

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
1.1	Whois aplikácia pre vyhľadanie domény	2
	Vyhľadanie domény	3
	Informácie o vyhľadanej doméne	3
	Zhodnotenie k whois aplikácii	6
1.2	Cieľová stránka e-shopu	7
	Používateľské rozhranie a dizajn stránky	7
	Domovská stránka	7
	Prihlásenie a registrácia	8
	Nákupný košík	9
	Informácie o doručení	10
	Informácie o platbe	11
	Server a riadiaca časť systému	15
	Databáza	16
	Databázový model	17
1.3	Scenáre s použitím e-shopu	19
	Prelamovanie slabých hesiel – slovníkový útok	19
	Ukradnutie produktu odoslaním falošnej informácie	19
	Ukradnutie produktu prístupom do priečinka	19
	SQL injekcia pre zmenu emailovej adresy admina	19

1 Technická dokumentácia

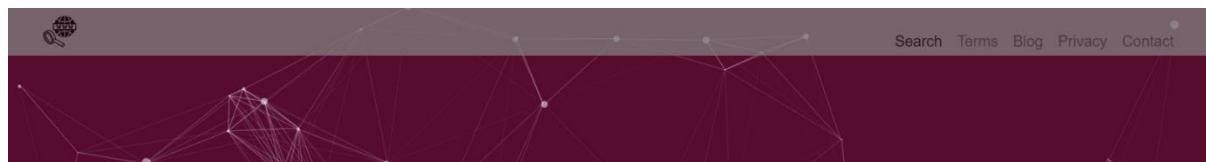
K aplikáciám bola vytvorená ich technická dokumentácia. Uvádzame tu dokumentáciu k backendu a frontendu eshopu. Zdokumentovaná je aj Whois aplikácia. V dokumentácii uvádzame používateľské rozhrania, použité služby a funkcionality konkrétnej aplikácie.

1.1 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 potenciálne hrozby. Reprezentuje nástroj, na základe ktorého môže používateľ vyhľadať informácie o nájdených hrozbách a použiť ich pre potenciálny 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

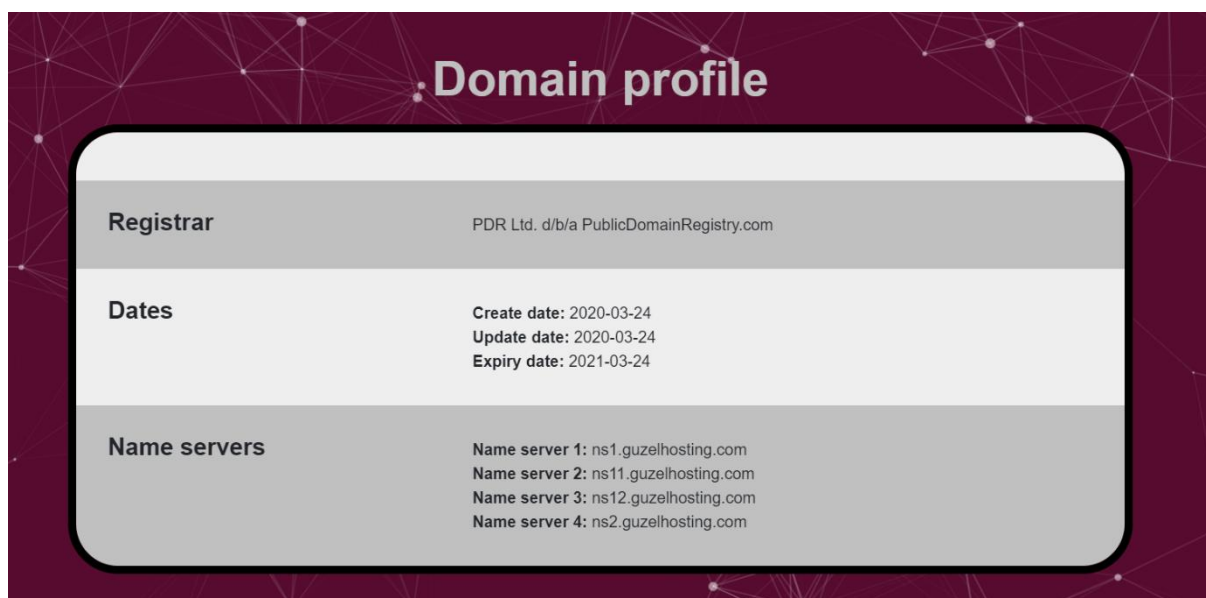
Používateľ po načítaní stránky vloží názov domény do okna v strede obrazovky a stlačí tlačidlo Search. Formulár je zobrazený na Obrázku 1. Reťazec je hľadaný v uprostred doménových mien. Výsledok môže obsahovať tento reťazec kdekoľvek v názve domény. Vrátený je len jeden výsledok, preto by dopyt mal 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 tvorcach stránky. Päta je zobrazená na Obrázku 3.



