Slovenská technická univerzita v Bratislave

Fakulta informatiky a informačných technológií

Ilkovičova 2, 842 16 Bratislava 4



**Technická Dokumentácia**

*Tímový projekt*

Tím č. 19

**Vypracoval:** Jakub Perdek **Vedúci projektu:** Ing. Pavol Helebrandt Phd.

**Obsah**

[1 Technická dokumentácia 2](#_Toc58316133)

[1.1 Whois aplikácia pre vyhľadanie domény 2](#_Toc58316134)

[Vyhľadanie domény 3](#_Toc58316135)

[Informácie o vyhľadanej doméne 3](#_Toc58316136)

[Zhodnotenie k whois aplikácii 6](#_Toc58316137)

[1.2 Cieľová stránka e-shopu 7](#_Toc58316138)

[Používateľské rozhranie a dizajn stránky 7](#_Toc58316139)

[Domovská stránka 7](#_Toc58316140)

[Prihlásenie a registrácia 8](#_Toc58316141)

[Nákupný košík 9](#_Toc58316142)

[Informácie o doručení 10](#_Toc58316143)

[Informácie o platbe 11](#_Toc58316144)

[Server a riadiaca časť systému 15](#_Toc58316145)

[Databáza 16](#_Toc58316146)

[Databázový model 17](#_Toc58316147)

[1.3 Scenáre s použitím e-shopu 19](#_Toc58316148)

[Prelamovanie slabých hesiel – slovníkový útok 19](#_Toc58316149)

[Ukradnutie produktu odoslaním falošnej informácie 19](#_Toc58316150)

[Ukradnutie produktu prístupom do priečinka 19](#_Toc58316151)

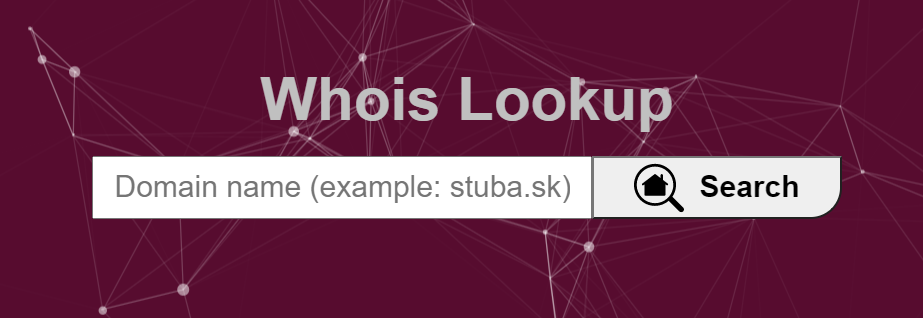
[SQL injekcia pre zmenu emailovej adresy admina 19](#_Toc58316152)

Technická dokumentácia

K aplikáciám bola vytvorená ich technická dokumentácia. Uvádzame tu dokumentáciu k backendu a frontendu eshopu. Zdokumentovaná je aj Whois aplikácia. V dokumentácii uvádzame používateľské rozhrania, použité služby a funkcionalitu konkrétnej aplikácie.

Whois aplikácia pre vyhľadanie domény

Aplikácia slúži na vyhľadávanie informácií v databáze o konkrétnej doméne. Databáza je získaná z internetu a bude doplnená o ďalšie domény zahrnuté v scenároch. Dodatočne k informáciám o konkrétnej doméne môžu byť pridané aj potencionálne hrozby. Reprezentuje nástroj, na základe ktorého môže používateľ vyhľadať informácie o nájdených hrozbách a použiť ich pre potencionálny útok alebo obranu konkrétnej aplikácie. Zároveň sa predpokladá, že získa zručnosti pri práci s takýmto nástrojom. Navrhnutý dizajn má približovať meniacu sa sieť internetových prepojení.



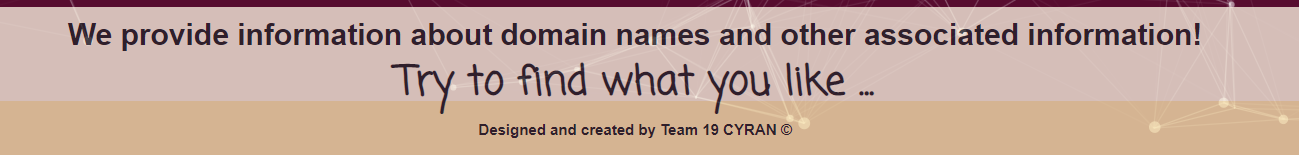
Obrázok 1: Okno vyhľadávača



Obrázok 2: Navigácia vyhľadávača

Vyhľadanie domény

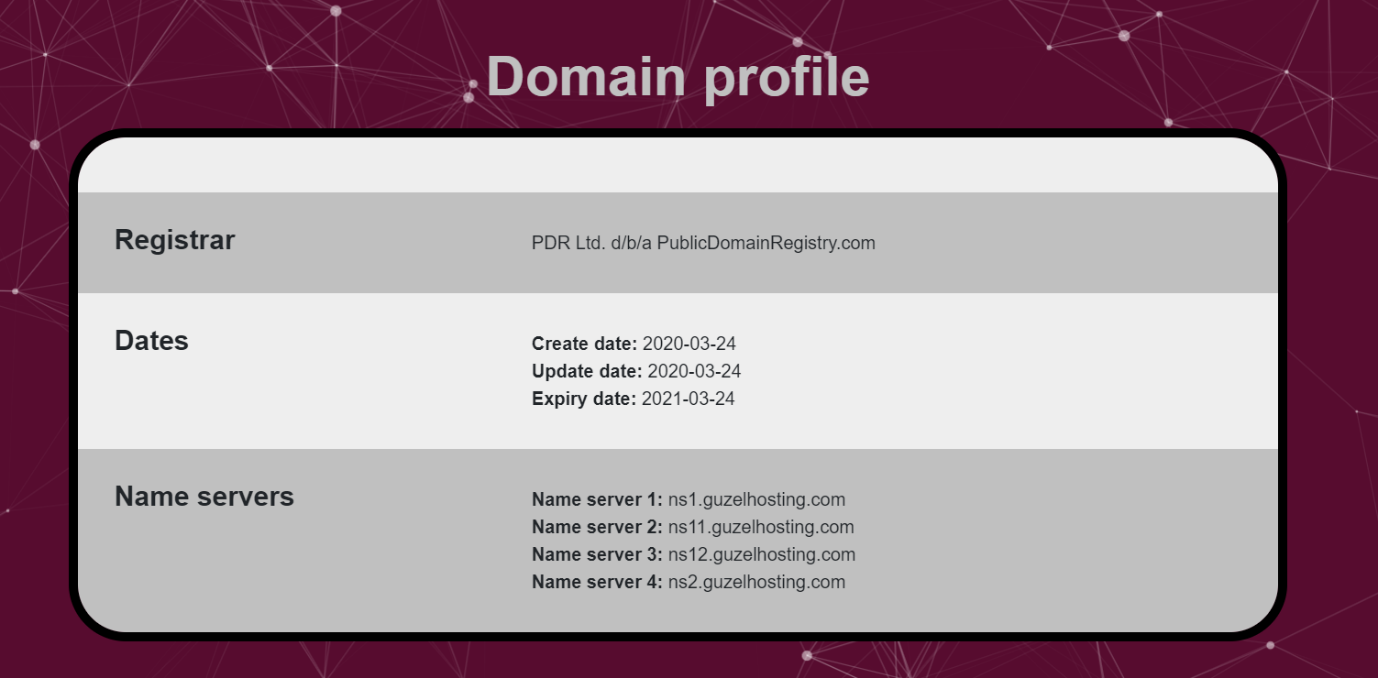
Používateľ po načítaní stránky vloží názov domény do okna v strede obrazovky a stlačí tlačidlo Search. Formulár je zobrazený na Obrázku 1. Reťazec je hľadaný v uprostred doménových mien. Výsledok môže obsahovať tento reťazec kdekoľvek v názve domény. Vrátený je len jeden výsledok, preto by dopyt mal byť čo najpresnejší. Hlavnú stránku tvorí lista v hlavičke obsahujúce logo vľavo a menu tlačidlá na vpravo. Lišta je zobrazená na Obrázku 2. Päta stránky informuje o možnostiach tohto webu. Na jej samom spodku sa nachádzajú informácie o tvorcoch stránky. Päta je zobrazená na Obrázku 3.



