Online Clearingové centrum

Bakalářská práce

Mykyta Boiko
Vedoucí práce: Ing. Stanislav Kuznetsov

Fakulta informačních technologií
České vysoké učení technické v Praze

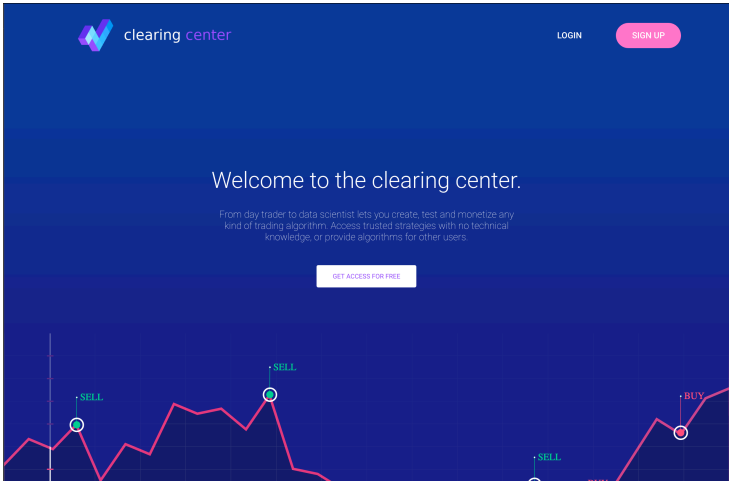
22. 5. 2019

Osnova

Úvod

- Kryptoměny
- Algoritmické obchodování
- Obchodní signál

Online Clearingové centrum



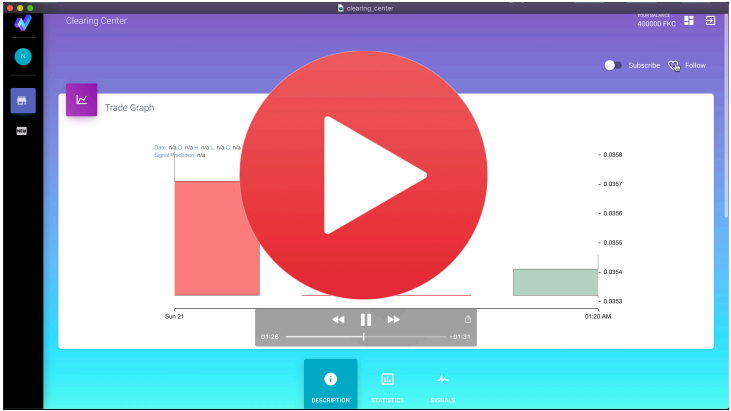
Obrázek: Úvodní stránka webové aplikace

Cíle práce

Hlavními cíly této práce jsou:

1. Vytvoření prototypu webové aplikace pro obchodování krypto signály
   - Navrhnout Front-End a Back-End prototypu, vybrat příslušné technologie a implementovat
   - Navrhnout API pro všechny účastníky a implementovat
2. Navrhnout možné rozšíření prototypu do budoucna.

DEMO



Obrázek: Ukázka funkčnosti aplikace

Vyber technologie

Použité technologie:

- **Back-End**
  - PHP 7
    - Symfony 4 - framework PHP, který zjednodušuje proces vývoje webové aplikace
    - DoctrineORM - ORM framework nabizejici objektovy přístup k datové vrstve
- **Front-End**
  - Javascript
    - React - open source knihovna pro vytváření uživatelských rozhraní
    - Redux - řídí správu stavu (stavový kontejner pro ReactJS)
- **Communication protocol**
  - HTTP protokol - zajišťuje komunikaci mezi Back-End a Front-End

Jelikož, jeden z hlavních cílů práce je v reálném čase oznamovat uživatelovi o obdrženém signálu, byla potřeba najít vhodnou technologii umožňující rychlou a efektivní komunikaci.

Web Application Messaging Protocol

Komunikace v reálném čase mezi serverem a klientem je implementována pomocí protokolu Web Application Messaging Protocol.

