

UNIVERZITA KOMENSKÉHO V BRATISLAVE
FAKULTA MATEMATIKY, FYZIKY A INFORMATIKY

INTERAKTÍVNY PORTÁL NA VYUČOVANIE
DYNAMICKÉHO PROGRAMOVANIA
BAKALÁRSKA PRÁCA

2016
MICHAL SMOLÍK

UNIVERZITA KOMENSKÉHO V BRATISLAVE
FAKULTA MATEMATIKY, FYZIKY A INFORMATIKY

INTERAKTÍVNY PORTÁL NA VYUČOVANIE
DYNAMICKÉHO PROGRAMOVANIA
BAKALÁRSKA PRÁCA

Študijný program: Informatika
Študijný odbor: 2508 Informatika
Školiace pracovisko: Katedra informatiky
Školiteľ: Michal Foríšek, PhD

Bratislava, 2016
Michal Smolík



Univerzita Komenského v Bratislave
Fakulta matematiky, fyziky a informatiky

ZADANIE ZÁVEREČNEJ PRÁCE

Meno a priezvisko študenta:

Študijný program: informatika (Jednoodborové štúdium, bakalársky I. st., denná forma)

Študijný odbor: 9.2.1. informatika

Typ záverečnej práce: bakalárska

Jazyk záverečnej práce: slovenský

Názov:

Cieľ:

Literatúra:

**Kľúčové
slová:**

Vedúci:

Katedra: FMFI.KI - Katedra informatiky

Vedúci katedry: doc. RNDr. Daniel Olejár, PhD.

Dátum zadania:

Dátum schválenia:

doc. RNDr. Daniel Olejár, PhD.
garant študijného programu

.....
študent

.....
vedúci práce

Pod'akovanie:

Abstrakt

Klíčové slová:

Abstract

Keywords:

Obsah

Úvod	1
1 Úloha a použitie portálu	2
2 Server	3
2.1 Použité technológie	3
2.1.1 Django 1.9	3
2.1.2 REST framework	3
2.2 Testovač	4
2.2.1 Stiahnutie vstupov a poslanie výstupov	4
2.2.2 Testovanie skriptom u používateľa	4
2.2.3 Testovanie na servri	5
2.3 Bezpečnosť	5
2.3.1 Autorizácia	5
2.3.2 Prihlasovanie cez externé portály	5
2.3.3 Protokoly	6
2.4 Administrácia	6
2.4.1 Pridávanie a hodnotenie úloh	6
2.4.2 Zbieranie dát o používateľoch	7
2.4.3 Oprávnenia používateľa a administrátora	7
3 Výučba	9
4 Ďalšie funkcie	10
Záver	11

Úvod

Kapitola 1

Úloha a použitie portálu

Krátka úvodná kapitola v ktorej si povieme čo náš portál dokáže a ako to pomáha výučbe

Kapitola 2

Server

V tejto kapitole sa oboznámime s vnútorným fungovaním servera, používaných bezpečnostných protokoloch a možnosťami poskytovanými administrátorovi.

2.1 Použité technológie

2.1.1 Django 1.9

Django je open source framework nad programovacím jazykom Python, ktorý uľahčuje vývoj a údržbu webových aplikácií. Poskytuje funkcionality servera na nízkych úrovniach (správa databázy, HTTP komunikácia a iné), čo umožňuje vývojárovi sa sústrediť na tvorbu samotného obsahu. Django takisto ponúka jednoducho implementovateľné možnosti ochrany pred niektorými najbežnejšími útokmi, ako napríklad XSS, SQL injection alebo CSRF.

Server používa framework Django 1.9 pre jednoduchosť vývoja spravovania databáz, autentifikácie používateľov a prostredia pre administrátora.

2.1.2 REST framework

Django REST framework je v projekte využitý na jednoduché a prehľadné zobrazovanie obsahu databázy, odpovedí na HTTP požiadavky a na implementáciu token autorizácie. Umožňuje priamo v prehliadači poslať a zobrazíť odpovede na požiadavky, čo zjednodušuje debugovací proces. Taktiež uľahčujú aj implementáciu externej OAuth autorizácie o ktorej si povieme neskôr.

