**SVEUČILIŠTE U ZAGREBU**

**FAKULTET ORGANIZACIJE I INFORMATIKE U VARAŽDINU**

***Problemski zadatak iz kolegija Sigurnost informacijskih sustava***

PROVJERA VJERODOSTOJNOSTI .NET

U Varaždinu, siječanj 2017.

**SVEUČILIŠTE U ZAGREBU**

**FAKULTET ORGANIZACIJE I INFORMATIKE U VARAŽDINU  
*Problemski zadatak iz kolegija Sigurnost informacijskih sustava***

PROVJERA VJERODOSTOJNOSTI .NET  
Opisna dokumentacija problema iz kolegija Sigurnost informacijskih sustava

U Varaždinu, siječanj 2017.

Sadržaj

[Uvod 4](#_Toc472163908)

[Postavke 4](#_Toc472163909)

[Registracija 6](#_Toc472163910)

[Prijava 11](#_Toc472163911)

[Popis slika 15](#_Toc472163912)

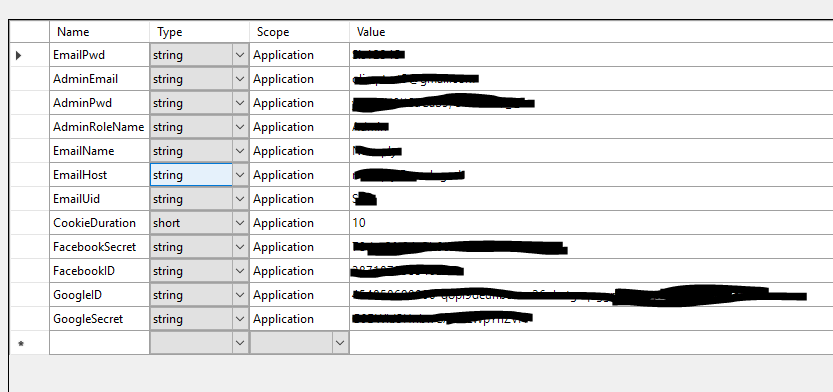
# Uvod

Kako sigurnost informacijskih sustava postaje sve važniji faktor u poslovanju, potrebno je u svim dijelovima poslovanja IS[[1]](#footnote-1) biti svjestan sigurnosti. Ovdje će se sagledati sigurnost iz aspekta pisanja programskog koda i osmišljavanja arhitekture. Ovdje je riječ o provjeri vjerodostojnosti od dva koraka pomoću elektronske pošte i sve vezano uz registraciju korisnika (zapamti me, zapamti me na ovom pregledniku, poništi lozinku, …) i prijave pomoću vanjskih servisa (Facebook, Google).

Korištena tehnologija je .NET MVC u programskom jeziku C# za pisanje web aplikacije, sve se vrti na IIS Serveru i kao SUBP se koristi SQLExpress koji je dovoljan u demonstrativne svrhe, a ukoliko bi se koristilo u produkciji potrebna je konfiguracija ovisna o potrebama. Za slanje elektronske pošte koristi se [SendGrid](https://sendgrid.com) koji je postavljen na Azure. Aplikacija je adaptivna te se može koristiti na mobitelima, tabletima i desktop računalima.

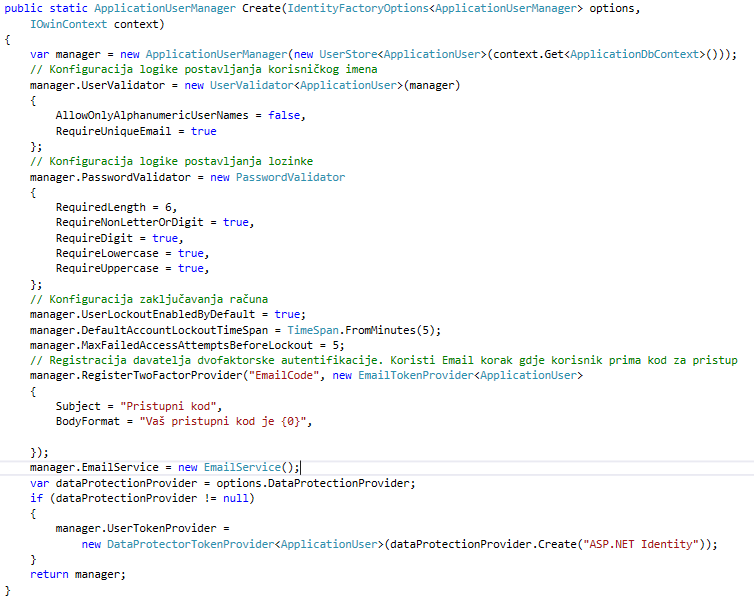
Demo aplikacije nalazi se na <http://sisauth.azurewebsites.net/> poveznici.