Obrázok 3: Päta vyhľadávača

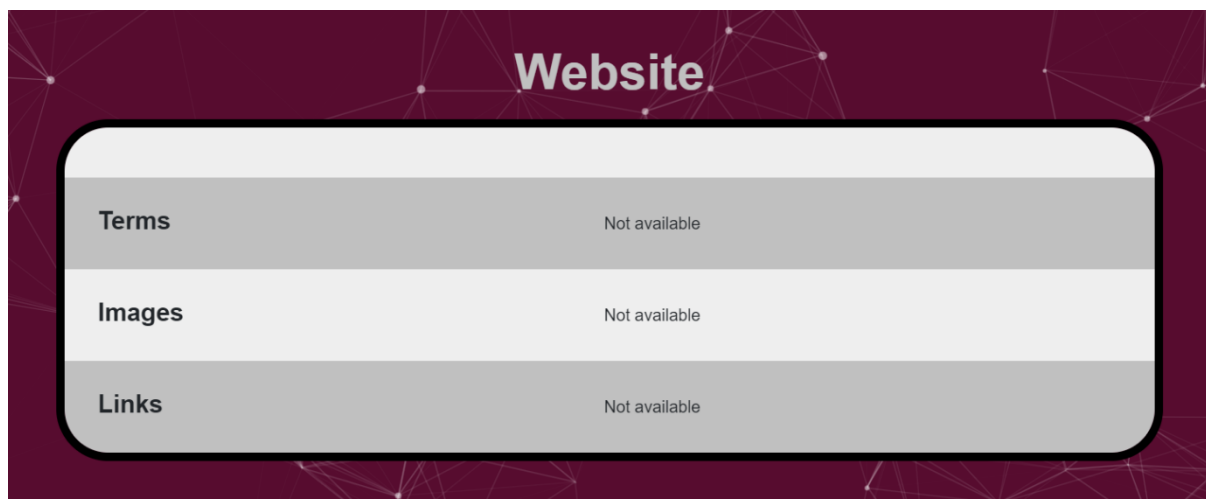
Informácie o vyhladanej doméne

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 nezberáme, ale v budúcnosti môže byť riešenie rozšírené o preliezač webu, ktorý získa tieto informácie. Táto časť je zobrazená na Obrázku 5.



Website	
Terms	Not available
Images	Not available
Links	Not available

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.

Whois Record

Domain: 01cukurovabims.com
Registrant:
Create date: 2020-03-24
Update date: 2020-03-24
Expiry date: 2021-03-24

Domain registrar name: PDR Ltd. d/b/a PublicDomainRegistry.com
Domain registrar whois: whois.publicdomainregistry.com
Domain registrar url: http://www.publicdomainregistry.com

Registrant name: SELMAN SAGMEN
Registrant address: S.Cengiz KARACA Mah. 1048 Cad. 9/3
Registrant city: ANKARA
Registrant state: CANKAYA
Registrant zip: 06530
Registrant country: Turkey
Registrant email: frmseymen@gmail.com
Registrant phone: +90.5363013647

