Nástroj pro správu databáze teroristických útoků

Michal Vávra

Bakalářská práce
2023

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
Ústav informatiky a umělé inteligence

Akademický rok: 2022/2023

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Michal Vávra**
Osobní číslo:	**A19473**
Studijní program:	**B3902 Inženýrská informatika**
Studijní obor:	**Softwarové inženýrství**
Forma studia:	**Prezenční**
Téma práce:	**Nástroj pro správu databáze teroristických útoků**
Téma práce anglicky:	**A Web Application for the Database Administration of Terrorist Attacks**

Zásady pro vypracování

1. Specifikujte požadavky na webovou aplikaci a uveďte technologie, které použijete.
2. Vytvořte návrh webové aplikace pro správu databáze teroristických útoků.
3. Implementujte navržené řešení v testovacím prostředí.
4. Přeneste data ze současného řešení do Vašeho.
5. Prověřte funkčnost a zabezpečení systému s jeho uživateli.
6. Zpracujte základní uživatelský manuál.

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam doporučené literatury:

1. MESSENLEHNER, Brian a Jason COLEMAN. _Building Web Apps with WordPress: WordPress As an Application Framework_. 2019. ISBN 9781491990087. Dostupné také z: https://search.ebscohost.com/login.aspx?direct=true&db=nlebk&an=2328775&scope=site
2. WORDPRESS/APACHE MOST WEAPONIZED WEB/APP FRAMEWORKS. _Computer Security Update_ [online]. 2020, **21**(4), 6 [cit. 2021-11-30]. ISSN 27681009. Dostupné z: https://search.ebscohost.com/login.aspx?direct=true&db=edsjsr&an=edsjsr.48597920&scope=site
3. ROBIN NIXON. _Learning PHP, MySQL_. 2021. ISBN 9781492093824. Dostupné také z: https://search.ebscohost.com/login.aspx?direct=true&db=nlebk&an=2971735&scope=site
4. MARKUS GRAY. _Beginning PHP: Master the Latest Features of PHP 7 and Fully Embrace Modern PHP Development_. 2018. ISBN 9781789535907. Dostupné také z: https://search.ebscohost.com/login.aspx?direct=true&db=edsebk&an=1862353&scope=site
5. FRANKE, Don. _Cyber security basics: protect your organization by applying the fundamentals_. [USA]: [Don Franke], 2016, 101 s. ISBN 9781522952190

Vedoucí bakalářské práce: **Ing. David Malaník, Ph.D.**
Ústav informatiky a umělé inteligence

Datum zadání bakalářské práce: **2. prosince 2022**
Termín odevzdání bakalářské práce: **26. května 2023**

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky
L.S.

doc. Ing. Jiří Vojtěšek, Ph.D. v.r.
děkan

prof. Mgr. Roman Jašek, Ph.D., DBA v.r.
ředitel ústavu

Ve Zlíně dne 7. prosince 2022

Prohlašuji, že

- beru na vědomí, že odevzdáním bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně;
- byl/a jsem seznámen/a s tím, že na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – bakalářskou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně, dne 24.5.2023

Michal Vávra, v.r.
podpis studenta

ABSTRAKT

Bakalářská práce se zabývá návrhem a implementací webové aplikace pro správu databáze teroristických útoků. V teoretické části je provedena rešerše existujících řešení, specifikace požadavků na webovou aplikaci, jsou popsány kroky pro návrh systému a technologie použité pro implementaci řešení. Praktická část se věnuje návrhu a implementaci konkrétního systému. Webová aplikace je vytvořena pomocí frameworku CodeIgniter s využitím databázového systému MySQL.

Klíčová slova: Systém pro správu databáze, Teroristické útoky, Webová aplikace, PHP, MVC, CodeIgniter

ABSTRACT

The bachelor thesis deals with the design and implementation of a web application for managing a database of terrorist attacks. The theoretical part includes a research study of existing solutions, specification of requirements for a web application, description of steps for system design, and the technology used for implementing the solution. The practical part focuses on designing and implementing a specific system. The web application is created using the CodeIgniter framework and utilizing the MySQL database system.

Keywords: Database management system, Terrorist attacks, Web application, PHP, MVC, CodeIgniter

Tímto bych chtěl poděkovat vedoucímu mé bakalářské práce Ing. Davidu Malaníkovi, Ph.D. za odborné rady a vedení práce.

Dále bych chtěl poděkovat zadavatelce Ing. Doře Kotkové, Ph.D. za přínosné konzultace během vývoje webové aplikace.

Prohlašuji, že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

OBSAH

ÚVOD

Teroristické útoky jsou nebezpečnou hrozbou vyskytující se po celém světě. Důvody k páchání teroristických útoků lze rozdělit do mnoha kategorií, které je možné zaznamenávat a s těmito informacemi dále pracovat. To vedlo k vytvoření tohoto systému, který bude za použití webové aplikace umožňovat správu databáze teroristických útoků.

Teoretická část bakalářské práce popisuje postup při návrhu a vývoji webové aplikace. Na úvod je vypracována rešerše existujících řešení, po které následuje specifikace požadavků systému pro správu databáze teroristických útoků. Jsou popsány nástroje určené pro sestavení návrhu webové aplikace, vysvětleny nejčastější útoky na webovou aplikaci a přínosy testování aplikace s uživateli. V poslední části jsou popsány technologie použité při vývoji aplikace, která je vytvořena ve frameworku CodeIgniter.

Praktická část se skládá z návrhu a implementace webové aplikace pro správu databáze teroristických útoků. Návrh aplikace obsahuje model případů užití, ke kterému jsou vytvořeny konkrétní scénáře, wireframe a popis navržené databáze. Implementační část řeší instalaci webové aplikace, přenesení dat ze současného řešení, zabezpečení a testování aplikace s koncovými uživateli. V závěrečné části je vytvořen uživatelský manuál.

