WELCOME ALL

TOPIC: BROKEN ACCESS CONTROL

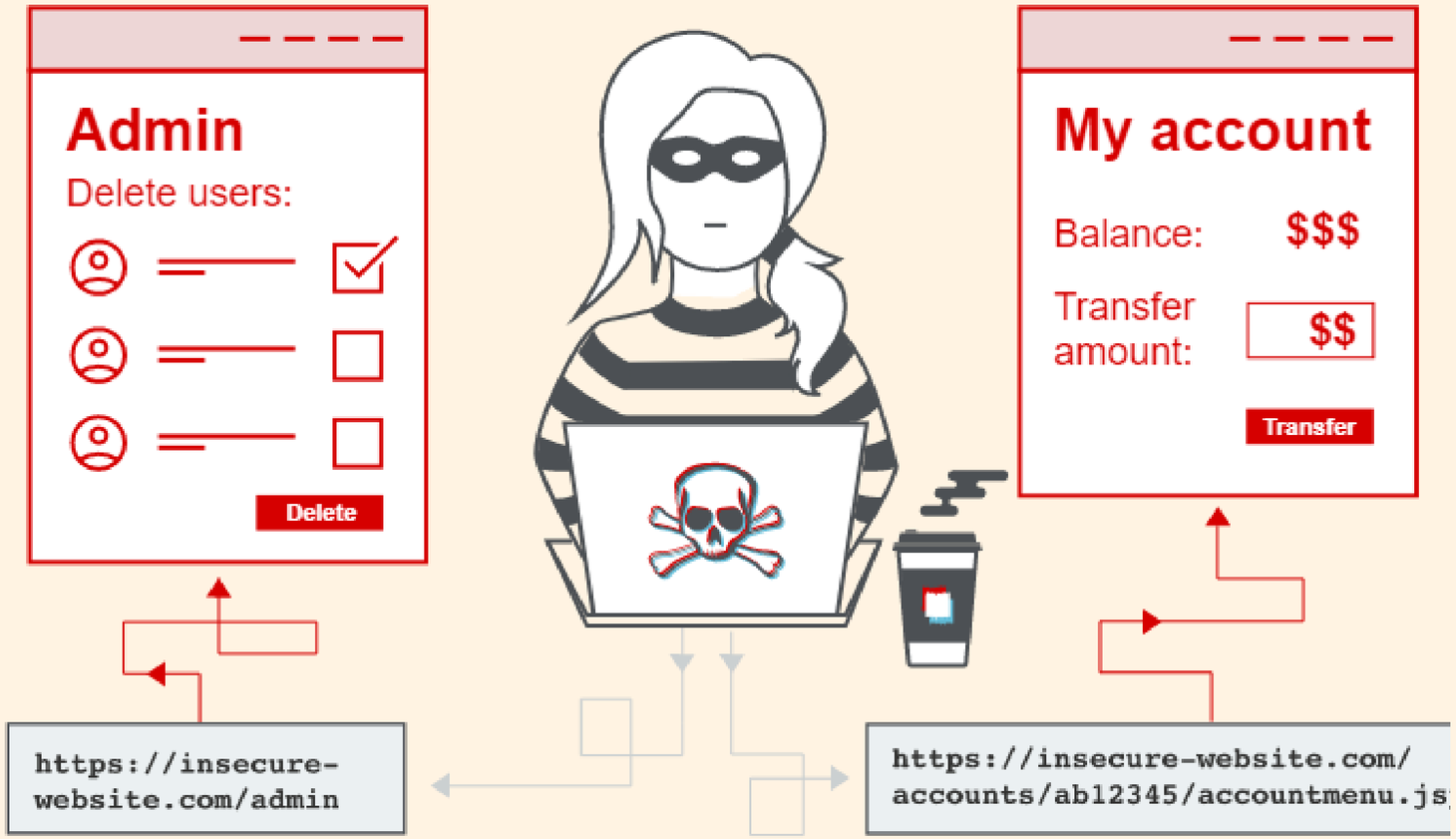
PRESENTED BY:

SAUMYA MUTALIK
CHAITANYA OZA
PRIYANSHU GANDHI

Broken Access Control

What is access control?

In the context of web applications, access control is dependent on authentication and session management:

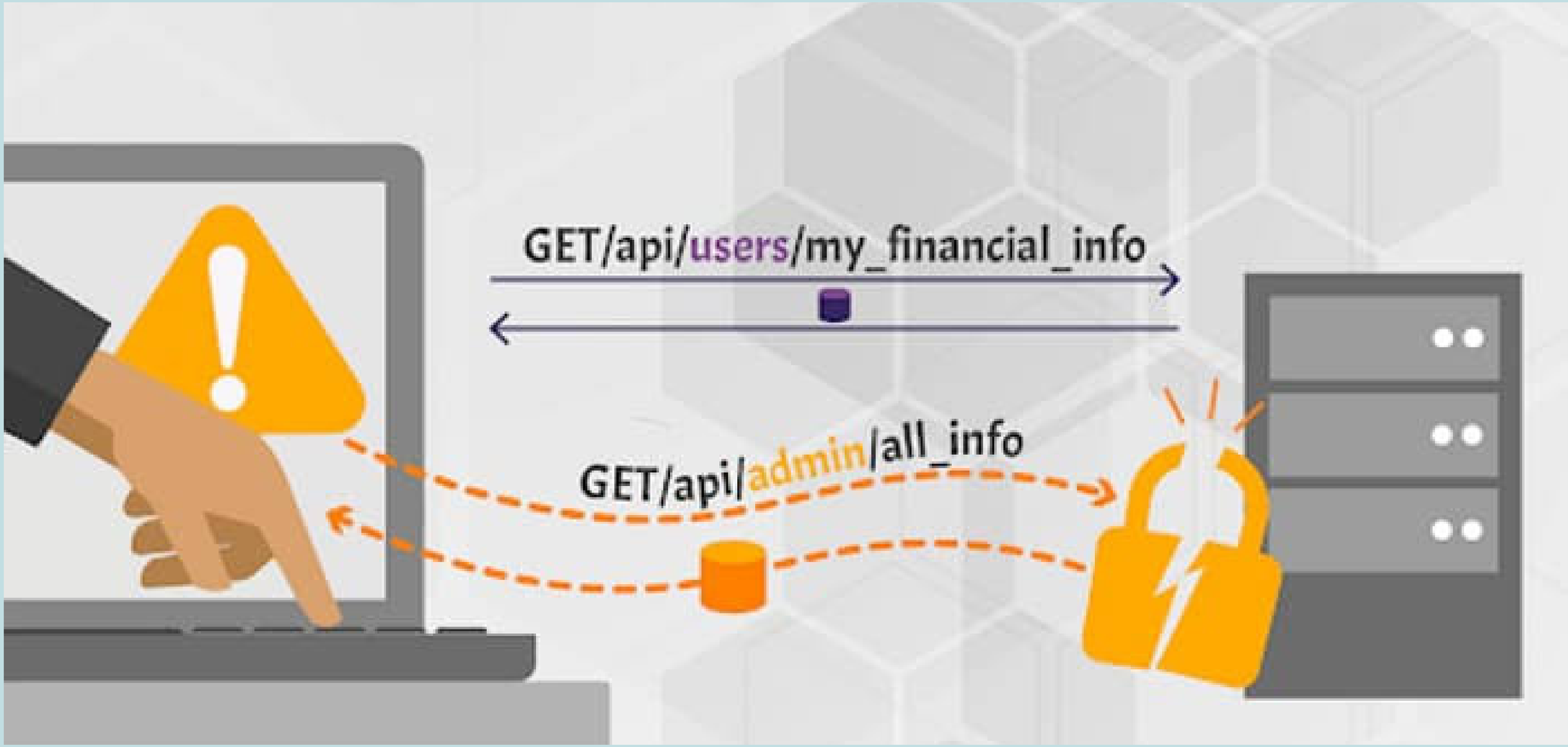


what is broken access control?

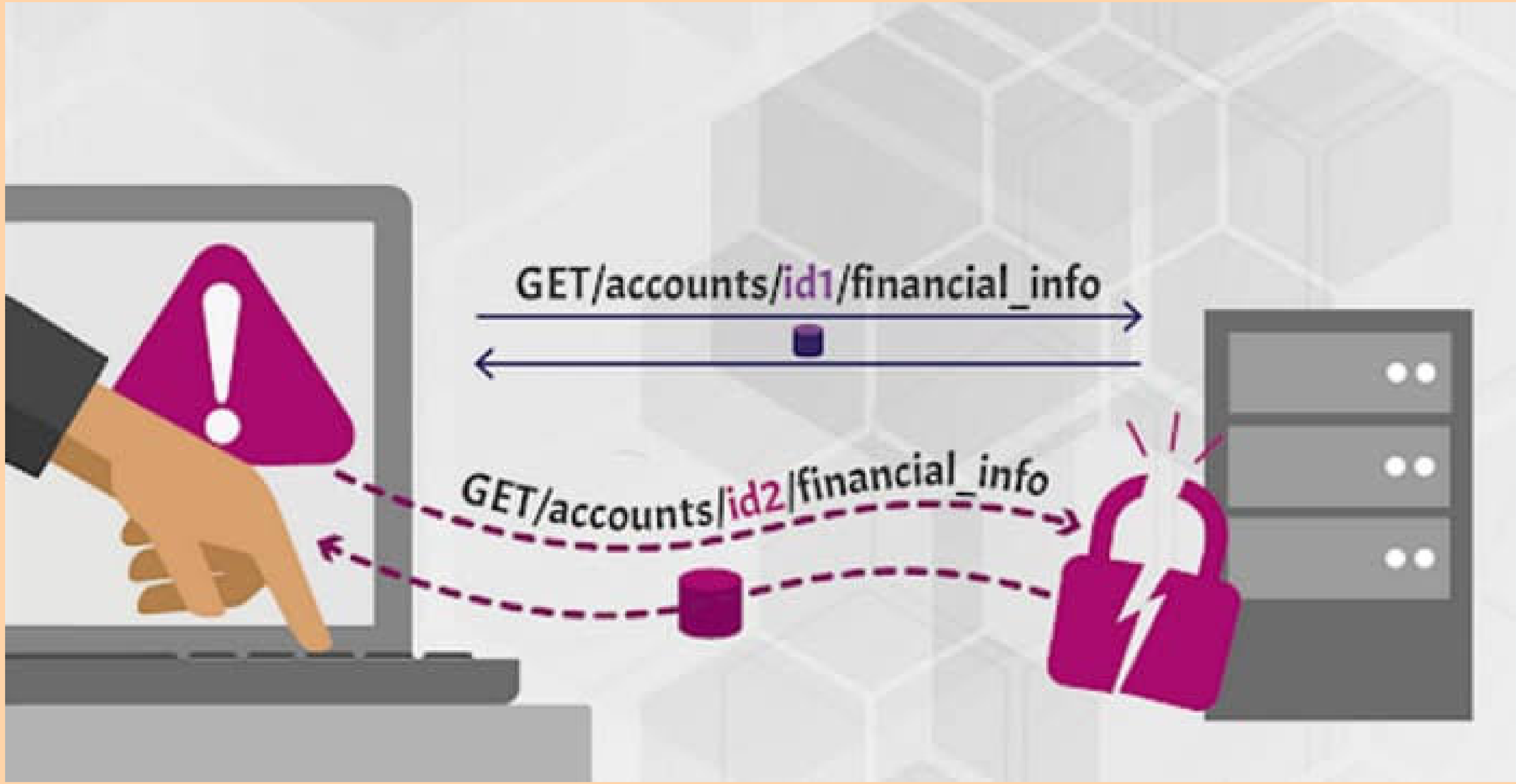
Broken access controls are a commonly encountered and often critical security vulnerability. Design and management of access controls is a complex and dynamic problem that applies business, organizational, and legal constraints to a technical implementation.

BROKEN ACCESS CONTROL EXAMPLES

Example #1:The application uses unverified data



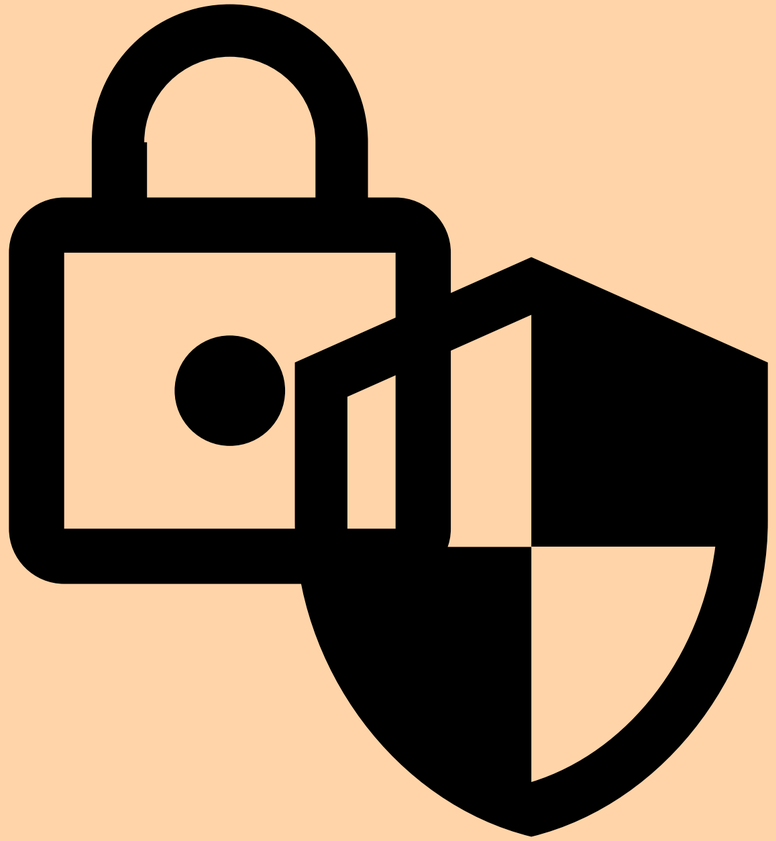
Example #2:An attacker simply force browses to target URLs



Secure your web application

Why is Broken Access Control important?

How to secure Broken Access Control ?



Client Side Caching

File Permissions

Insecure Id's

Forced Browsing Past Access Control Checks

Path Traversal

The policy should document what types of users can access the system, and what functions and content each of these types of users should be allowed to access.

The access control mechanism should be extensively tested to be sure that there is no way to bypass it.

Is everything clear so far?

Feel free to make this an open discussion for questions or clarifications before proceeding.

Thank you for joining today's class.

Use this space for announcements, homeworks, or ways students can approach you if ever they have questions.