2.2 Testovač

Testovač je najdôležitejšia časť portálu, pretože dokáže zmerať schopnosti používateľa. Sú tri možné spôsoby testovania:

2.2.1 Stiahnutie vstupov a poslanie výstupov

Toto je najjednoduchší spôsob implementácie testovača. Používateľ si z nášho portálu si stiahne testovacie vstupy na ktorých spustí svoj program, výstup zapíše do súbora a súbor pošle na server, ktorý skontroluje správnosť odpovede.

Veľká výhoda tohto prístupu je jeho jednoduchosť, ale má značnú nevýhodu: nezaručuje že používateľ napísal optimálny program. Účelom portálu je učiť používateľov dynamické programovanie, ale tento testovač umožňuje správne vyriešiť úlohu aj hrubou silou.

Tento problém by sa dal obísť používaním úloh, ktoré majú mimoriadne časovo zložité riešenie hrubou silou (napríklad $O(2^n)$), ktoré by na väčších vstupoch vyžadovali niekoľko dní počítania. Toto riešenie je samozrejme nežiadúce keďže veľmi obmedzuje výber úloh. Preto bude používané iba počas procesu vývoja a nie vo finálnom produkte.

2.2.2 Testovanie skriptom u používateľa

Druhý možný spôsob testovania je rovnaký ako predošlý, až na jednu zmenu: používateľ si stiahne testovací skript, ktorý spustí používateľom zadany program na vstupoch, ktoré stiahne z nášho servera. Potom odošle výstupy a tie sú porovnané so správnymi odpoveďami.

Toto riešenie nám umožňuje merať čas potrebný na beh programu, čo je značné vylepšenie oproti predošlému riešeniu, pretože ak používateľ nijak nezasiahne do skriptu, vieme zistiť či sa mu podarilo úlohu riešiť dynamickým algoritmom.

Používateľ ale môže skript viacerými spôsobmi napadnúť, napríklad manipulovať s časovým obmedzením alebo získať vstupy, vyriešiť ich iným, pomalším algoritmom a vytvoriť program ktorý pre každý vstup vypíše správny výstup zo súboru alebo priamo zapísaný v zdrojovom kóde.

Tieto chyby sa dajú vyriešiť zabezpečením skriptu proti útokom, ale žiadna ochrana nie je stopercentná. Mohli by sme teda napríklad neakceptovať výsledky, ktorých podozrivo vyzerajúce časy (t.j. časy, ktoré sa nesprávajú podľa krivky, časy dlhšie ako limit, ktoré ale skript sa nezastavil atď.). Toto riešenie ale nie je akceptovateľné, pretože by mohlo prepustiť falšované výsledky alebo odmietnuť správne riešenie.

Na ochranu vstupov sa dá použiť procedurálna generácia alebo náhodné vyberanie z väčšej množiny vstupov, ale tie pridávajú prácu administrátorovi a komplikujú pridávanie nových úloh.

2.2.3 Testovanie na serveri

Tretí spôsob testovania prebieha na našom serveri. Používateľ pošle zdrojový kód svojho riešenia, ten na serveri skompilujeme a vyhodnotíme s časovým obmedzením behu.

Veľkou výhodou je, že používateľ nemá prístup k testovaným vstupom a správnym výstupom, takže úloha nebude vyhodnotená za správne vyriešenie pri neoptimálnom programe kvôli vyprchaniu časového limitu (závisí od dĺžky vstupu a časového limitu, ktoré zadáva administrátor). Rovnako je oveľa ťažšie napadnúť a upraviť testovač.

Nevýhodou testovača je napríklad zložitá implementácia, pretože musí viesť kompilovať čo najviac programovacích jazykov a zároveň musíme dávať pozor aby poslaný program nijako nenarušoval bezpečnosť servera (nečítal z pamäte ktorú nealokoval, nespúšťal žiadne iné programy, nepoužíval niektoré systémové volania a podobne). Ďalšou nevýhodou sú nároky na výpočtový čas servera: keďže proces testovania spúšťa program na serveri, môže server spomaliť.

