

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

<b>1</b>	<b>Požiadavky riešenia</b>	<b>3</b>
1.1	Scenáre	3
1.2	Nasadenie	3
1.3	Nefunkcionálne požiadavky	4
<b>2</b>	<b>Big Picture</b>	<b>5</b>
2.1	Úvod	5
2.2	Ciele	5
2.3	Ohraničenia	6
2.4	Globálne ciele na zimný semester	6
2.5	Globálne ciele na letný semester	7
2.6	Celkový pohľad na systém	8
<b>3</b>	<b>Technická dokumentácia</b>	<b>9</b>
3.1	Whois aplikácia pre vyhľadanie domény	9
	Vyhľadanie domény	10
	Informácie o vyhladanej doméne	10
	BCrypt a overenie jeho vlastností	13
	Schéma ku databáze	15
	Zhodnotenie k whois aplikácii	16
3.2	Ciel'ová stránka e-shopu	17
	Používateľské rozhranie a dizajn stránky	17
	Domovská stránka	17
	Prihlásenie a registrácia	18
	Nákupný košík	19
	Informácie o doručení	20
	Informácie o platbe	21
	Správa rolí používateľov	25
	Server a riadiaca časť systému	26
	Databáza	27
	Databázový model	28
3.3	Scenáre s použitím e-shopu	30
	Prelamovanie slabých hesiel – slovníkový útok	30
	Ukradnutie produktu odoslaním falošnej informácie	30
	Ukradnutie produktu prístupom do priečinka	30
	SQL injekcia pre zmenu emailovej adresy admina	30
	SQL injekcia pre získanie informácií z whois	32
3.4	Logovanie v aplikácii	33
	Analýza dát zo Sentry	34
	Analýza dát z Google forms	40

<b>3.5</b>	<b>Posudky na prototyp tímu č. 19</b>	<b>43</b>
	Posudok na základe používateľského testovania	43
	Posudky jednotlivých testerov z bezpečnostného semináru	44

# 1 Požiadavky riešenia

Podľa zadania a následných konzultácií s product ownerom boli identifikované nasledovné požiadavky riešenia:

- Navrhnuť simulačné prostredie spolu s vybranými scenármi pre testovanie kybernetickej ochrany
- Použiť platformu (simulačného prostredia) pre realizáciu tohto prostredia (Odporúčanie použiť KYPO)
- Tvorba simulačného prostredia na jednom fyzickom PC pomocou viacerých virtuálnych strojov

## 1.1 Scenáre

- Otestovať už existujúce scenáre
- Navrhnuť 2-3 vlastné scenáre vhodné do výučby na FIIT
- Implementovať navrhnuté prostredie a scenáre na prostriedkoch FIIT
- Otestovať navrhnuté prostredie a scenáre na prostriedkoch FIIT
- Scenáre by mali slúžiť na podporu a zlepšenie výučby predmetov informačnej a sieťovej bezpečnosti.
- Identifikácia vhodných typov scenárov pre zapracovanie do problematiky
- Identifikácia vhodných typov problémov pre zapracovanie do scenárov
- Scenáre by mali zaujať hráča
- Zakomponovanie špeciálnych vlastností virtuálnych systémov s dôrazom na ich vplyv na existujúce a aj nové zraniteľnosti a detekcie (resp. prevencie prienikov zneužívajúcich tieto zraniteľnosti)
- Obsahom scenárov by malo byť zabezpečenie rôznych systémov ako aj rôzne prieniky do nich

## 1.2 Nasadenie

- Nasadenie výsledného riešenia pomocou virtuálnych strojov
- Nasadenie simulačného prostredia v prostredí OpenStack

- Nasadenie výsledného riešenia s minimalizáciou manuálnych úkonov a zásahov zo strany pedagóga

## **1.3 Nefunkcionálne požiadavky**

- Riešenie by malo byť dynamicky škálovateľné podľa aktuálnych potrieb a dostupných prostriedkov

## 2 Big Picture

### 2.1 Úvod

Cyran projekt je zameraný na možnosť zlepšenia a testovania svojich schopností v simulovanej realite kyberpriestoru. Účastníci riešia rôzne úlohy a snažia sa odvrátiť útoky alebo sa infiltrovať do počítača cudzej osoby, prípadne podniknúť inú formu útoku. Cieľom je nájsť potencionálnu zraniteľnosť systému pre tím, ktorý sa obraňuje, prípadne získať informáciu v najčastejšie v podobe textového reťazca od brániaceho sa tímu.

### 2.2 Ciele

V rámci projektu je naším hlavným cieľom zostrojiť aplikáciu využívajúcu platformu KYPO, ktorá by používateľom umožnila vzdelávať a súperiť v oblasti kybernetickej ochrany formou vytvorených hier. Každá hra bude založená na originálnom scenári pre otestovanie a prípadne aj naučenie používateľa rôznymi technikami, na ktoré bude orientovaný. Ďalšími vedľajšími cieľmi, ktoré poslúžia pre realizáciu hlavného cieľa alebo naplňajú novú funkcionality, ktorá podporuje požiadavky riešenia sú:

- Použitie platformy KYPO pri realizácii aplikácie ako aktualizovaného prostredia
- Analýza problematiky kybernetickej bezpečnosti
- Návrh scenárov zameraných na špeciálne situácie akými sú chyby v systéme alebo oboznámenie sa s rôznymi nástrojmi
  - Tieto scenáre budú mať edukatívny charakter
  - Náповedy by mali slúžiť pre ponorenie používateľa do problému
  - Herný systém by mal identifikovať schopnosti a úroveň hráča pre lepší herný zážitok a poučenie z hry
  - Akcie používateľa by sa mali zaznamenávať pre identifikáciu rôznych návykov
  - Overenie na základe dotazníkov a rozhovorov by malo slúžiť na hľadanie vhodného scenáru pre konkrétnu problematiku

- Analýza novo nájdených zraniteľností
- Automatizácia procesov vyhodnocovania priebehu hry
  - Rozhodnutie ktoré schváli koordinátor
  - Automatické rozhodovanie
- Tvorba docker image-ov pre jednoduché nasadenie aplikácie
- Nasadenie aplikácii na OpenStack ako želaného miesta
- Dôraz pri návrhu a implementácii na objektové prístupy, architektúru s podpory interoperability a rozšíriteľnosti riešenia

## 2.3 Ohraničenia

Ohraničenia, ktoré náš systém bude mať budú počet realizovaných scenárov a overenia s konkrétnymi študentmi pre dĺžku trvania projektu.

## 2.4 Globálne ciele na zimný semester

Pre nedostupnosť KYPO platformy sme realizovali webovú aplikáciu ako samostatný celok fungujúci aj mimo platformy KYPO. Po získaní prístupu k platforme aplikáciu hodláme nasadiť na jeden z uzlov do OpenStacku.

Globálne ciele na zimný semester sú

- Použitie platformy KYPO pri realizácii aplikácie ako aktualizovaného prostredia
- Analýza problematiky kybernetickej bezpečnosti
- Návrh scenárov zameraných na špeciálne situácie akými sú chyby v systéme alebo oboznámenie sa z rôznymi nástrojmi
  - Tieto scenáre budú mať edukatívny charakter
  - Náповedy by mali slúžiť pre ponorenie používateľa do problému
  - Herný systém by mal identifikovať schopnosti a úroveň hráča pre lepší herný zážitok a poučenie z hry

- Akcie používateľa by sa mali zaznamenávať pre identifikáciu rôznych návykov
- Overenie na základe dotazníkov a rozhovorov by malo slúžiť na hľadanie vhodného scenáru pre konkrétnu problematiku
- Analýza novo nájdených zraniteľností
- Automatizácia procesov vyhodnocovania priebehu hry
  - Rozhodnutie ktoré schváli koordinátor
  - Automatické rozhodovanie
- Tvorba docker image-ov pre jednoduché nasadenie aplikácie
- Dôraz pri návrhu a implementácii na objektové prístupy, architektúru s podpory interoperability a rozšíriteľnosti riešenia

## 2.5 Globálne ciele na letný semester

Globálne ciele na letný semester sú

- Použitie platformy KYPO pri realizácii aplikácie ako aktualizovaného prostredia
- Kontajnerizácia a nasadenie vytvorených aplikácií v minulom semestri
- Zlepšenie vytvorenej webovej aplikácie
  - Vylepšenie dizajnu, hrateľnosti, realizácie konfigurovateľných chýb v aplikácii
- Návrh scenárov zameraných na špeciálne situácie akými sú chyby v systéme alebo oboznámenie sa z rôznymi nástrojmi
  - Tieto scenáre budú mať edukatívny charakter
  - Nápovedy by mali slúžiť pre ponorenie používateľa do problému
  - Herný systém by mal identifikovať schopnosti a úroveň hráča pre lepší herný zážitok a poučenie z hry
  - Akcie používateľa by sa mali zaznamenávať pre identifikáciu rôznych návykov
  - Overenie na základe dotazníkov a rozhovorov by malo slúžiť na hľadanie vhodného scenáru pre konkrétnu problematiku
  - Analýza novo nájdených zraniteľností



- Automatizácia procesov vyhodnocovania priebehu hry
  - Rozhodnutie ktoré schváli koordinátor
  - Automatické rozhodovanie
- Tvorba docker image-ov pre jednoduché nasadenie aplikácie
- Dôraz pri návrhu a implementácii na objektové prístupy, architektúru s podpory interoperability a rozšíriteľnosti riešenia