Obrázok 3: Päta vyhľadávača

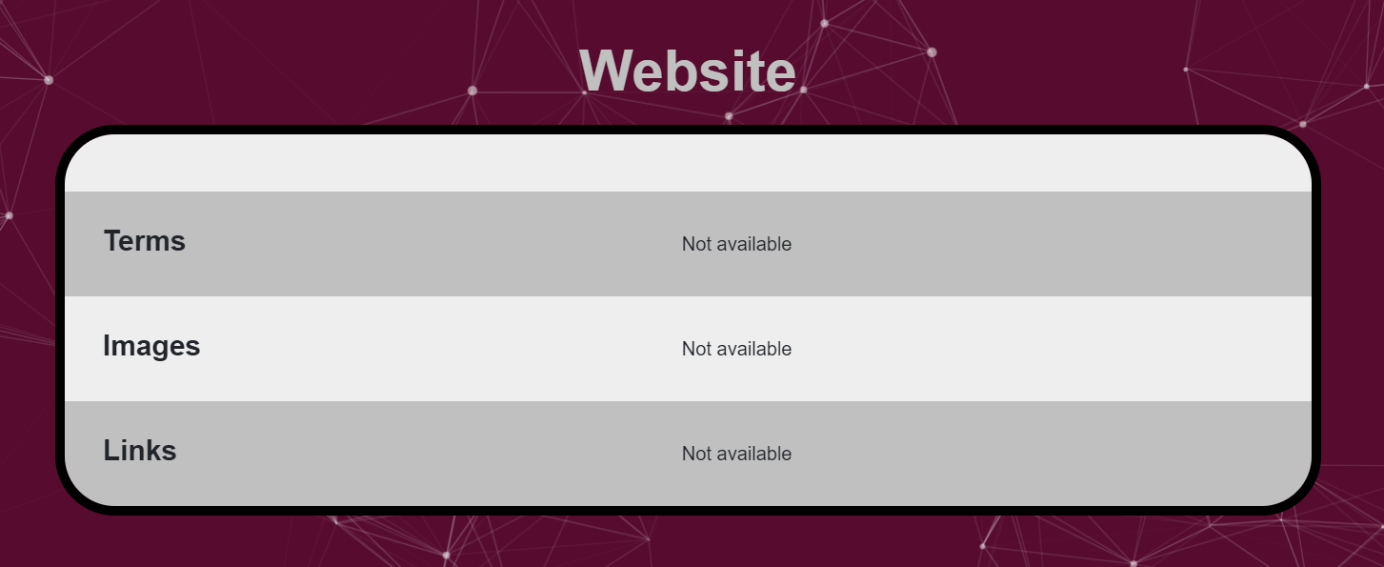
Informácie o vyhľadanej doméne

Pokiaľ bolo vyhľadanie úspešné zobrazia sa dostupné informácie o konkrétnej doméne. Zahŕňajú informácie o registračnej doméne, dátumoch vzniku, úpravy a doby platnosti. V základnom popise sú uvedené aj menné servery. Doménový profil je zobrazený na Obrázku 4.



Obrázok 4: Profil domény

Základné zozbierané informácie o stránke je možné uviesť a neskôr získať z časti pre informácie o stránke. Tvorí ju základná štatistika o výskyte termov, obrázkov a odkazov na stránke. V našom riešení tieto informácie neuvádzame ani nezbierame, ale v budúcnosti môže byť riešenie rozšírené o preliezač webu, ktorý získa tieto informácie. Táto časť je zobrazená na Obrázku 5.

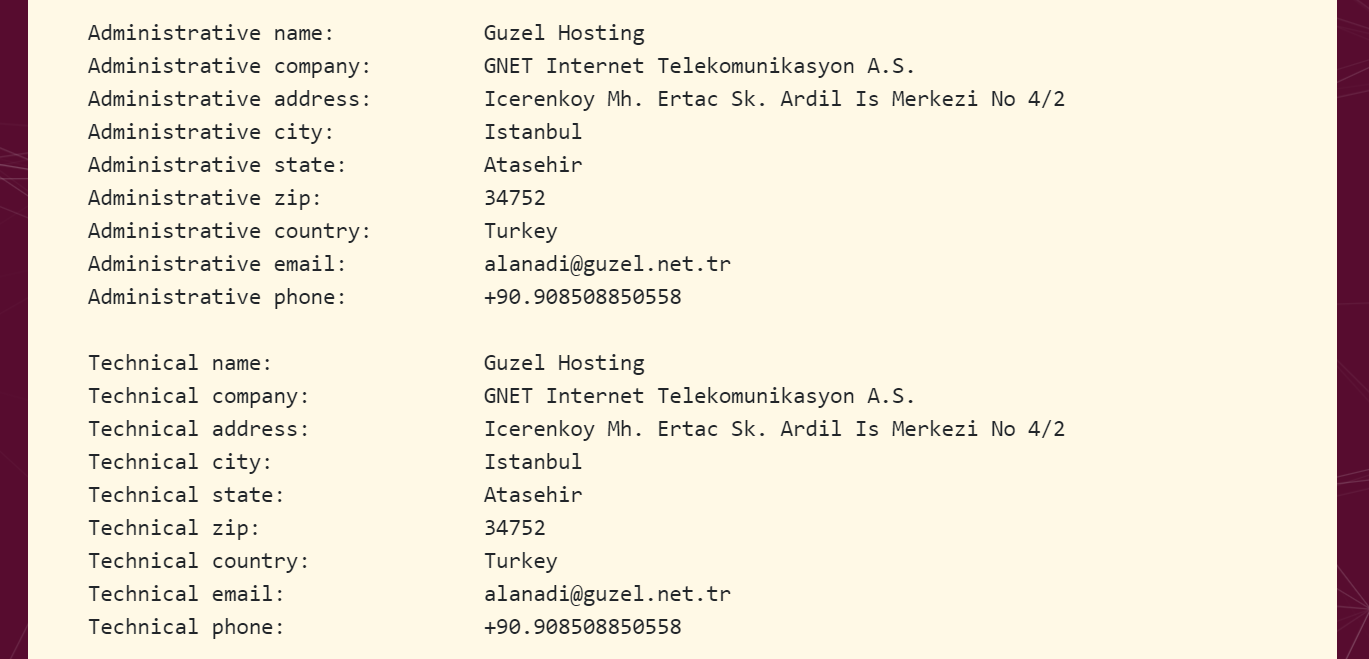


Obrázok 5: Informácie o stránke

Podrobnejšie informácie sme vložili do samostatného okna. Zobrazujeme tu všetky dostupné informácie z databázy pre konkrétnu doménu. Obsahom sú mailové adresy, telefónne čísla, adresy a ďalšie informácie o administratíve, platbách, prípadne o technickom stave pokiaľ sú k dispozícii. Pokiaľ niektorá informácia nebola nájdená alebo chýba v databáze, potom sa vo výslednom výpise nezobrazí. Ukážky výpisu pre doménu cukurovabims.com sú zobrazené na Obrázkoch 6 až 8.



