Introduction to the OWASP Top 10 – 2021

Risk A7: Authentication and Identification Failures

Key Concepts

Key Concept 1: Digital Identity

- The digital identity is a set of attributes
- These attributes relate to a person or organization
- Examples: age, bank balance, username, or password

Key Concept 2: Identification

- The act of showing or sharing attributes relating to your identity
- Example: In the airport you must show your passport to identify yourself

Key Concept 3: Authentication

- The process of confirming the identity of a user
- During this process, the identity presented is being verified

Additional Information

The digital identity of a person (or an organization) is a set of attributes. Attributes are characteristics that relate to the person (or the organization). Examples of digital identity attributes include your age, your bank balance, your username, your password, to name a few.

Identification carries an action; this is a *doing* word. Identification is the act of showing (sharing) some of your identity attributes. As an example, consider in the airport you must show your passport to identify yourself.

Authentication is the process of confirming the identity of a person (or an organization). During the authentication process, the digital identity is presented by showing (sharing) the required digital identity attributes. Based on the attributes presented, the identity is confirmed as valid, or invalid.

Definition of A7

Authentication and Identification Failures: Being able to perform successful attacks that disclose identity attributes on the system or web application in use.

For Example: A web application is allowing authentication controls to be either subverted or bypassed.

- Forgot-password flaw or weakness
- Weak or misconfigured identity attributes
  - 4-character password, with no complexity
  - Despite logout, a session remains valid

Additional Information

The definition of A7 of 2021 – Identification and Authentication Failures – is being able to perform successful attacks that disclose identity attributes on the system or web application in use.

This means that your web application or API is allowing for authentication controls to be either subverted or completely bypassed.

One example of subverted authentication controls is forgot-password processes that allow you to enumerate active users. A variation of that is a forgot-password process on your web application that asks you *"what is the first color of your car?"* and has a drop-down menu from which to select your answer.

A second example is the case of identification and authentication failures because of weak or misconfigured identity attributes. A classic case for this is a website that requires only a 4-character password, with no complexity. A 4-character password is a weak attribute of identity, as it is easy to guess the password and impersonate another user.

A final example of A7 failures occurs when, despite the user selecting to logout, the session the user has on the website remains valid. Here the identifiers the web application issues to the user are not correctly invalidated during logout or after a period of inactivity.

Code Example

The following example illustrates how sensitive information can be leaked from authentication systems through error messages. In the bad example, the error messages explicitly states if the username was valid or not. This can lead to a successful *username enumeration* attack that allows the attacker to verify the existence of usernames in the system. In the good example, the login error message is generic and does leak the existence of usernames like we see in the bad example.

Bad Example

```
if (user.equals(username)) {
 if (pass.equals(password)) {
  response.set("Invalid Password");
 } else {
  response.authoriseUser(user);
 }
} else {
```

```
  response.set("Invalid Username");
}
```

Good Example

```
if (user.equals(username) && pass.equals(password)) {
 response.authoriseUser(user);
else {
 response.set("Invalid Username or Password");
  }
}
```

Additional Information

With this good example we have shown you how to avoid user enumeration on the login page of your website, by returning the same message back to the user, regardless of if they provided the wrong username, or the wrong password.

Challenges

The most difficult point to secure for any web application is the **point of interaction with the user.**

You must factor in many attack scenarios and several types of attack techniques

- **Credential stuffing:** short, breached password list against 1000s of accounts
- **Brute force attacks:** millions of password authentication attempts being sent to one account

Additional Information

We now understand how the risk of identification and authentication failures can materialize, let us look at why it is a common issue.

The most difficult point to secure for any web application is the point of interaction with the user. Simply put, this is because the user is always right, can always change their mind and must be allowed to make mistakes. At the same time of allowing flexibility for the users on our web application, we must also think of attackers trying to bypass or subvert our identification and authentication controls.

Furthermore, there are many attack scenarios and several types of attack techniques that we need to factor in our design and implementation of identification and authentication controls. Take for example credential stuffing, where the attacker tries a brief list of passwords across 100s or 1000s of accounts. Another example are brute force attacks where for one account, attackers try a large list of (millions of) passwords, until they find the one user password that is correct for that one account.

Getting that user interaction and user experience right, while protecting from all these attacks, especially during the process of establishing the user's identity and authenticating them, can be a very daunting task.

Best Protection Strategies

FEMALE

Force strong credentials e.g., passwords
Ensure user registration and recovery are hardened
Manage authenticated sessions and tokens
Alert on attacks e.g., brute force
Limit failed login attempts
Enable multi-factor authentication

Additional Information

Above you have some of the best protection strategies against A7 of the Top 10 – Identification and Authentication Failures.