Week 1

Building Psychological Safety & Tech Training 1:

Tech Training 1:

* IDOR: Insecure direct object reference

A screenshot of a computer

Description automatically generated with medium confidence

* A type of access control vulnerability that arises when an application uses user-supplied input to access objects directly

A screenshot of a computer

Description automatically generated with medium confidence

* vulnerability in top link is that we can change the customer website
* change txt file number
* How does IDOR work:
  + this dwells in session management where the user has to be authenticated and or authorized

A picture containing application

Description automatically generated

* IDOR mitigation:
  + Access Control: With the exception of public resources, deny by default
    - policy driven although the policy may not be implicit
  + Reusage
  + Alerts
    - e.g. recaptcha bots trying to brute force passwords
    - user multiple password failures
  + Indirect object reference
    - don't reference data directly. basically have the user end indirectly reference the data
    - making the object reference either inaccessible, or at least not easily predictable
    - goes hand in hand with access control

Text

Description automatically generated

* Ssh keys are also another way to mitigate against IDOR
* I think modern day frameworks have IODR on by default.
* Case studies:
  + <https://medium.com/h4x00r/my-very-first-bug-a-dreaded-dupe-and-then-an-idor-jackpot-d01b69f6fbae>
  + <https://infosecwriteups.com/add-description-to-instagram-posts-on-behalf-of-other-users-6500-7d55b4a24c5a>
  + <https://infosecwriteups.com/disclose-private-attachments-in-facebook-messenger-infrastructure-15-000-ae13602aa486>
  + hackerone.com/bug-bounty-programs
  + Takeaway: These people are doing this using the same sw were using (burp)

A screenshot of a computer

Description automatically generated with medium confidence

Building Psychological Safety:

A screenshot of a computer

Description automatically generated

Text

Description automatically generated

Diagram

Description automatically generated