Obrázok 6: Podrobnejšie informácie

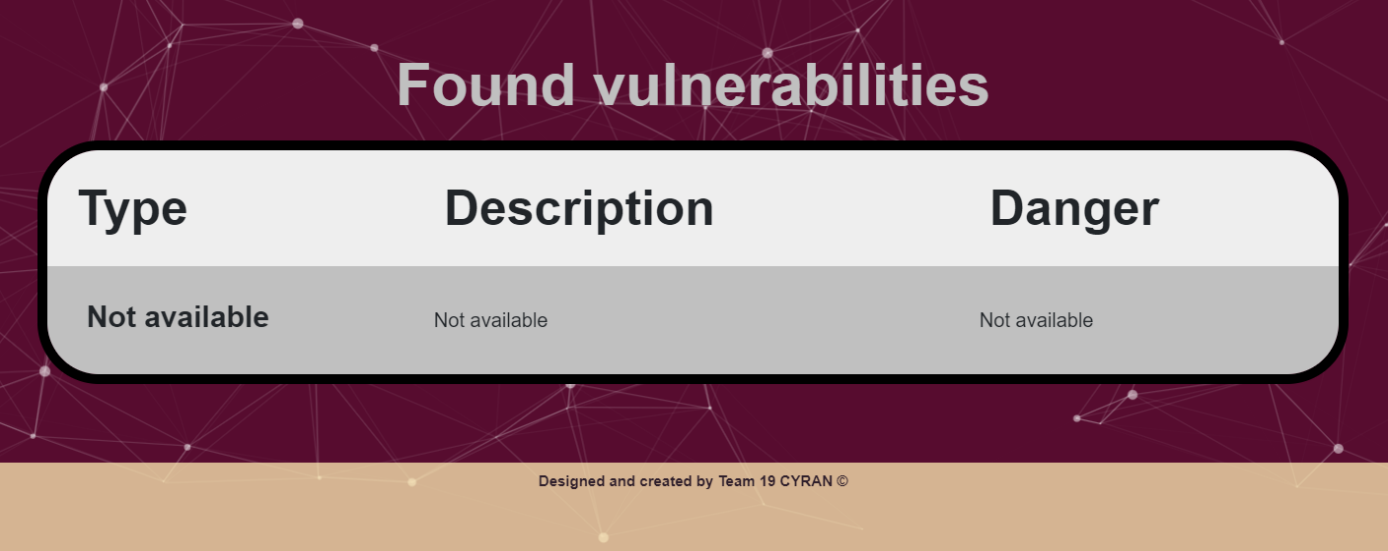


Obrázok 7: Podrobnejšie informácie pokračovanie 1



Obrázok 8: Podrobnejšie informácie pokračovanie 2

Podstatným informačným obsahom pre penetračného testera alebo útočníka sú informácie o zraniteľnostiach. Vytvorili sme pre ne samostatnú tabuľku. V prípade scenára je možné poskytnúť používateľovi informáciu o zraniteľnostiach domény, na základe čoho by mal byť schopný dohľadať doplňujúce informácie a urobiť vhodnú akciu. Databáza whois ale informácie o zraniteľnostiach neobsahuje.



Obrázok 9: Nájdené hrozby

Zhodnotenie k whois aplikácii

Vyhľadanie a zber informácií je podstatnou časťou penetračného testovania. Vytvorili sme preto aplikáciu pre vyhľadanie informácií o konkrétnej doméne. V rámci bezpečnostných scenárov by do databázy ktorú aplikácia využíva mali byť pridané informácie o doménach bežiacich v sandboxe, respektíve o webových objektoch bezpečnostných scenárov. Predpokladáme, že bežne dostupné whois servery tieto informácie nebudú mať, a to hlavne z dôvodu dostupnosti nami pridaných webových lokalít. Pridanie vlastných zraniteľností do informácií o doméne by malo vylepšiť hrateľnosť scenárov a podnietiť používateľa vyhľadať si informácie o nich. Rovnako pri vypnutí niektorých zraniteľností je zhotovené riešenie flexibilné, keďže je potrebné len zmeniť hodnotu uloženú v databáze.

Cieľová stránka e-shopu

Tento dokument popisuje základné komponenty webovej stránky, ktoré budú súčasťou scenára. Táto webová stránka bude cieľom kybernetických útokov.

Webová stránka elektronického obchodu je navrhnutá ako klasický webový obchod, kde má používateľ môže:

* prihlásiť sa
* registrovať sa
* vyhľadať produkty
* pridať produkty do košíka
* vybrať dodávateľa a miesto dodania
* vybrať spôsob platby
* zaplatiť online

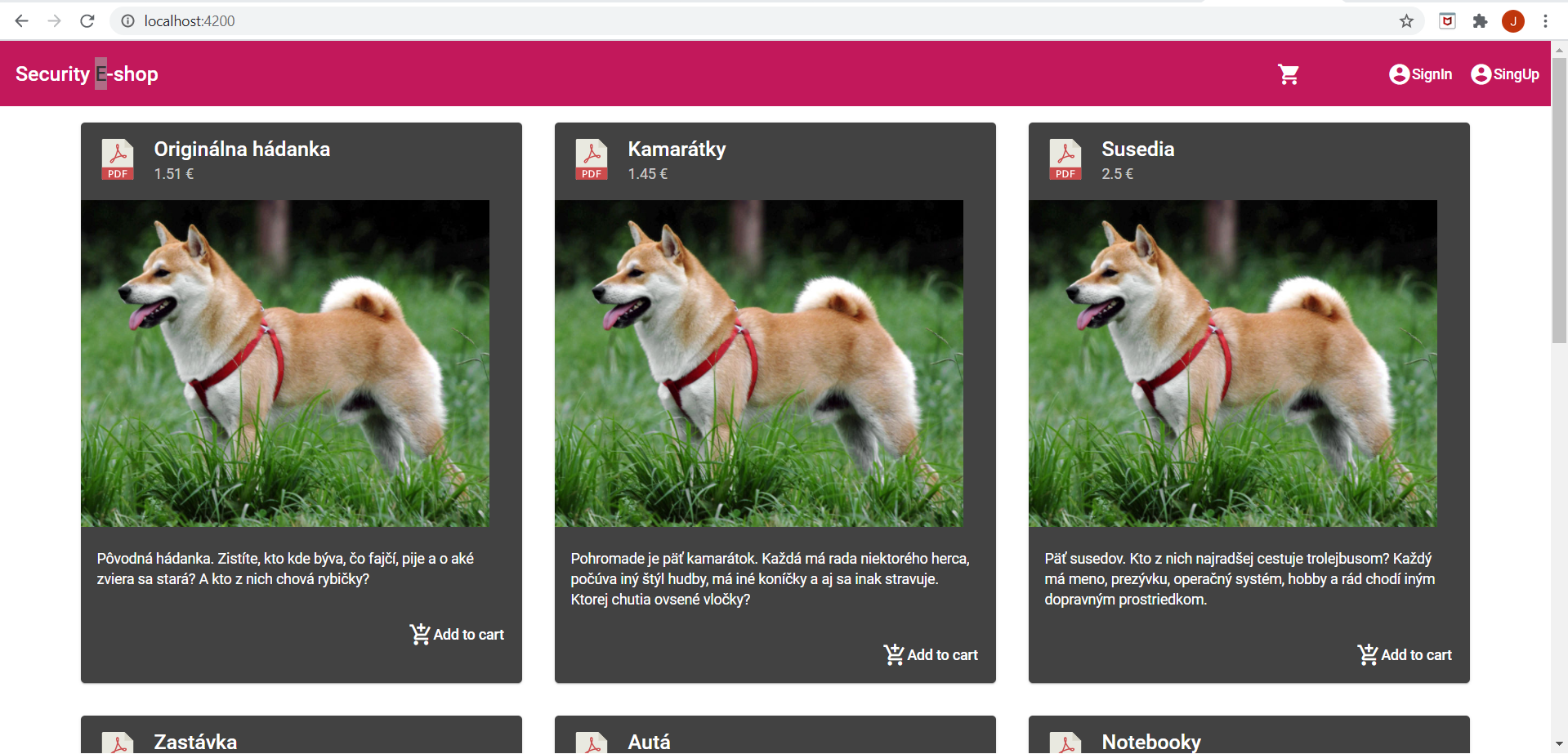
Stránka je koncipovaná ako fiktívny cieľ s cieľom využiť jej nedostatky a uskutočniť rôzne typy kybernetických útokov. Lokalita ako celok bude veľmi dynamická, aby sa v neskorších scenároch mohla technológia webu prispôsobiť povahe útoku, napríklad zmenám v databáze alebo funkčnosti alebo backendu samotnému.

Používateľské rozhranie a dizajn stránky

Ako technológia pre frontend bol použitý Angulár. Webové sídlo sa skladá z 3 hlavných stránok. Prvou stránkou je domovská stránka, ktorá je hlavnou prezentáciou webu elektronického obchodu.