Obrázok 6: Podrobnejšie informácie

Administrative name: Guzel Hosting
Administrative company: GNET Internet Telekomunikasyon A.S.
Administrative address: Icerenkoy Mh. Ertac Sk. Ardil Is Merkezi No 4/2
Administrative city: Istanbul
Administrative state: Atasehir
Administrative zip: 34752
Administrative country: Turkey
Administrative email: alanadi@guzel.net.tr
Administrative phone: +90.908508850558

Technical name: Guzel Hosting
Technical company: GNET Internet Telekomunikasyon A.S.
Technical address: Icerenkoy Mh. Ertac Sk. Ardil Is Merkezi No 4/2
Technical city: Istanbul
Technical state: Atasehir
Technical zip: 34752
Technical country: Turkey
Technical email: alanadi@guzel.net.tr
Technical phone: +90.908508850558

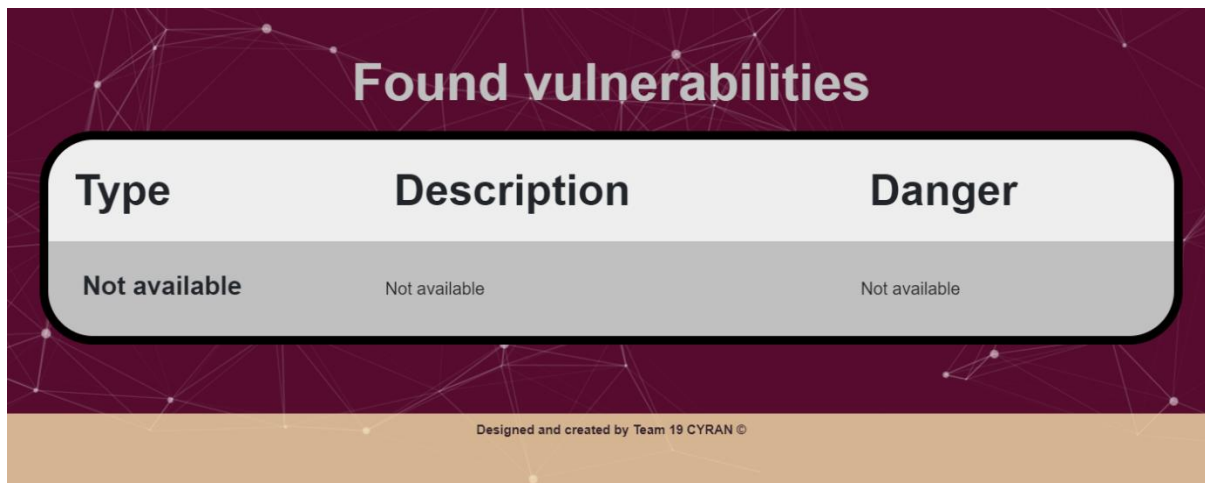
Obrázok 7: Podrobnejšie informácie pokračovanie 1

Name server 1: ns1.guzelhosting.com
Name server 2: ns11.guzelhosting.com
Name server 3: ns12.guzelhosting.com
Name server 4: ns2.guzelhosting.com

Domain status 1: clientTransferProhibited

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.



The image shows a web interface with a dark purple background and a network diagram pattern. A white rounded rectangle contains a table with the title 'Found vulnerabilities'. The table has three columns: 'Type', 'Description', and 'Danger'. All three cells in the table contain the text 'Not available'. Below the table, there is a small text credit: 'Designed and created by Team 19 CYRAN ©'.

Type	Description	Danger
Not available	Not available	Not available

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.