## 2.6 Celkový pohľad na systém

### Diagram nasadenia

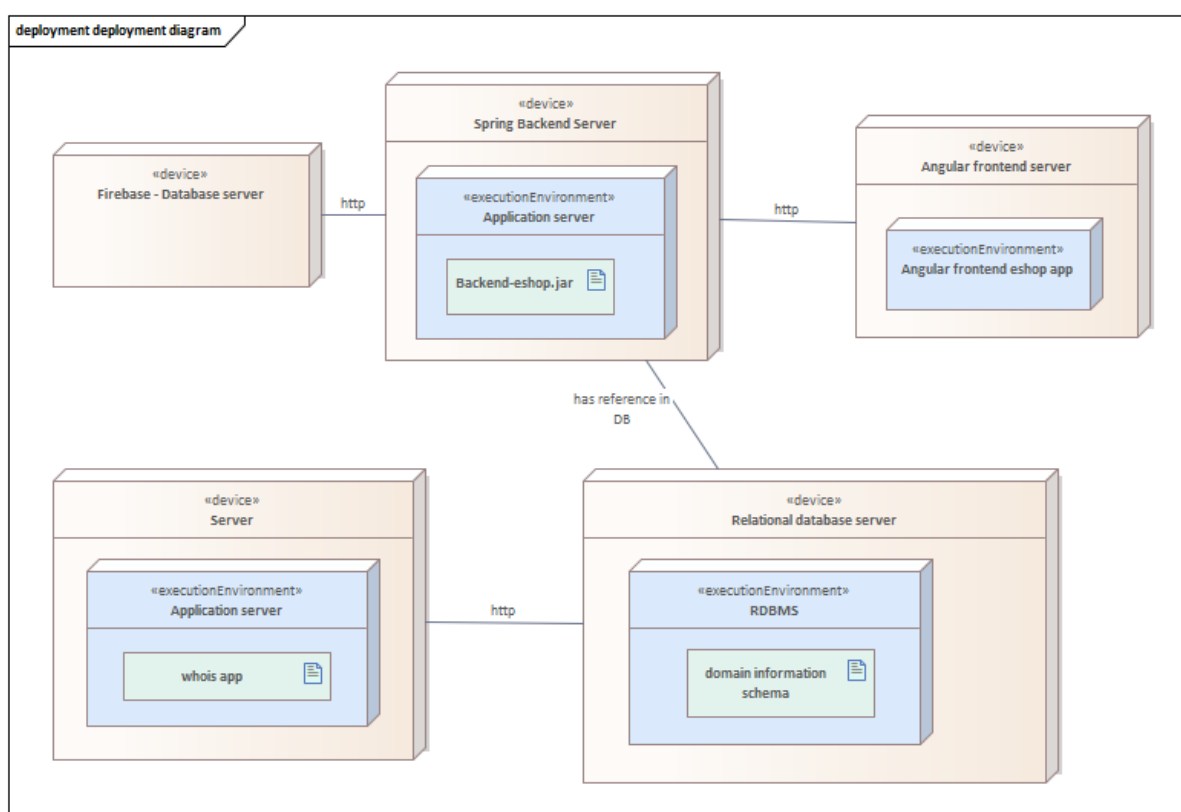


Diagram 1: Fyzické rozvrhnutie systému

## 3 Technická dokumentácia

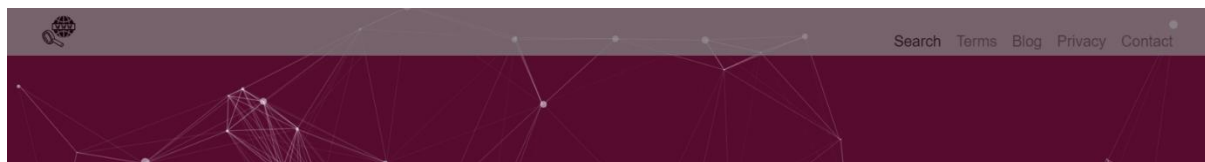
K aplikáciám bola vytvorená ich technická dokumentácia. Uvádzame tu dokumentáciu k backendu a frontendu eshopu. Zdokumentovaná je aj Whois aplikácia. V dokumentácii uvádzame používateľské rozhrania, použité služby a funkcionality konkrétnej aplikácie.

### 3.1 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

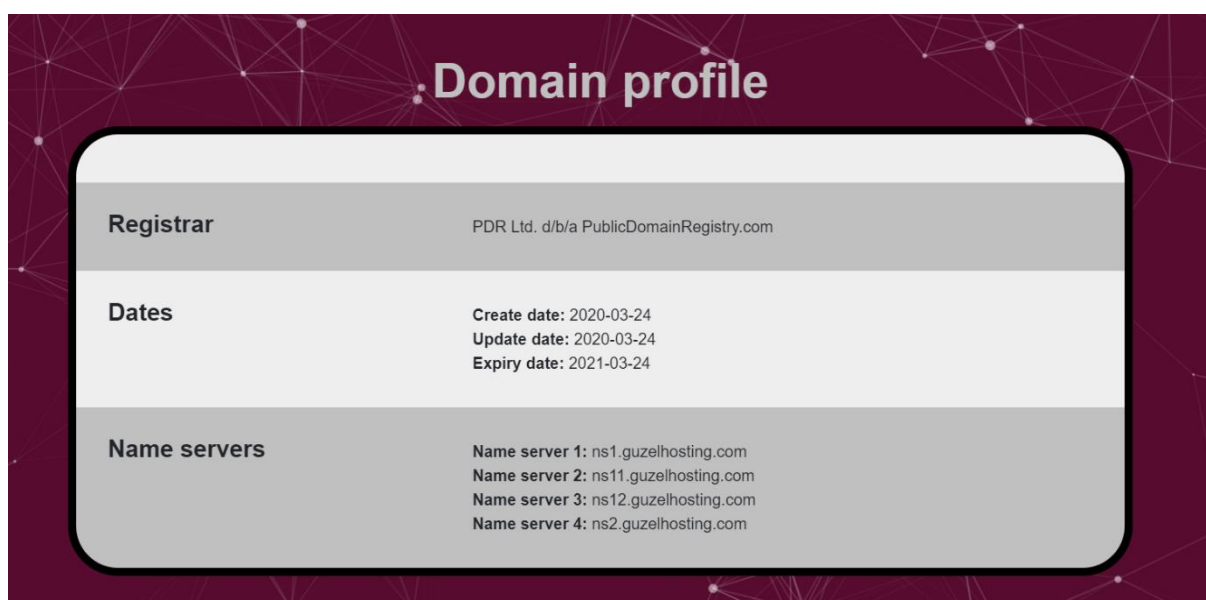
Používateľ po načítaní stránky vloží názov domény do okna v strede obrazovky a stlačí tlačidlo Search. Formulár je zobrazený na Obrázku 1. Reťazec je hľadaný v uprostred doménových mien. Výsledok môže obsahovať tento reťazec kdekoľvek v názve domény. Vrátený je len jeden výsledok, preto by dopyt mal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

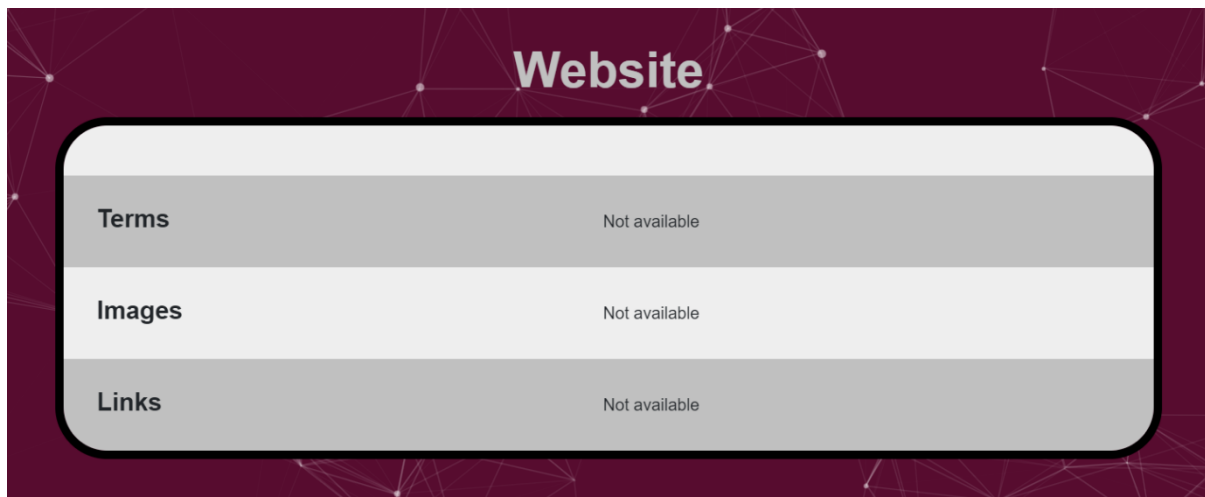
## Informácie o vyhladanej doméne

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 chyba 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**

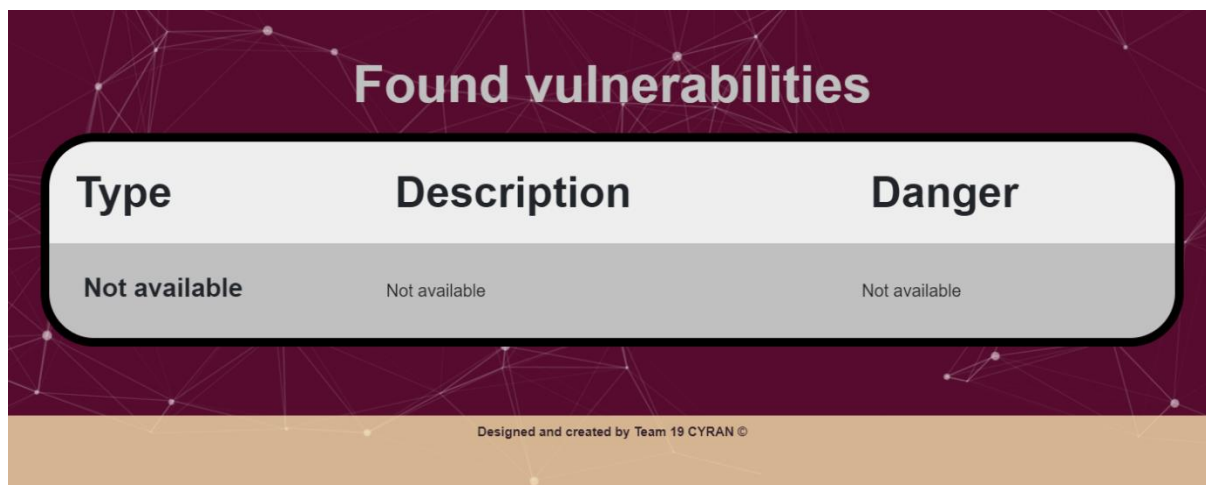
Administrative name: Guzel Hosting  
Administrative company: GNET Internet Telekomunikasyon A.S.  
Administrative address: Icerenkoy Mh. Ertac Sk. Ardil Is Merkezi No 4/2  
Administrative city: Istanbul  
Administrative state: Atasehir  
Administrative zip: 34752  
Administrative country: Turkey  
Administrative 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'. The first row of data contains the text 'Not available' in each column. 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

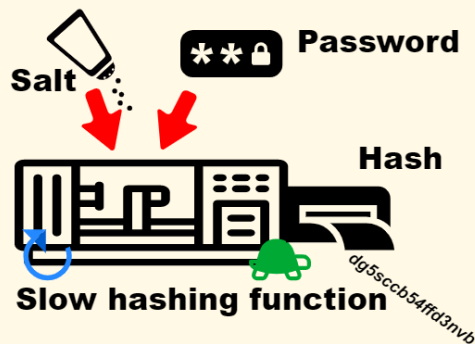
Obrázok 9: Nájdene hrozby

## BCrypt a overenie jeho vlastností

Doplnok umožňujúci dozvedieť sa niečo o fungovaní BCrypt algoritmu a reálne si vyskúšať vygenerovať a následne overiť heslo by malo byť pre používateľov, ktorý sa s ním nestretnú praktické. Malo by to byť hlavne kvôli dlhšej dobe čakania na výsledok pri vyššej hodnote soli, keďže sa jedná o pomalú hashovú funkciu. Funkcionalita vznikla ako podporná časť semi-automatického prelamovania hesiel v security eshope. Útočník si službou môže pomôcť pri overovaní zhody hashu s hádanými reťazcami. Úvodný text môžete vidieť na obrázku 10. Formuláre pre šifrovanie a dešifrovanie sú zobrazené na obrázku 11.