# Postavke



Slika 1 - Datoteka s postavkama

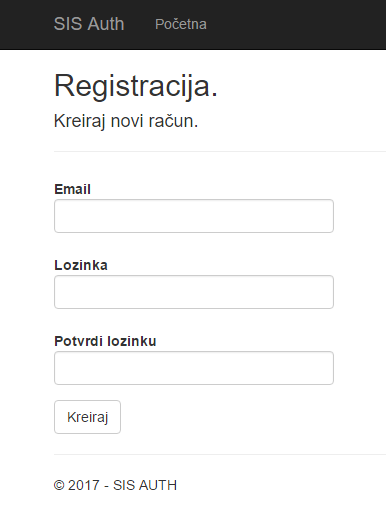
U postavkama imam postavke za slanje elektronske pošte, inicijalnog korisnika koji je administrator, trajanje kolačića, pristup vanjskim servisima...



Slika 2 - definiranje pravila

Na gornjoj slici je prikazan izvorni kod metode koja kreira pravila. U komentarima je navedeno za svaki dio što radi. Npr. vidimo kod gdje se definira logika postavljanja lozinke. Koja je minimalna dužina, da li treba posebni znak, broj, malo slovo, veliko slovo. Što se tiče djela s zaključavanjem računa to sprječava napade grube sile (engl.  *Brute Force*)