1.2 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

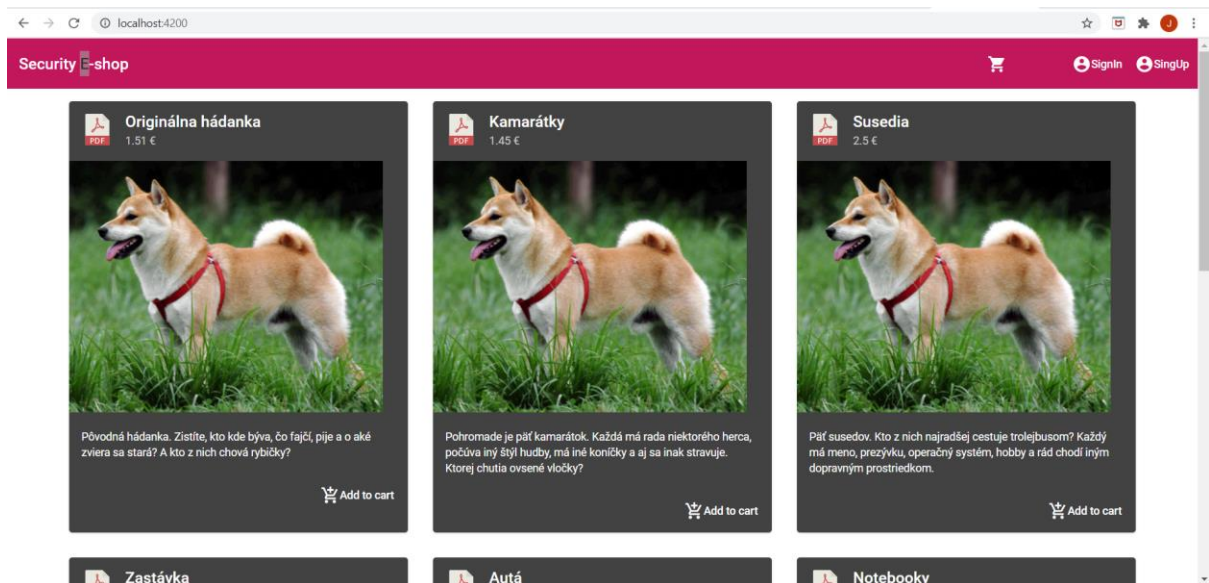
Stránka je koncipovaná ako fiktívny cieľ s cieľom využiť jej nedostatky a uskutočniť rôzne typy kybernetických útokov. Lokalita ako celok bude veľmi dynamická, aby sa v neskorších scenároch mohla technológia webu prispôbiť povahe útoku, napríklad zmenám v databáze alebo funkčnosti alebo backendu samotnému.

