

The background features a dark blue gradient with several concentric, glowing light blue circles. Four hexagonal icons, each containing a glowing padlock, are positioned at the top-left, top-right, bottom-left, and bottom-right of the frame. A large, semi-transparent dark blue rectangle is centered on the right side of the image.

IAM Demo Shop

Secure E-Commerce Implementation with Keycloak

SSO · 2FA · RBAC


ICT GANPAT UNIVERSITY

IAM PROJECT

IAM IN E-COMMERCE DEMO

 **RAHUL PRAJAPATI**

ENROLL NO: 23162171020

 **DIVYANSH SHARMA**

ENROLL NO: 23162171023

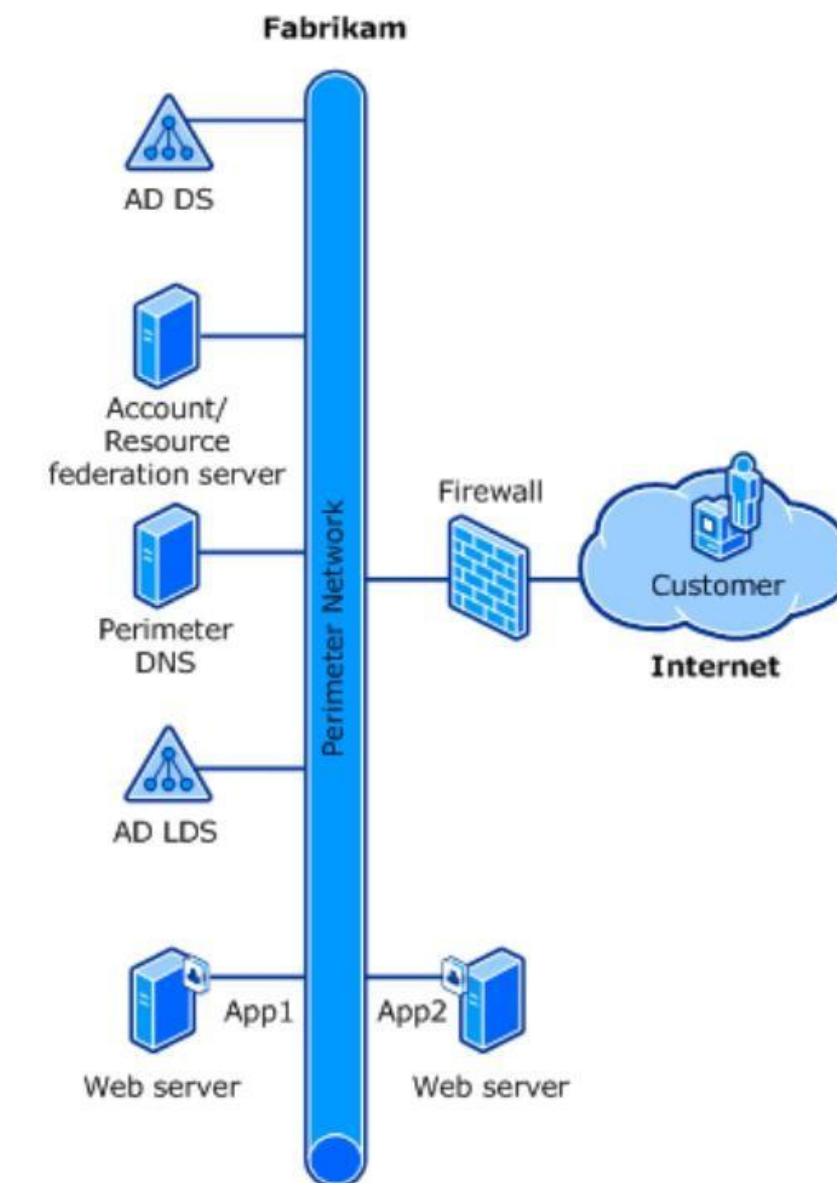
Project Overview

What is it?

A demonstration of a secure e-commerce frontend that offloads identity management to a dedicated provider.

Key Technologies

- ✓ **Keycloak:** Open Source Identity and Access Management.
- ✓ **Frontend:** Vanilla JavaScript & HTML5.
- ✓ **Security:** Standard protocols (OIDC / OAuth2).



Core Security Features



SSO

Single Sign-On allows users to log in once and access multiple applications without re-entering credentials.



2FA / MFA

Two-Factor Authentication adds a layer of security using Time-based One-Time Passwords (TOTP).



RBAC

Role-Based Access Control restricts sensitive areas (like Admin pages) based on assigned user roles.