Nakoľko pri tomto testovači je najťažšie mať správne výsledky v časovom limite a nemať optimálne riešenie, v portáli je implementovaný tento testovač. Ak ale sa zvýši popularita nášho portálu a vznikne problém s rýchlosťou testovania, bude možno treba zvážiť buď vylepšenie hardvéru servera alebo implementáciu predošlého testovača (2.2.2)

2.3 Bezpečnosť

2.3.1 Autorizácia

Portál používa token autentifikáciu ktorá z pohľadu používateľa vyzerá nasledovne:

Používateľ pri prihlasovaní pošle prihlasovacie meno a heslo (tento krok je iný pri prihlasovaní cez externú doménu) a ako odpoveď dostane náhodne vygenerovaný reťazec o dĺžke približne 40 znakov. Potom všetky požiadavky na používateľove dáta musia v hlavičke uviesť tento token, inak budú zamietnuté. Server si pamätá používateľov token až kým sa používateľ neodhlási alebo mu nevyprší platnosť po dlhšej neaktivite.

Všetky požiadavky musia obsahovať token, čo pomáha používateľa chrániť napríklad pred CSRF útokom. Na rozdiel od cookies, prehliadač nepridáva token do hlavičky automaticky a teda väčšina CSRF útokov bude zamietnutých.

2.3.2 Prihlasovanie cez externé portály

Portál má viacero možností prihlasovania sa cez externé portály. Použijeme prihlasovaciu schému OAuth 2.0, aby komunikácia s externým portálom prebiehala iba pri

prihlasovaní po ktorom používateľov prehliadač komunikuje so serverom ako keby sa prihlásil priamo na náš portál bez využitia externej služby.

Prihlasovanie cez OAuth 2.0 prebieha nasledovne:

1. Používateľ sa prihlási na externý portál a potvrdí našej aplikácii vyžiadané oprávnenia
2. Od externého portálu získa prístupový token na ten externý portál
3. Tento token pošle nášmu serveru
4. Náš server pošle token externému portálu spolu s tajným ID našej aplikácie, aby externý portál vedel, že požiadavka prišla od našej aplikácie
5. Ak externý portál potvrdí požiadavku, náš server vráti používateľovi náš token a ďalej komunikujú iba s týmto novým tokenom.

Pomocou tejto schémy sa bude dať prihlásiť cez Facebook, Google+ a GitHub. (Tajné ID použité v kroku 3 je prístupné iba administrátorom)

2.3.3 Protokoly

Aby sme chránili používateľové dáta a token, všetky požiadavky obsahujúce osobné dáta používajú šifrovaný protokol HTTPS. Keďže HTTPS je pomalší na spracovanie, používame ho iba na potrebné požiadavky. Preto verejne známe informácie, ako napríklad zadania úloh alebo ich zoznam, nemusia byť chránené a používajú rýchlejší HTTP.

2.4 Administrácia

2.4.1 Pridávanie a hodnotenie úloh

Pridávanie a spravovanie úloh je hlavnou povinnosťou administrátora. Administrátor okrem zadávania úloh musí poskytnúť aj vzorové riešenie, prípadne nejaké rady k riešeniu úlohy a zaradiť ju podľa obtiažnosti.

Keďže obtiažnosť úlohy sa niekedy ťažko odhaduje, používatelia budú mať možnosť po správnom vyriešení úlohu ohodnotiť. Budú mať možnosť (ale nie povinnosť) ohodnotiť jej obtiažnosť a zaujímavosť na stupnici od 1 do 5. Tieto hodnotenia sa budú priemerovať.

Administrátor by sa mal snažiť, aby každá úloha mala čo najvyššie hodnotenie zaujímavosti. S hodnotením zložitosti je to ale inak: žiadna úloha by nemala byť príliš ľahká ani príliš ťažká, preto ideálny priemer hodnotenia zložitosti je 3.