Domovská stránka

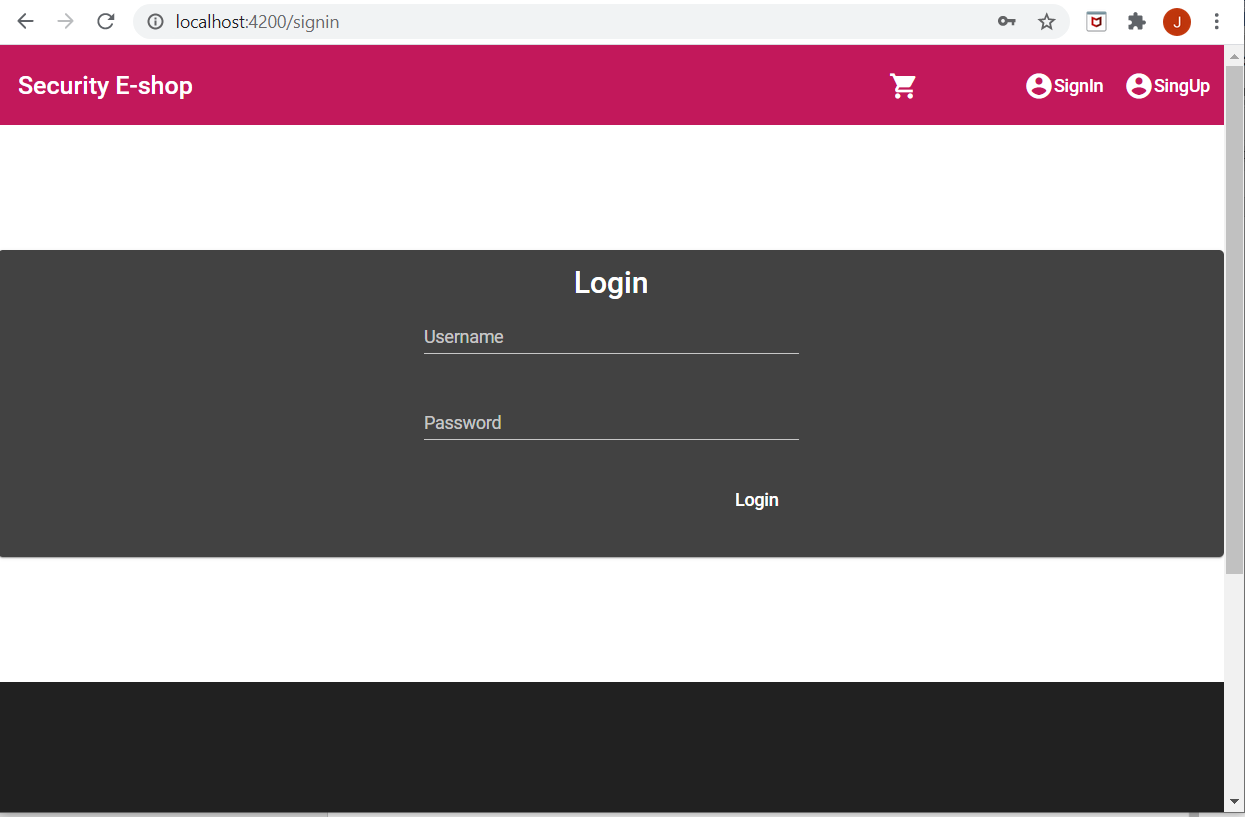
V zobrazení domovskej stránky môže používateľ prehľadávať produkty bez predchádzajúceho prihlásenia alebo registrácie. Odtiaľ si môže zvoliť, či prejde registráciou / prihlásením, alebo podrobnejším vyhľadávaním produktu.



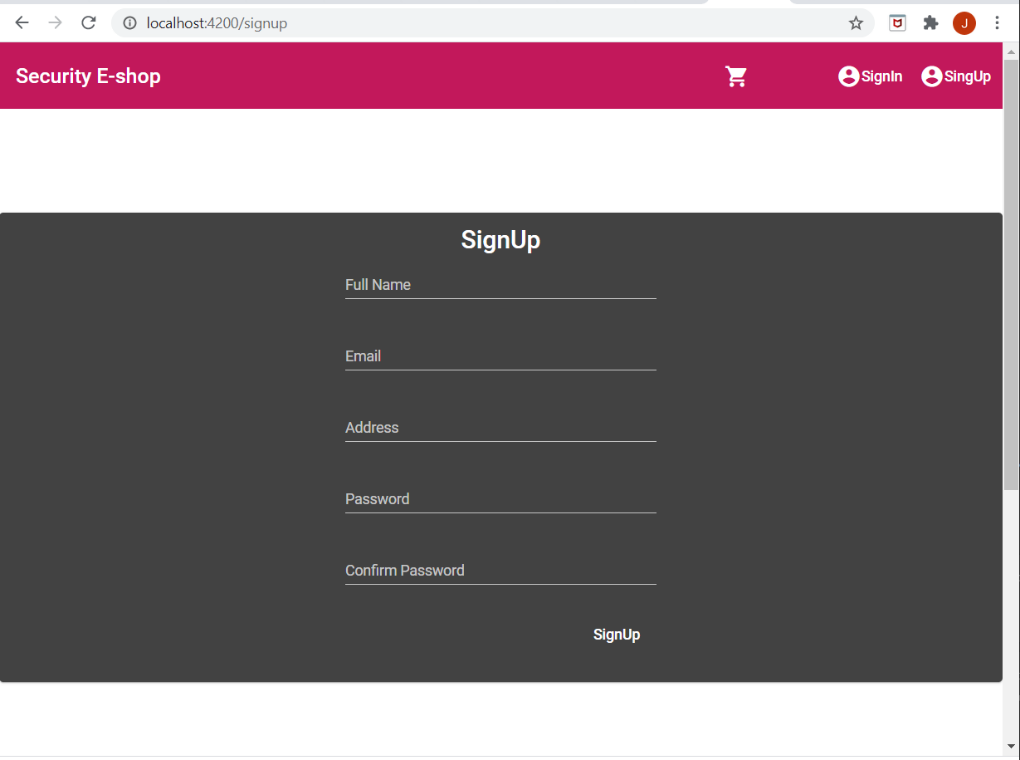
Obrázok 10 Zobrazenie domovskej stránky

Prihlásenie a registrácia

Z domovskej stránky sa môže používateľ prejsť na stránku s prihlasovaním alebo registráciou.



