High Level Description:

Single Sign-On (SSO) is a widely spread and accepted online authentication method. This project aims to demonstrate a user identity inconsistency vulnerability created through the reuse of user identities and propose a Service Provider method of mitigation for said vulnerability.

Requirements:

Functional:

SaferSSO must include an SP with SSO capable registration and authentication, using OAuth for authentication with the IdP. The SP will also demonstrate how user accounts can be compromised with a reused identity token from the IdP. The SP will also contain a method of mitigation that can be switched on and off to demonstrate its effectiveness.

- SP with SSO capabilities
- SP with authorized and unauthorized pages for vulnerability demonstration
- IdP capable of providing token for SSO
- SP side mitigation to user identity inconsistency vulnerability

Non-Functional:

- Mitigation must be toggleable for demonstration purposes
- The SP and IdP should be able to run on both virtual machines and containers
- The design framework will need to be self-contained and run without an internet connection

Risks:

Technology Risks

- The SP will have an active vulnerability that could be potentially exploited beyond the original scope of the project
- Access to virtual machine is restricted to on campus
- Potential domain is not accessible

Skill Risks

- Most members of the team have limited knowledge of Django
- Most members of the team have limited knowledge of SAML

Definition of Done:

List of Minimal Requirements

- Working demonstration of vulnerability
- Working mitigation of vulnerability
- Working SP and IdP to facilitate SSO

Tests:

- Demonstration of vulnerability

- Demonstration of mitigation

Delivery:

- Publish on the web at end of semester