Role-Based Access Control (RBAC)



Granular Permissions

The application checks the `realmAccess.roles` token claim to determine user privileges.

 **Customer:** Can view products, cart, and profile.

 **Admin:** Exclusive access to `/pages/admin.html`.



IAM Demo Shop

Keycloak, SSO • 2FA • RBAC

Login with SSO

Secure E-Commerce with Keycloak

This demo shows how an e-commerce website uses **Keycloak** for **Single Sign-On (SSO)**, **Two-Factor Authentication (TOTP)**, and **role-based access control (RBAC)**.

- 🔑 Centralized identity in Keycloak (no passwords in app).
- 📱 2FA enforced via TOTP (Google Authenticator, etc.).
- 👤 Roles like customer and admin control access.

Login & Experience SSO

View ID Token in Console

Status

Not authenticated

2FA

TOTP via Keycloak

Featured Security Courses

Fake products – real IAM demo 🤖

Intro to Cyber Security

Beginner

Understand basic threats, passwords, phishing, and safe browsing.

₹999

Add to Cart

Identity & Access Management Deep Dive

IAM & SSO

OAuth2, OIDC, SAML, SSO, federation and governance in one course.

₹1,499

Add to Cart

Red Team Lab

Advanced

Practice attacking and defending modern web applications.

₹1,999

Add to Cart

Admin Area – Role Based Access

Only users with admin role in Keycloak should see the admin dashboard.