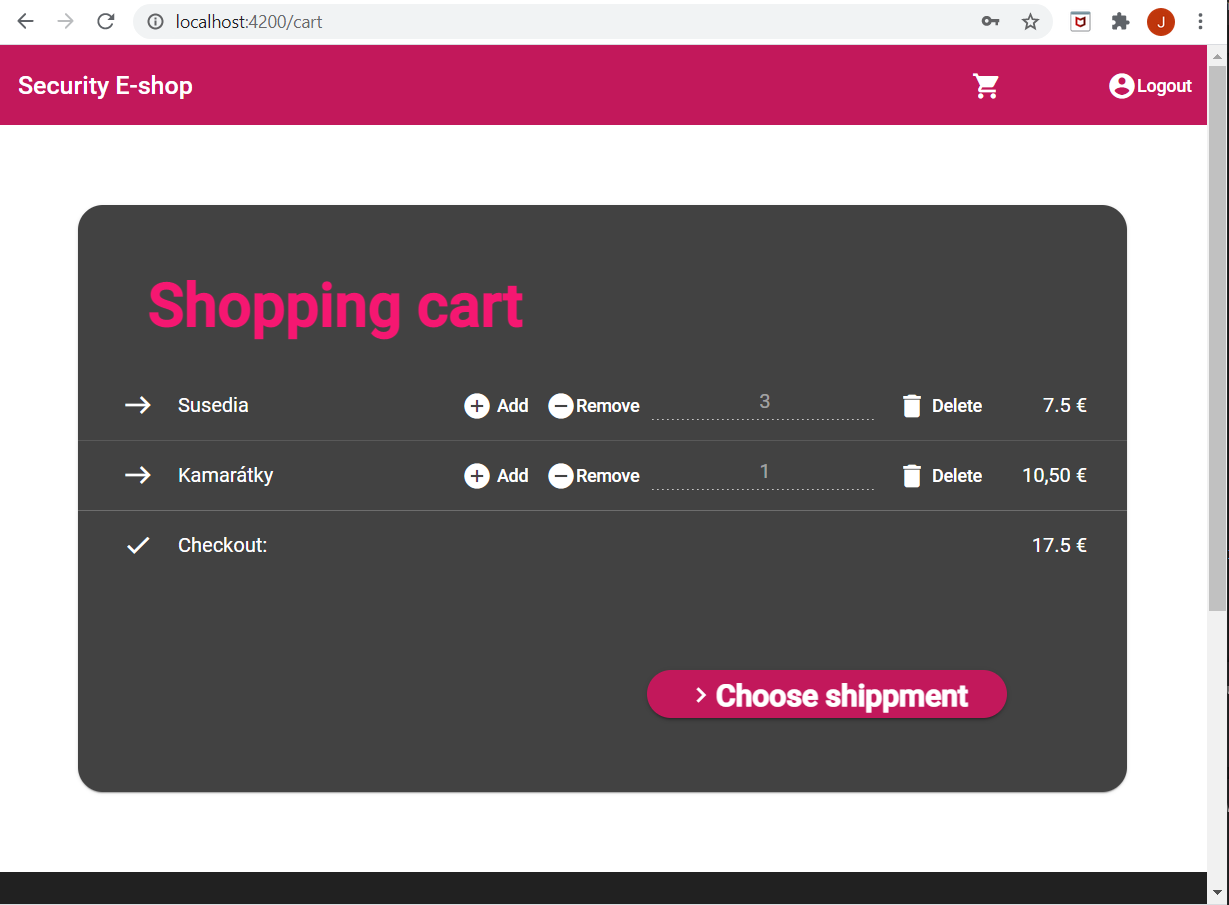
Obrázok 11: Formulár na prihlásenie



Obrázok 12 Formulár na registráciu

Nákupný košík

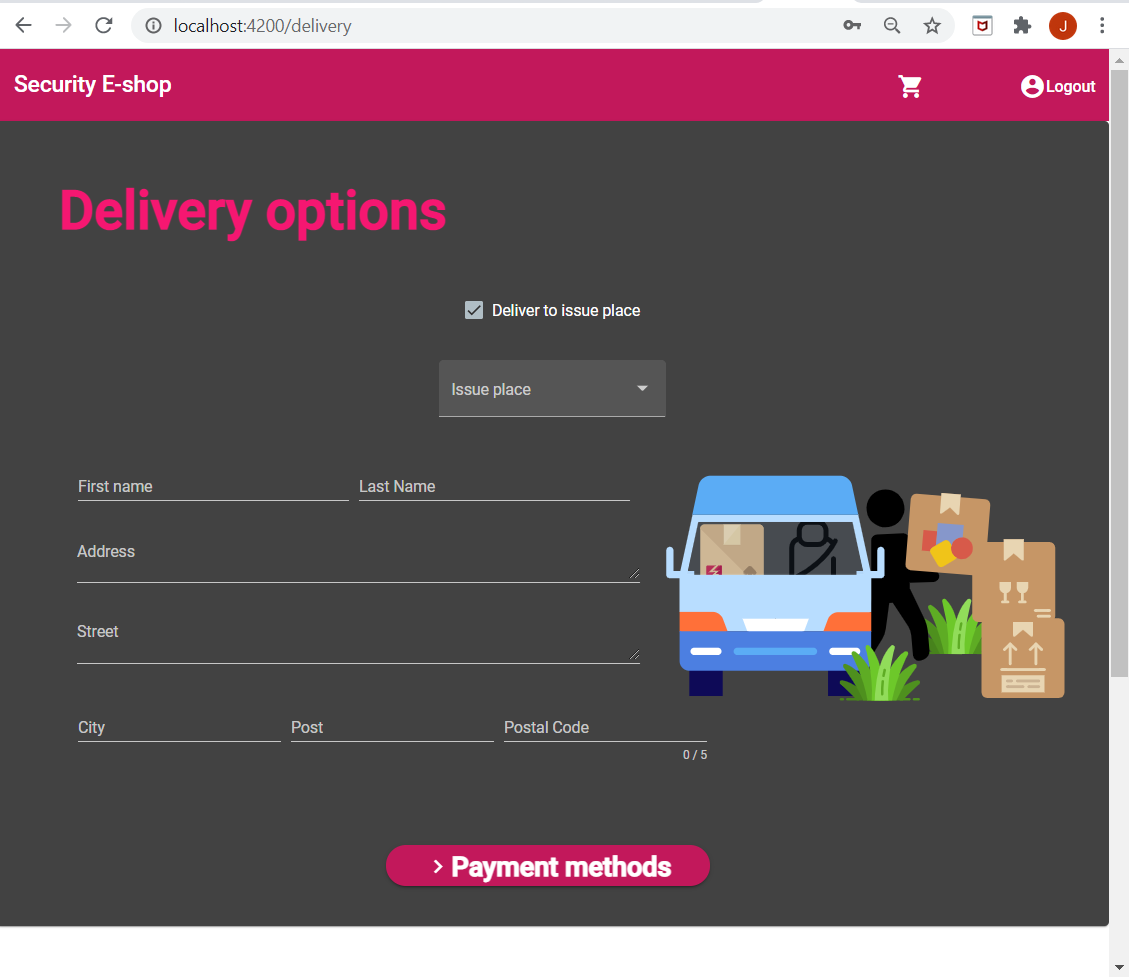
Zobrazenie nákupu začína presmerovaním na zobrazenie nákupného košíka. Tu si používateľ vyberie požadované množstvo vybraných produktov, a prechádza na výber spôsobu doručenia.



Obrázok 13 Zobrazenie nákupného košíka

Informácie o doručení

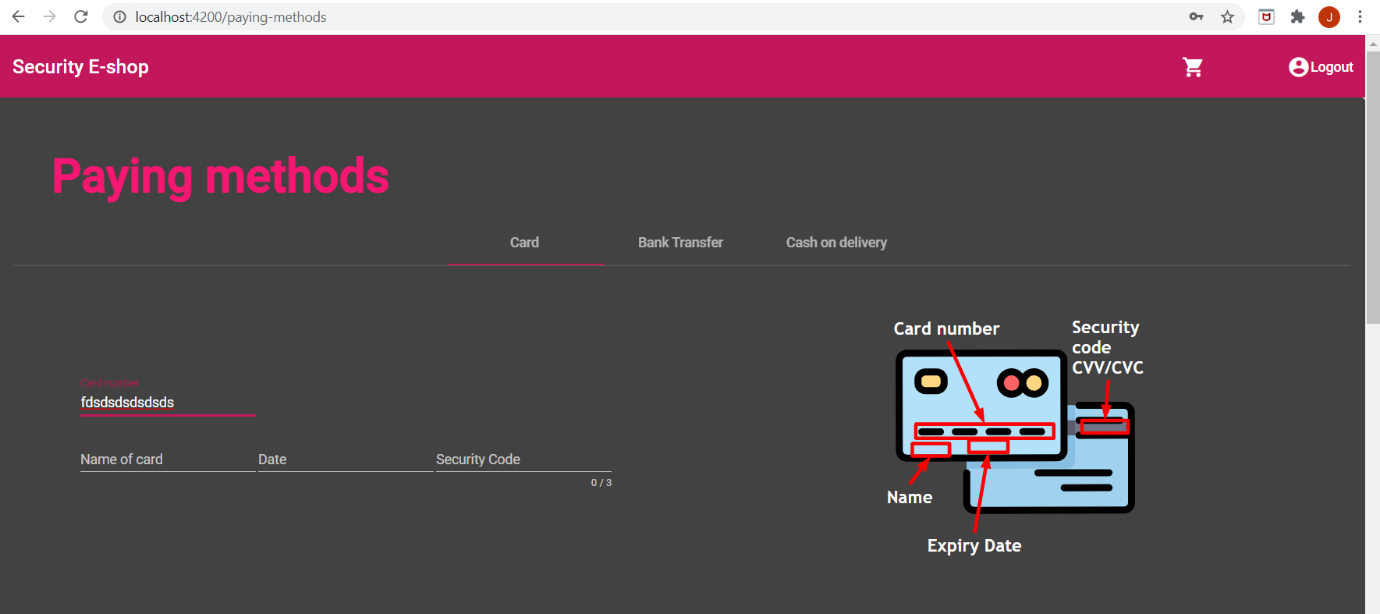
Do formuláru na Obrázku 5 používateľ vloží informácií o príjemcovi objednávky.