Používateľské rozhranie a dizajn stránky

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

Domovská stránka

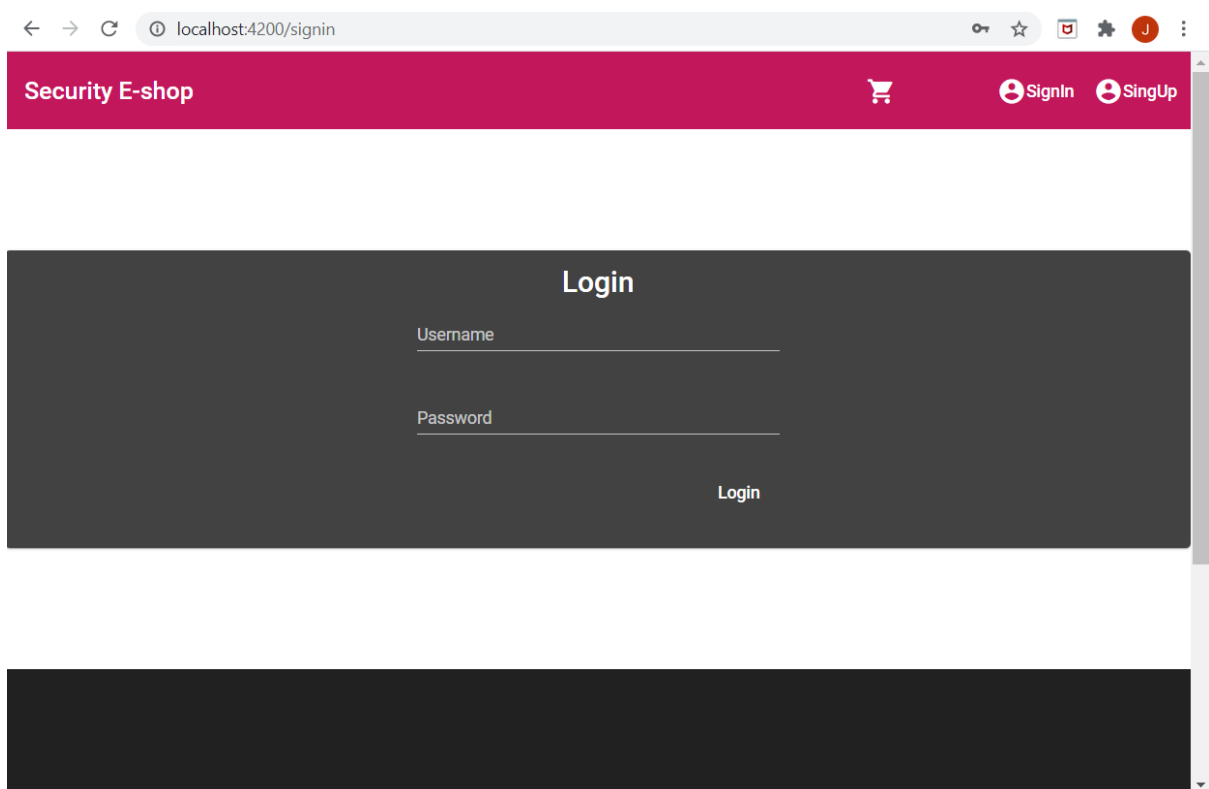
V zobrazení domovskej stránky môže používateľ prehľadávať produkty bez predchádzajúceho prihlásenia alebo registrácie. Odtiaľ si môže zvoliť, či prejde registráciou / prihlásením, alebo podrobnejším vyhľadávaním produktu.



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

Security E-shop

SignUp

Full Name

Email

Address

Password

Confirm Password

SignUp

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.

Security E-shop

Shopping cart

→ Susedia	+ Add - Remove	3	Delete	7.5 €
→ Kamarátky	+ Add - Remove	1	Delete	10,50 €
✓ Checkout:				17.5 €

> Choose shipment

Obrázok 13 Zobrazenie nákupného košíka

Informácie o doručení

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

Security E-shop

Logout

Delivery options

☒ Deliver to issue place

Issue place

First name Last Name

Address

Street

City Post Postal Code

0 / 5

> Payment methods

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.

