4 Common Security Issues Found In Password-Based Login

By Srishti Singh

Password-based login is the most commonly used form of authentication, but it's not always the most secure. This blog covers some of the common security issues found in password-based login systems and how to avoid them.

Passwordless Login | Cx | Mfa | Authentication

Introduction

The use of passwords as the primary means of authentication has been under scrutiny for as long as they have been in existence. Passwords are meant to be used by authorized users only, but they are easily compromised by malicious actors, and thus, they have increasingly become a larger security risk.

This article discusses some common security issues found in password-based login systems and how to avoid them.

Vulnerabilities in Password-based Login

Passwords are one of the most vulnerable forms of user authentication. We can see this in practice when we look at how they're put to use.

Oftentimes users may reuse the same password across multiple websites, which means that if an attacker manages to break into one of their accounts, they can compromise all of them. It's not uncommon for users to even have the same password for their email as they do for their online banking.

Beyond the lack of uniqueness in passwords, there are other security issues with them as well. If a user doesn't update their password regularly, it can be easier for an attacker to crack it over time. Not only that, but it's also common for users to choose weak passwords that contain no numbers or special characters and include simple words (such as "password" itself).

Some of the most common security issues in password-based login include:

1. Brute Force Attack

A brute force attack is a method of hacking that uses trial and error to crack passwords (e.g., login credentials and encryption keys) by attempting a large amount of combinations for them. It is a simple yet reliable tactic that is often used when the attacker has only a limited amount of information about its target, such as a username or when they know the general structure of the password, but not its specific content.

Consequences of brute force attacks

- Your personal and valuable data is at risk.
- Hackers spread malware to cause disruptions in a network.
- Hackers hijack targeted systems for malicious activities.
- Such attacks can ruin your company's reputation.

How to prevent brute force attacks?

- Use longer passwords with varied character types.
- Change your passwords frequently.
- Use different usernames for every site.
- Use a password manager to track your online login info automatically.

2. Phishing Attacks

A phishing attack is a common type of cyber attack, where the hackers send fraudulent communications through email that appears to come from a reputable source. Using this method, hackers try to steal sensitive data like credit cards and login information. Sometimes hackers do this to install malware on the victim's device and obtain employee login information or other details for an attack against a specific company.

Types of phishing attacks

- **Deceptive phishing**: This type of attack uses "spoofed" email addresses so that the victim believes the message is from a legitimate email address. Attackers will typically use the name of a real person within the company to try and convince the victim that they need to take action on a matter immediately.
- **Spear-phishing**: This type of attack is personalized, targeting specific individuals or departments in an organization. Spear-phishers will do research to find out who they're trying to target, and craft their emails specifically for them—using personal details like names, job titles, locations, and more in order to gain their trust.
- **Whaling:** Whaling targets high-level employees within an organization through spear-phishing techniques. Often times these attacks will happen over phone calls or video conferences rather than email because they're usually targeting CEOs and CTOs of an organization.

How to avoid phishing attacks?

- Protect all devices in the organization using security software.
- Use a mandatory update policy on devices that access your network.
- Use multi-factor-authentication.
- Open and read your emails mindfully to avoid the security risk.

3. Credential Stuffing

Credential stuffing is a type of cyber attack in which attackers use credentials obtained through a data breach on one service to log in to another unrelated service.

If an attacker has a list of usernames and passwords obtained from a breach of a popular department store, he uses the same login credentials to try and log in to the site of a national bank. The attacker knows that some customers of that department store are the customers of that particular bank too. They can withdraw money if any customers use the same usernames and passwords for both services. But these attacks are known to have a low success rate.

The Digital Shadows Photon Research states that the number of stolen username and password combinations currently available on the dark web is more than twice the number of humans on the planet.

How to prevent credential stuffing?

- Use unique passwords for different web services.
- Use risk-based authentication.
- Use bot management to stop malicious bots from making login attempts without impacting legitimate logins.

4. Dictionary Attack

A dictionary attack is a type of brute-force attack in which the hacker attempts to break the encryption or gain access by spraying a library of terms or other values. This library of terms includes words in a dictionary or number sequences. Poor password habits such as updating the passwords with sequential numbers, symbols, or letters make dictionary attacks easier.

Common dictionary attack vulnerabilities

- Sensitive URLs such as admin pages are sometimes accessible publicly.
- Some applications will not force users to use a strong password during registration. It ends up with users creating passwords like user name, company name, and 12345. Some applications do not enforce password requirements too. These all are some added advantages for hackers.

How to prevent dictionary attacks?

- Use different combinations of passwords that include upper and lower case alphabets, special characters, and numbers.
- Use a long string password with more characters to prevent cracking.
- Reset passwords frequently.

Bottom line

The problem is that the current digital environment exposes authentication systems to more vulnerabilities than ever before, and those vulnerabilities are growing at an exponential rate.

The tips discussed in this blog can help you avoid the pitfalls that come with password-based login systems.

Written by Srishti Singh

SEO specialist at LoginRadius, music lover, aspiring for new challenges. Dedicated to driving quality results with her innovative marketing tactics.

Featured Posts

- What is Cloud Identity and its Benefits?
- The Legal Implications of SSO: Privacy, Security, and Compliance
- Data Privacy Laws for 2023: A Closer Look at 9 Key Regulations
- 4 Reasons Why SSO Integrations Are a Must-Have For Online Businesses

Security | Authentication | Cx | Data Security | Claim Solution | Customer-Experience | Mfa | Identity Management | Compliance | Data Privacy