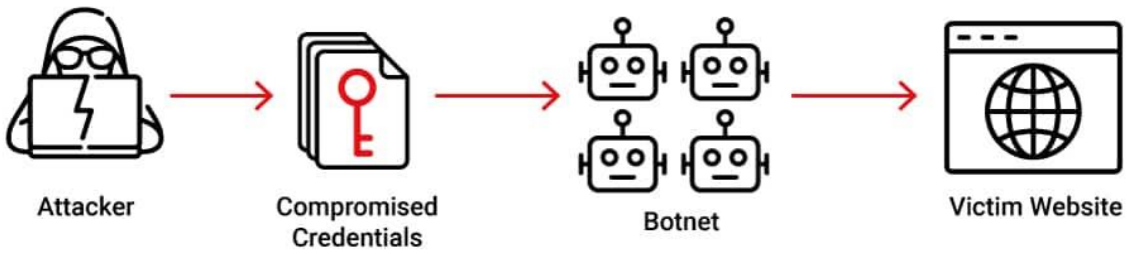
Broken Authencation

I. What is Broken Authencation ?

Broken authentication is an umbrella term for several vulnerabilities that attackers exploit to impersonate legitimate users online. Broadly, broken authentication refers to weaknesses in two areas: session management and credential management. Both are classified as broken authentication because attackers can use either avenue to masquerade as a user: hijacked session IDs or stolen login credentials.

In recent years, broken authentication attacks have accounted for many of the worst data breaches, and security experts sound the alarm about this underrecognized threat. The Open Web Application Security Project (OWASP) has included it in its "Top 10" list of the biggest web application security risks since 2017. By 2020, broken authentication had climbed to the number two spot.



II. Some types of common broken authencation attack

A. Session Management Attacks

1. Session Hijacking

Without appropriate safeguards, web applications are vulnerable to session hijacking, in which attackers use stolen session IDs to impersonate users' identities. The most straightforward example of

session hijacking is a user who forgets to log out of an application and then walks away from their device. A hacker can then continue their session.

2. Session ID URL Rewriting

Another common avenue for session hijacking is "URL rewriting." In this scenario, an individual's session ID appears in the URL of a website. Anyone who can see it (such as via an unsecured Wi-Fi connection) can piggyback into the session. This is how Zoombombing happened.

3. Session Fixation

One commonly overlooked best practice is to rotate session IDs after a user logs in, instead of giving a user the same ID before and after authentication. Web applications that fail to do this are vulnerable to a session fixation attack, which is a variation of session hijacking.

B. Exploit Weak and Compromised Credentials

Malicious actors use various methods to steal, guess, or trick users into revealing their passwords.

1. Credential Stuffing

When attackers access a database filled with unencrypted emails and passwords, they frequently sell or give away the list for other attackers to use. These attackers then use botnets for brute-force attacks that test credentials stolen from one site on different accounts. This tactic often works because people frequently use the same password across applications.

2. Password spraying

Password spraying is a little like credential stuffing, but instead of working off a database of stolen passwords, it uses a set of weak or common passwords to break into a user's account.

3. Phishing Attacks

Attackers typically phish by sending users an email pretending to be from a trusted source and then tricking users into sharing their credentials or other related information. It can be a broad-based attempt that hits everyone at an organization with the same phony email, or it can take the form of a "spear phishing" attack tailored to a specific target.

III. What Is the Impact of Broken Authentication ?

Attackers have to gain access to only a few accounts, or just one admin account to compromise the system. Depending on the domain of the application, this may allow money laundering, social security fraud, and identity theft, or disclose legally protected highly sensitive information.

IV. How to Prevent it ?

A. Update Session Management

1. Control Session Length

Every web application automatically ends sessions at some point, either after logout, a period of no activity, or a certain length of time. Tailor your session length to the type of user and the application they're using.

2. Rotate and Invalidate Session IDs

As we discussed, the best way to prevent session fixation is to issue a user with a new session ID after login. Similarly, sessions and authentication tokens must be immediately invalidated after a session ends, so attackers can't reuse them.

3. Don't Put Session IDs in URLs

There are so many ways that URL rewriting can end up exposing session IDs, so your safest bet is not to go that route. Use cookies generated by a secure session manager.

B. Tighten Password Policies

1. Implement Multi-Factor Authentication (MFA)

OWASP's number one tip for fixing broken authentication is to "implement multi-factor authentication to prevent automated, credential stuffing, brute force, and stolen credential reuse attacks."

2. Don't Permit Weak Passwords

When designing your application's login page, OWASP recommends following NIST guidelines on password length and

complexity. They also advise automatically rejecting any of the most common passwords on the web.

3. Don’t Store Passwords in Cleartext

A strong password storage strategy is critical to mitigate data breaches that put the reputation of any organization in danger. Hashing is the foundation of secure password storage. The premise of hashing is simple: given arbitrary input, output a random string of a specific length.

What's important to highlight is that the hashing operation is irreversible. An attacker cannot determine the original password by looking at the hashed password. However, if two users choose the same password, the hash will be the same. You can add random data to the password to guarantee that the output of the hashing process is unique. This random data is known as a "salt".

4. Use Breached Password Protection

Use an identity and access management (IAM) platform with breached password protection. When the platform discovers a compromised credentials cache, it will notify you if any of your users were compromised. Those users will be locked out until they change their passwords, so attackers can't use their compromised passwords against you in a credential stuffing attack.

C. Guard Against Attacks

1. Conduct Workplace Phishing Training

Teaching your workforce how to spot malicious emails is a project you must take seriously and update frequently. As phishing attacks get more sophisticated, they become harder to spot, and the only way to combat this threat is to keep your staff informed.

2. Implement Brute-Force Protection

Attacks involving broken authentication can compromise not only your data but also crash your site. Traffic can spike by 180x during a credential stuffing attack, so brute-force protection is an absolute must to stay online. It works by limiting the number of times a specific IP address can attempt to log in, so bots can’t flood your system.

3. Employ anomaly detection

A sophisticated IAM system doesn't look at just logins and session IDs to determine whether a user is legitimate or malicious. It should also flag other types of suspicious behavior. Anomaly detection will alert you if, for instance, an employee logs off at 10 p.m. in North America and logs back on at 3 a.m. in Bangladesh

Reference:

Auth0 : https://auth0.com/blog/what-is-broken-authentication/

OWASP: https://owasp.org/www-project-top-ten/2017/A2_2017-Broken_Authentication

Hacksplaining: https://www.hacksplaining.com/owasp

Web Security Academy: https://portswigger.net/web-security/authentication