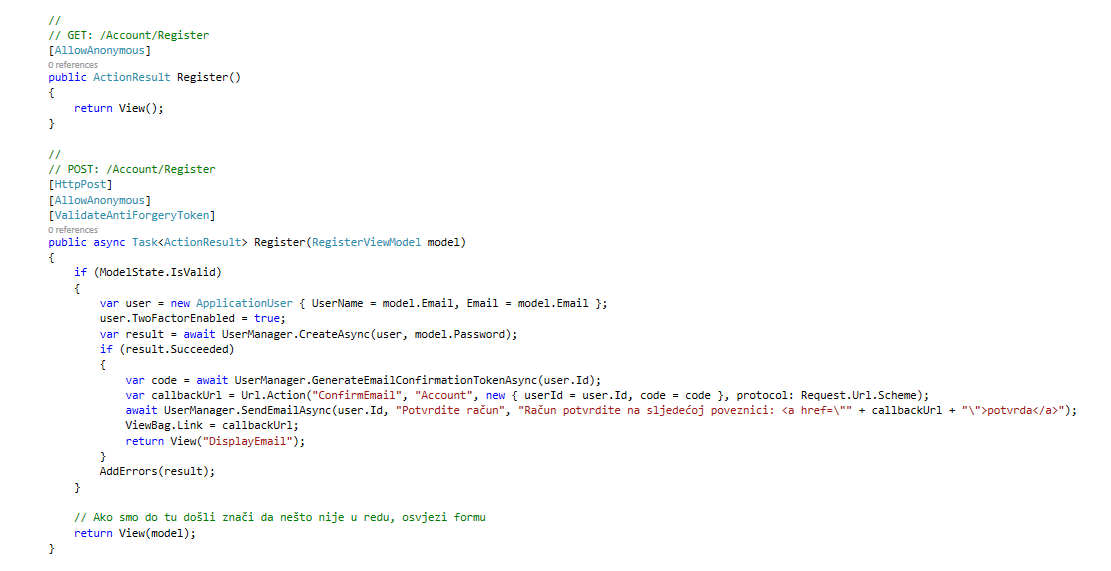
# Registracija



Slika 3 - forma za registraciju



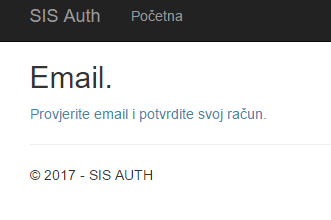
Slika 4 - Razor pogled forme



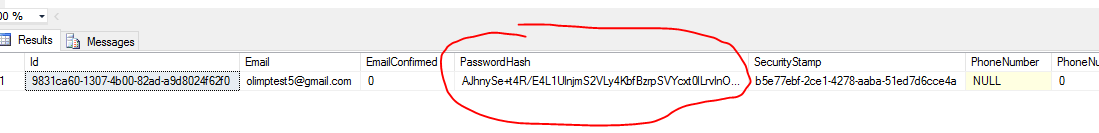
Slika 5 - GET i POST akcija registracije

Za registraciju je prikazan i razor pogled iz razloga što se u njemu vidi jedna ključna stvar, a to je pomoćna metoda @Html.AntiForgeryToken(). Razor se za vrijeme kompajliranja pretvara u čisti html sadržaj. U tom trenutku navedena pomoćna metoda generira jedinstveni token koji pomaže u sprječavanju XSS napada. Kao što vidimo i na post metodi Register imamo anotaciju pod nazivom ValidateAntiForgeryToken koja uspoređuje token s requestom i provjerava da li je to zaista pravi.

Nakon registracije šalje se email za potvrdu.

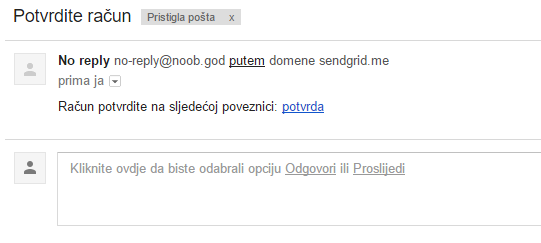


Slika 6 - nakon unosa podataka registracije

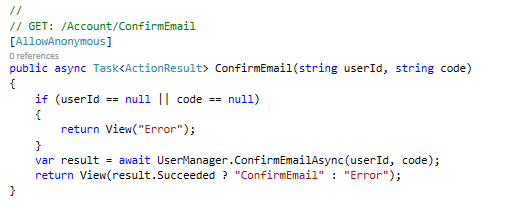


Slika 7 - korisnik u bazi

Kao što vidimo korisnik je pohranjen, ima određene zastavice, poput da li se radi o provjeri vjerodostojnosti od dva koraka ili ne, da li je račun potvrđen, … ali nam je najvažnije uočiti PasswordHash polje koje predstavlja sažetak lozinke. Nikada se ne smije spremati, slati ili bilo što raditi s lozinkom u čistom tekstu. Ona se unosi samo u polje lozinka i nakon toga se sve dalje radi s sažetkom vrijednosti lozinke. Naravno, mora se koristiti dobra funkcija sažimanja jer inače nema smisla.