Server bude poskytovať administrátorovi možnosť posúvať úlohy vyššie a nižšie v poradí, v ktorom ich používatelia riešia. Takisto bude označovať úlohy, ktoré majú príliš vysokú alebo príliš nízku obtiažnosť vzhľadom na úroveň riešiteľa a navrhovať nové miesto v poradí, kam ich zaradiť. Podobne bude označovať úlohy, ktoré sú považované za najmenej zaujímavé a bude na administrátorovi aby posúdil, či daná nezaujímavá úloha je dôležitá pre proces výučby alebo či ju možno zmeniť alebo odstrániť.

2.4.2 Zbieranie dát o používateľoch

Náš portál okrem vyučovania dynamického programovania je schopný aj zbierať údaje o schopnostiach používateľov a ich zlepšovaní sa postupom cez naše vyučovanie. Server bude zbierať viacero možných dát o používateľskej aktivite:

- Počet navštívených návodových a teoretických stránok na našom portáli
- Frekvencia návštev počas riešenia úloh (ako často používateľ používa naše návody na pomoc s riešením)
- Priemernú frekvenciu a dĺžku návštev nášho portálu
- Čas od prečítania úlohy po jej správne vyriešenie (nie veľmi dôležitý, pretože neberie do úvahy prestávky pri riešení)
- Počet neúspešných pokusov o riešenie
- Rozdiel priemerného a používateľovho hodnotenia úlohy (až keď bude dostatočne veľa hodnotení aby tento údaj niečo znamenal)

Z týchto údajov budeme vedieť zistiť ako efektívne je vyučovanie (napríklad, žiak sa pravdepodobne zlepšil ak prvé úlohy označoval ťažšie ako priemer a neskôršie ľahšie) a prípadne implementovať automatické zadávanie úloh podľa používateľových schopností.

2.4.3 Oprávnenia používateľa a administrátora

Bežní používatelia majú prístup iba k učebným materiálom, odomknutým úlohám (vyriešeným aj nevyriešeným) a svojim riešeniam. Ďalšie úlohy sa používateľovi odomknú, iba ak správne vyrieši všetky prerekvizitové úlohy. Všetky dáta zozbierané servrom (2.4.2) budú od používateľa skryté, pretože by mohli spôsobiť frustráciu u pomalšie sa učiacich používateľov.

Administrátor bude mať prístup ku všetkým úlohám, riešeniam, zozbieraným dátam všetkých používateľov a ich priemerom. Bude mať aj možnosť manuálne meniť niektoré hodnotenia a odomykať alebo zamykať používateľom úlohy.

Túto možnosť obchádzať pravidlá administrátorovi dávame pre prípad, že vznikne chyba a používateľovi sa napríklad odomkne úloha ku ktorej nemal mať prístup alebo neodomkne taká, ktorej všetky prerekvizity splnil. Používateľ v prípade takejto chyby bude môcť kontaktovať administrátora, ktorý preverí či naozaj nastala chyba a bude ju môcť napraviť bez debugovania servera, čo môže trvať príliš dlho.

Kapitola 3

Výučba

Tu si predstavíme užívateľské prostredie a proces výučby.

Kapitola 4

Ďalšie funkcie

Tu rozoberieme ostatné funkcie a možnosti portálu ktoré neboli spomenuté v iných kapitolách

Záver

Literatúra

- [1] Django documentation. <https://docs.djangoproject.com/en/1.9/>. [2015-12-07].
- [2] Facebook login for the web with the javascript sdk. <https://developers.facebook.com/docs/facebook-login/web>. [2015-12-07].
- [3] Javascript promise. https://developer.mozilla.org/en/docs/Web/JavaScript/Reference/Global_Objects/Promise. [2015-12-07].
- [4] React documentation. <https://facebook.github.io/react/index.html>. [2015-12-07].
- [5] Daniel Roy Greenfield and Audrey Roy Greenfield. *Two Scoops of Django: Best Practices for Django 1.8*. Two Scoops Press, 2015.