## Slow hashing functions

Hashing using salt is basic hashing technology. It is based on combination password with salt. In older implementations value of salt was based on time value of setting password to user. Newest implementations are using random numbers. Algorithm should use slow hashing function for generating hash slowly as prevention for possible attacks. Value of salt is usually stored with password. Bcrypt is one of algorithms which use salt.



Obrázok 10: Pomalé hashové funkcie

### BCrypt encryptor

Salt:

Given text:

Converted text:

Apply BCrypt

### BCrypt validator

Guessed text:

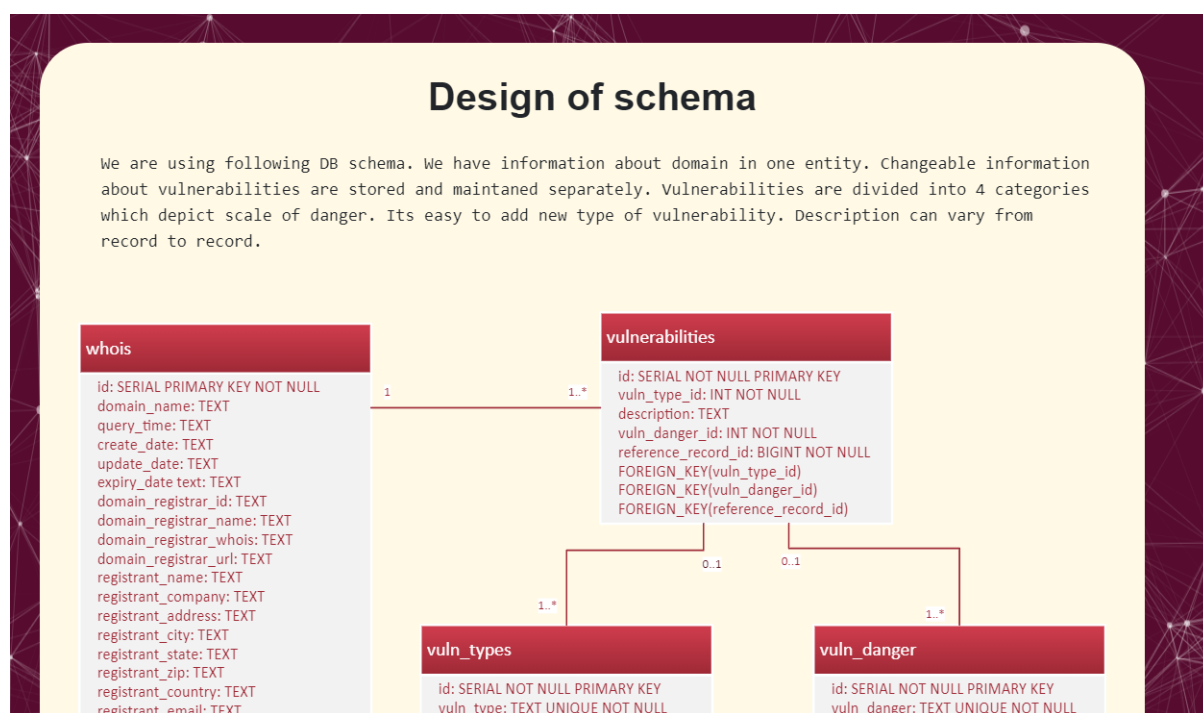
Given hash:

Answer:

Apply BCrypt

# Schéma ku databáze

Predpokladáme, že whois aplikácia chce prezentovať svoju schému ukladania dát. Po doplnení častí zo zraniteľnosťami obsahuje 4 tabuľky. Pôvodná tabuľka obsahuje podstatné informácie o doméne. Ostatné slúžia na popis zraniteľností, ktoré sa môžu často meniť ako aj pridávať nové typy hrozieb. Zároveň sme chceli aj kategorizovať úroveň nebezpečnosti hrozieb. Schéma okrem toho má používateľovi slúžiť na možnosť uplatniť pokročilú SQL injekciu, keďže pokročilé vyhľadanie whois aplikácia zatiaľ neobsahuje a špecifické potreby používateľa rovnako nie sú zahrnuté. Pri budúcom zlepšovaní aplikácie by funkcionality mohla byť prístupná menej skúseným používateľom a pre tých skúsenejších ponechaná možnosť SQL injekcie pri získavaní dát. Obrázok so zobrazenou schémou môžete vidieť na obrázku 12.



Obrázok 11: Schéma ku databáze



## 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.

## 3.2 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

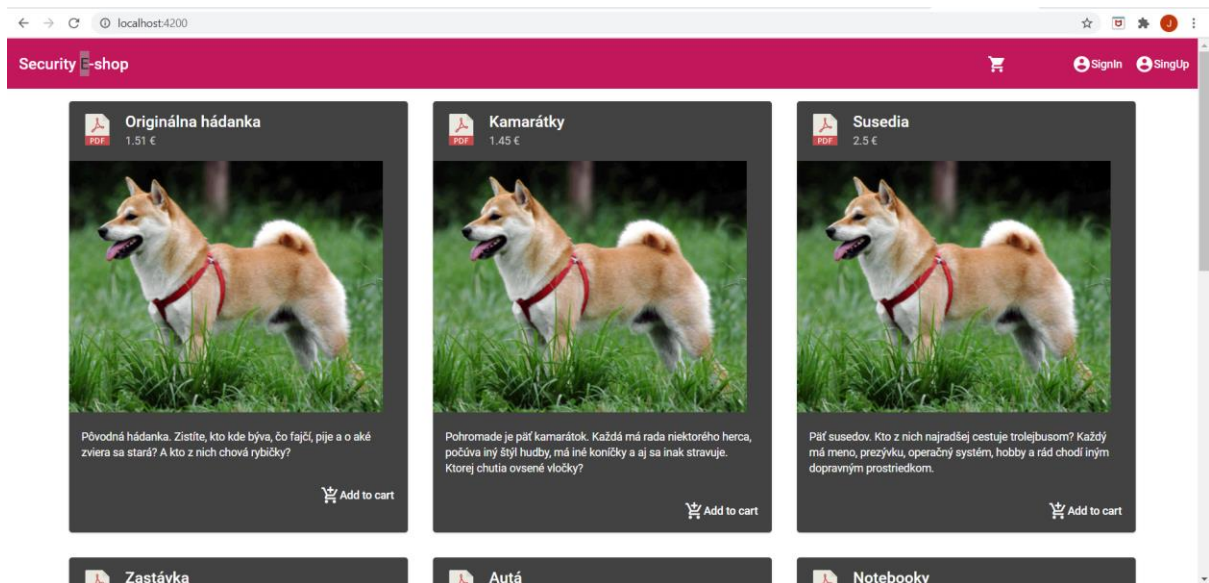
Stránka je koncipovaná ako fiktívny cieľ s cieľom využiť jej nedostatky a uskutočniť rôzne typy kybernetických útokov. Lokalita ako celok bude veľmi dynamická, aby sa v neskorších scenároch mohla technológia webu prispôbiť povahe útoku, napríklad zmenám v databáze alebo funkčnosti alebo backendu samotnému.

## 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

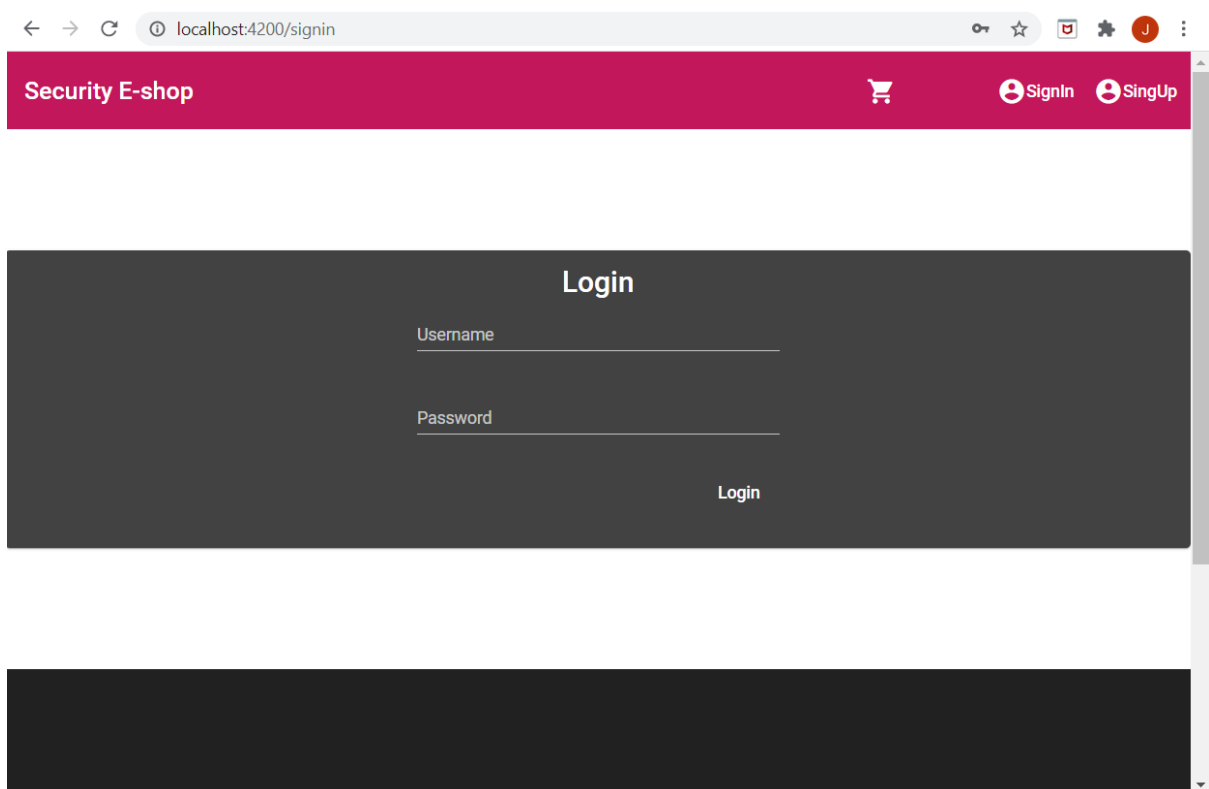
V zobrazení domovskej stránky môže používateľ prehľadávať produkty bez predchádzajúceho prihlásenia alebo registrácie. Odtiaľ si môže zvoliť, či prejde registráciou / prihlásením, alebo podrobnejším vyhľadávaním produktu.



