How do Hackers get Hashed Passwords?

infosecscout.com/how-do-hackers-get-hashed-passwords

Patrick Fromaget

It is a common thing to hear people complain of fraudsters hacking their accounts. One wonders how possible this is, since most people never reveal their passwords. For many, such acts lead to losing their funds, while others get locked out from their social media handles. But how do passwords get hacked in the first place?

As a whole, your passwords are always stored in a database or backend storage on each website or app you use. Passwords are not kept in plain text, but in hashed format (encrypted one way or another). By using specific attack strategies, hackers may access to this hashed password.

In this article, I will give you 5 examples of how hackers can get hashed passwords. They will then use techniques like brute-force or a rainbow table to decrypt the weaker passwords in the database.

5 Ways Hackers Can Find your Passwords

SQL Injection

An SQL injection method involves inserting an SQL command into a data plane to alter predefined commands. It uses malicious codes for databases stored at the backend to manipulate information access.

The success of the attack result from exploiting or manipulating the security vulnerability of a web page.

An impact comes in the form of giving unauthorized views of users' details. It also offers attackers administrative rights to databases. In extreme situations, attackers spoof identity or change balances. They tamper with existing data, destroy or make them unavailable.

Phishing

Phishing is the most common hacking method used by cybercriminals. You probably heard the name before now. It entails disguising malicious content as reliable communication.

What happens here is that unsuspecting victims release sensitive information and passwords to fraudsters. Many of the attacks disguise as friendly content, leading users into believing its authenticity.

The possibility and success arise via the use of malicious software. Attackers observe activities on a site, including the navigation of victims. Therefore, they transparently mirror a site and retrieve vital information and carry out attacks. By this means, it becomes easy to hash a password since they see all operations. The activities used in achieving successes include:

1. **Identifying a target.**
2. **Creating emails or texts that appear genuine.**
3. **Attaching dangerous links.**
4. **Use of emotions** (like fear, urgency, or greed) to lure victims into opening such links

Hacking altogether appears challenging to prevent. However, my recommendation is to exercise extra caution with sensitive information. The truth is, hacking involves intelligent and calculated moves.

Brute Force Attack

A brute-force attack involves a trial-and-error method. It uses an application program to decode encrypted keys and login information. One fundamental way to carry out this method is by guessing the password. Attackers employ the use of relevant clues.

For example, most people reuse their passwords, and a previous data breach exposes them. Another means is the use of reverse brute force. Here, attackers take commonly used passwords and try to guess associated usernames. Brute force attackers also employ a sort of automated processing.

It allows multiple quantities of passwords to get fed into a system. The idea is to input all possible passwords until the attacker gets the right one.

You can read this article to learn more on how brute-force attacks really work.

Malware

Malware operates by recording every activity on a system. For example, with passwords, hackers design software applications to screen-grab a login process. A copy of the file then goes to hacker central.

Most malware takes the form of a screen scraper or keylogger- they also get an existing web browser file containing saved passwords from the browsing history.

The malware then puts a polite request for the browser's data encrypted tool to decrypt information. Of course, such requests, that look like the user's, appear safe—leaving the system with no choice but to honor the request.

The only way to escape such attacks is through proper encryption. I also advise you to enter passwords rather than trusting your browser for safekeeping manually.

Exfiltration (leaked data)

Hackers carry out exfiltration of hashed passwords through leaked data. Once there's a security breach on a company's database, hacking becomes easy. The next step involves cracking your password.

Exfiltration happens when the algorithm for a company's website gets weak. Copying, retrieving, and transferring data to another server becomes possible. So, data not adequately protected becomes an easy target for hackers.

Master your cyber security skills:
Secure your spot in the Accelerator Program, with early access to exclusive resources.
Get 1000+ classes, unlimited mentorship, and more.
Here is a tool you can use to quickly check if you email address is linked to a recent data breach.

Related questions

Can I retrieve my hacked account?

As cyberspace and its related technology improve, so do the criminals and attackers. They go after the databases of companies for various reasons. Once you discover the hacking of your hashed password, I suggest you do a variety of things:

- Change your username
- Try resetting all your user's passwords.
- Change your security question.
- Also, recover all your data from backups.
- Warn your contacts
- Guard against a reoccurrence.

What can a hacker do with a hashed password?

Generally, they access your details and look for information about you to glean. The idea is to get all they can to defraud you or your loved ones. Also, your account becomes an avenue to carry out other criminal activities.

How do I protect my hashed passwords?

Use complex words that you can remember (here is a strong password generator I like for this). Try as much as possible to avoid using special dates, pet names, or the names of loved ones.

A password comprising of words, numbers, and special character becomes the idea. Finally, never reveal your password or write it somewhere. Memorize it.

Whenever you're ready for more security, here are things you should think about: