Project Topic:
Broken Object-level Authentication

Team Members:

S.no.	Roll no.	Name
1	**22M2106**	SAKSHAM AGRAWAL
2	**22M0761**	ABHISHEK DIXIT
3	**22M0770**	NIKHIL SHARMA
4	**22M0809**	SOMIL SWAPNIL CHANDRA

Abstract:

Object-level authentication (OLA) is a security mechanism that ensures that access to specific objects within a system is restricted to authorized users only. However, in recent years, there have been numerous cases of broken object-level authentication, where attackers have been able to gain unauthorized access to sensitive data by exploiting vulnerabilities in OLA implementations. This project aims to demonstrate broken object-level authentication, including its causes and consequences.

Introduction:

Object-level authentication is a crucial security mechanism that helps protect sensitive data by ensuring that only authorized users can access specific objects within a system. OLA can be implemented using a variety of techniques, such as access control lists, role-based access control, or attribute-based access control. However, despite its importance, OLA is not always implemented correctly, leaving systems vulnerable to attacks.

Broken object-level authentication occurs when attackers are able to bypass OLA mechanisms and gain unauthorized access to sensitive data. This can happen due to a variety of reasons, including misconfigured permissions, weak authentication

mechanisms, or insufficient access control policies. Broken OLA can have serious consequences, such as data breaches, financial losses, or reputational damage.

This project will investigate the causes of broken OLA, including a common vulnerability and display the cause of such vulnerability, which is **“inefficient management of login sessions”.**

The Project:

The project involves a simple demonstration of a dashboard of a website which is accessible by either entering the correct password or by completing two-factor authentication in case of some risk. But, a vulnerability which is described below, is present in the website, which causes **“broken object-level authentication”** and hence allows the attacker to exploit the vulnerability to attack the website.
Note: The code to the website has been included in the “Project Code” folder.

The Vulnerability:

In the included code, line number 202 of “app.py”
I.e. **session['logged_in']=False**
has been commented, which becomes a vulnerability in session management and hence can cause the client/attacker to access the dashboard without completing the Two-Factor authentication (2FA) process by directly adding “/dashboard” to the URL.

The Solution:

If that line is included in the code, the session logged_in value becomes **False** at the time when the email for two-factor authentication is sent to the client and hence, the client **can not use the above-mentioned vulnerability** to enter the dashboard without completing the two-factor authentication.

References:

- https://owasp.org/www-project-top-ten/
- https://owasp.org/Top10/A01_2021-Broken_Access_Control/
- https://www.microsoft.com/en-in/security/business/security-101/what-is-two-factor-authentication-2fa