Security E-shop

Paying methods

Card Bank Transfer Cash on delivery

Card number
fdsdsdsdsds

Name of card Date Security Code 0 / 3

Card number Security code CVV/CVC Name Expiry Date

Obrázok 15 Formulár na zadanie informácií o platbe

Card number
fdsdsdsdsds

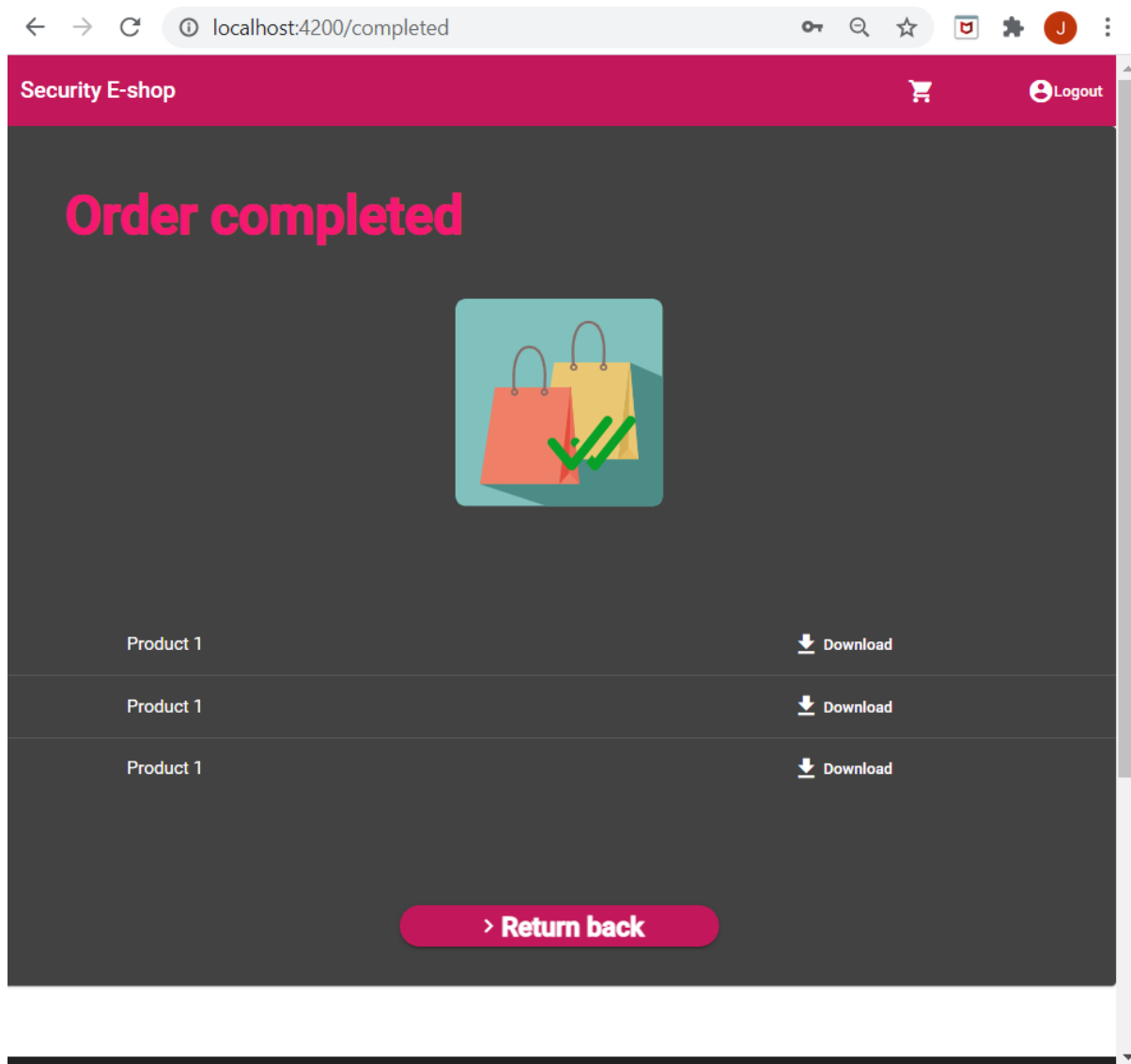
Name of card Date Security Code 0 / 3

Card number Security code CVV/CVC Name Expiry Date

Price to pay in €
30.95

> Finish order

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 zákaznicke účty. Vyhľadávať môže podľa dvoch atribútov: meno a e-mail. Po kliknutí na tlačidlo Search (hľadať) budú vygenerovaní všetci používatelia, ktorí vyhovujú dopytu.

Eshop management

Customers Products

Enter some input Max 100 characters 0/100 Search according Choose which parameter find **Search**

ID	Username	Email	Change username	Change email
7	ijani@firm1.com	ijani@firm.sk	Jan Change	email@e Change
5	janko	janko@uniba.sk	Jan Change	email@e Change
3	jan	jan1@stuba.sk	Jan Change	email@e Change
6	racek1	racekjan@racekpro1.sk	Jan Change	email@e Change
16	perdek	perdek.jakub@gmail.com	Jan Change	email@e Change


Items per page: 10 1 - 10 of 100 < >

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.