Obrázok 12 Zobrazenie domovskej stránky

## Prihlásenie a registrácia

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



Obrázok 13: Formulár na prihlásenie

Security E-shop

SignUp

Full Name

Email

Address

Password

Confirm Password

SignUp

Obrázok 14 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 15 Zobrazenie nákupného košíka

# Informácie o doručení

Do formuláru na Obrázku 17 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 16: 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 17 Formulár na zadanie informácií o platbe

Card number  
fdsdsdsdsds

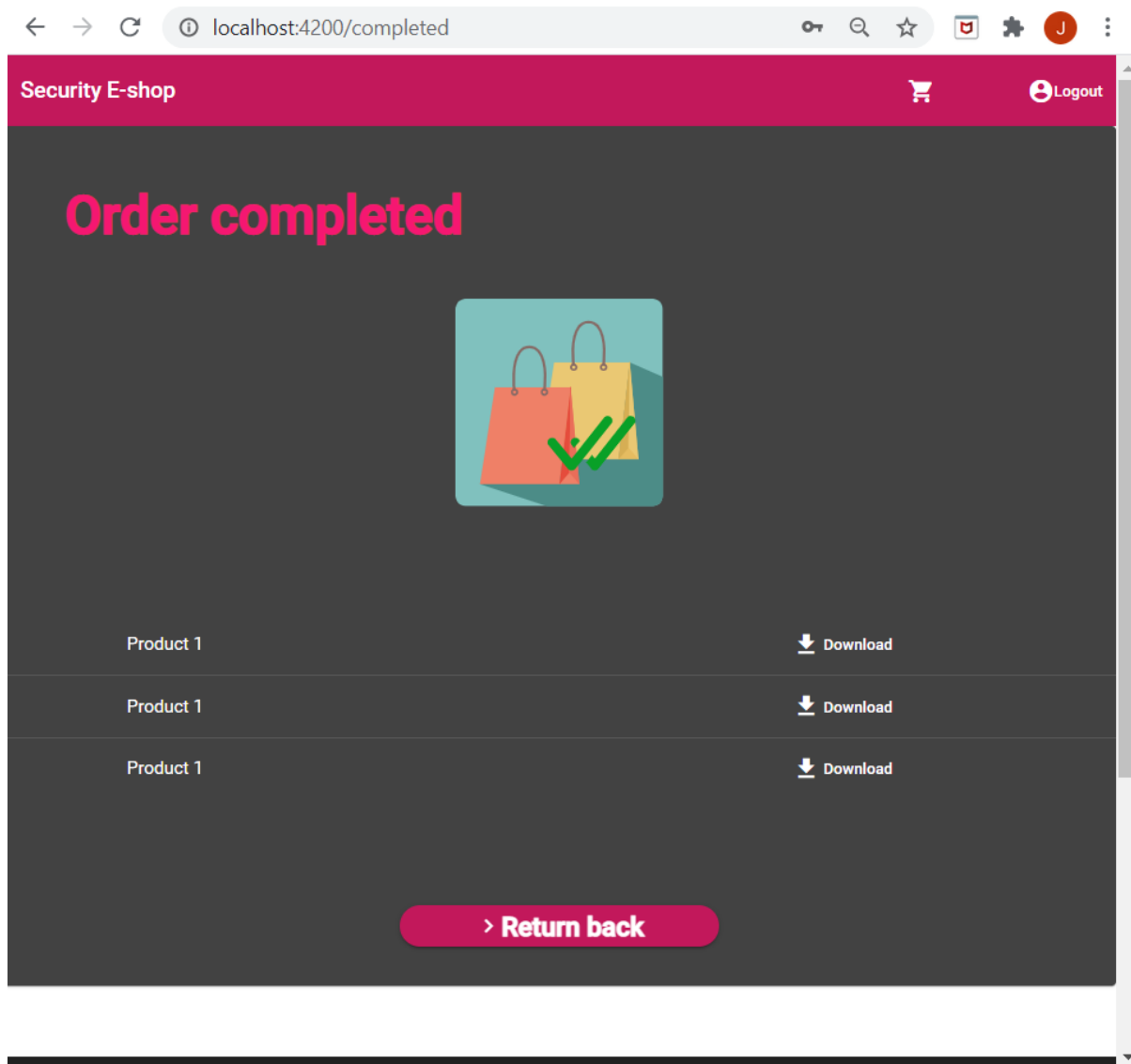
Name of card Date Security Code 0 / 3

Card number Security code CVV/CVC Name Expiry Date

**Price to pay in €**  
30.95

> Finish order

Obrázok 18: Možnosť podporiť e-shop



**Obrázok 19: 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 <b>Change</b>	email@e <b>Change</b>
5	janko	janko@uniba.sk	Jan <b>Change</b>	email@e <b>Change</b>
3	jan	jan1@stuba.sk	Jan <b>Change</b>	email@e <b>Change</b>
6	racek1	racekjan@racekpro1.sk	Jan <b>Change</b>	email@e <b>Change</b>
16	perdek	perdek.jakub@gmail.com	Jan <b>Change</b>	email@e <b>Change</b>

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


Obrázok 20: 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 21: Vyhľadávanie používateľa

Podľa rozhrania na obrázku 22 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

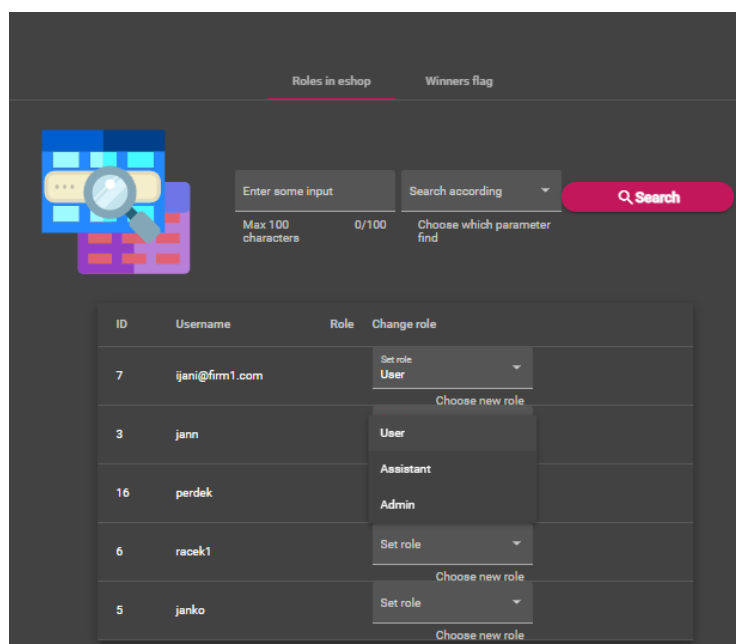
Description



Obrázok 22: Správa produktov

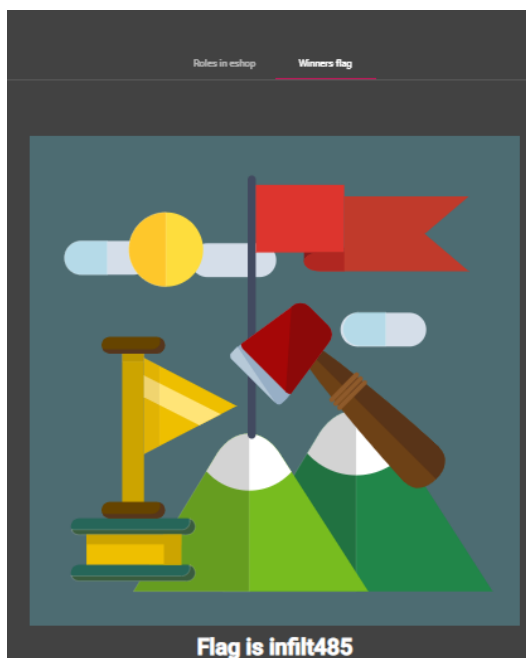
## Správa rolí používateľov

V ďalšom okne má používateľ s administrátorskými právami možnosť spravovať roly ostatných používateľov. Kliknutím na jeden z účtov a potom na pole Zmeniť úlohu môže správca priradiť rolu ďalšiemu používateľovi: bežný používateľ, asistent alebo správca.



Obrázok 23 Možnosť zmeny užívateľských rolí

V tejto časti systému sa nachádza aj flag, ktorý by sa útočník v systéme mal pokúsiť získať. Ak sa útočníkovi podarilo prebiť do časti pre zmenu rolí používateľa, uvidí flag z obrázku nižšie a jeho štítok.



Obrázok 24 Flag ktorý je potrebné získať

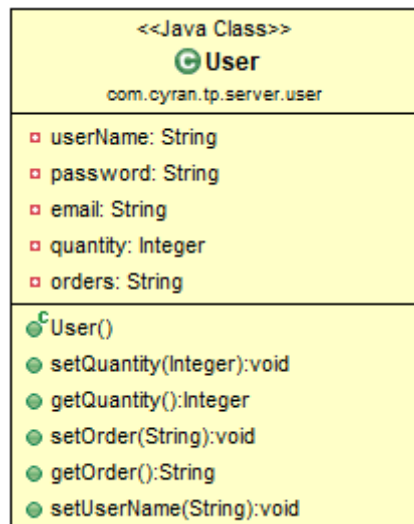
## Server a riadiaca časť systému

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.

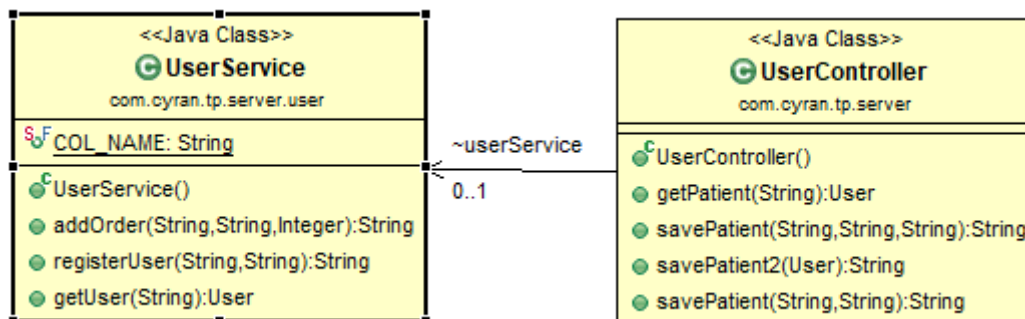
Na ďalšom diagrame tried môžeme vidieť hlavné triedy, z ktorých každá predstavuje jednu zo základných entít databázy.