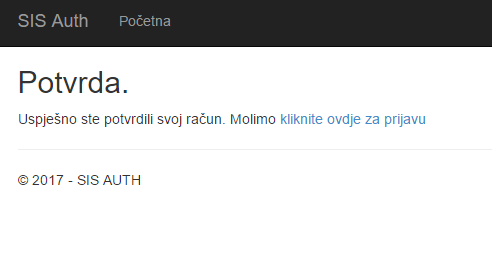


Slika 8 - email za potvrdu

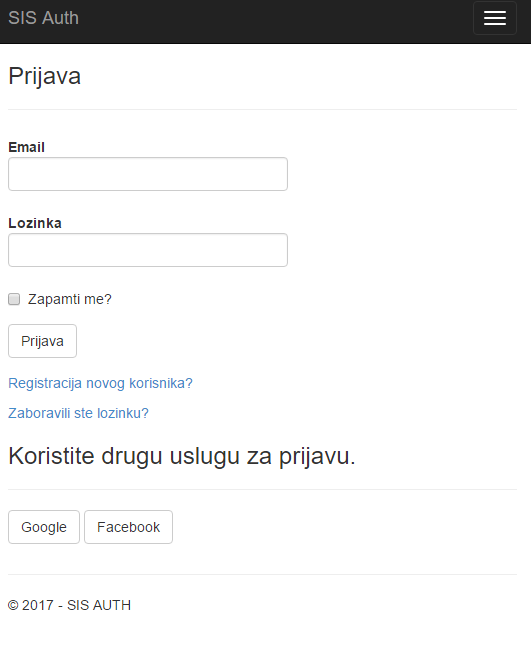


Slika 9 - akcija potvrde

Tu ukoliko sve prođe dobro, tj. ako su ispravni i poveznica nije istekla vodi nas na dolje prikazani ekran.

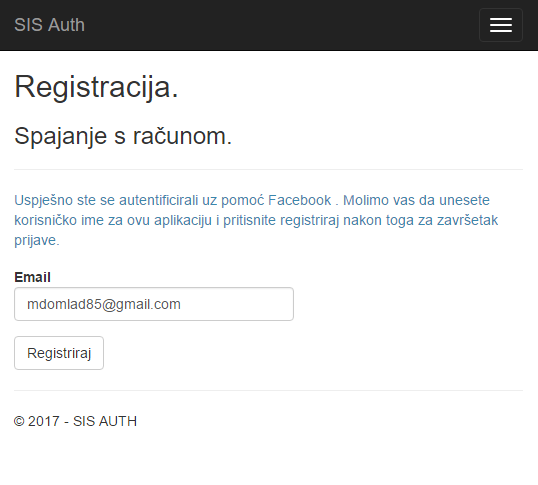


Slika 10 - potvrda



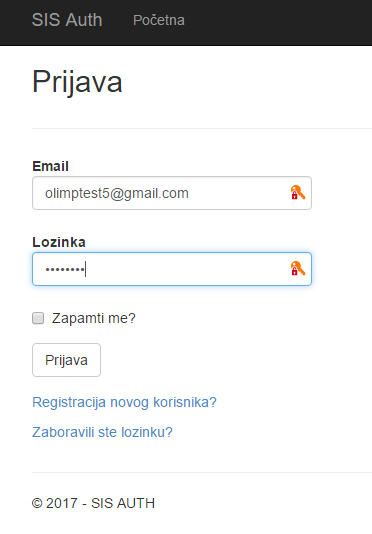
Slika 11 - Prijava

Osim navedenog načina moguće se i registrirati putem vanjskih servisa. U tom slučaju idemo na prijava i na tom ekranu ukoliko imamo registrirane vanjske servise postojati će odabir istih. Ako se registracija izvrši na taj način onda ćemo morati spojiti računom s email-om tj. imati ćemo dodatan korak kao na sljedećoj slici. U tom slučaju ne treba potvrditi račun kao u normalnoj registraciji. To je iz razloga što koristimo servise treće strane kojima **vjerujemo** (to je ključno kod CA isto tako) i na taj način vjerujemo da su potrebne provjere prošli. U tom slučaju nemamo postavljenu lozinku i istu možemo postaviti u upravljanju korisničkim računom što je kasnije detaljno objašnjeno.



Slika 12 - Spajanje računa

# Prijava

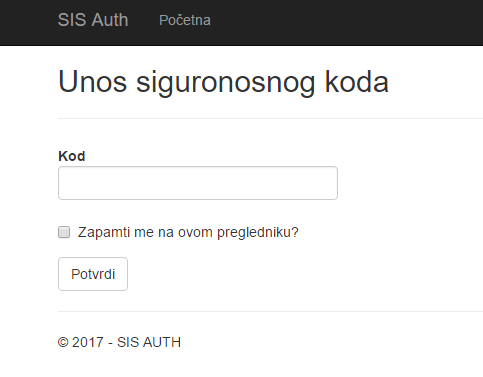


Slika 13 - Forma za prijavu



Slika 14 - POST akcija prijave

Kako koristimo provjeru vjerodostojnosti u dva koraka, nakon prijave prebacuje se na ekran gdje nas traži odabir pružatelja vjerodostojnosti drugog koraka ( u našem slučaju je email, ali može biti bilo koji – npr. Tekstualna poruka). Zapamti me ovdje pamti samo login detalje, drugi dio je poseban.