Pro Symfony framework existuje řešení - ***ThruwayBundle***, což je implementace PHP programu WAMP.

Další důležitý cíl je zajistit maximální bezpečnost všech provedených transakcí a přenosů dat. Řesením bylo implementace nasledujicí bezpečnostní vrstvy:

Autentizace založená na Xsrf-Jwt protokolu

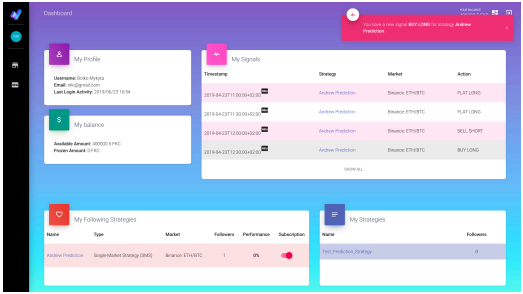
Princip:

1. Ukládáme JWT token do HTTP-only cookie.
2. V JWT ukládáme hašovanou verzi tokenu XSRF.
3. Po přihlášení posíláme klientovi token XSRF, aby ho mohl uložit do lokálního úložiště.

Až klient pošle požadavky, je JWT automaticky odeslán s každým požadavkem přes cookies a následovně se posílá token XSRF přes HTTP hlavičku. Na straně serveru probíhá prehašovani pro porovnání s tím, co je v JWT na serveru.

Vysledek : Nas JWT je chráněn před odcizením pri XSS útoku a chráněn před XSRF útokem.

Funkce aplikace - strucny vycet I



Obrázek: Oznameni uzivatele o ziskani noveho signalu

1. Registrace / prihlášení uživatelu (potvrzující e-mail)
2. Registrace / přidání nových strategie (API klíč pro danou strategii + přidání do marketplacu)
3. Marketplace se všemi strategiemi.

Funkce aplikace - strucny vycet II

4. Poskytování statistych dát strategii v její profilu(+ zobrazení OHCL grafu, výkonnosti, neplatných signálů)
5. Možnost buď sledovat (přidat do seznamu oblíbených) nebo se přihlásit k odběru za poplatek (obdržení signálu)
6. Rychlé oznámení uživatele o obdržení nového signálu prostřednictvím notifikace
7. Platební systém, podobně jako u chytrých kontraktů (vývojář nezíská příjem, než smlouva nebude splněna)
8. Poskytování historii platebních transakcí, obdržených signálů.

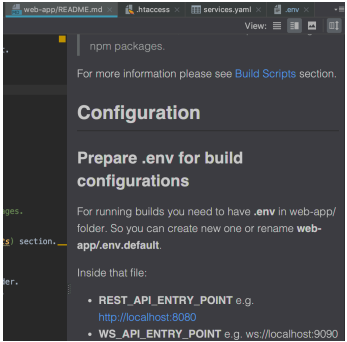
Shrnutí výsledku a budoucnost projektu

1. Splnení zadání
   - Zadání je splneno dle vytycených cílu
2. Budoucí rozšíření
   - Doplnit další predikční řešení
   - Přidat řešení s odlišným typem automatizace
3. Přínos pro mě
   - Zkušenost s vývojem webových aplikací a implementací bezpečných prostředků

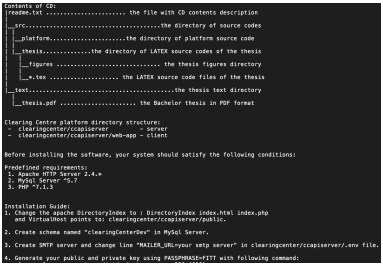
Dekuju za pozornost!

Otázky oponenta

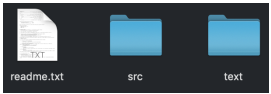
1. Why the text part of the thesis is so poor?
2. Do you have an installation guide at least in the electronic form?



(a) Readme.md klientu z git repo



(b) Readme.txt soubor



(c) Obsah přiloženého média