Current user roles: guest

Go to Admin Dashboard

IAM DEMO E-COMMERCE

Sign in to your account

Username or email

Password



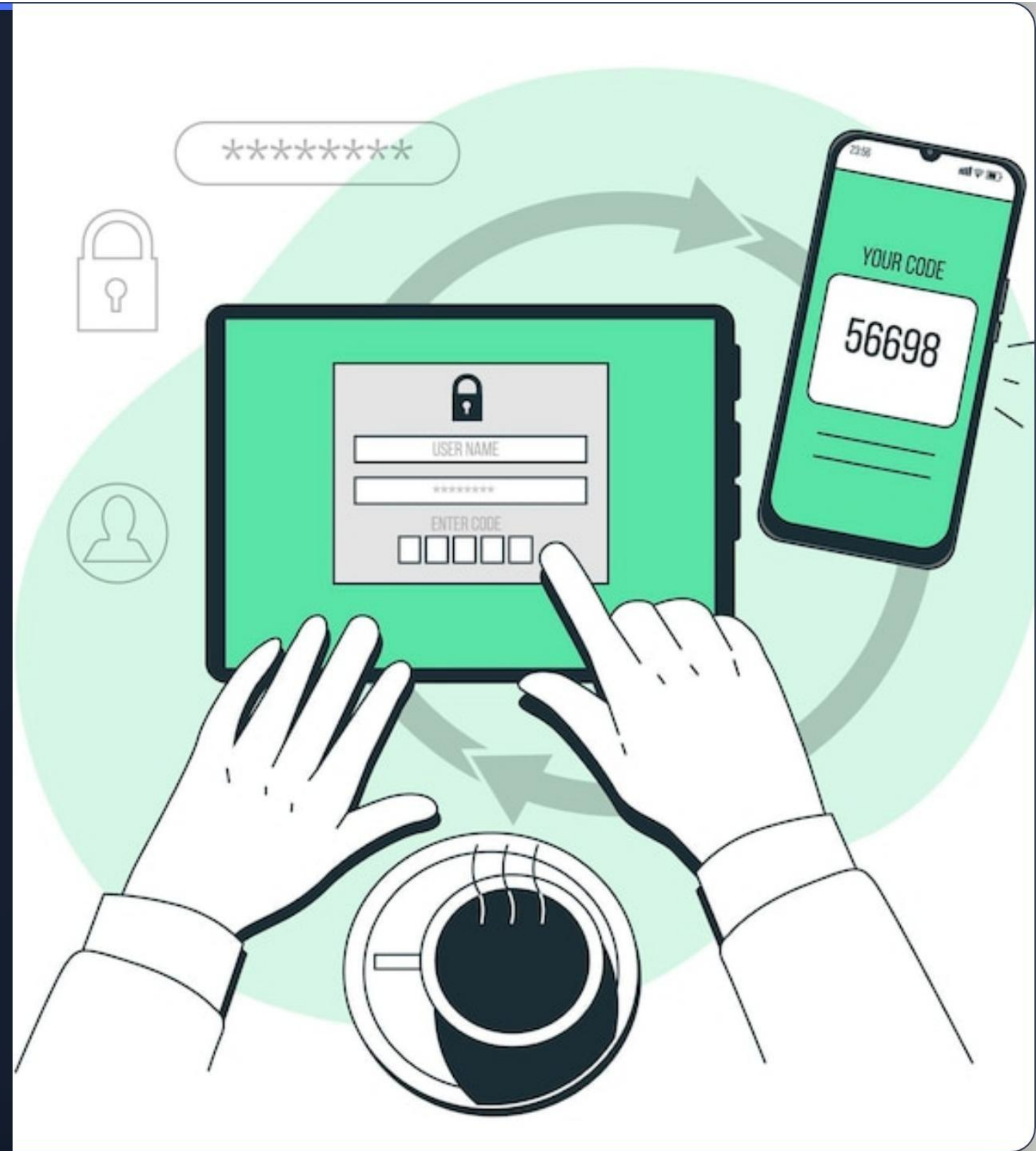
Sign In

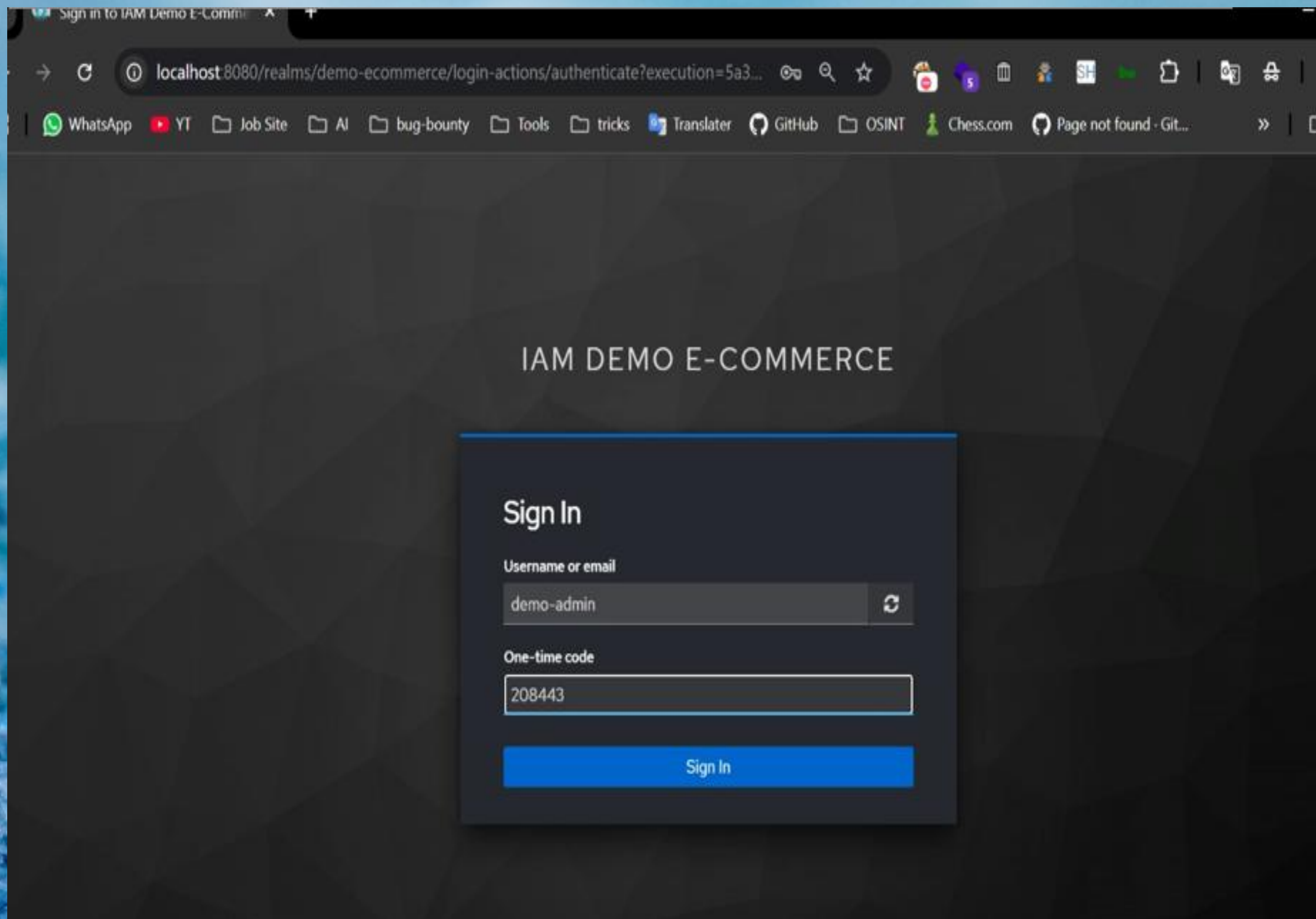
Enhanced Security with 2FA

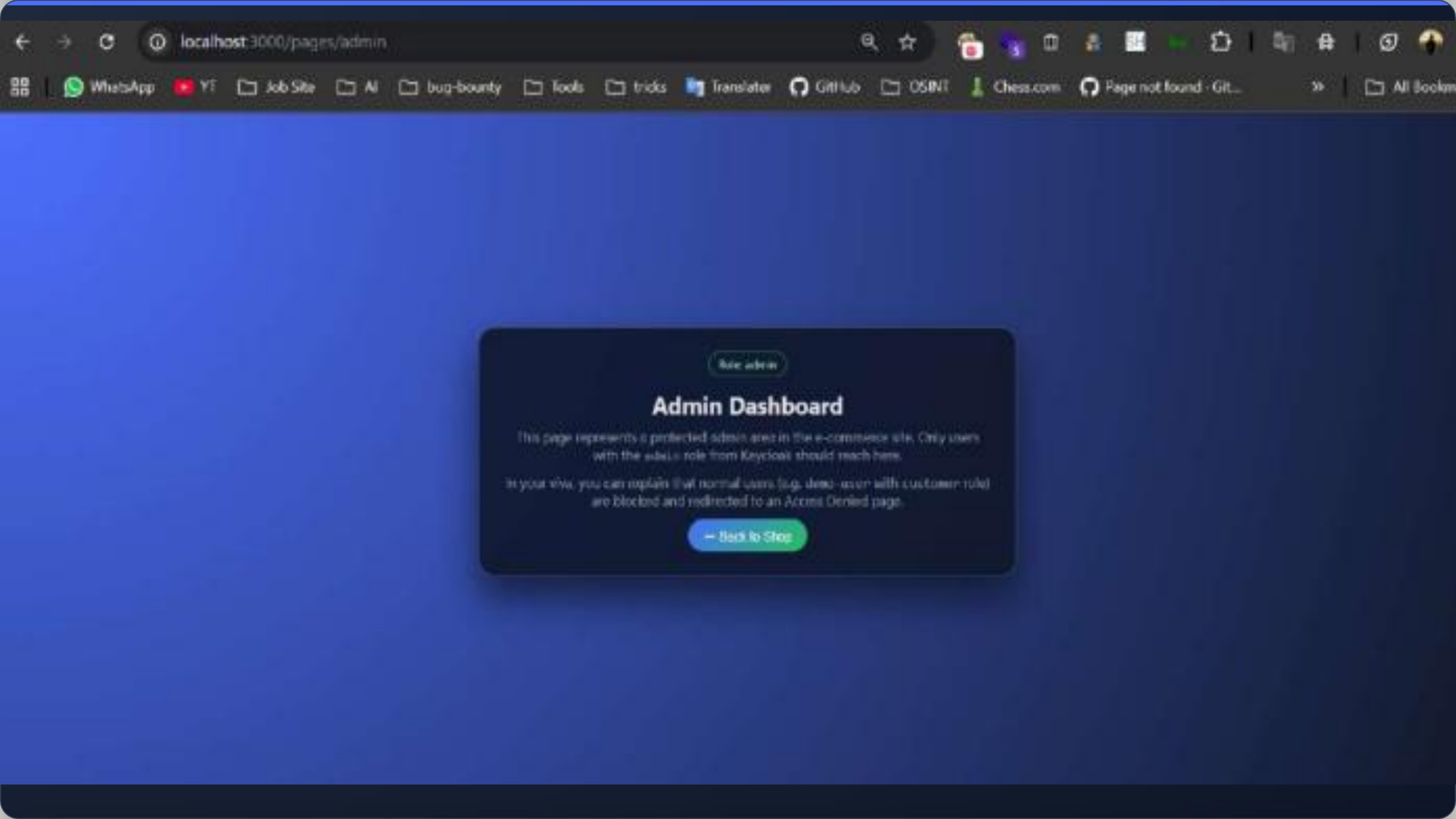
The Authentication Flow

1. User clicks "Login" in the app.
2. Redirected to Keycloak login page.
3. After password, Keycloak challenges for **TOTP** code (Google Authenticator).
4. Upon success, Keycloak returns an **Identity Token** to the app.

✓ Ensures compromised passwords don't lead to breaches.







Role: admin

Admin Dashboard

This page represents a protected admin area in the e-commerce site. Only users with the `admin` role from Keycloak should reach here.

In your view, you can explain that normal users (e.g. demo-user with customer role) are blocked and redirected to an Access Denied page.

[← Back to Shop](#)



