What is Credential stuffing? What is the difference between Credential stuffing and Brute Force?

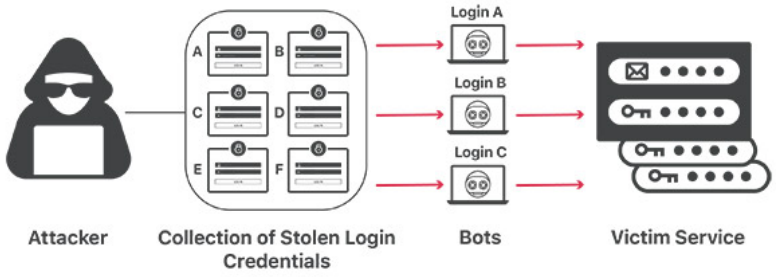
Credential stuffing is a cyber attack in which credentials obtained from a data breach on one service are used to attempt to log into another unrelated service.

What is Credential stuffing?

Credential stuffing is a cyber attack in which credentials obtained from a data breach on one service are used to attempt to log into another unrelated service.

For example, an attacker could obtain a list of usernames and passwords obtained from breaching a large department store and use the same credentials to attempt to log into a national bank's website. . The attacker hopes that a small portion of that department store's customers also have an account at this bank, and they reuse the same username and password for both services.

Credential stuffing attacks are popular thanks to the huge list of breached credentials being traded and sold on the black market. The proliferation of these lists, combined with advances in Credential stuffing tools that use bots to bypass traditional login protections, have made Credential stuffing a popular attack vector.



What makes the Credential stuffing attack so effective?

Statistically, Credential stuffing attacks have a very low success rate. Many estimates put it at around 0.1%, which means that for every thousand accounts an attacker tries to crack, they will succeed almost once. The large volume of credential collections being transacted by attackers makes it worthwhile to perform a Credential stuffing attack, despite the low success rate.

These collections contain millions and in some cases billions of logins. If an attacker has a million sets of credentials, this could yield about 1,000 successfully cracked accounts. If even a small percentage of cracked accounts yield profitable data (usually in the form of credit card numbers or sensitive data that can be used in

phishing attacks) the attack is valuable. On top of that, an attacker can repeat the process using the same set of credentials across many different services.

Advances in bot technology also make Credential stuffing a viable attack. Security features built into web application login forms often include intentional time delay and IP address blocking of users who have failed multiple login attempts. Modern Credential stuffing software circumvents these protections by using bots to simultaneously attempt several logins that appear to come from different types of devices and originate from different IP addresses. together. The goal of a malicious bot is to make an attacker's login attempts indistinguishable from normal login traffic, and it's very effective.

Often, the only sign that helps a company realize that they are under attack is an increase in the total volume of login attempts. Even then, the targeted company would have a hard time stopping these efforts without affecting legitimate users' ability to log into the service.

The main reason Credential stuffing attacks work is because people reuse passwords. Studies show that the majority of users, by some estimates up to 85%, reuse the same login information for multiple services. As long as this practice continues, Credential stuffing will still work.

What is the difference between Credential stuffing and Brute Force?

OWASP classifies Credential stuffing as a subset of Brute Force attacks. But, strictly speaking, Credential stuffing is very different from traditional Brute Force attacks. Brute Force attacks attempt to guess passwords without context or clues, using random characters sometimes combined with common password suggestions. Credential stuffing, on the other hand, uses exposed data, greatly reducing the number of possible correct answers.

A good defense against Brute Force attacks is a strong password consisting of several characters and including uppercase letters, numbers, and special characters. But password strength does not protect users from Credential stuffing attacks. It doesn't matter how strong the password is. If passwords are shared across different accounts, Credential stuffing can still be damaging.

How to prevent Credential stuffing

How users can prevent Credential stuffing

From the user's point of view, protecting against Credential stuffing is pretty straightforward. Users should always use unique passwords for different services (an easy way to achieve this is to use a password manager). If a user always uses a unique password, Credential stuffing won't work with their account. As an added security measure, users are encouraged to always enable two-factor authentication when available.

How companies can prevent Credential stuffing

Preventing Credential stuffing is a more complex challenge for companies operating authentication services. Credential stuffing occurs due to data breaches at other companies. A company targeted by a Credential stuffing attack does not necessarily have a security breach.

A company may ask its users to provide unique passwords but cannot effectively enforce this as a rule.

Some applications will run the submitted password against a database of already compromised passwords, before accepting the password as a countermeasure against Credential stuffing, but this is not secure - the user can may be reusing passwords from a service that has not been breached.

Providing additional login security features can help reduce Credential stuffing. Enabling features like two-factor authentication and requiring users to fill in a captcha when logging in also helps prevent malicious programs. While both of these features are inconvenient for users, many will agree that mitigating the security threat is worth the trade-off.

The strongest defense against Credential stuffing is a bot management service. Bot management uses rate limiting in conjunction with IP databases to prevent malicious bots from making login attempts without compromising legitimate logins.