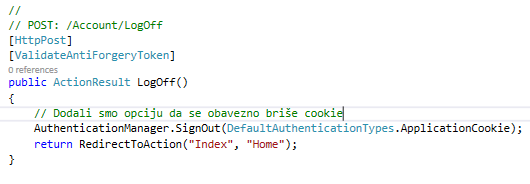
Slika 15- Unos siguronosnog koda

Ako odaberemo zapamti me na ovom pregledniku na tom računalu i pregledniku više neće biti drugog koraka provjere vjerodostojnosti. Tako da najbolja kombinacija je odabrana provjera od dva koraka i na računalima kojima vjerujemo jednostavno odaberemo ovu opciju i tako smo se daleko više osigurali od otuđivanja lozinke na nepouzdanim računalima (ukoliko se negdje drugdje logiramo, npr. na sveučilištu).



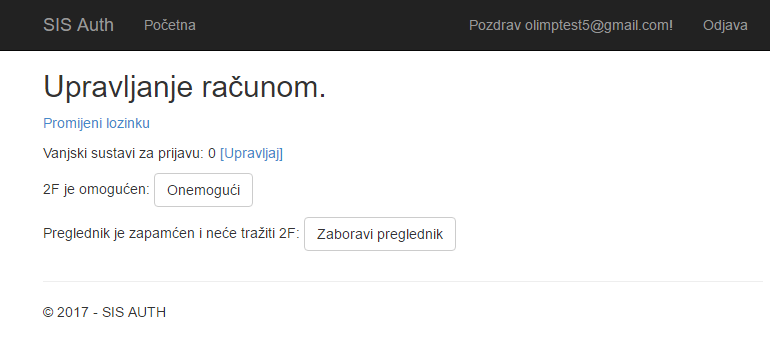
Slika 16 - Email sa kodom za potvrdu

Nakon toga idemo na početnu stranica koja nije središte događanja tako da je nećemo ni prikazivati, ionako je rudimentarna. Ali sada nam se promijenila navigacijska traka i sada vidimo poveznice korisničko ime i odjavu, umjesto prijave i registracije. Dok kliknemo odjavu odjaviti ćemo se iz računa. Jako je važno pozvati metodu i dodati opciju da se obriše kolačić jer inače nemamo dobru sigurnost ako ne obrišemo kolačić. Netko bi ga mogao dohvatiti i ako nismo ulogirani.

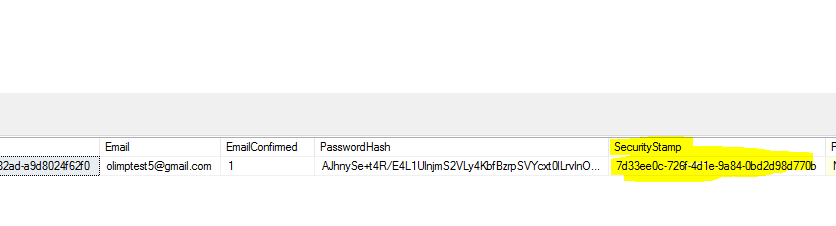


Slika 17 - Odjava

Ako kliknemo na drugu poveznicu, tj. na korisničko ime idemo na upravljanje korisničkim računom kako je pokazano na slici ispod.

