Identity Management Testing

Aim :

To familiarize tools for testing identity management using Burpsuite

Description:

Identity management (ID management) is the organizational process for ensuring individuals have the appropriate access to technology resources.This includes the identification, authentication and authorization of a person, or persons, to have access to applications, systems or networks. This is done by associating user rights and restrictions with established identities.

Managed identities can also refer to software processes that need access to organizational systems. Identity management can be considered an essential component for security. Identity management includes authenticating users and determining whether they're allowed access to particular systems. ID management works hand-in-hand with identity and access management (IAM) systems. Identity management is focused on authentication, while access management is aimed at authorization.

The main goal of identity management is to ensure only authenticated users are granted access to the specific applications, systems or IT environments for which they are authorized. This includes control over user provisioning and the process of onboarding new users such as employees, partners, clients and other stakeholders.

Identity management also includes control over the process of authorizing system or network permissions for existing users and the offboarding of users who are no longer authorized to access organization systems.

ID management determines whether a user has access to systems and sets the level of access and permissions a user has on a particular system. For instance, a user may be authorized to access a system but be restricted from some of its components.Identity governance, the policies and processes that guide how roles and user access should be administered across a business environment, is an important aspect of identity management. Identity governance is key to successfully managing role-based access management systems.

Identity management is an important part of the enterprise security plan, as it is linked to both the security and productivity of the organization.In many organizations, users are granted more access privileges than they need to perform their functions. Attackers can take advantage of compromised user credentials to gain access to organizations' network and data. Using identity management, organizations can safeguard their corporate assets against many threats including hacking, ransomware, phishing and other malware attacks.

Identity management systems add an additional layer of protection by ensuring user access policies and rules are applied consistently across an organization.

Procedure:

1. **Test-Role-Definitions**

   Burp Suite Enterprise Edition uses a role-based access control model. You manage permissions for users using roles and groups:

   - ✓ A user represents a person who has access to Burp Suite Enterprise Edition via the web interface, or a system that has access via one of the APIs.
   - ✓ A role is a set of permissions to perform specific actions, such as scheduling and deleting scans. You assign roles to groups of users.
   - ✓ A group is a collection of users with an assigned set of roles.

2. **Test User Registration Process**

   Verify that the identity requirements for user registration are aligned with business and security requirements:

   - ✓ Can anyone register for access?
   - ✓ Are registrations vetted by a human prior to provisioning, or are they automatically granted if the criteria are met?
   - ✓ Can the same person or identity register multiple times?
   - ✓ Can users register for different roles or permissions?
   - ✓ What proof of identity is required for a registration to be successful?
   - ✓ Are registered identities verified?

   Validate the registration process:

   - ✓ Can identity information be easily forged or faked?
   - ✓ Can the exchange of identity information be manipulated during registration?

3. **Testing for Account Enumeration and Guessable User Account**

   The scope of this test is to verify if it is possible to collect a set of valid usernames by interacting with the authentication mechanism of the application. This test will be useful for brute force testing, in which the tester verifies if, given a valid username, it is possible to find the corresponding password.

Often, web applications reveal when a username exists on system, either as a consequence of mis-configuration or as a design decision. For example, sometimes, when we submit wrong credentials, we receive a message that states that either the username is present on the system or the provided password is wrong. The information obtained can be used by an attacker to gain a list of users on system. This information can be used to attack the web application, for example, through a brute force or default username and password attack.

The tester should interact with the authentication mechanism of the application to understand if sending particular requests causes the application to answer in different manners. This issue exists because the information released from web application or web server when the user provide a valid username is different than when they use an invalid one.

4.Testing for Weak or Unenforced Username Policy

- Determine the structure of account names.
- Evaluate the application’s response to valid and invalid account names.
- Use different responses to valid and invalid account names to enumerate valid account names.
- Use account name dictionaries to enumerate valid account names.