Broken Authentication: Methodology and Prevention

In this article we will see that how hacker/penetration testers can exploit broken authentication vulnerability, in the authentication system of a website. In the end we will also see some ways by which you can prevent issues related to authentication of your website.

Before we discuss about ways in which a hacker/penetration tester can exploit broken authentication vulnerability, we must know the answer of these two questions.

**What is broken authentication?**

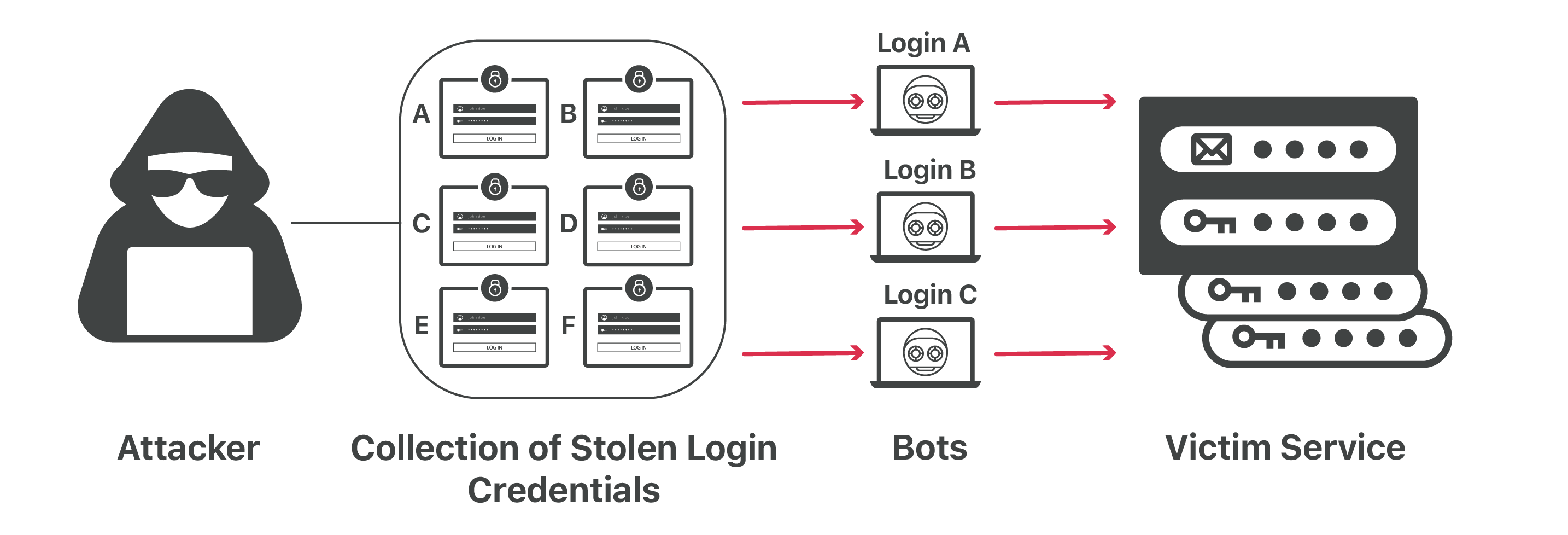
Authentication is broken when attackers are able to compromise passwords, keys or session tokens, user account information, and other details to assume user identities. Due to weakness in design and implementation of identity and access controls, the prevalence of broken authentication is widespread.

**What is the impact of broken authentication?**

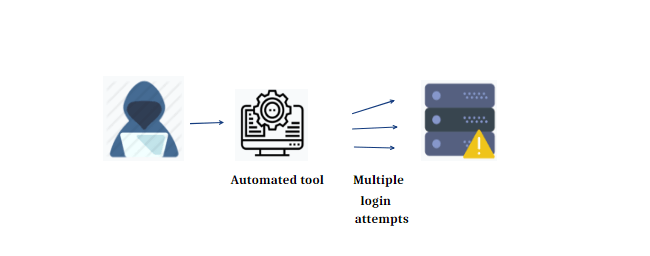
In summary, broken authentication and session management has the potential to steal a user login data, or forge session data, such as cookies, to gain unauthorized access to websites. However, there are clear and easy solutions to prevent your site from being affected by this vulnerability.

Now let’s discuss the way a hacker/penetration tester can exploit this vulnerability.

1. Credential stuffing attack:
   * An attack where the attacker uses lists of compromised credentials to breach a system.
   * Typically uses a bot to automate this process.
   * Has success rate around 0.1%.



1. Brute force and weak passwords:
   * Brute force involves trying common passwords or random combinations to login.
   * Take advantage of weak passwords.
   * Works best on services that do not limit login attempts.



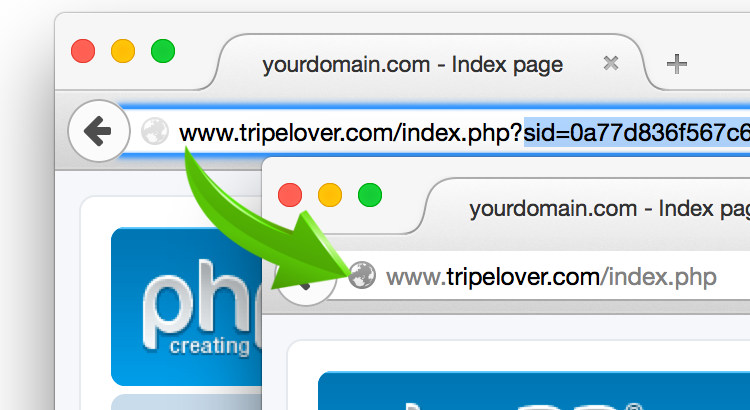
1. Weak credential recovery:
   * When a user forgot their password, they may need to recover it.
   * Password recovery should only work for the user who owned the account.
   * Methods such as recovery questions can be easily guessed, if the hacker/penetration tester knows the person or had done a very good reconnaissance on the target user.



1. Missing multi-factor authentication:
   * Multi-factor authentication can help add a layer of security to authentication.
   * Options such as biometrics, phone and e-mail based authentication are good options.
   * Missing multi-factor authentication makes brute force and credential stuffing more effective.



1. Exposed session ID:
   * If a session ID is exposed through URL or cookies, it can be used by an attacker to authenticate.
   * Session IDs should be properly handles, ideally only on the server side.



So far we have discussed most common ways to exploit broken authentication vulnerability, now it’s time to see some safety measures to prevent this vulnerability.

* Implement some form of multi-factor authentication.
* Use a password policy to prevent weak logins.
* Do not ship with default credentials, such as “admin:admin” or “root:password”
* Limit failed login attempts.
* Keep session IDs on server side.



So this was all about methodology and prevention of broken authentication vulnerability. I hope you liked it and learned something new from it.

If you have any doubt, question, quires related to this topic or just want to share something with me, than please feel free to contact me.