Broken Authentication

1 min

Authentication is complicated to get right. Broken Authentication is considered one of the most critical web vulnerabilities, and the consequences of getting it wrong can be disastrous. Moreover, authentication is a big, obvious target for attackers, meaning that it will almost certainly be probed for vulnerabilities.

A secure, trusted third-party service is the best way to authenticate. There's a reason that so many websites support signing in with Google, Apple, etc… Not only is it convenient, but it's generally considered more secure for users and less risky for organizations.

Here are just a few of the ways that authentication systems can fail:

- Allowing weak passwords.
- Using the wrong type of

Preview: Docs Loading link description

cryptography

.

- Using the wrong cryptographic algorithms.
- Using the correct kind of cryptography with the correct algorithm but misconfiguring it.
- Preprocessing passwords incorrectly.
- Managing sessions incorrectly.
- Not supporting

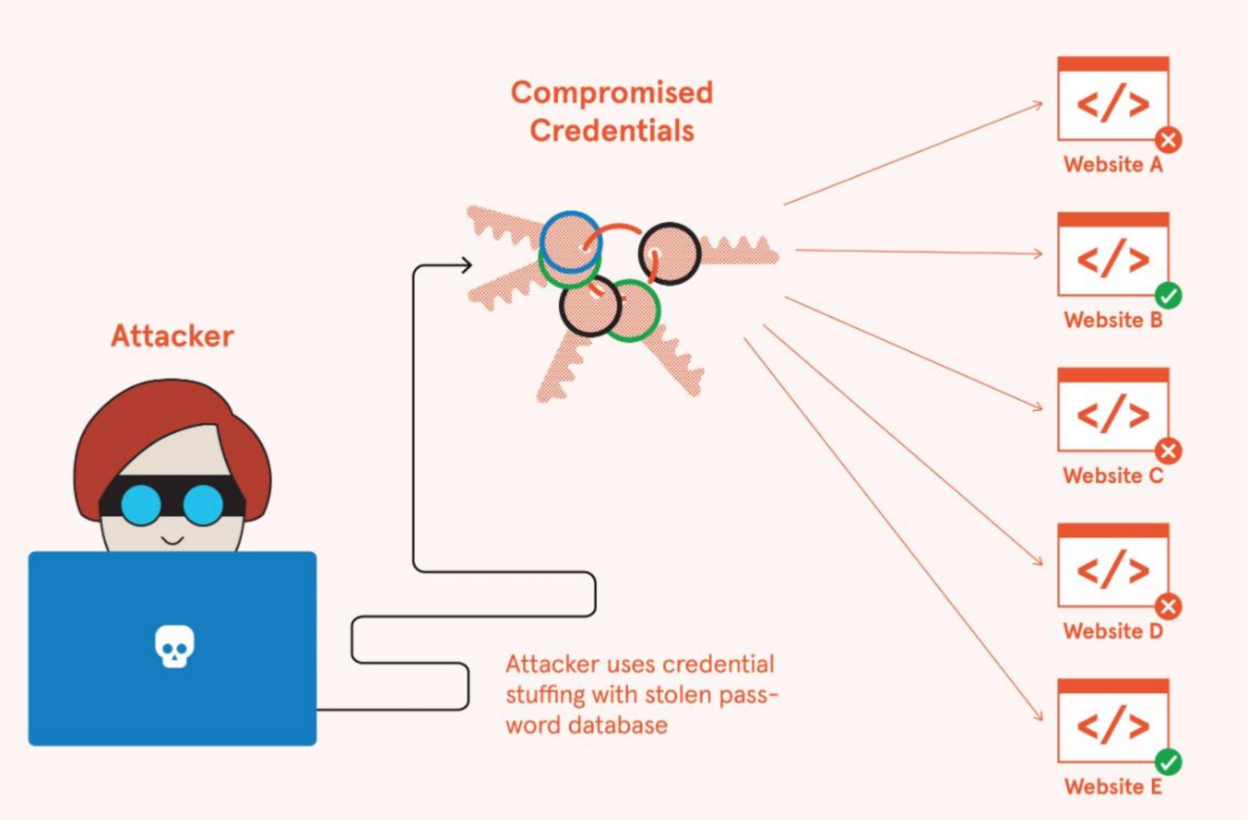
Preview: Docs Loading link description

multi-factor authentication

.

- Implementing multi-factor authentication incorrectly.
- Having insecure default credentials.
- Having insecure admin credentials.
- Insufficient protection against brute-force attacks.
- Insufficient protection against credential-stuffing attacks.

Authentication is one area you should leave to the experts as much as possible.


Compromised Credentials
Website A
Website B
Website C
Website D
Website E
Attacker
Attacker uses credential stuffing with stolen password database