Name:erfan ahmadbeigi

Master:mr.milad nourian nasab

**Password Spraying Attack**

A Password Spraying Attack is a type of brute force attack where a malicious actor attempts the same password on many accounts before moving on to another one and repeating the process. This is effective because many users use simple, predictable passwords, such as "password123."

A common practice among many companies is to lock a user out after a number of failed log in attempts (usually 3-5 attempts) in a short of time. Becuase of the nature of a password spraying attack, a bad actor is able to avoid being detected and locked out of an account, which is a common problem with regular brute force attacks.

### Example:

"I was asked to change my password when my bank fell victim to a password spraying attack. It turns out some hacker managed to try millions of username and password combinations against the bank's users - and I was one of them.

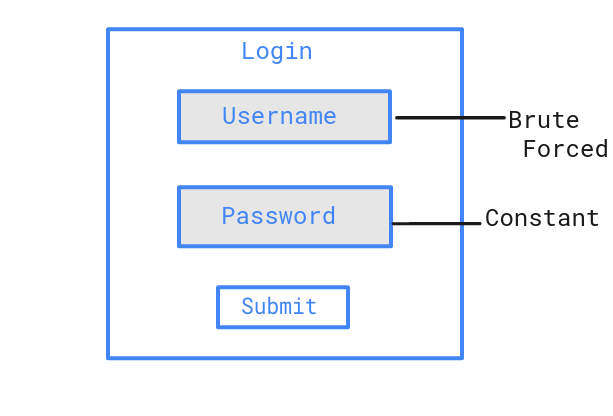
# Password Spraying Attack

**Author:** Rishu Ranjan

## Description

**Password spraying** is a type of brute force attack. In this attack, an attacker will brute force logins based on list of usernames with default passwords on the application. For example, an attacker will use one password (say, Secure@123) against many different accounts on the application to avoid account lockouts that would normally occur when brute forcing a single account with many passwords.

This attack can be found commonly where the application or admin sets a default password for the new users.



## Mitigations

* Brute force preventation should be on both field, i.e., Username and Password.
* Set account lockout policies after a certain number of failed login attempts to prevent credentials from being guessed. Implement CAPTCHA, if lockout is not a viable option.
* The admin managed application should force users to change their password on first login with default password.
* Use multi-factor authentication. Where possible, also enable multi-factor authentication on externally facing services.
* **Preventing Password Spraying**
* The simplest way to prevent password spraying, [credential stuffing](https://doubleoctopus.com/security-wiki/threats-and-tools/credential-stuffing/), and other credential-based attacks is simply using an authentication solution that does not require passwords as the first factor of authentication.

#### WHAT IS A RAINBOW TABLE?

A rainbow table is a precomputed table for reversing cryptographic hash functions. They are used for cracking password hashes. Using a rainbow table requires less computer processing time and more storage than a brute-force attack which calculates a hash on every attempt. Salting the password hash renders the rainbow table attack infeasible.

**How to Avoid Being a Victim of Password Spraying Attacks**

To avoid being a victim, it is recommended that you:

* Enable and properly configure multi-factor authentication (MFA)
* Enforce the use of strong passwords
* Regularly review your password management program
* Maintain a regular cadence of security awareness training for all company employees
* Ensure your Help Desk has well-documented procedures for password resets for user lockouts