Obrázok 25 Diagram základných tried



Obrázok 26 Trieda User entity



Obrázok 27 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 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

### 3.3 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 zaplatenia zmenením odoslaných informácií na backend
- Ukradnutie produktu prístupom do adresára s produktami
- SQL injekcia pre zmenu emailu admina
- SQL injekcia pre získanie záznamu z Whois s najväčším počtom zraniteľností a získanie bližšieho popisu k nim – záznam o security eshope

#### 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

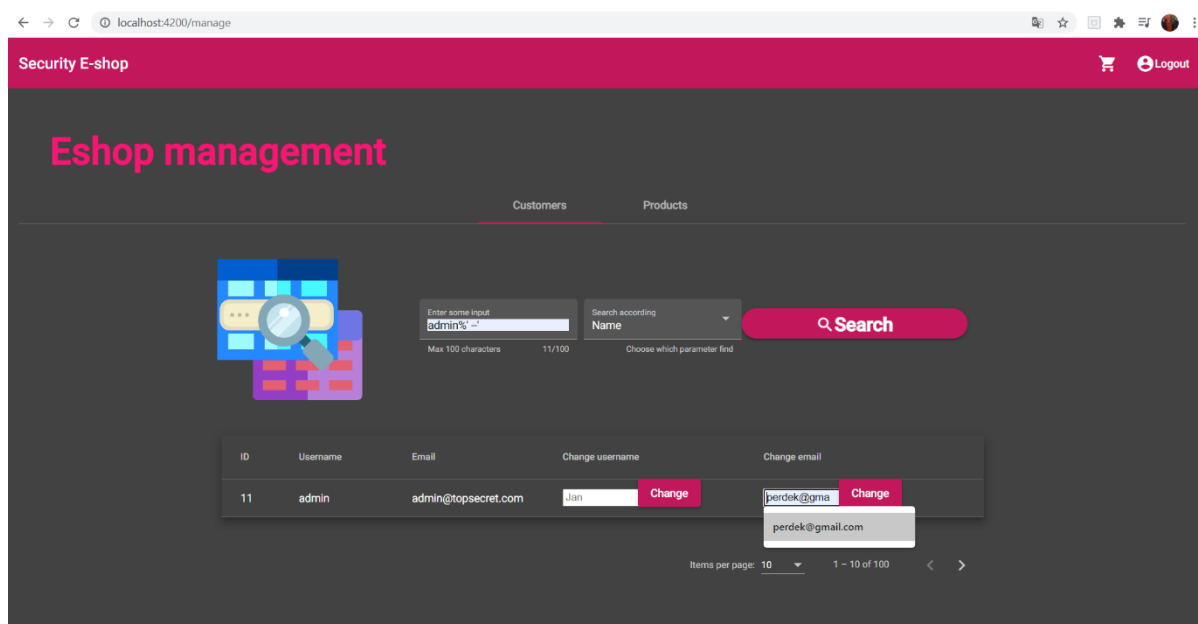
Útočník prehľadá možné adresy kde by sa súbory mohli nachádzať a stiahne potrebné súbory z nich. Je potrebné aby tieto adresáre boli pre útočníka prístupné.

#### SQL injekcia pre zmenu emailovej adresy admina

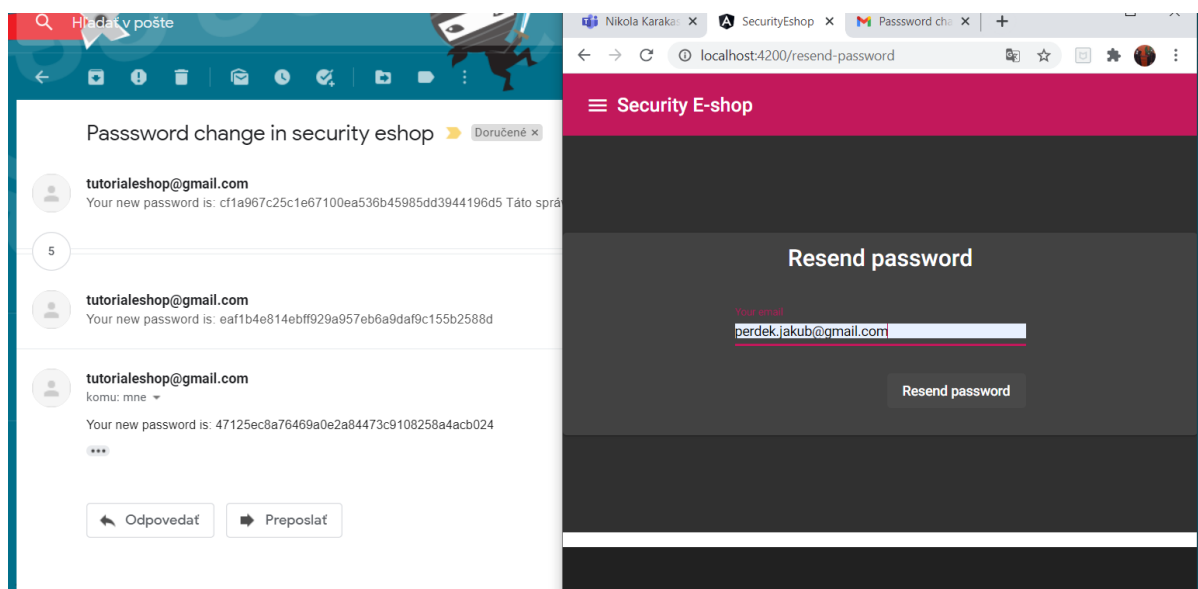
Pri vypisovaní všetkých používateľov v časti systému určenej pre pracovníka eshopu bude účet s oprávneniami správcu vynechaný. SQL dopyt, ktorý vypíše všetkých používateľov, je nasledovný:

*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.



Obrázok 28: Aplikovanie SQL injekcie



Obrázok 29: Generovanie a poslanie hesla na email pri jeho strate

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 privilégia 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 29 a 30 popisujú uvedený implementovaný útok.

## SQL injekcia pre získanie informácií z whois

Vytvorili sme aj komplexnú injekciu, ktorá vyžaduje väčšie úsilie. Vo whois aplikácii nie je realizovaná a pravdepodobne vzhľadom na účel aplikácie ani nebude sprístupnená funkcionality pre agregáčnejšie funkcie umožňujúce napríklad získať doménu s najväčším počtom zraniteľností a podobne. Útočník na základe pokročilejšej SQL injekcie nechá vyhľadať záznam najväčším počtom zraniteľností. Pri SQL dopyte používame funkciu one, takže bude musieť použiť LIMIT 1 v príkaze. Rovnako jediný vstup z ktorého sa dá urobiť injekcia je ohraničený znakmi % a '. Pre získanie ostatných dát musí ukončiť prvý príkaz a začať písať druhý s agregáčnou funkciou, a to tak že vráti len jeden výsledok. Príklad takéhoto príkazu môže vyzeráť nasledovne:

```
a%' OR 1=1;
```

```
SELECT * FROM whois, (  
    SELECT COUNT(vulnerabilities.reference_record_id) AS count, whois.id AS ww  
    FROM whois  
    LEFT JOIN vulnerabilities ON whois.id = vulnerabilities.reference_record_id  
    GROUP BY whois.id  
    ORDER BY count DESC  
    LIMIT 1  
) ww  
WHERE ww = whois.id  
LIMIT 1 --'
```

## 3.4 Logovanie v aplikácii

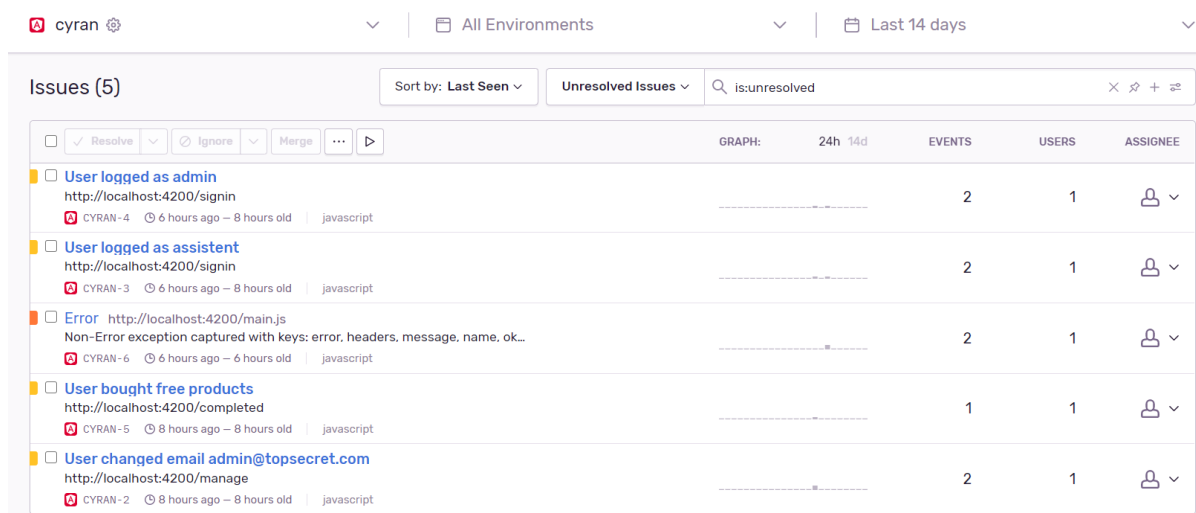
Do aplikácie sme zapracovali aj logovanie s použitím služieb Sentry. Logovanie má veľký význam, hlavne v rámci používateľského prieskumu. Očakávame identifikáciu potencionálnych chýb, ale hlavne možnosť reálne zachytiť pokrok používateľa pri realizácii scenárov. Význam logovania je:

- Pre možnosť zachytiť pokrok používateľa
- Pre odhalenie chýb, ktoré vzniknú pri používaní aplikácie
- Pre možnosť porovnať výsledné hodnoty z prieskumu s reálnym používaním aplikácie
- Pre možnosť sťažiť útočníkovi infiltráciu – za odhalenie môže byť aplikovaný bodový postih

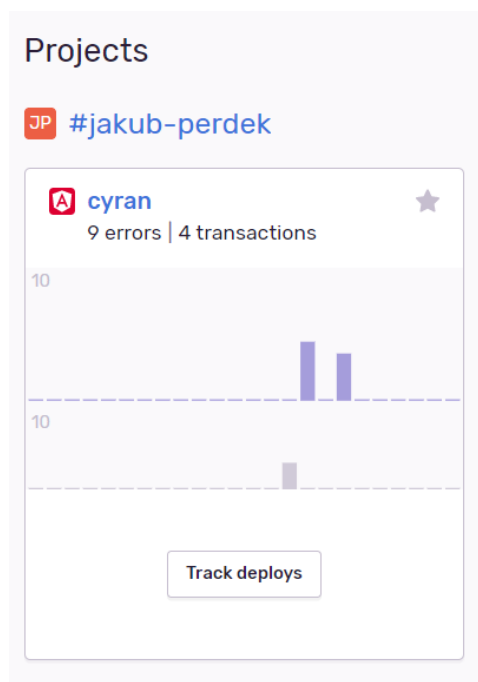
Developérsky plán v Sentry umožňuje v čase písania dokumentácie prijať až 5000 chybových, varovných prípadne iných správ a následne za pomoci knižnice tretej strany napísanej v jazyku python je možné tieto logy exportovať do csv súboru. Knižnica má názov sentry2csv.

Vytvorili sme varovné správy umožňujúce identifikovať, či útočník získal prístup k účtu user alebo admin. Ďalej, či bola zmenená emailová adresa v účte pre používateľa admin. Okrem toho sme ešte v rámci kúpy produktu vytvorili správu informujúcu, že používateľ obišiel možnosť zaplatiť za produkty, aj napriek tomu, že BurpSuite tieto súbory ihneď identifikuje a prístup priamo k nim takúto správu nevyvolá.