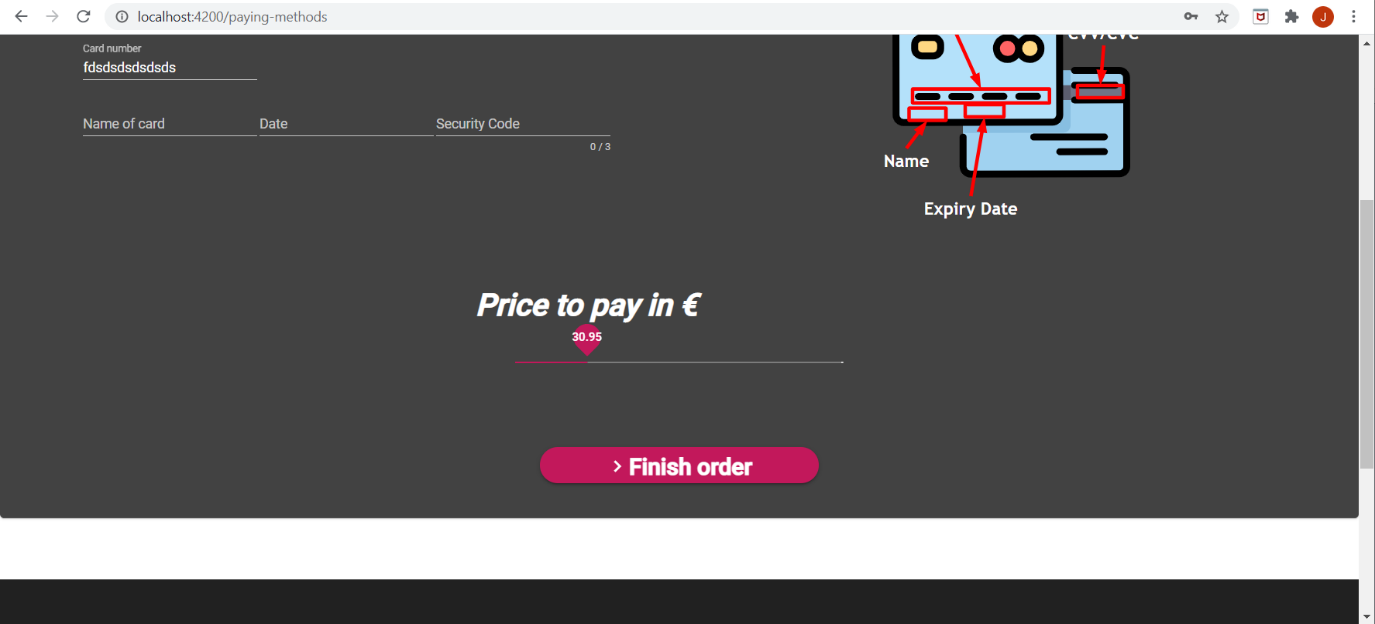
Obrázok 14: Formulár na zadanie informácií o príjemcovi objednávky

Informácie o platbe

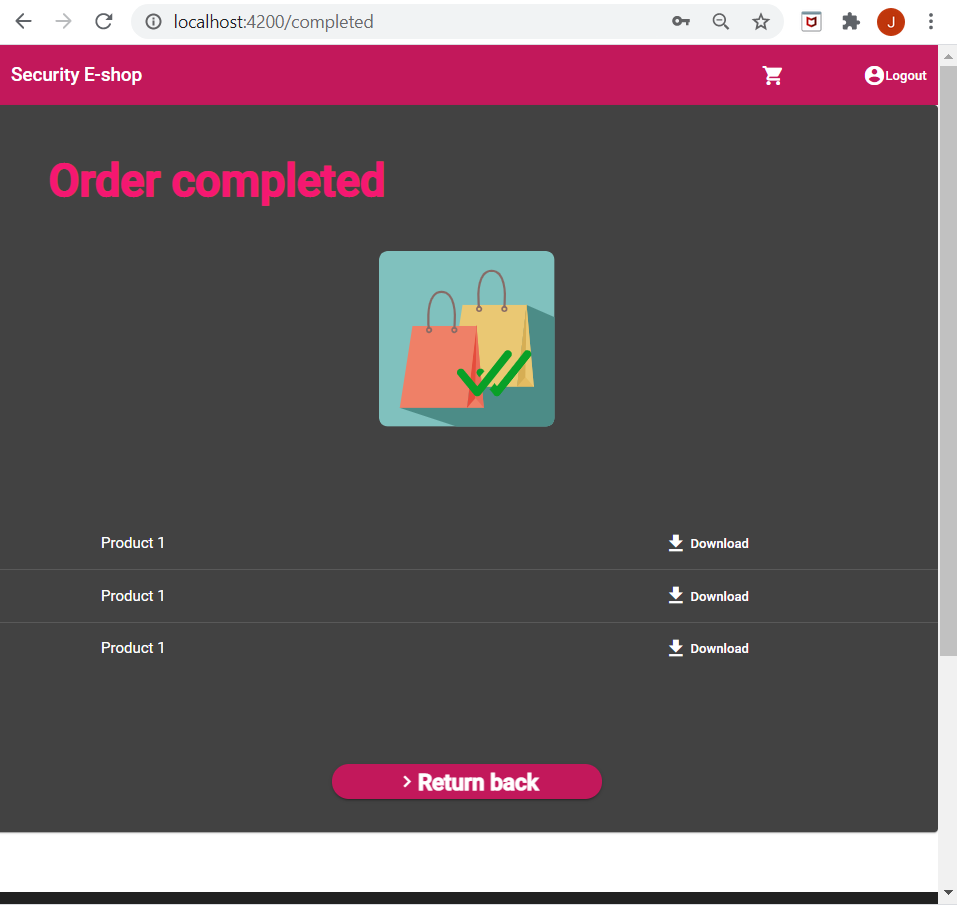
Proces elektronického nákupu končí výberom spôsobu platby a zadaním platobných údajov. Môže si vybrať medzi platbou kartou online, bankovým prevodom alebo poslaním na dobierku. Pri platbe kartou online sa používateľovi zobrazí formulár pre zadanie informácií o platobnej karte Následne klikne na tlačidlo pre dokončenie objednávky, a zobrazí sa mu správa o úspešnej alebo neúspešnej transakcii.



Obrázok 15 Formulár na zadanie informácií o platbe



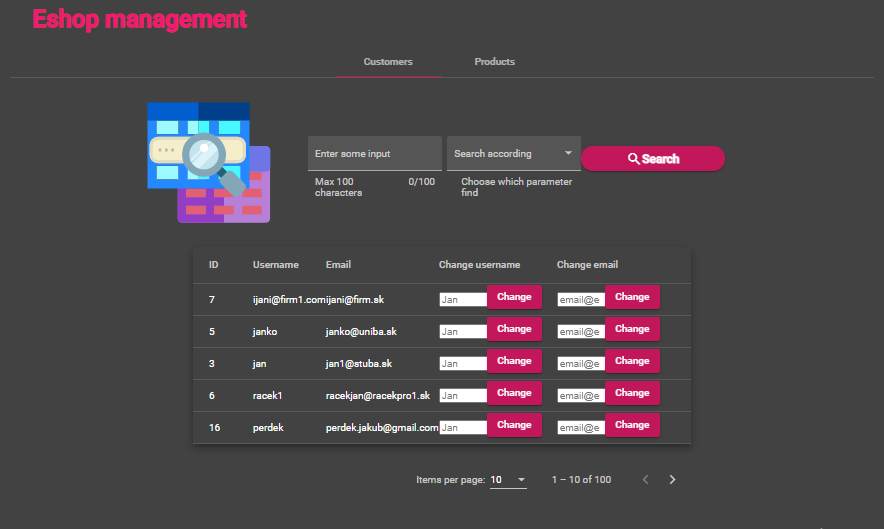
Obrázok 16: Možnosť podporiť e-shop



Obrázok 17: Možnosť stiahnuť zakúpený tovar

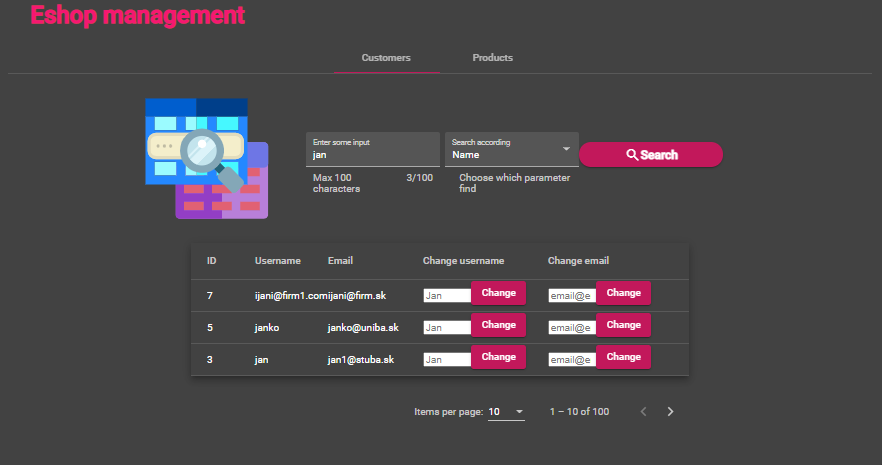
**Správa používateľov a produktov**

Používateľ s oprávneniami pracovníka obchodu bude mať oprávnenie nad ostatnými používateľmi a produktmi. V tomto rozhraní má možnosti upravovať zákaznícke účty. Vyhľadávať môže podľa dvoch atribútov: meno a e-mail. Po kliknutí na tlačidlo Search (hľadať) budú vygenerovaní všetci používatelia, ktorí vyhovujú dopytu.