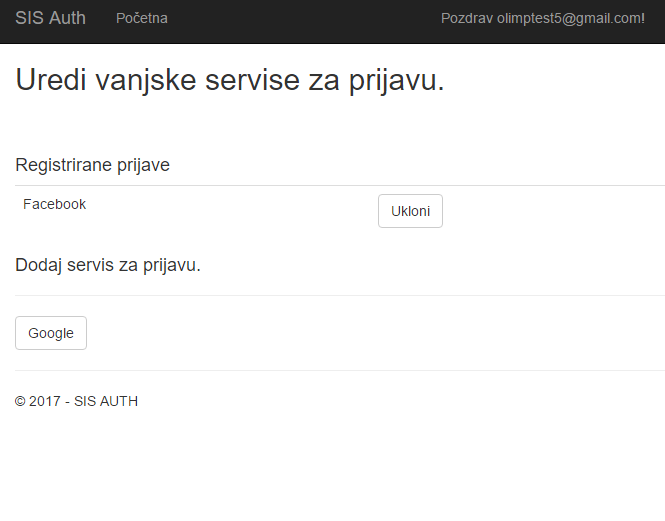


Slika 18 - Upravljanje računom

Promjena lozinke je klasična priča što se tiče dizajna i forme. Mora se unijeti stara i nova te potvrda nove. Logika ispod je isto takva da usporedi sažetak trenutne lozinke i usporedi s onim u bazi i ako se podudaraju onda doda sažetak nove vrijednosti. Sada nam je bitan SecurityStamp da možemo i dalje biti sigurni u ispravnost prijavljenog korisnika. 

Slika 19 - Siguronosni token

Vanjski sustavi za prijavu mogu biti razni. Trenutno je implementiran facebook i google.



Slika 20 - Vanjski servisi za prijavu

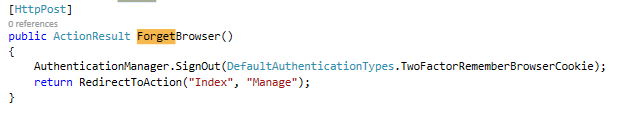


Slika 21 - Kod za prijavu na vanjski servis

Za prijavu na vanjski servis šaljemo upit sa parametrom u kojem se nalazi odabrani pružatelj. I onda preusmjeravamo na login kod pružatelja sa korisnikovim identifikatorom i poveznice na koju će se vratiti odgovor s vanjskog servisa.

Sljedeći je omogućavanje/onemogućavanje drugog koraka provjere vjerodostojnosti koja je detaljno objašnjena ranije.

Na kraju imamo zapamti/zaboravi preglednik. Zapamti smo isto tako detaljno objasnili ranije, a zaboravi preglednik poništava radnju.



Slika 22 - Metoda zaboravi preglednik

Ovdje je promjena za razliku od odjave u tome što brišemo drugačiji kolačić, a sve ostalo je isto.

# Popis slika

[Slika 1 - Datoteka s postavkama 4](#_Toc472163886)

[Slika 2 - definiranje pravila 5](#_Toc472163887)

[Slika 3 - forma za registraciju 6](#_Toc472163888)

[Slika 4 - Razor pogled forme 6](#_Toc472163889)

[Slika 5 - GET i POST akcija registracije 7](#_Toc472163890)

[Slika 6 - nakon unosa podataka registracije 7](#_Toc472163891)

[Slika 7 - korisnik u bazi 7](#_Toc472163892)

[Slika 8 - email za potvrdu 8](#_Toc472163893)

[Slika 9 - akcija potvrde 8](#_Toc472163894)

[Slika 10 - potvrda 8](#_Toc472163895)

[Slika 11 - Prijava 9](#_Toc472163896)

[Slika 12 - Spajanje računa 10](#_Toc472163897)

[Slika 13 - Forma za prijavu 11](#_Toc472163898)

[Slika 14 - POST akcija prijave 11](#_Toc472163899)

[Slika 15- Unos siguronosnog koda 12](#_Toc472163900)

[Slika 16 - Email sa kodom za potvrdu 12](#_Toc472163901)

[Slika 17 - Odjava 13](#_Toc472163902)

[Slika 18 - Upravljanje računom 13](#_Toc472163903)

[Slika 19 - Siguronosni token 13](#_Toc472163904)

[Slika 20 - Vanjski servisi za prijavu 14](#_Toc472163905)

[Slika 21 - Kod za prijavu na vanjski servis 14](#_Toc472163906)

[Slika 22 - Metoda zaboravi preglednik 15](#_Toc472163907)

1. IS – skraćenica koja označava Informacijski sustav [↑](#footnote-ref-1)