I. TEORETICKÁ ČÁST

1 POSTUP VÝVOJE WEBOVÉ APLIKACE

Pro úspěšný vývoj a udržitelnost webové aplikace je zásadní správné navržení pracovních postupů k čemuž jsou využívány UML diagramy. Před samotnou implementací je nutné porozumět požadavkům zadavatele a na základě toho sestavit návrh celého systému. UML diagramy slouží k pohledu na systém z určitého úhlu. Navržené UML diagramy programátorům zajistí vše, co je potřebné k orientaci v daném řešení. Diagramy je možné sestavit jak na papír, tak za pomocí počítačových programů, jedním z nich je například Enterprise Architect. [1] Po dokončení návrhu aplikace následuje implementace, která je prověřena testováním s koncovými uživateli.

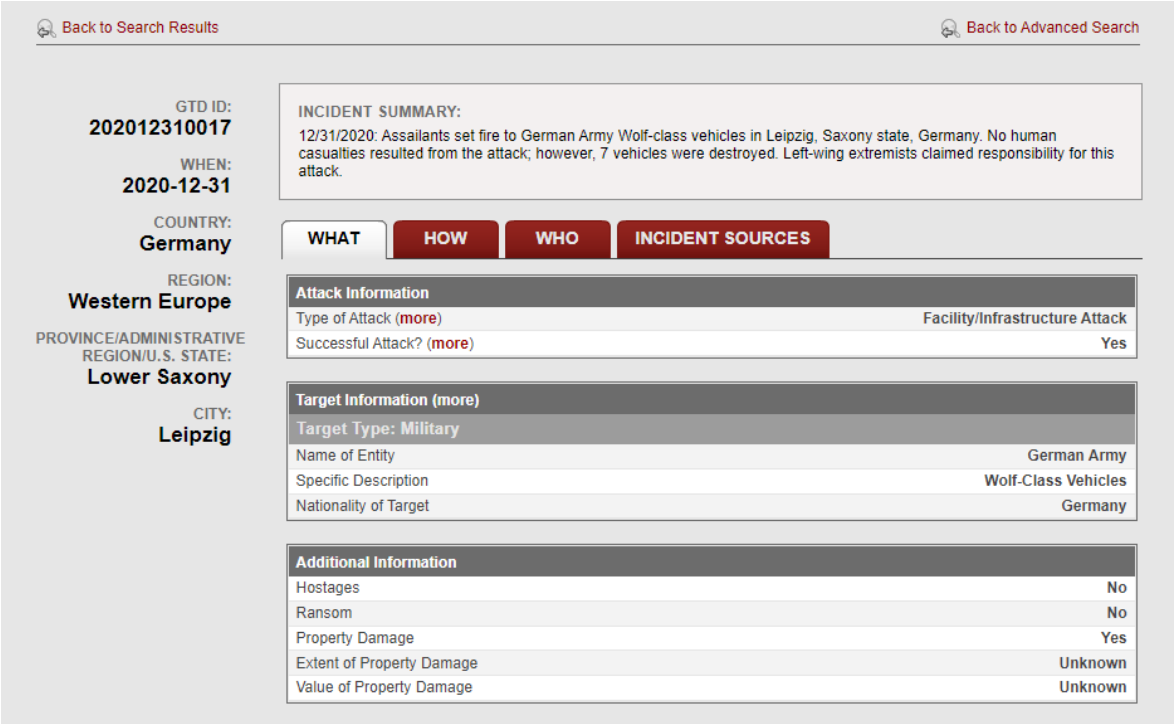
1.1 Rešerše

Organizace zabývající se sběrem a analýzou dat o teroristických útocích přináší významný přínos v boji proti terorismu. Sběr těchto dat má za cíl zlepšit bezpečnost a umožnit lepší porozumění této problematiky. Informace zaznamenávané těmito organizacemi se mohou lišit jejich úplností, kvalitou a dostupností. Existující systémy jsou často placené nebo úplně tajné. Je tedy obtížné najít systém, který by poskytoval aktuální informace o útocích, se kterými by bylo možné dále pracovat. Největší volně dostupná databáze, která zde bude popsána se nazývá Global Terrorism Database.

1.1.1 Global Terrorism Database

Global Terrorism Database [2] je volně přístupná databáze obsahující k dnešnímu dni záznamy o teroristických událostech po celém světě od roku 1970 do roku 2020. V těchto letech zaznamenali více než 200 000 případů a aktuálnější data budou zveřejněny později. U jednotlivých incidentů jsou k dispozici informace o datu a místě incidentu, použitých zbraní, povaze cíle, počtu obětí a útočnících. Informace jsou získávány z důvěryhodných zdrojů.

The National Consortium for the Study of Terrorism and Responses to Terrorism zveřejňuje tyto útoky prostřednictvím webu Global Terrorism Database ve snaze zvýšit porozumění teroristickému násilí, aby jej bylo možné snáze studovat a případně porazit. [2]



Obrázek 1. Global Terrorism Database – detail útoku [3]

Hlavní nevýhodou a důvodem proč Global Terrorism Database nelze využít pro práci zadavatele je neaktuálnost dat. Pro tým analytiků v čele s Ing. Dora Kotková, Ph.D. je důležitý přístup k aktuálním informacím, které budou obsahovat podrobné detaily o útocích. Analytici využívají data o útocích pro vytváření grafů (aktuálně řešeno v excelu) a analýz. Existující systémy nebyly pro tyto účely ideální, proto bylo zapotřebí vytvořit vlastní systém, který bude kromě správy dat umožňovat taky vytváření grafů a zobrazení útoků na mapě.