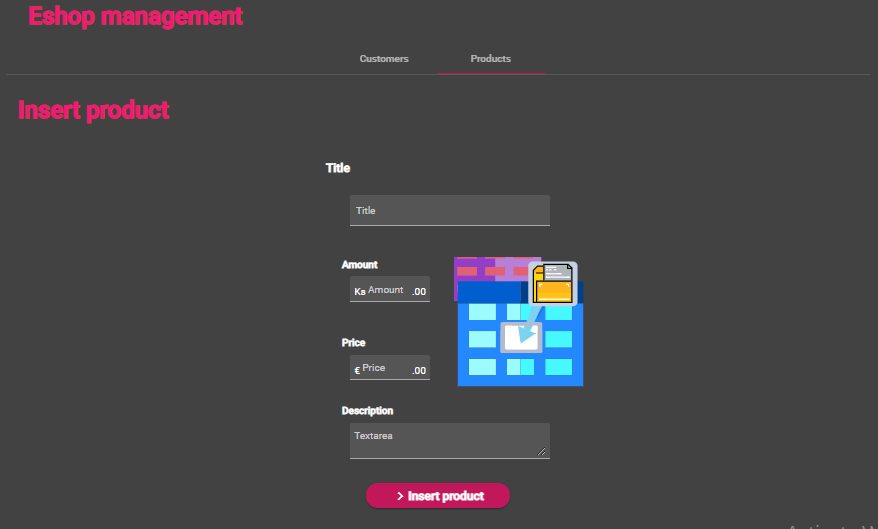
Obrázok 18: Správa používateľov

V ďalších krokoch môže správca zmeniť ich mená alebo e-mailové adresy. Kliknutím na tlačidlo Change (zmeniť) vykonáte a potvrdíte, že sa vykonáva.



Obrázok 19: Vyhľadávanie používateľa

Podľa rozhrania na obrázku 20 môže používateľ s vyššími oprávneniami pridávať nové produkty do databázy obchodu. Po zadaní všetkých informácií o produkte klikne na tlačidlo Insert product (vložiť produkt). Nový produkt bude pridaný do databázy obchodov.



Obrázok 20: Správa produktov

Server a riadiaca časť systému

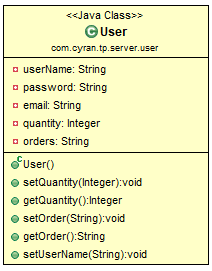
Pre riadiacu časť systému bol zvolený programovací jazyk Java, pričom nad ním je využívaný rámec Spring. Závislosti FireStore sa priamo pridávajú do projektu pomocou správcu závislostí Maven.

Na ďalšom diagrame tried môžeme vidieť hlavné triedy, z ktorých každá predstavuje jednu zo základných entít databázy.

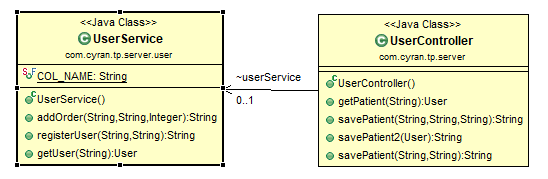
Timeline

Description automatically generated

Obrázok 21 Diagram základných tried



Obrázok 22 Trieda User entity



Obrázok 23 Diagram tried obsluhujúcich User entitu

Metódy na diagrame triedy sú pomerne priame a popisujú funkcie slúžiace entite Používateľa. V tomto okamihu poskytuje back-end funkčnosť registrácie a prihlásenia, ako aj objednávania produktov.

Databáza

Ako prvú možnosť implementácie databázy, webový obchod používa flexibilnú databázu NoSql od spoločnosti Google, FireStore. Firestore je optimalizovaný na ukladanie veľkých zbierok malých dokumentov. FireStore je ľahko škálovateľná cloudová databáza založená na dokumentoch.

Databázový model

Štruktúru databázy tvoria 3 primárne modely:

* model používateľa ( Users )
* model produktu ( Products )
* model objednávky ( Orders )

**Users**

Model používateľa predstavuje registrovaného používateľa, ktorý si úspešne vytvoril účet na webovej stránke. Používateľský model má nasledujúce atribúty:

* userId – jedinečné ID používateľa, na základe ktorého sa vykonáva identifikácia používateľa
* userName – jedinečné užívateľské meno k účtu
* email – e-mailová adresa používateľa
* password – heslo na prístup k používateľskému účtu
* orders – atribút, ktorý odkazuje na model objednávky, tj. hovorí o objednávkach vykonaných z používateľského účtu

**Products**

Model produktov predstavuje entitu všetkých produktov, ktoré e-shop ponúka. Skladá sa z nasledujúcich atribútov:

* productId - jedinečné identifikačné číslo produktu
* productName - názov produktu
* price - cena produktu
* description - krátky popis produktu
* quantity - číslo, ktoré predstavuje množstvo dostupných produktov
* url - adresa URL, kde sa nachádza obrázok produktuOrders

**Orders**

Modul Objednávky predstavuje kolekciu všetkých objednávok zadaných v e-shope. Skladá sa z nasledujúcich atribútov:

* orderId - jedinečné číslo objednávky, na základe ktorého je identifikovaná
* creditCard - informácie o kreditnej karte, z ktorej bola platba vykonaná
* shipmentAddress - adresa, na ktorú má byť objednávka doručená
* userName - meno používateľa, ktorý zadal objednávku
* cartInfo - obsahuje presnejšie informácie o objednávke a skladá sa z 2 atribútov:
  + finalPrice - konečná cena objednávky
  + výrobok - odkaz na model výrobku. Obsahuje zoznam objednaných produktov v rámci jednej objednávky

**Rozhrania API servera**

Nasledujúca tabuľka popisuje rozhrania, ktoré možno použiť na vytvorenie databázových požiadaviek.

|  |  |  |  |
| --- | --- | --- | --- |
| **Operation** | **HTTP method** | **path** | **returns** |
| Get Single User | GET | /getUser | JSON of User |
| Register a User | POST | /register | userId |
| Get a Single Product | GET | /getProduct | JSON of Product |
| Create a Product | POST | /create/product | productId |
| Update a Product | POST | /update/product | productId |
| Create a Order | POST | /create/order | orderId |

Tabuľka 1: Rozhrania API servera

**Model Users (v postgres SQL databáze)**

Model používateľa predstavuje registrovaného používateľa, ktorý si úspešne vytvoril účet na webovej stránke. Tabuľka bola vytvorená pre možnosť použiť SQL útoky. Databáza využíva hosting na <https://www.elephantsql.com/>. Používateľský model má nasledujúce atribúty:

* id – jedinečné ID používateľa, na základe ktorého sa vykonáva identifikácia používateľa
* name – jedinečné užívateľské meno k účtu
* email – e-mailová adresa používateľa
* password – heslo na prístup k používateľskému účtu

Scenáre s použitím e-shopu

Vytvorený eshop umožňuje realizáciu niekoľkých scenárov za predpokladu, že budú splnené pre nich určené požiadavky.

* Prelamovanie slabých hesiel – slovníkový útok
* Ukradnutie produktu bez zaplatenia zmenením odoslaných informácií na backend
* Ukradnutie produktu prístupom do adresára s produktami
* SQL injekcia pre zmenu emailu admina

Prelamovanie slabých hesiel – slovníkový útok

Útočník použije nástroj na prelamovanie slabých hesiel, pričom použije ľubovoľný nástroj pre to určený. Môže využiť aj dostupné slovníky. Pre uplatniteľnosť scenára nesmie aplikácia určovať požiadavky na silu hesla a zároveň musí byť slabé heslo prítomné v systéme.

Ukradnutie produktu odoslaním falošnej informácie

Útočník použije nástroj burpsuite alebo iný nástroj ktorý mu umožní zmeniť obsah http requestu na server. Nastaví nulovú hodnotu. Server nesmie kontrolovať vstupu. Kontrola vstupov by mala byť len na používateľskom rozhraní.

