ALGEBRA UNIVERSITY

Katedra za sistemsko inženjerstvo i kibernetičku sigurnost

ASBP

Lab 6 – OAuth

Uvod

Cilj današnje vježbe je razumjeti osnove Oautha.
OAuth (Open Authorization) je protokol otvorenog standarda dizajniran za sigurnu autorizaciju, omogućujući aplikacijama trećih strana ograničen pristup korisničkim resursima bez izlaganja njihovih vjerodajnica. To postiže delegiranjem pristupa pomoću tokena umjesto izravnog dijeljenja osjetljivih informacija poput lozinki. Tijek OAuth obično uključuje tri primarna aktera: vlasnika resursa (korisnika), klijenta (aplikaciju treće strane) i poslužitelj za autorizaciju (davatelj identiteta). Klijent zahtijeva pristup od vlasnika resursa, koji ovlašćuje poslužitelj za izdavanje pristupnog tokena, koji klijent može koristiti za interakciju s poslužiteljem resursa (npr. API) u ime korisnika.
Srž sigurnosti OAuth-a leži u korištenju pristupnih tokena i opcionalnih tokena za osvježavanje. Pristupni tokeni, obično JWT-ovi (JSON Web Tokens), vremenski su ograničeni i dodjeljuju određene dozvole definirane opsegom. Tokeni za osvježavanje, ako su dostupni, omogućuju klijentu da zatraži nove pristupne tokene nakon isteka bez potrebe za ponovnom provjerom autentičnosti korisnika. OAuth podržava nekoliko tijekova, kao što su tijek autorizacijskog koda, implicitni tijek i tijek vjerodajnica klijenta, od kojih je svaki prilagođen različitim slučajevima upotrebe, osiguravajući fleksibilnost i sigurnost za različite aplikacije.

OAuth se naširoko koristi na internetu za omogućavanje sigurne integracije između usluga i aplikacija. Na primjer, platforme društvenih medija kao što su Google, Facebook i Twitter implementiraju OAuth kako bi korisnicima omogućile prijavu na web stranice trećih strana koristeći svoje društvene račune. Ovaj proces, koji se često naziva "Prijava na društvene mreže", eliminira potrebu da korisnici pamte više vjerodajnica, a istovremeno osigurava da aplikacije trećih strana nikada ne dobiju izravan pristup svojim lozinkama. Umjesto toga, aplikacije dobivaju pristupni token koji daje ograničena, opoziva dopuštenja.
Osim društvenih prijava, OAuth pokreće API interakcije između aplikacija, kao što je integracija CRM alata s uslugom pohrane u oblaku. Na primjer, kada aplikacija kao što je Zapier zatraži pristup korisnikovom Google disku, OAuth osigurava da korisnik izričito pristane na tražene opsege (npr. čitanje datoteka). Autorizacijski poslužitelj izdaje pristupni token koji je ograničen na odobrenje korisnika, omogućujući integraciji da sigurno funkcionira uz zadržavanje korisnikove kontrole nad njihovim podacima.

Vježba

Sve korake predavač će raditi kao demonstraciju, ali se preporučuje da ih student i sam ponovi.

1. Otvorite GitHub račun. To će se koristiti kao pružatelj usluga OAuth-a. U stvarnosti se može koristiti bilo koja internetska usluga, GitHub je ovdje samo kao primjer.
2. Preuzmite aplikaciju Postman. Osnovna ideja ove aplikacije je testiranje različitih vrsta zahtjeva prema web poslužiteljima, korištenje web pretraživača u takvim situacijama je nezgodno jer im nedostaju napredne mogućnosti koje Postman i slične aplikacije nude.
3. Slijedite upute na GitHub stranicama o tome kako pristupiti API pozivima

   https://docs.github.com/en/rest/authentication/authenticating-to-the-rest-api?apiVersion=2022-11-28

Bilješke:

Tokeni su vremenski ograničeni i ograničeni resursima. To znači da možete definirati čemu token služi i koliko dugo vrijedi.
U slučaju GitHub tokeni mogu biti "standardni" i "finegrained". To u osnovi znači da možete stvoriti tokene koji imaju pristup svemu ili možete točno definirati čemu token može pristupiti.