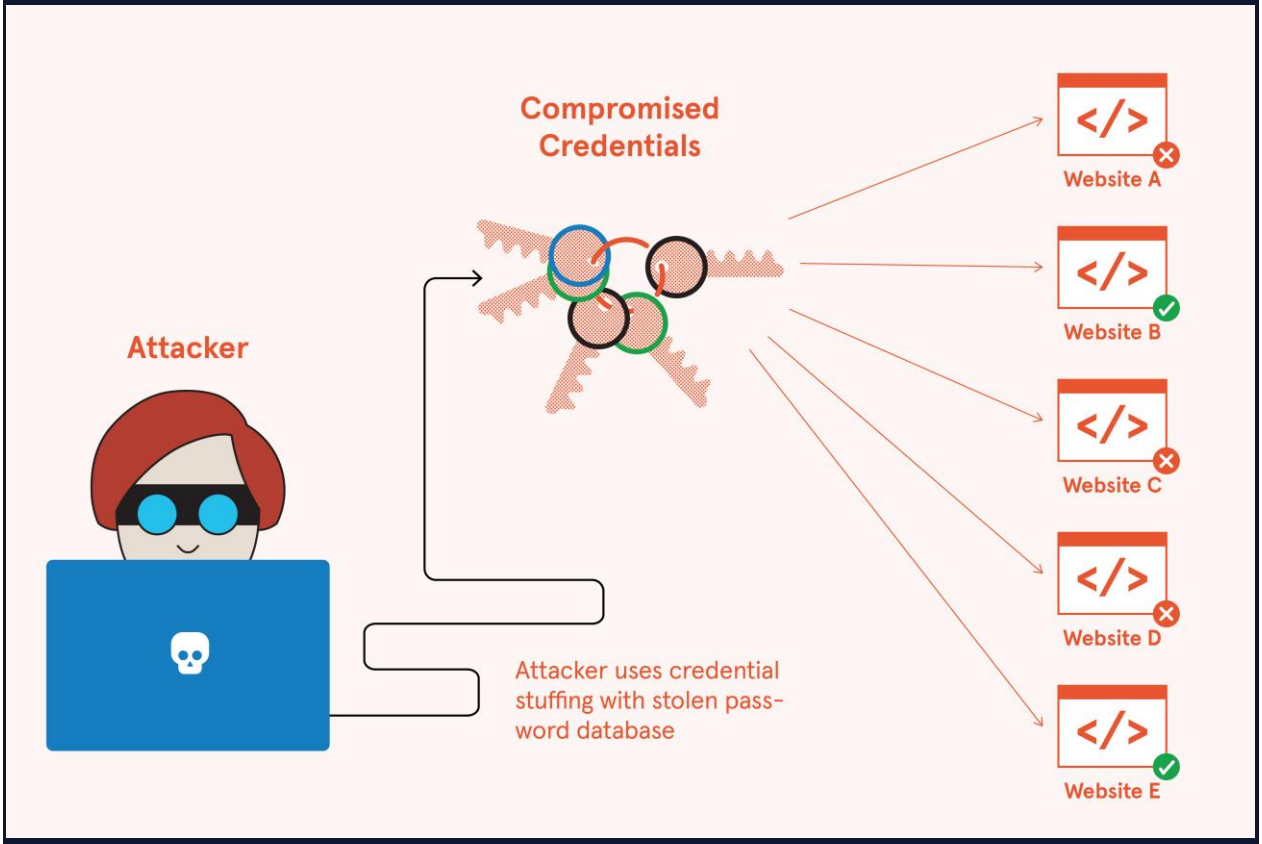
The World of Identification and Authentication Failures

This article will discuss Identification and Authentication Failures: What they are, how they happen, and why they're dangerous.



What Are Identification and Authentication Failures?

Authentication is the process of establishing identity. The identity might belong to a person, a computer, or something else.

Identification and Authentication Failures are a category of vulnerability where the systems we use for authentication fail insecurely. This category often overlaps with other vulnerabilities in the OWASP Top 10, particularly Cryptographic Failures and Insecure Design.

Why Do Identification and Authentication Failures Happen?

Identification and Authentication Failures can take on many different forms. However, we can observe some general trends in common category examples.

Password Problems

For such a commonly-used authentication method, passwords have many problems. Some of these problems are innate to passwords, while others can be (though aren't always) mitigated through careful design choices.

One common mistake is allowing weak passwords, either due to low length or complexity or because the passwords are well-known and likely to be used in dictionary attacks (more on that topic later). Allowing weak passwords is one of the top examples of Identification and Authentication Failures. It's not just user-provided passwords that can be an issue; insecure default credentials are another issue that is more common than they should be (many home routers have "admin" as the username and password for configuration, for example).

Other common mistakes include how passwords are managed and stored by the authentication system. Improperly stored passwords are an all-to-common example of Identification and Authentication Failures and Cryptographic Failures. Insecure account recovery systems, such as requesting answers to secret questions, also overlap with Insecure Design.

Automated Attacks

Sometimes people need a few tries to type their password correctly, and that's fine. What's not fine is if your system allows someone to continuously enter an incorrect password without rate-limiting their requests or locking them out entirely and alerting the security team.

In addition to regular brute-force attacks where an attacker simply tries many passwords hoping to get lucky, another technique is known as *credential stuffing*. Imagine a website, Website A, has a data breach, and several username and password combinations are leaked. Attackers will try those combinations on other websites, assuming that at least some people who used Website A will have accounts on other websites with the same credentials. This problem is exacerbated by password-based authentication, where it's impossible to verify that a user hasn't reused their password somewhere else (yet another issue with passwords).

Token Troubles

Something you may take for granted is that you don't have to log in to a website every time you navigate to a different page. We can thank token-based authentication for that. The short version of how it works is that when

you log in to a website, you get a cookie with a unique token. From there on, you send the token to the website with your requests, which verifies the token to authenticate that the requests come from you.

However, those tokens must be treated correctly, like any other cryptographic secret. Transmitting a token so an attacker can intercept it is a bad idea. Reusing tokens is also a bad idea. Every time you log in, you should get a new token; any previous tokens should be invalidated. Finally, tokens shouldn't last forever. They should be invalidated on logout, after a period of inactivity, or after a set amount of time. Doing anything incorrectly will qualify as an identification or authentication failure.

Mandated MFA

Finally, OWASP counts not supporting Multi-Factor Authentication (MFA) or poorly supporting MFA as an identification failure. Despite being the *default* form of authentication for decades, passwords are full of issues, and cybersecurity best practices include moving away from exclusively password-based authentication and towards multi-factor authentication.

Why Are Identification and Authentication Failures Dangerous?

The purpose of authentication is to establish identity, and identity is tied to authorization and privileges. If authentication fails insecurely, an attacker can impersonate someone and appropriate their privileges and authorization. The severity of this can range from bad to catastrophic, depending on the authorization of the person being impersonated. The worst-case scenario is usually an attacker successfully gaining administrator-level authorization.