Okrem toho logujeme aj prípadné chyby. Ručný test potvrdil, že v prípade výpadku databázy tieto správy sú naďalej logované.



Obrázok 30: Zaznamenané logy



Obrázok 31: Projekt v sentry.io

Správy sú odosielané z aplikácie a následne zachytávané a zobrazované v projekte ako je zobrazené na obrázku 31. Vytvorený projekt cyran v rámci služieb sentry.io zobrazuje obrázok 32. Výsledný súbor so získanými logmi je zobrazený na obrázku 33.

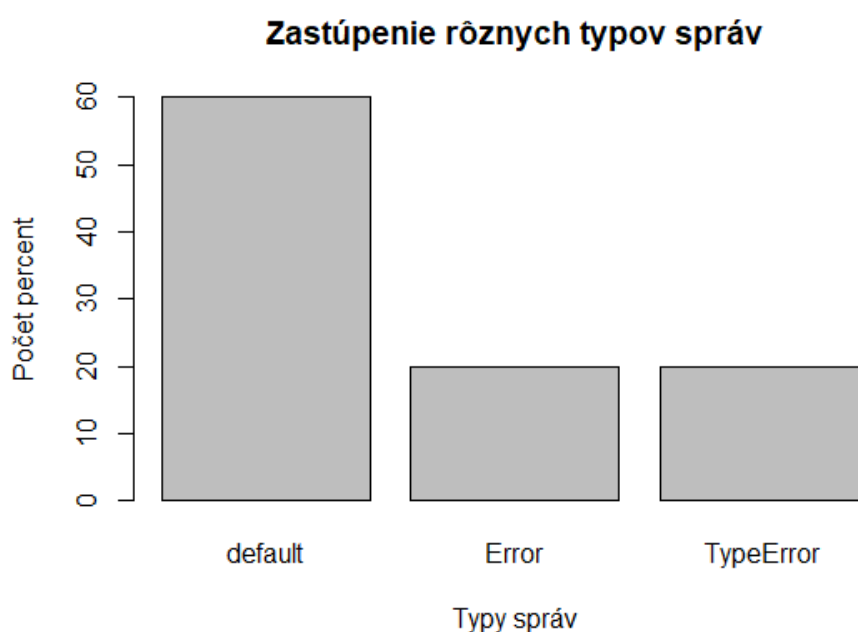
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
1	Error,Location,Details,Events,Users,Notes,Link																
2																	
3	default,http://localhost:4200/signin,User logged as assistant,2,1,,https://sentry.io/organizations/jakub-perdek/issues/2300743017/																
4																	
5	Error,http://localhost:4200/main.js,"Non-Error exception captured with keys: error, headers, message, name, ok...",2,1,,https://sentry.io/organizations/jakub-perdek/issues/2300848250/																
6																	
7	default,http://localhost:4200/completed,User bought free products,1,1,,https://sentry.io/organizations/jakub-perdek/issues/2300754646/																
8																	
9	default,http://localhost:4200/signin,User logged as admin,1,1,,https://sentry.io/organizations/jakub-perdek/issues/2300745018/																
10																	
11	default,http://localhost:4200/manage,User changed email admin@topsecret.com,2,1,,https://sentry.io/organizations/jakub-perdek/issues/2300710095/																
12																	

Obrázok 32: Získané logy vo formáte csv

## Analýza dát zo Sentry

Po skončení používateľského testovania sme pomocou skriptu získali reporty od používateľov, ktoré sa zaznamenali do Sentry. Výsledné údaje obsahovali niekoľko stĺpcov. Prvým bol typ záznamu. Mohla to byť bežná varovná správa označovaná ako východzia alebo rôzne druhy chýb. Nasledovala lokácia webovej stránky na ktorej používateľ vyvolal udalosť z ktorej vznikol report. Tretím v poradí boli detailné informácie popisujúce report. Pri varovnej

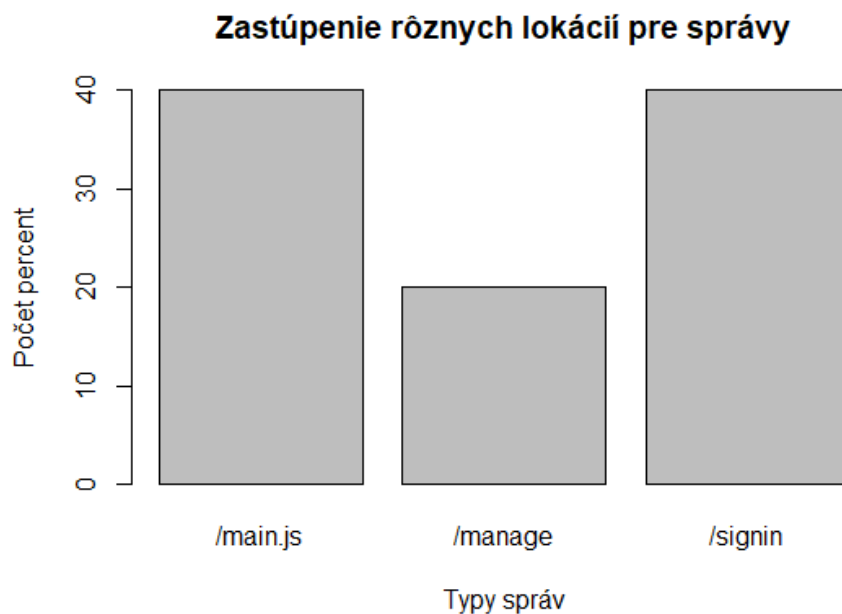
správe to bol obsah tejto správy. Napríklad obsahom bolo, že sa používateľ prihlásil ako admin. Ďalšie dva stĺpce boli číselné. Prvý z nich obsahoval informáciu o počte udalostí s konkrétnym typom záznamu. Druhý identikoval počet jedinečných používateľov, od ktorých sa konkrétny report vygeneroval. Súbor obsahoval ešte stĺpce ako poznámky alebo link na stránku zo Sentry, ale tie z hľadiska vyhodnotenia nemali význam, keďže poznámky neboli zaznamenané žiadne a link je z hľadiska spracovania zbytočný. Uvedené stĺpce sme podrobili analýze a následne sme ich aj vizualizovali.



**Obrázok 33: Zastúpenie rôznych typov správ**

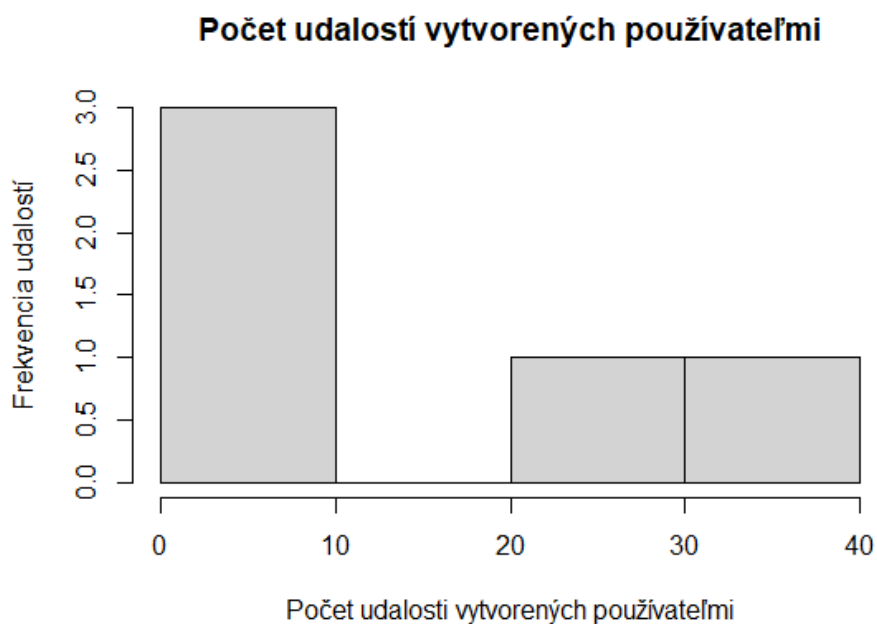
Informácie o akciách používateľa tvorili 60 percent. Zvyšných štyridsať percent tvorili chyby vzniknuté pri používaní aplikácie. Boli zapríčinené chybou v prehliadači používateľa. Polovica percent z týchto chýb boli typové chyby.

Reporty boli generované z rôznych stránok frontendu. Najviac udalostí bolo generovaných po prihlásení používateľa a z hlavného javascriptovského súboru, ktorých bolo až 40 percent. Tie druhé chyby vznikli v javascriptovom súbore. Udalosti pri prihlásení tvorili dva základné súčasti scenárov ako vzniknutie do účtu asistenta v obchode a nakoniec aj admina. Zvyšných dvadsať percent pochádzalo s manažérskeho prostredia asistenta v eshope, kde bola generovaná udalosť zmena emailu administrátora pomocou SQL injekcie.



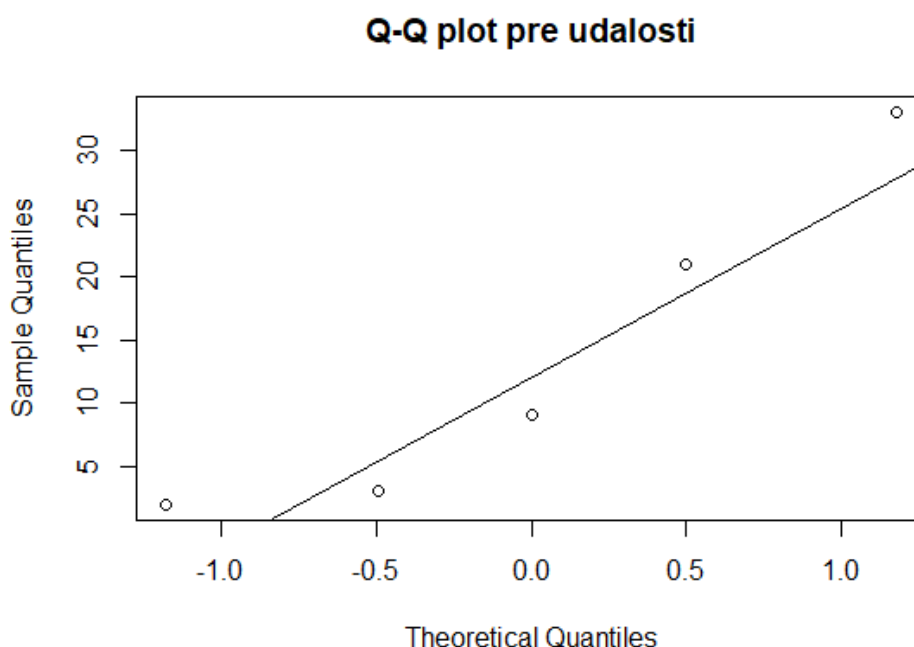
**Obrázok 34: Zastúpenie rôznych lokácií**

Ďalej sme vyhodnotili frekvencie pri jednotlivých počtoch udalostí. Konkrétny report sa vygeneroval v 3 prípadoch maximálne v 10 kusoch. Pri veľkosti od 20 do 30 kusov to bolo len pri jednom type reportu. Rovnako jeden typ reportu mal frekvenciu od 30 do 40 kusov. Používatelia pri riešení na tomto úseku pravdepodobne nevedeli ako pokračovať. Najviac frekventovanou udalosťou bol jeden druh chyby a hneď po nej to bolo prihlásenie do účtu asistenta v eshope.