Eshop management

Customers Products



Max 100 characters 3/100

Choose which parameter find

ID	Username	Email	Change username	Change email
7	ijani@firm1.com	ijani@firm.sk	<input type="text" value="Jan"/> <input type="button" value="Change"/>	<input type="text" value="email@e"/> <input type="button" value="Change"/>
5	janko	janko@uniba.sk	<input type="text" value="Jan"/> <input type="button" value="Change"/>	<input type="text" value="email@e"/> <input type="button" value="Change"/>
3	jan	jan1@stuba.sk	<input type="text" value="Jan"/> <input type="button" value="Change"/>	<input type="text" value="email@e"/> <input type="button" value="Change"/>

Items per page: 10 1 – 10 of 100 < >

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.

Eshop management

Customers Products


Insert product

Title

Amount

Price

Description



Obrázok 20: Správa produktov

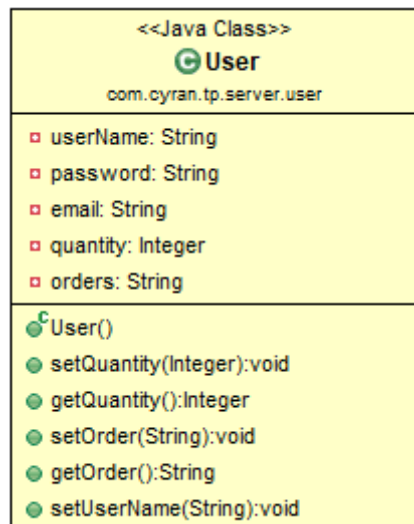
Server a riadiaca časť systému

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.

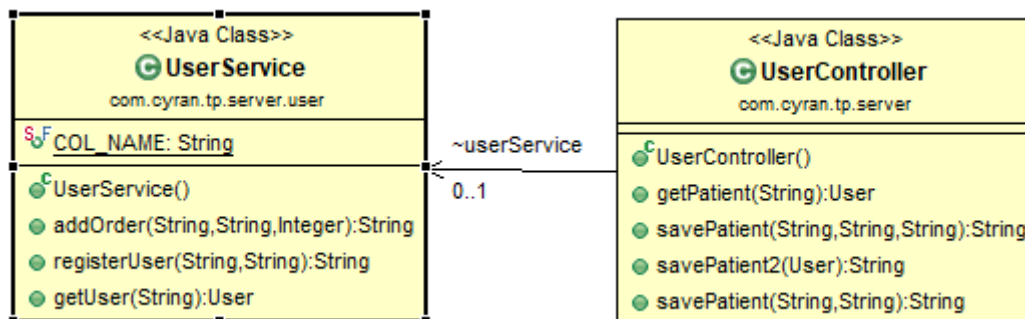
Na ďalšom diagrame tried môžeme vidieť hlavné triedy, z ktorých každá predstavuje jednu zo základných entít databázy.



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 Používateľ. V tomto okamihu poskytuje back-end funkčnosť registrácie a prihlásenia, ako aj objednávanie 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

1.3 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 zaplattenia 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 adresy boli pre útočníka prístupné.

