Slovenská technická univerzita v Bratislave Fakulta informatiky a informačných technológií

Ilkovičova 2, 842 16, Bratislava 4

Analýza správy účtov

BlockPay
Blockchain Busters

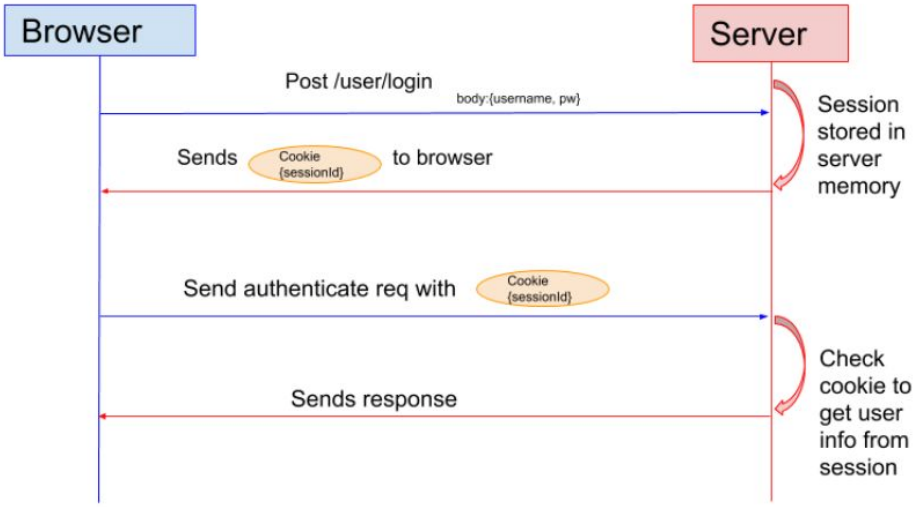
Tímový projekt
Tím č. 20
Vedúci: Ing. Kristián Košťál
fiittim201920@gmail.com

Vypracoval: Lenka Koplíková

Protokol HTTPS neukladá stavy a preto treba nájsť spôsob, ako stavy pri prepínaní stránok na webe zachovať. Používajú sa na to tokeny alebo session.

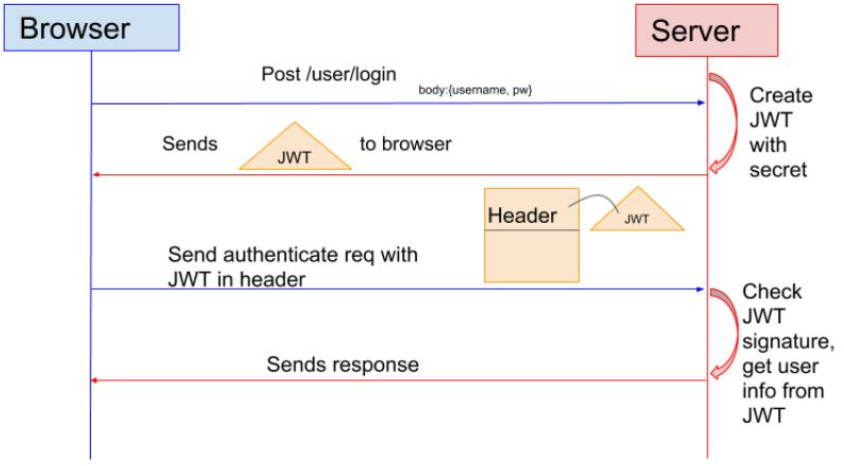
Session-based authentication

Pri session-based autentifikácii vytvorí server session pre používateľa po tom, ako sa prihlási. Session ID je následne uložené v cookie vo webovom prehliadači. Kým je používateľ prihlásený, tento cookie je zaslaný spolu s každým requestom a porovnaný so session informáciou uloženou v pamäti.



Token-based authentication

Autentifikácia založená na tokenoch využíva JSON Web Token (JWT). V tomto prípade server vytvorí JWT s tajomstvom a pošle ho klientovi. Klient si uloží tento JWT (zväčša do lokálneho úložiska) a vloží ho do hlavičky každého requestu. Server validuje JWT v každom requeste.



Porovnanie

Najväčším rozdielom je fakt, že pri tokenoch je stav uložený na strane klienta, zatiaľ čo pri session je uložený na serveri.

Škálovateľnosť:

- session-based autentifikácia: ak veľa užívateľov používa systém naraz, môže nastať problém (keďže sú informácie uložené na serveri)
- token-based autentifikácia: nie je problém so škálovateľnosťou

Viacero zariadení:

- session-based autentifikácia: za bežných okolností fungujú cookies iba na jednej doméne alebo jej sub-doménach (ak sú cross-domain, tak sú zväčša zakázané webovým prehliadačom). Môže sa vyskytnúť problém, ak sú API volané z rôznych domén na mobilné a webové zariadenia
- token-based autentifikácia: nie je problém s cookies, keďže sú informácie uložené v hlavičke requestu

Vo všeobecnosti je odporúčané používanie tokenov. Jedinou nevýhodou je fakt, že veľkosť tokenu je väčšia ako session ID a obsahuje viacero informácií o používateľovi. Treba si dávať pozor na to, aby iba najpotrebnejšie informácie boli uložené v tokene. Citlivé informácie by sa mali vynechať aby sa vyhlo XSS bezpečnostným útokom.