**Obrázok 35: Počet udalostí vygenerovaných používateľmi**

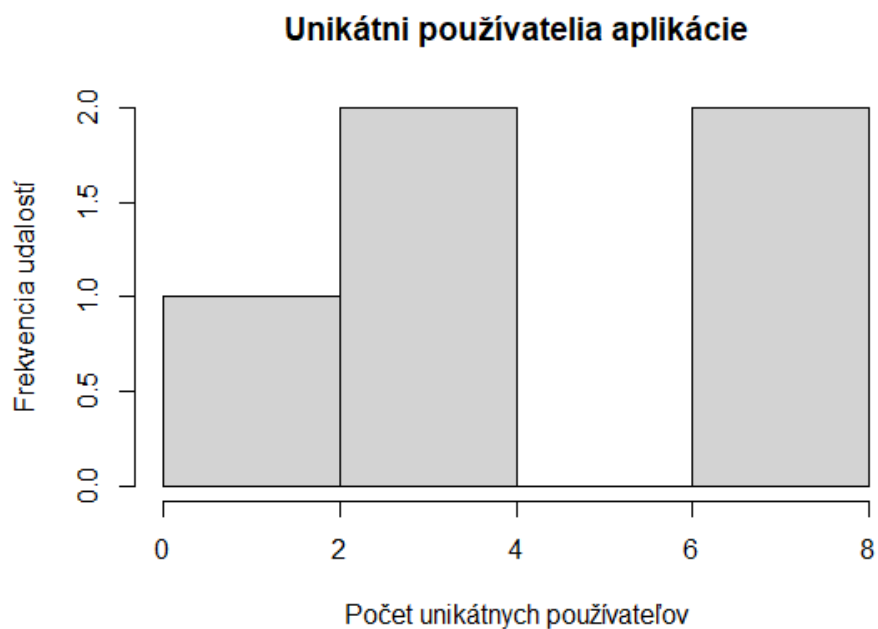
Pri udalostiach nás zaujímal aj ich rozdelenie. Vytvorili sme preto QQplot a na základe okometrickej metódy sme usúdili, že je to normálne rozdelenie. Následne sme na finálne potvrdenie tohto predpokladu použili Shapiro-Wilkov test normálnosti. V tomto teste vyšlo  $W = 0.96307$ ,  $p\text{-value} = 0.7982$ , pričom  $p$  bolo vysoké. Dáta sú normálne ak  $p > 0.05$ . V tomto teste vyšlo  $0.7982 \gg 0.05$ , čo potvrdzuje, že dáta sú normálne. Netreba zabudnúť, že test bol realizovaný iba na piatich reportovacích správach.



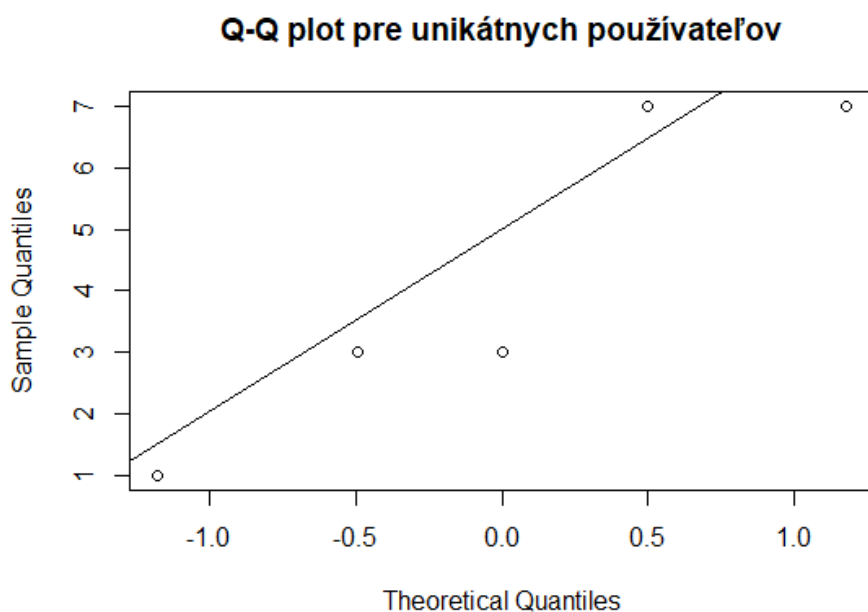
**Obrázok 36: QQ plot pre udalosti**

Analyzovali sme aj unikátnych používateľov. Zároveň informácia o nich je veľmi dôležitou kvôli prehľadu o počte zúčastnených hlavne vzhľadom na počet generovaných udalostí. V dvoch prípadoch sa vygenerovali 2 udalosti. V prvom prípade pre 2 až 4 používateľov a v druhom pre 6 až 8 používateľov. Jedna udalosť sa vygenerovala 0 až 2 používateľom. Opäť aj v tomto prípade chybová udalosť a vniknutie do účtu asistenta boli časté udalosti.

Aj v prípade unikátnych používateľov sme testovali či dáta sú normálne. Na základe okometrickej metódy boli niektoré body viditeľne vzdialené od priamky v diagrame. Testovanie Shapiro-Wilksovou metódou však aj v tomto prípade potvrdilo normálnosť dát. Hodnoty testu boli  $W = 0.89495$ ,  $p\text{-value} = 0.4064$ . Hodnota bola menšia ako v predchádzajúcom prípade ale stále mnohonásobne väčšia ako 0.05. Analyzovaných reportov aj v tomto prípade bolo len 5.



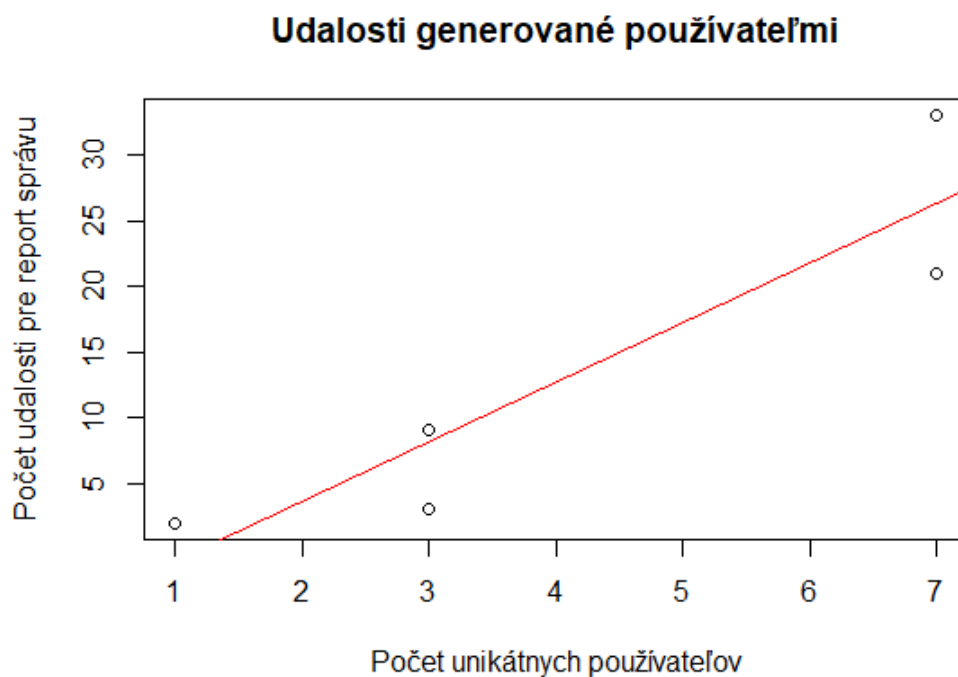
**Obrázok 37: Unikátni používatelia aplikácie**



**Obrázok 38: QQ plot pre unikátnych používateľov**

Finálnym vyhodnotením bola závislosť unikátnych používateľov od udalostí. Zostrojili sme lineárny model a preň aj graf. Body od zostrojenej priamky boli mierne vzdialené. Pri analýze modelu sa aj potvrdilo, že vzdialenosť bodov je badateľná. Hodnota  $p$  vyšla 0.0274, čo je menej ako 0.05 a postačuje to na zamietnutie nulovej hypotézy, ale reálne by táto hodnota mala byť niekoľkonásobne menšia. Determinačný koeficient vyšiel 0.844. Tento výsledok

potvrdil, že model dobre zachytáva vlastnosti dát. Táto hodnota ale zvykne kolísať pri väčšom množstve dát. V našom prípade bolo analyzovaných len 5 reportov.



**Obrázok 39: Udalosti generované používateľmi**

```

Coefficients:
              Estimate Std. Error t value Pr(>|t|)
(Intercept)  -5.417      5.428  -0.998   0.3918
Users         4.528      1.122   4.035   0.0274 *
---
Signif. codes:  0 '***' 0.001 '**' 0.01 '*' 0.05 '.' 0.1 ' ' 1

Residual standard error: 6.022 on 3 degrees of freedom
Multiple R-squared:  0.8444,    Adjusted R-squared:  0.7926
F-statistic: 16.28 on 1 and 3 DF,  p-value: 0.02737

```

**Obrázok 40: Výsledky pre vyhodnotenie lineárnosti modelu**

***Základné údaje o používateľoch:***

Priemer je: 4.2  
 Maximálna hodnota je: 7  
 Minimálna hodnota je: 1  
 Rozsah je: 6  
 Variancia je: 7.2  
 Modus je: 7  
 Medián je: 3

***Základné údaje o udalostiach:***

Priemer je: 13.6  
 Maximálna hodnota je: 33  
 Minimálna hodnota je: 2  
 Rozsah je: 31  
 Variancia je: 174.8  
 Modus je: 2  
 Medián je: 9



# Analýza dát z Google forms

Spätnú väzbu používateľa zadali aj do google forms dotazníkov.

**Počet meraní: 6**

**Úlohy:**

1. Prelomenie hesla pre používateľa user.
2. Získanie administrátorských údajov pomocou SQL injekcií.
3. Získanie vlajky.
4. Odoslanie prvého requestu pri pokuse o ukradnutie produktu.
5. Zmenenie hodnôt v druhom requeste na 0.
6. Získanie súboru pomocou URL adresy.

**Úspešnosť účastníkov:**

0. Celý kurz prešlo 50% účastníkov.
1. Heslo používateľa user prelomilo 100% účastníkov.
2. Administrátorské údaje pomocou SQL injekcií získalo 83.3% účastníkov.
3. Vlajku získalo 100% účastníkov
4. Prvý request pri pokuse o ukradnutie produktu odoslalo 100% účastníkov.
5. V druhom requeste zmenilo hodnoty na 0 33.3% účastníkov.
6. Súbory pomocou zmeny URL získalo 33.3% účastníkov.