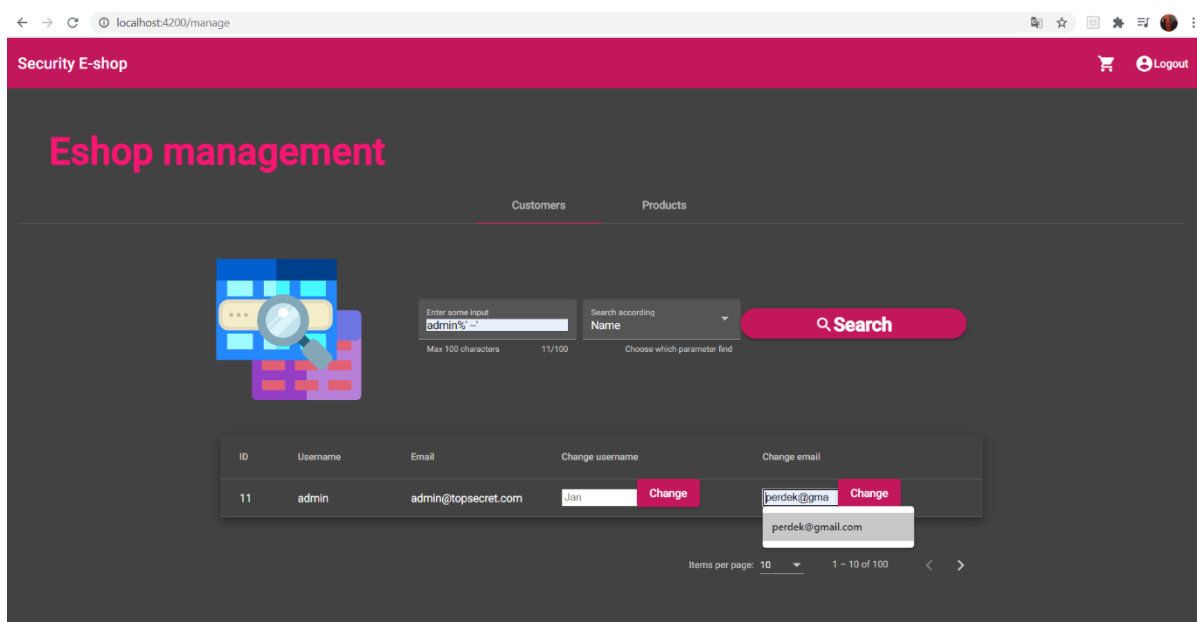
SQL injekcia pre zmenu emailovej adresy admina

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:

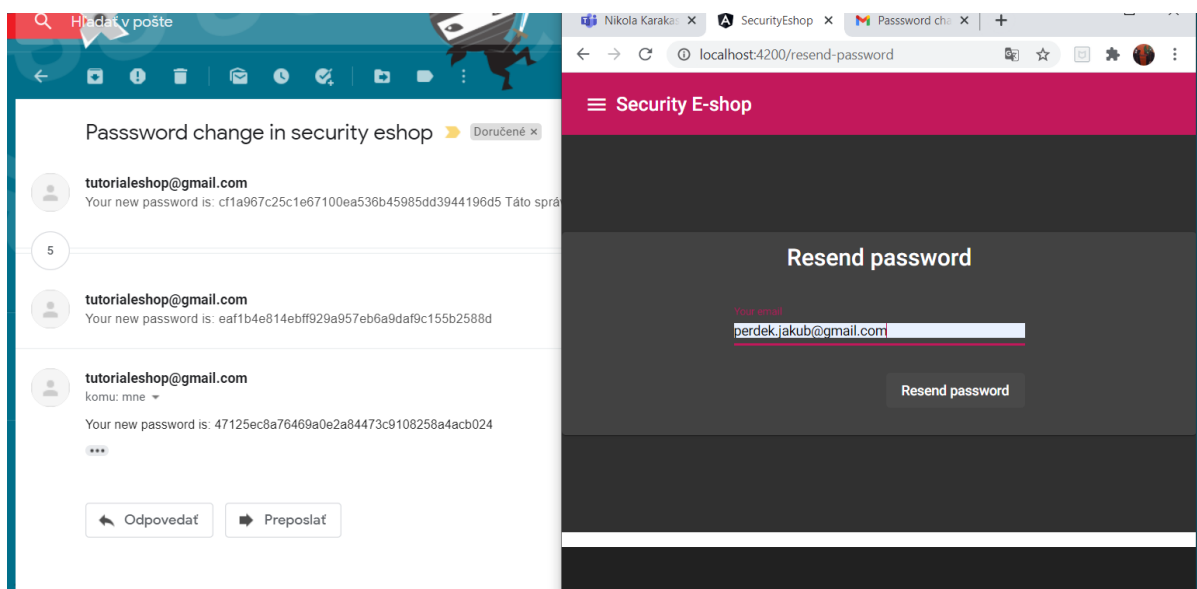
```
SELECT name, email FROM users WHERE name LIKE '%a%' AND name != 'admin'.
```

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