Ukradnutie produktu prístupom do priečinka

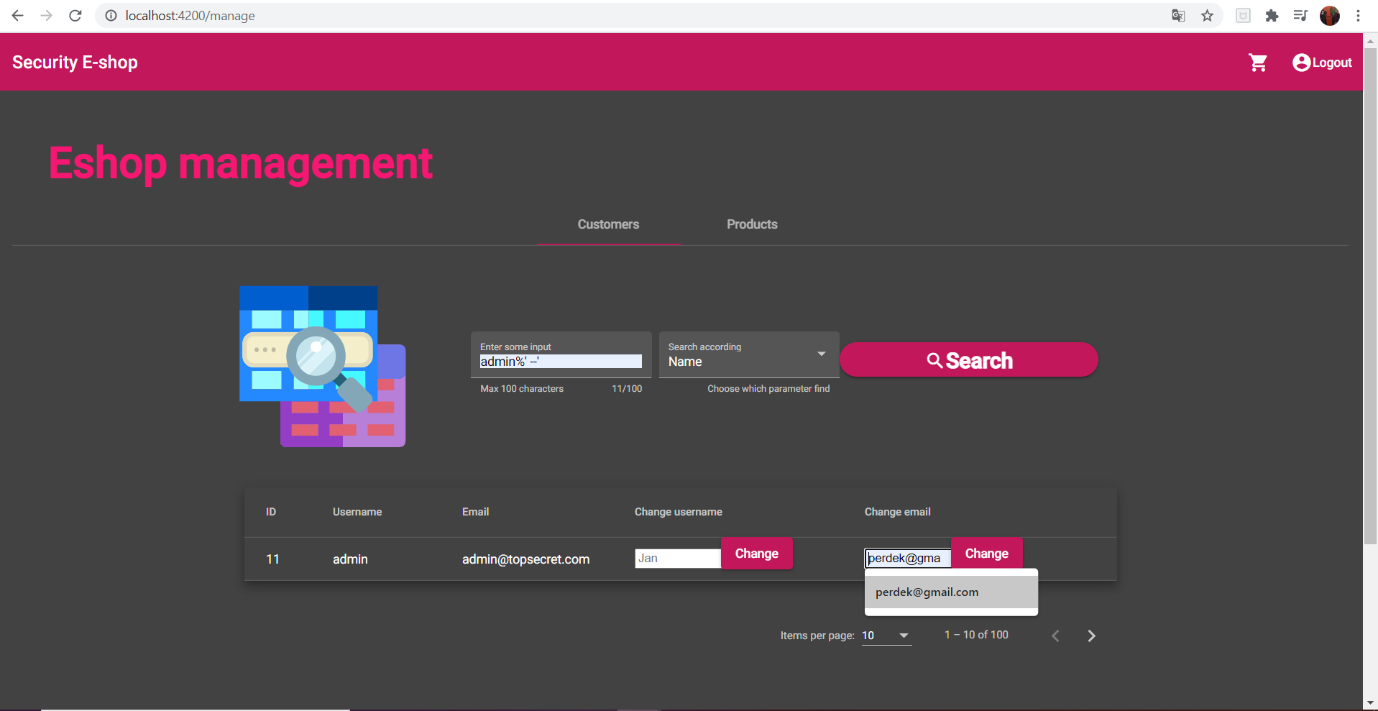
Útočník prehľadá možné adresy kde by sa súbory mohli nachádzať a stiahne potrebné súbory z nich. Je potrebné aby tieto adresáre boli pre útočníka prístupné.

SQL injekcia pre zmenu emailovej adresy admina

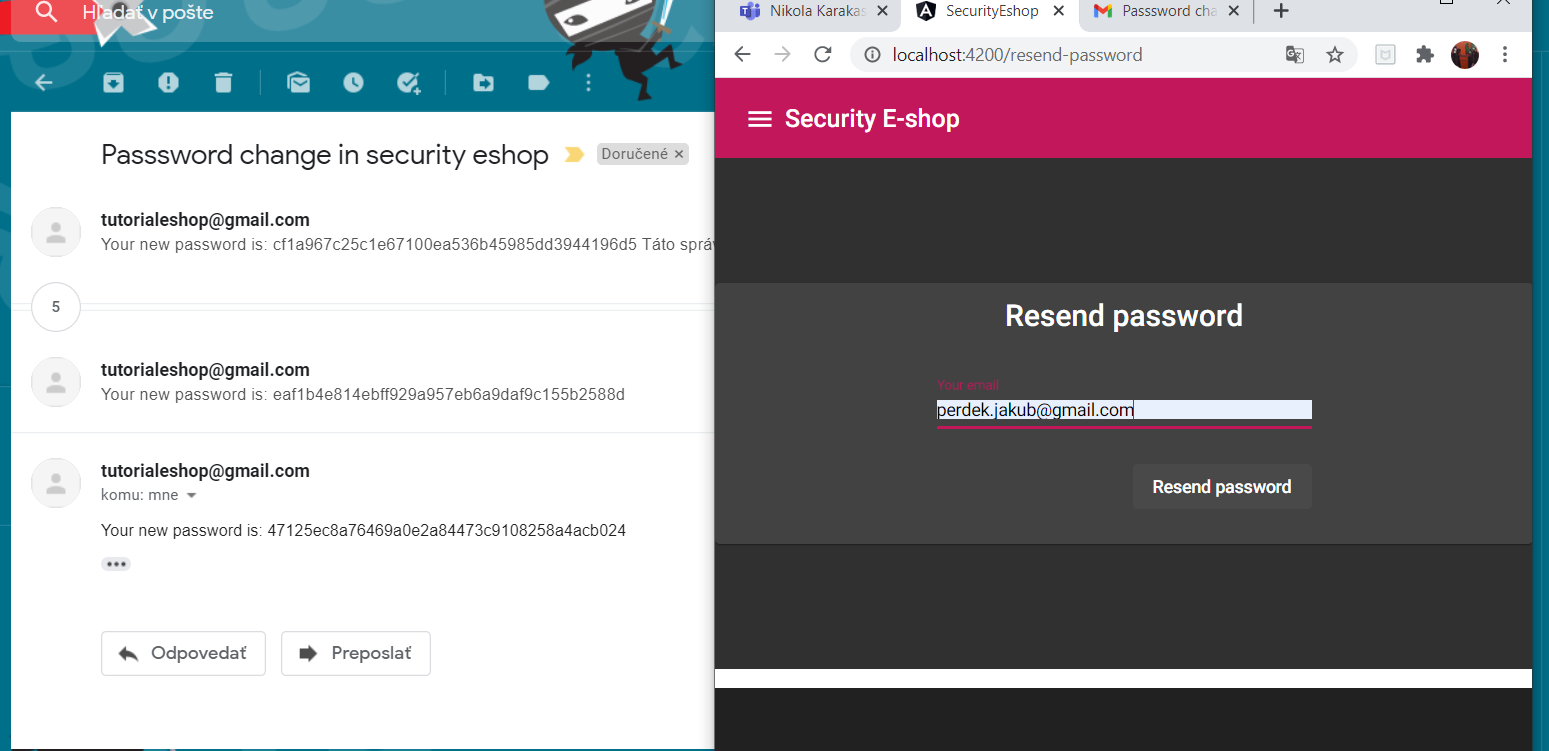
Pri vypisovaní všetkých používateľov v časti systému určenej pre pracovníka eshopu bude účet s oprávneniami správcu vynechaný. SQL dopyt, ktorý vypíše všetkých používateľov, je nasledovný:

*SELECT name, email FROM users WHERE name LIKE '%a%' AND name != 'admin'.*

Útočník sa pokúša vytvoriť SQL injekciu tak, aby získal informácie o účte s oprávneniami správcu. To je možné vykonať pridaním nasledujúceho dotazu: *admin%' --'* do pola za vyhľadávanie používateľov podľa mena. Následne útočník v roli predavača zmení email používateľa na nejaký, ku ktorému má prístup. Potom sa odhlási a nechá si vygenerovať nové heslo pre zmenený email. Na zadaný email mu bude doručené zmenené heslo, ktoré použije pri prihlasovaní. Na základe tohto útoku útočník získal privilégiá admina. Tento útok môže realizovať pracovník obchodu, ale primárne je určený v spojení s útokom prelamovania hesiel, v ktorom útočník sa na základe slabého hesla dostane do role pracovníka v obchode. Pracovník v obchode má nižšie práva ako samotný admin. Obrázky 24 a 25 popisujú uvedený implementovaný útok.



Obrázok 24: Aplikovanie SQL injekcie



Obrázok 25: Generovanie a poslanie hesla na email pri jeho strate