V rámci dřívější diplomové práce byl vytvořen systém, který měl za cíl naplnit potřeby zadavatele. Po implementaci ale došlo k zásadní změně požadavků na databázi, což vytvořilo potřebu na větší zásah do funkcionality celého systému napsaného v jazyce Java. Tento jazyk má na fakultě malé zastoupení programátorů, proto bylo od předělání tohoto řešení upuštěno. Následně vznikl nový požadavek na vytvoření systému v jazyce PHP, který bude implementován na základě nových požadavků.

Primární účel systému zůstal stejný, tedy umožnit analytikům zaznamenávat a spravovat data týkající se teroristických útoků. Databáze systému bude efektivně ukládat všechny potřebné informace. Mezi další požadované funkce webové aplikace patří vytváření grafů, zobrazení útoků na mapě a zobrazení informací o týmu.

1.2 Specifikace požadavků webové aplikace

Specifikace požadavků je důležitou součástí při tvorbě aplikací. Na základně kvality specifikace požadavků závisí úspěch celého projektu. V případě nepřesností ve specifikaci požadavků může nastat situace, kdy bude nutné předělat určitou část aplikace a na základě toho nemusí být zadání splněno v řádném termínu. [4]

Při vytváření systému pro správu databáze teroristických útoků je stěžejní vytvořit databázi, která bude efektivně ukládat záznamy a bude tak tvořit základ celého systému. Hlavním přínosem této databáze bude jednotné uložiště přístupné všem analytikům odkudkoliv a kdykoliv. Díky tomu budou mít analytici přístupnou vždy aktuální verzi databáze, která se bude spravovat pomocí webové aplikace.

Webová aplikace, stejně jako databáze bude vytvořena na základě specifikace požadavků zadavatele tak, aby byla zajištěna co nejjednodušší obsluha systému. Vytvořená databáze bude vycházet z excelového souboru, který se skládá z těchto sloupců: pořadí, země, město, rok, měsíc, datum, den v týdnu, typ měkkého cíle, detail typu měkkého cíle, teror, epicentrum útoku, modus operandi, detail modu operandi, detail výbušniny, ochranka, čas, peak, k útoku se přihlásili, počet mrtvých, počet zraněných, potenciál obětí, počet útočníků, jméno útočníka, pohlaví útočníka, věk útočníka, státní příslušnost útočníka, lokalita útoku vzhledem k bydlišti, původ (2. generace/rodiče) útočníka, propojení s jinými útoky, poznámky, odkaz, souřadnice, Maryland.

Dalším krokem bude návrh webové aplikace, ta se bude dělit na dvě části, a to uživatelská a administrativní. Tyto části budou mít přístupná data na základě uživatelských rolí. Administrativní část bude správcům databáze zajišťovat jednoduchou práci s daty, která se skládá převážně z přidávání, upravování a mazání záznamů. Uživatelská část bude zobrazovat úvodní stránku, grafy, novinky, kontakt, stránku „O nás“ a mapu, která bude přístupná pouze přihlášeným uživatelům.

1.3 Funkční požadavky

Funkční požadavky mají za úkol popsat chování výsledné aplikace. [5]

1.3.1 Neregistrovaný uživatel

- Neregistrovaný uživatel má možnost vyplnit registrační formulář, poté musí počkat na ověření adminem
- Neregistrovaný uživatel si může zobrazit úvodní stránku
- Neregistrovaný uživatel si může zobrazit grafy, které budou označeny jako veřejné
- Neregistrovaný uživatel si může zobrazit novinky
- Neregistrovaný uživatel si může zobrazit kontakt
- Neregistrovaný uživatel si může zobrazit stránku „O nás“

1.3.2 Registrovaný uživatel

- Registrovaný uživatel má zpřístupněné všechny možnosti jako neregistrovaný uživatel
- Registrovaný uživatel se po ověření adminem může přihlásit
- Registrovaný uživatel si může zobrazit veřejné grafy
- Registrovaný uživatel může vytvářet soukromé i veřejné grafy
- Registrovaný uživatel může zobrazit mapu útoků
- Registrovaný uživatel si může změnit osobní údaje
- Registrovaný uživatel si může změnit heslo

1.3.3 Správce

- Správce má zpřístupněné všechny možnosti jako registrovaný uživatel
- Správce má přístup do administrace
- Správce může nahrávat útoky z CSV souboru
- Správce může exportovat seznam útoků do excelové tabulky
- Správce může přidávat upravovat, mazat a filtrovat útoky
- Správce může přidávat upravovat a mazat novinky
- Správce může přidávat, upravovat, mazat a filtrovat epicentra, typy měkkých cílů, lokalita k bydlišti, modus operandi, města, země, barvy grafů

1.3.4 Admin

- Admin může vykonávat operace všech rolí
- Admin si může zobrazit všechny registrované uživatele
- Admin může ověřit nebo odebrat uživatele
- Admin může měnit role uživatelů
- Admin může vyhledat uživatele podle emailu

1.4 Nefunkční požadavky

Nefunkční požadavky se využívají k doplnění funkčních požadavků. Určují vlastnosti potřebné pro spolehlivý a bezpečný chod aplikace. [6]

- Aplikace bude využívat skriptovací programovací jazyk PHP
- Aplikace bude využívat relační databázový systém MySQL
- Aplikace bude využívat framework CodeIgniter
- Aplikace bude odolná vůči XSS a SQL Injection
- Aplikace bude bezpečně uchovávat hesla
- Aplikace bude podporovat webové prohlížeče Google Chrome, Mozilla Firefox, Opera, Microsoft Edge

1.5 Model případů užití

Model případů užití [7] se v jazyce UML používá pro zobrazení, jakým způsobem bude probíhat komunikace mezi uživateli (ti jsou označováni jako aktéři) a systémem. Tento model je tvořen na základě specifikace funkčních požadavků a vychází se z něj při sestavování scénářů, návrhu aplikace i uživatelské dokumentaci. Výsledný model obsahuje aktéry, případy užití a asociace.

