Unit 1 - Prework

Insecure Direct Object Reference (IDOR):

* Part or parts of a website that have been improperly exposed/ not protected.
* A poorly designed application exposes unauthorized content.
* IDOR is when code accesses a restricted resource based on user input, but fails to verify the user's authorization to access that resource
  + Put another way: there exists a "direct reference" to an "object" which is "insecure"
* Can a user/ attacker modify the URL and gain access to another account?
* To prevent attacks like this we use preventive machines:
  + Access Control
    - The application should an access control in order to check and ensure the user is authorized for the request, object, or service.
    - Developers should only use one user or session for indirect object references. It is also recommended to check the access before using a direct object reference from an untrusted source.
  + Change the direct object reference to an indirect object reference (encapsulation)
    - Logged in user sees list of 4 previous orders, Previous orders are numbered 1-4, User chooses order #2, The request sends ID='2', not the order ID, The ID of ‘2’ is indirect, it is only meaningful in user's scope
  + Use latest securities frameworks (WPA2, HTTPS)

* Imagine a web page that allows you to view your personal information. The web page that shows the user their information is generated based on a user ID. If this page was vulnerable to insecure Direct Object References an attacker would be able to modify the user identifier parameter to reference any user object in the system. Insecure Direct Object References occur when an application references an object by its actual ID or name. This object that is referenced directly is used to generate a web page. If the application does not verify that the user is allowed to reference this object, then the object is insecurely referenced.

Attackers can use insecure object references to compromise any information that can be referenced by the parameter in question. In the above example, the attacker can access any user's personal information.

The severity of insecure direct object references varies depending on the data that is compromised. If the compromised data is publicly available or not supposed to be restricted, it becomes a very low severity vulnerability. Consider a scenario where one company is able to retrieve their competitor's information. Suddenly, the business impact of the vulnerability is critical. These vulnerabilities still need to be fixed and should never be found in professional grade applications.

Prework

* + If you get a hex value (16 bytes) and multiply by 8 (to get bits) it returns 128 bits which is the exact length of a MD5 SUM
  + There is no tool that can automatically reverse a cryptographically secure hash
    - Only way to decipher is either cracking it yourself of downloading someone else's rainbow table
    - search hash crack
  + <https://crackstation.net/>
  + <https://www.hackerone.com/>