, MFA**

**Last Updated: March 6, 2023**

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 different ways to hack them, but most hackers will either try to crack the database root password or run a known database exploit. If you're comfortable with SQL statements and understand database basics, you can hack a database.

Method 1

## 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.

4 **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

## Method 2 of 3: Cracking the Database Root Password

1 **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.

- A reputable site with collected password lists is https://github.com/danielmiessler/SecLists/tree/master/Passwords.
- 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.** 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.

- 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.[3] 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.
- 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.[4]

- Only download from sites that you can trust. Research tools extensively before using them.

Method 3

## Method 3 of 3: Running Database Exploits

1 **Find an exploit to run.**[5] 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.

- 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.
- Be sure you research all exploits you plan to try so you know what to do in case of potential issues.

2 **Find a vulnerable network by wardriving.**[6] 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.

3 **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.

## Community Q&A

Question

### How would I hack a school exam council?

> Community Answer
>
> You have to figure out the parameters of the school exam council. What do you want to hack? Is wifi available? Do they have (connected) cameras in the room? A big part of being a hacker is finding an entry point. So, make sure you study the situation before doing anything big.

Question

### How do I hack a government database?

> Community Answer
>
> With difficulty. Governments across the world build in to their risk assessments the possibility of users with malicious intent and overseas government agencies and build in safeguards against these. Unless you are an experienced hacker, you will stand little to no chance of getting in. You're better off searching for tutorials and general advice on hacking data centers rather than specifically asking about government ones. I am a business analyst for a government organization currently working on data center replication.

Question

### How do I hack any WiFi password?

> Community Answer
>
> Often most people will use simple exploits. OSes Such as Kali Linux have a huge variety of tools.

See more answers

## Tips

- Always keep sensitive data behind a firewall.
- Make sure to protect your wireless networks with a password so wardrivers can’t use your home network to run exploits.
- Find other hackers and ask for tips. Sometimes the best hacking knowledge is kept off the public Internet.

## Warnings

- Gaining access to a database that isn’t yours is illegal.
- Never try to gain illegal access to a machine from your own network.
- Understand the laws and repercussions of hacking in your country.

## References

1. http://blog.red-database-security.com/2009/01/17/tutorial-oracle-sql-injection-in-webapps-part-i/
2. https://blog.udemy.com/sql-injection-tutorial/
3. http://opensourceeducation.net/database-auditing-with-open-source-tool/
4. http://www.openwall.com/john/doc
5. http://sectools.org
6. http://www.seattletimes.com/business/seattles-packed-with-wi-fi-spots/