**Vyhodnotenie:**

Môžeme vidieť že najväčšie problémy mali účastníci s úlohami 5 a 6, ktoré nespĺnilo až 67.7 % z nich.

**Náročnosti úloh:**

Úloha	Počet hlasov				
	Veľmi ľahké	Ľahké	Stredne ťažké	Ťažké	Veľmi ťažké
7. Prelomenie hesla pre používateľa user.	2	2	2	0	0
8. Získanie adminových údajov pomocou SQL injekcií.	1	3	1	1	0
9. Získanie vlajky.	2	2	2	0	0
10. Odoslanie prvého requestu pri pokuse o ukradnutie produktu.	1	3	1	1	0
11. Zmenenie hodnôt v druhom requeste na 0.	3	0	2	0	1
12. Získanie súboru pomocou URL adresy.	2	0	3	0	1

Obrázok 41: Náročnosti úloh

**Vyhodnotenie:**

Z tabuľky môžeme vidieť že používatelia hodnotili, ako najnáročnejšie, úlohy 5 a 6 a ako najjednoduchšie úlohy 1 a 3.

**Trvanie úloh**

Úloha	Počet hlasov					
	1-5 min.	5-10 min.	10-15 min.	15-20 min.	20-30 min.	30-45 in.
1. Prelomenie hesla pre používateľa user.	1	3	0	1	0	1
2. Získanie adminových údajov pomocou SQL injekcií.	1	2	2	1	0	0
3. Získanie vlajky.	2	4	0	0	0	0
4. Odoslanie prvého requestu pri pokuse o ukradnutie produktu.	1	4	1	0	0	0
5. Zmenenie hodnôt v druhom requeste na 0.	4	1	1	0	0	0
6. Získanie súboru pomocou URL adresy.	3	3	0	0	0	0

**Obrázok 42: Trvanie úloh****Vyhodnotenie:**

Z tabuľky môžeme vidieť, že najkratšie trvali úlohy 3 a 6 a jednému používateľovi trvala úloha 1 od 30 do 45 min.

**Celkové trvanie kurzu:**

20, 35, 40, 50, 65, 95 minút.

**Poznámky od používateľov:**

1. Úlohy skor nefungovali (teda posledne dve), odoslanie objednávky nepreslo, dostavam CORS missing allow header, pretože ten request nikde neprejde po 5 minútach čakania. Inak boli úlohy vpohode, ale trochu asi jednoduché. Urcite by som uvítal viac úloh, prípadne možno nie tak jednoznačné, že tam pridať trochu zakerných vecí :) Zvyšok feedbacku posiadam na xperdek@stuba.sk.
2. Všetko bolo pekne spracované a išlo to pomerne plynulo. Úlohy mierne sťažila dokumentácia, ktorá by mohla byť o niečo viac jednoznačnejšia. Za veľký problém

považujem setup Burp Suiu a určite by som niekde zakomponoval poznámku, že v prípade, ak nám nejde aj po vypnutí interceptu pripojiť sa na akúkoľvek stránku, tak stačí zmeniť port napríklad 8085. S týmto som strávil pekných pár minút, ale našťastie mi Jakub Pedrek a Nikola Karakaš boli ochotní pomôcť. Taktiež je vhdoné niekedy v dokumentácii pripomenúť, na ktorom lokálnom porte sa nachádza emailová schránka, keďže sa mi to v priebehu riešenia "podarilo úspešne" zabudnúť. Inak všetko hodnotím veľmi dobre a práca tímu sa mi naozaj páči.

3. lebo bolo treba sprístupniť port 8080 aj keď sa pisalo na dockeri, že not accessible, adresy na localhost a nie na 192.168....
4. Adresy sú fixnuté na localhost. Ja som spustil docker na inej IP a z druhého PC som sa na to chcel prihlásiť, ale nešlo to. SqlMap nefungoval, backend vracal 500-ky.

### **Vyhodnotenie:**

Z poznámok môžeme usúdiť že:

Problémy z úlohami 5 a 6, ktoré sme si všimli z predchádzajúcich hodnotní môže byť spôsobené technickými problémami alebo zlým pochopením úloh. Dokumentácia, hlavne príručka pre používateľov, by mohla byť viac prepracovaná a detailnejšia. Mohla by obsahovať informáciu na ktorom porte sa nachádza emailová schránka.

### **Celkové vyhodnotenie:**

Najväčší problém, ktorý sme z tejto spätnej väzby zaznamenali bol že niektorí používatelia mali problém dokončiť úlohy 5 a 6 kvôli technickým problémom špecifikovaným v poznámkach od používateľov. Ďalej môžeme z hodnotenia používateľov vidieť že úlohy 1 a 3 boli priveľmi ľahké. Používatelia by ocenili väčšie množstvo úloh.

## 3.5 Posudky na prototyp tímu č. 19

Na základe spätnej väzby z používateľského testovania sme vypracovali posudok podľa určeného protokolu. Rovnako sme zaslali posudky priamo na vypracovanie používateľom z používateľského testovania, ktorí boli účastníci bezpečnostného semináru. Niektorí nám neodpovedali. Od dvoch používateľov sa podarilo získať vyplnený protokol.

### Posudok na základe používateľského testovania

#### 1. Študenti bezpečnostného semináru: Posudok na prototyp tímu č. 19: CYRAN

---

##### 1.1. Úvod

Testovanie aplikácie vykonali študenti bezpečnostného semináru a každý z nich pridal spätnú väzbu a svoje postrehy. Projekt sa im veľmi páčil svojou originalitou ale rovnako aj kritizovali objavené nedostatky. Hodnotili, respektíve sa vyjadrovali ku kvalite výstupu, jednotlivým scenárom, kvalite používateľskej príručky a úrovni náročnosti, prípadne aj návrhu scenárov

##### 1.2. Hodnotenie prototypu

Študenti hodnotili jednotlivé scenáre, ktoré sa zároveň snažili prejsť. Rôzni používatelia mali rôznu úroveň schopností a znalostí z penetračného testovania. Niektorí zhrnuli iba identifikované chyby, ktoré ich pri riešení spomalili. Boli nimi nefunkčnosť vedľajšieho scenáru kvôli problémom s autentifikáciou do Firebase databázy, chýbajúce detaily v používateľskej príručke a podobne. Používatelia žiadali upraviť aj otázky v Google Forms pre možnosť lepšej spätnej väzby. Svoje postrehy zhrnuli v svojich emailoch.

Jeden používateľ sa vyjadril o priamočiarosti úloh a dobrým zakomponovaním šifrovaním hesla a potrebou vynásť sa pri jeho prelamaní. Zároveň by chcel viac podobných úloh nútiacich rozmyšľať. Sám poskytol aj nejaké návrhy pre uskutočnenie. Očakával aj nejakú základnú ochranu na frontende proti SQL injekciám.

Ďalší používateľ mal problém s opísanými chýbajúcimi detailami v používateľskej príručke, ale po kontaktovaní členov tímu sa podarilo všetko vyriešiť. K samotnému riešeniu sa vyjadril, že je to dosť dobré.

### 1.3. Hodnotenie práce tímu

Študenti sa nezaoberali prácou tímu, ale jednotliví členovia im počas testovania v prípade problémov asistovali poskytovaním rád a ďalšej pomoci. Najčastejšie problémy boli z BurpSuitom a chýbajúcou informáciou o lokálnom emailovom klientovi v používateľskej príručke, aj napriek tomu, že inštalačná príručka tento detail obsahovala.

### 1.4. Zhodnotenie

Aplikácia sa študentom páčila a pozitívne ju hodnotili. Zároveň poukazovali na nefunkčnosť jedného zo scenárov a nekompletnosť setupu BurpSuite nástroja spolu s chýbajúcou informáciou o lokálnom emailovom klientovi, ktorá bola spomenutá v inštalačnej príručke. Úlohy im prišli intuitívne, priamočiare, s originalitou zapracovania ale chceli by ich viac a s väčším sťažením riešenia týchto úloh. Väčšina študentov, ktorá produkt testovala dokončila hlavný scenár.

## **Posudky jednotlivých testerov z bezpečnostného semináru**

### 2. Účastník 1:

#### **Posudok na prototyp tímu č. 19: CYRAN**

---

#### 2.1. Hodnotenie prototypu

Celkovo si myslím, že tento projekt má potenciál, študenti dokázali navrhnuť celkom slušný prototyp, ktorý viac menej fungoval, aj keď bolo odhalených pár chýb, ktoré ale nebude zložité opraviť. Základný prototyp je dosť dobrý, aj keď ja by som uvítal viac rôznorodých úloh, ktoré treba v tejto hre splniť. Možno by sa tam hodili viaceré úrovne obtiažnosti. Inak bol prototyp solídny a dobre pripravený. Inštalácia bola jednoduchá a dokumentácia obsahovala zväčša dostatočné inštrukcie na splnenie potrebných krokov a úloh.

## 2.2. Zhodnotenie

Výsledok práce tímu je veľmi dobrý a splňa ciele, ktoré boli v tomto projekte určené. Implementácia je na veľmi dobrej úrovni, ale v niektorých častiach je úroveň nižšia, prípadne niektoré časti nie sú plne dokončené.

Pár nedostatkov informácií bolo už pri inštalácii projektu na vlastnom stroji, v tejto oblasti je určite možné vylepšiť dokumentáciu a pridať aj návody na riešenie bežných problémov s nasadením. Pri niektorých úlohách boli inštrukcie nedostatočné, a bolo potrebné investigovať problémy, ktoré bránili v splnení úlohy. Jedna úloha nefungovala vôbec, zdalo sa, že backend aplikácie nemá implementované potrebné API volanie.

Úlohy sa mi páčili, a niektoré by bolo lepšie zťažiť, a pridať ešte pár ďalších, aby hra trvala trochu dlhšie. Prípadne by som ocenil viac kreativity, aby sa z úloh študent naučil zaujímavé techniky, ktoré sa využívajú pri exploitatcii webových služieb.

## 3. Účastník 2 (tím č. 15): Posudok na prototyp tímu č. 19: CYRAN

---

### 3.1. Hodnotenie prototypu

Tím Y sa zaoberal projektom zameraným najmä na vytvorenie interaktívnej hry poukazujúcej na riziká a nebezpečenstvá spojené s manažovaním a tvorbou e-shopu. Pri testovaní som postupoval podľa dodanej príručky. Pripomienky k nej sme dodal už v čase testovania, t.j. Apríl 2021. V konečnom dôsledku sa mi podarilo všetko správne a bez väčších problémov nainštalovať. Musím zhodnotiť, že predvedený produkt na mňa pôsobil zaujímavo a jeho edukatívna forma priniesla svoje ovocie v podobe nadobudnutia nových znalostí. Pozitívne hodnotím najmä prístup, akým tvorcovia vysvetľujú danú problematiku. Jediným negatívom spojeným s projektom boli časte gramatické chyby, ktoré sa časom určite podarilo/podari odstrániť.