Aktéři jsou definování na základě uživatelských rolí, které budou se systémem pracovat. Případy užití definují kroky uživatele vedoucí k dosažení požadovaného cíle. Asociace se používají pro znázornění vazeb mezi aktéry a jejich komunikace s případy užití. [7]

1.6 Scénáře

Scénáře jsou používány k detailnějšímu popisu případů užití, které se vyskytují v modelu případů užití. Nemají definovanou základní podobu a můžou být popsaný v tabulce nebo prostým textem. Základní část by měl tvořit popis scénáře, aktéři, podmínky pro spuštění, hlavní, popřípadě alternativní scénář. [8]

1.7 Wireframe

Wireframe, taktéž nazývaný jako drátěný model se při návrhu webové aplikace využívá pro navržení vzhledu aplikace. Zároveň se ale nejedná o konečný vzhled aplikace, slouží spíše k zobrazení základního rozložení aplikace a následně je ještě nutné doladit další detaily a barevné složení aplikace. Po vytvoření wireframe bude mít vývojář jasnou představu o struktuře aplikace, to umožní rychlejší a efektivnější implementaci. [9]

1.8 Návrh databáze

Pro navržení efektivní a užitečné databáze je zapotřebí dodržet správný postup. Nejprve je zapotřebí analyzovat požadavky a zjistit účel databáze. Poté získat všechna existující data, přiřadit jim datové typy a provést rozčlenění do tabulek. Na závěr určit primární klíče a vztahy mezi tabulkami. [10]

Správně strukturovaná databáze šetří místo na disku odstraněním duplicitních dat, udržuje přesnost a integritu dat, umožňuje snadný přístup k datům. [10]

1.9 Zabezpečení webové aplikace

Webové aplikace mohou být vystaveny bezpečnostním hrozbám, jako jsou hackerské útoky, úniky dat, neoprávněný přístup a další. Webová aplikace by měla zajišťovat ověření uživatelů a s nimi spojené řízení přístupu, šifrování dat, ochranu proti útokům typu SQL Injection a XSS. Zmíněné typy útoků jsou popsány níže a konkrétní zabezpečení webové aplikace pro správu databáze teroristických útoků je popsáno v kapitole 4.3 „Implementace zabezpečení“.

1.9.1 SQL Injection

Technika útoku SQL Injection [11] je založena na vložení dotazu SQL prostřednictvím vstupních formulářů aplikace. Úspěšný útok dokáže číst, upravovat nebo mazat data z databáze. Útočníkům je tak umožněno falšovat identitu pro přihlášení do systému, manipulovat s daty, odhalit nebo znepřístupnit data a stávají se tak správci systému. Útoky SQL Injection

můžou mít velmi závažný dopad, který závisí dovednostech a představivostí útočníka. Důsledkem těchto útoků dochází ke ztrátě důvěrnosti aplikace. Útok je možný provést například za použití metaznaku do datového vstupu, to provede vložení SQL dotazu. Pro zabránění možnosti vložení metaznaku do databáze je možné využit funkci „espace“, která před nebezpečný znak umístí zpětné lomítko, to zabrání provedení SQL dotazu.

Příklad útoku pro získání výpisu uživatelů:

*SELECT * FROM Users WHERE Id = 105 OR 1=1;*

SQL kód zmíněný výše vypíše všechny řádky z tabulky „Users“, protože podmínka „OR 1=1“ bude vždy pravdivá.

1.9.2 Cross-Site Scripting – XSS

Cross-Site Scripting útoky [12] provádějí vkládání škodlivých skriptů do jinak neškodných webových aplikací. Ke vkládání škodlivých skriptů útočník využívá vstupní formuláře, které jsou následně vloženy do databáze a k jejich provedení dochází v okamžiku, kdy jsou data zobrazeny jinému uživateli. Tyto útoky je možné provést tam kde vstupní data od uživatele nejsou nijak ověřovány před vložením do databáze a zároveň jsou tyto data zobrazovány na výstupu. Prohlížeč koncového uživatele se domnívá, že se nachází na důvěryhodném zdroji, proto nepředpokládá, že by skriptu neměl důvěřovat a spustí ho. Škodlivý skript může přistupovat ke všem souborům cookies, tokenům relace nebo jiným citlivým informacím, které prohlížeč uchovává. Zároveň je pomocí těchto skriptů možné přepsat obsah HTML stránky.

Pro ochranu před XSS je v PHP možné využít funkci „htmlspecialchars“, která speciální znaky uloží do databáze ve formátu určeném pro pozdější bezpečné přečtení.

Příklad útoku pro vložení jednoduchého skriptu:

<script>alert("skript byl vložen");</script>

Za pomocí příkladu výše je vložen JavaScript, který zobrazí vyskakovací okno s popisem.

1.10 Testování s koncovými uživateli

Testování s koncovými uživateli [13] je poslední částí pří vývoji webové aplikace. Jedná se o důležitý krok pro zajištění intuitivní a správně fungující aplikace, která bude vyhovovat představám zadavatele. Jedná se o proces, kdy je aplikace podrobena skutečnému vytížení a

je tak možné odhalit a opravit problémy dříve, než dojde k zahájení oficiálního provozu. Zpětná vazba uživatelů může pomoci také s vylepšením aplikace.

Uživatelské testování umožňuje zadavateli ověřit, zda aplikace odpovídá úvodní specifikaci požadavků. Během testování by měly být vyzkoušeny všechny funkce systému, které se můžou skládat z přidávání, úpravy a mazaní dat. Dále by měla být prověřena bezpečnost systému a vyzkoušen přístup k jednotlivým částem aplikace na základě přidělených uživatelských rolí. Ověření funkčnosti a zabezpečení webové aplikace je popsáno v kapitole 4.4 „Testování funkčnosti a zabezpečení systému s uživateli“.

2 POUŽITÉ TECHNOLOGIE

2.1 PHP

PHP [14] je široce používaný open source skriptovací jazyk. Je vhodný pro vývoj webových aplikací v kombinaci s HTML. Pro psaní PHP kódu se využívá speciální značení, do kterého je nutné kód zabalit, začátek je označen: „<?php“ a konec: „?>“. PHP je generováno na straně serveru a společně s HTML kódem je odesláno klientovi. Výhodou je, že uživatel nemá přístup k surovému kódu a je mu zobrazen pouze konečný vzhled stránky. PHP je považováno za jednoduché pro nováčky, ale zároveň nabízí spoustu funkcí pro pokročilé programátory.

2.2 MySQL

Jedná se o systém pro správu relačních databází. Umožňuje ukládání a správu dat za pomoci SQL příkazů. MySQL ukládá data do tabulek, které se skládají z řádků a sloupců. MySQL je jedním z nejpopulárnějších open-source databázových systémů. [15]

2.3 CodeIgniter

CodeIgniter [16] je systém s otevřeným zdrojovým kódem využívaný pro vývoj webových stránek v jazyce PHP. Tento framework využívá návrhový vzor MVC. Je vytvořen pro vývojáře, kteří potřebují využít jednoduchou a komplexní sadu nástrojů určenou k rychlému vývoji aplikace. Obsahuje bohatou sadu knihoven pro běžně potřebné aplikace a úlohy. CodeIgniter využívá v základu malého počtu knihoven, ty je možné přidávat podle potřeby.

2.4 Návrhový vzor MVC

Rozděluje aplikací do tří základních logických částí: model, view, controller. Model zpracovává data, se kterými aplikace pracuje, využívá databázové dotazy pro zobrazení, přidání nebo úpravu dat. View vytváří uživatelské rozhraní aplikace, obsahuje data shromážděny modelem, ty jsou předány prostřednictvím controlleru. Controller slouží jako prostředník mezi modelem a view, tím zaručuje bezproblémovou komunikaci mezi uživatelem a systémem. [17]

2.5 HTML

HTML [18] je hypertextový značkovací jazyk pro vytváření webových stránek. Skládá se z několika prvků, díky kterým je popsána struktura webové stránky. HTML určují prohlížeči, jak se má obsah zobrazit (označuje například nadpisy, odstavce, odkazy).

2.6 CSS

CSS [19] se používá k popisu vzhledu a formátování dokumentu napsaného ve značkovacím jazyce. Využívá se k tvorbě uživatelského rozhraní webových stránek a aplikací. Styly umožňují definovat vlastnosti (barvu, písmo, ohraničení a další) pro libovolný HTML prvek na stránce.

2.7 Bootstrap

Bootstrap [20] je populární HTML, CSS a JavaScript framework pro vývoj responzivních webových stránek. Umožňuje snadný a rychlý vývoj. Obsahuje šablony pro tabulky, formuláře, tlačítka, navigaci a další HTML elementy. Je kompatibilní s většinou prohlížečů.

2.8 JavaScript

Javascript [21] je objektově orientovaný programovací jazyk určený k tvorbě moderních dynamických aplikací a webových stránek. Javascript se spouští na straně klienta. Klient zašle požadavek na server, následně server vygeneruje stránku, poté prohlížeč provede skript. Takto může uživatel změnit obsah stránky, aniž by došlo k jejímu obnovení. JavaScript se využívá například pro filtrování, řazení nebo validaci dat.

2.9 Visual Studio Code

Jedná se o bezplatný textový editor od společnosti Microsoft. Je k dispozici na operační systémy Windows, Linux i macOS. Tento editor je možné rozšířit o další funkce, které usnadní vývoj aplikací, zároveň podporuje vysoké spektrum programovacích jazyků a stává se tak stále populárnějším nástrojem pro vývoj. [22]

2.10 MySQL Workbench

MySQL Workbench [23] je nástroj pro vizuální návrh databáze. Je vyvíjen a udržován společností Oracle. Poskytuje vývoj SQL, datové modelování, migraci dat a nástroje pro konfiguraci serveru, správu uživatelů a zálohování. Umožňuje migraci dat například z Microsoft SQL Server, SQLite, Microsoft Access do MySQL.

2.11 Enterprise Architect

Enterprise Architect [24] je softwarový nástroj pro návrh architektury aplikace. Cílem návrhu je efektivní dosažení stanovených cílů. Umožňuje provádět analýzy procesů, plánování a navrhování aplikací. Vytváří základní kostru aplikace a umožňuje jednodušší implementaci.

II. PRAKTICKÁ ČÁST

3 NÁVRH SYSTÉMU PRO SPRÁVU TERORISTICKÝCH ÚTOKŮ

Návrh webové aplikace vychází ze specifikace požadavků uživatele. Na základě těchto požadavků je vytvořen model případů užití a z něj vycházející scénáře. Dále jsou v této části navrženy wireframy a databáze.

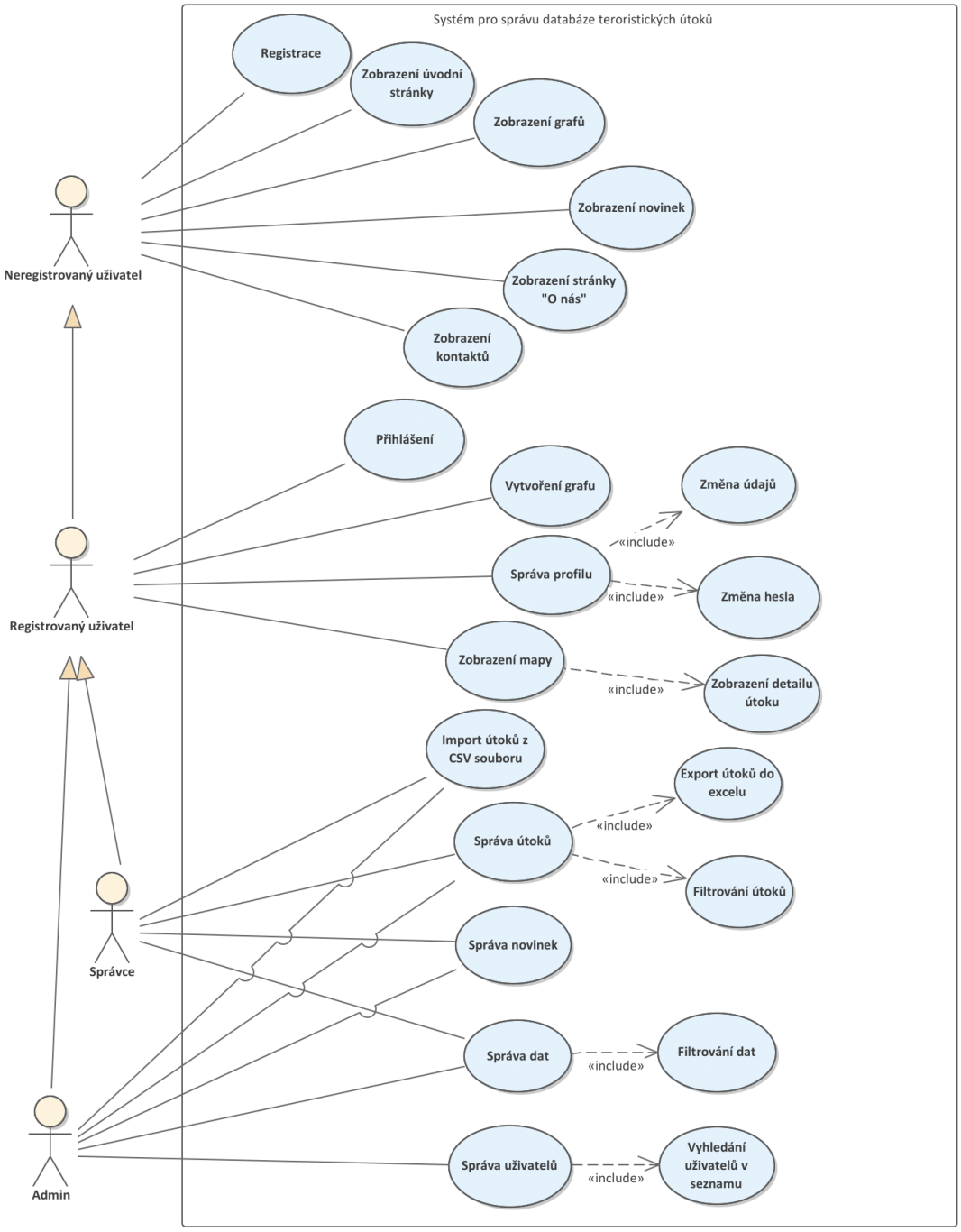
3.1 Model případů užití

Ze specifikace požadavků vyplívají čtyři aktéři: neregistrovaný uživatel, registrovaný uživatel, správce a admin. Tito aktéři budou vykonávat požadované operace.

Neregistrovaný uživatel má přiděleny případy užití pro registraci, zobrazení úvodní stránky, zobrazení grafů, zobrazení novinek, zobrazení stránky „O nás“, zobrazení kontaktů. Případy užití neregistrovaného uživatele dědí i všichni ostatní aktéři.

Registrovaný uživatel má přiděleny případy užití pro přihlášení, vytvoření grafu, správu profilu, která zahrnuje případy užití pro změnu údajů a změnu hesla, dále má tento aktér přiřazeno zobrazení mapy, kde je možnost zobrazit detail útoku. Tyto případy užití dědí aktéři správce a admin.

Aktér správce má případy užití import útoků z CSV souboru, správa útoků obsahující export útoků do excelu a filtrování útoků, dále má správce přiřazenou správu novinek a správu dat, která obsahuje případ pro filtrování dat. Správcovi případy užití má přiřazeny i aktér Admin, který má navíc případ užití pro správu uživatelů, ke kterému je připojen případ užití pro vyhledání uživatelů v seznamu.



Obrázek 2. Model případů užití webové aplikace

3.2 Scénáře případů užití

V této části jsou na základě modelu případů užití vytvořeny scénáře popisující interakci mezi aktéry a systémem. Scénáře jsou zpracovány do tabulek, které obsahují id, název, aktéry, vstupní podmínku a hlavní, popřípadě alternativní scénář.

3.2.1 Registrace

Registrace uživatele umožní po ověření účtu adminem využívat více funkcí systému. Registrační formulář se skládá z jména, příjmení, firmy, pozice, emailu, hesla a potvrzení hesla. Po úspěšném odeslání formuláře je uživateli a adminovi zaslán email o nové registraci.

Tabulka 1. Scénář případu užití Registrace

ID: UC001		
Název: Registrace		
Primární aktér: Neregistrovaný uživatel		
Vedlejší aktéři: Registrovaný uživatel, Správce, Admin		
Vstupní podmínka: Žádná		
Hlavní scénář:		
Krok	Aktér/Systém	Popis
1	Aktér	V navigační liště klikne na tlačítko „Registrace“.
2	Systém	Zobrazí registrační formulář, který se skládá z polí: jméno, příjmení, firma, pozice, email, heslo, potvrzení hesla a tlačítka pro odeslání formuláře.
3	Aktér	Vyplní registrační formulář a stiskne tlačítko pro registraci.
4	Systém	Přesměruje uživatele na přihlášení, zobrazí hlášku o úspěšné registraci a odešle email informující o nové registraci.
Alternativní scénář:		
2a	Aktér	Vyplní a odešle neplatný údaj.
2a1	Systém	Zobrazí hlášku o chybném údaji.

3.2.2 Zobrazení úvodní stránky

Znázorňuje přesměrování na úvodní stránku aplikace, která je přístupná i neregistrovaným uživatelům.

Tabulka 2. Scénář případu užití Zobrazení úvodní stránky

ID: UC002		
Název: Zobrazení úvodní stránky		
Primární aktér: Neregistrovaný uživatel		
Vedlejší aktéři: Registrovaný uživatel, Správce, Admin		
Vstupní podmínka: Žádná		
Hlavní scénář:		
Krok	Aktér/Systém	Popis
1	Aktér	Klikne v navigační liště na tlačítko „DoVA“.
2	Systém	Zobrazí úvodní stránku.

3.2.3 Zobrazení grafů

Přesměrování na stránku s grafy je umožněno všem aktérům, zobrazení se však liší na základě rolí. Neregistrovaný uživatel uvidí pouze veřejné grafy. Registrovaný uživatel, správce a admin budou mít navíc zobrazeny tlačítka na přidaní, úpravu a mazání grafů.

Tabulka 3. Scénář případu užití Zobrazení grafů

ID: UC003		
Název: Zobrazení grafů		
Primární aktér: Neregistrovaný uživatel		
Vedlejší aktéři: Registrovaný uživatel, Správce, Admin		
Hlavní scénář:		
Krok	Aktér/Systém	Popis
1	Aktér	Klikne v navigační liště na tlačítko „Databáze“.
2	Systém	Zobrazí grafy na základě oprávnění aktéra.

3.2.4 Zobrazení novinek

Zobrazení novinek může provést libovolný aktér a výsledné zobrazení se nebude lišit na základě uživatelských rolí.

Tabulka 4. Scénář případu užití Zobrazení novinek

ID: UC004		
Název: Zobrazení novinek		
Primární aktér: Neregistrovaný uživatel		
Vedlejší aktéři: Registrovaný uživatel, Správce, Admin		
Hlavní scénář:		
Krok	Aktér/Systém	Popis
1	Aktér	Klikne v navigační liště na tlačítko „Novinky“.
2	Systém	Zobrazí seznam novinek.

3.2.5 Zobrazení stránky „O nás“

Zobrazení této stránky může provést libovolný aktér a výsledné zobrazení se nebude lišit na základě uživatelských rolí.

Tabulka 5. Scénář případu užití Zobrazení stránky „O nás“

ID: UC005		
Název: Zobrazení stránky „O nás“		
Primární aktér: Neregistrovaný uživatel		
Vedlejší aktéři: Registrovaný uživatel, Správce, Admin		
Vstupní podmínka: Žádná		
Hlavní scénář:		
Krok	Aktér/Systém	Popis
1	Aktér	Klikne v navigační liště na tlačítko „O nás“.
2	Systém	Zobrazí stránku informační stránku.

3.2.6 Zobrazení kontaktů

Zobrazení stránky kontaktů může provést libovolný aktér a výsledné zobrazení se nebude lišit na základě uživatelských rolí.

Tabulka 6. Scénář případu užití Zobrazení kontaktů

ID: UC006		
Název: Zobrazení kontaktů		
Primární aktér: Neregistrovaný uživatel		
Vedlejší aktéři: Registrovaný uživatel, Správce, Admin		
Vstupní podmínka: Žádná		
Hlavní scénář:		
Krok	Aktér/Systém	Popis
1	Aktér	Klikne v navigační liště na tlačítko „Kontakt“.
2	Systém	Zobrazí stránku s kontaktními údaji.

3.2.7 Přihlášení

Stránka pro přihlášení je přístupná všem aktérům, ale k provedení tohoto scénáře musí být uživatel zaregistrovaný a jeho účet ověřen adminem.

Tabulka 7. Scénář případu užití Přihlášení

ID: UC007		
Název: Přihlášení		
Primární aktér: Registrovaný uživatel		
Vedlejší aktéři: Správce, Admin		
Vstupní podmínka: Žádná		
Hlavní scénář:		
Krok	Aktér/Systém	Popis
1	Aktér	V navigační liště klikne na tlačítko „Přihlášení“

2	Systém	Zobrazí přihlašovací formulář s polem email, heslo a tlačítkem pro přihlášení.
3	Aktér	Vyplní přihlašovací formulář a stiskne tlačítko pro přihlášení.
4	Systém	Ověří údaje a přesměruje uživatele na stránku „Profil“.
Alternativní scénář:		
2a	Aktér	Vyplní a odešle neplatné údaje.
2a1	Systém	Ověří údaje a zobrazí hlášku o chybě během přihlášení.

3.2.8 Vytvoření grafu

Tento scénář může provést pouze přihlášený uživatel. K vytvoření grafu je zapotřebí vyplnit formulář, který se skládá z povinných polí titulek, osa Y, osa X, typ grafu, druh grafu a nepovinných filtrů, které určují například barvu grafu, datum, zemi, město, epicentrum, modus operandi nebo typ měkkého cíle útoku.

Tabulka 8. Scénář případu užití Vytvoření grafu

ID: UC008		
Název: Vytvoření grafu		
Primární aktér: Registrovaný uživatel		
Vedlejší aktéři: Správce, Admin		
Vstupní podmínka: Uživatel je přihlášen a má přiřazenou roli Uživatele, Správce nebo Admina. Uživatel se nachází na stránce „Databáze“.		
Hlavní scénář:		
Krok	Aktér/Systém	Popis
1	Aktér	Klikne na tlačítko „Přidat graf“.
2	Systém	Zobrazí formulář pro přidání grafu.
3	Aktér	Zadá povinné parametry a stiskne tlačítko „Vytvořit graf“.
4	Systém	Vloží graf do databáze a přesměruje na stránku s grafy.

3.2.9 Správa profilu

Spravovat svůj profil můžou všichni registrovaní uživatelé. Po přesměrování na tuto stránku mají uživatelé umožněnu změnu jména, příjmení, firmy, pozice, emailu nebo hesla.

Tabulka 9. Scénář případu užití Správa profilu

ID: UC009		
Název: Správa profilu		
Primární aktér: Registrovaný uživatel		
Vedlejší aktéři: Správce, Admin		
Vstupní podmínka: Uživatel je přihlášen a má přiřazenou roli Uživatele, Správce nebo Admina.		
Hlavní scénář:		
Krok	Aktér/Systém	Popis
1	Aktér	Klikne v navigační liště na tlačítko „Profil“.
2	Systém	Zobrazí informace o profilu.
3	Aktér	Vybere úpravu dat nebo hesla.
Alternativní scénář:		
3a	Aktér	Upraví požadovaná data a odešle požadavek.
3a1	Systém	Zobrazí hlášku o úspěšném nebo neúspěšné úpravě dat.
3b	Aktér	Vyplní a odešle formulář pro změnu hesla.
3b1	Systém	Zobrazí hlášku o úspěšném nebo neúspěšné změně hesla a pošle informační email.

3.2.10 Zobrazení mapy

Zobrazení mapy je zpřístupněno pouze přihlášeným uživatelům, mapa bude centrovaná na Evropu, uživatel má možnost mapu posouvat a přibližovat, zároveň má zobrazeny body označující polohu útoku a při kliknutí na jednotlivé body jsou zobrazeny základní informace o útoku. Mapa bude vygenerována použitím JavaScriptové knihovny Leaflet.

Tabulka 10. Scénář případu užití Zobrazení mapy

ID: UC010		
Název: Zobrazení mapy		
Primární aktér: Registrovaný uživatel		
Vedlejší aktéři: Správce, Admin		
Vstupní podmínka: Uživatel je přihlášen a má přiřazenou roli Uživatele, Správce nebo Admina.		
Hlavní scénář:		
Krok	Aktér/Systém	Popis
1	Aktér	Klikne v navigační liště na tlačítko „Mapa“.
2	Systém	Zobrazí mapu s teroristickými útoky.
Alternativní scénář:		
2a	Aktér	Klikne na bod zaznamenaný v mapě.
2a1	Systém	Zobrazí vyskakovací okno s detailem útoku.

3.2.11 Import útoků z CSV souboru

Tento scénář může provést pouze uživatel s rolí správce nebo admina. Přesměrování na import útoků je možné z navigační lišty v administrátorské části. Aktér nejprve vybere CSV soubor s útoky, následně odešle formulář a systém zpracuje požadavek. V případě, že uživatel zvolí nesprávný typ souboru, systém import neprovede.

Tabulka 11. Scénář případu užití Import útoků z CSV souboru

ID: UC011
Název: Import útoků z CSV souboru
Primární aktéři: Správce, Admin
Vedlejší aktér: Žádný

Vstupní podmínka: Uživatel je přihlášen a má přiřazenou roli Správce nebo Admina. Uživatel se nachází v administrátorské části.		
Hlavní scénář:		
Krok	Aktér/Systém	Popis
1	Aktér	Klikne v navigační liště na tlačítko „Import útoku z CSV“.
2	Systém	Zobrazí stránku s polem pro vybrání souboru.
3	Aktér	Vybere CSV soubor a stiskne tlačítko „Importovat data“.
4	Systém	Nahraje data ze souboru do databáze a zobrazí hlášku s počtem přidaných útoků.
Alternativní scénář:		
3a	Aktér	Vybere nesprávný typ souboru.
3a1	Systém	Zobrazí chybovou hlášku.

3.2.12 Správa útoků

Správa útoků je přístupná v administrátorské části aplikace pro uživatelské role správce a admina. Po načtení stránky se zobrazí tabulka s útoky a tlačítky pro editaci a smazání jednotlivých útoků, dále je možné útoky přidávat, popřípadě filtrovat. Přidání a editace útoku mají vlastní formuláře, které se zobrazí po kliknutí na tlačítko. Poslední funkce je export tabulky s útoky do excelového souboru.

Tabulka 12. Scénář případu užití Správa útoků

ID: UC012
Název: Správa útoků
Primární aktéři: Správce, Admin
Vedlejší aktér: Žádný
Vstupní podmínka: Uživatel je přihlášen a má přiřazenou roli Správce nebo Admina. Uživatel se nachází v administrátorské části.
Hlavní scénář:

Krok	Aktér/Systém	Popis
1	Aktér	Klikne v navigační liště na tlačítko „Útoky“.
2	Systém	Zobrazí seznam útoků včetně tlačítek pro práci s útoky.
3	Aktér	Vybere z možností: Přidat, Editovat nebo Smazat útok.
4	Systém	Načte stránku pro přidání, úpravu nebo smazání zvoleného útoku.
5	Aktér	Provede požadovaný úkon a stiskne potvrzovací tlačítko.
6	Systém	Zobrazí informační hlášku.
Alternativní scénář:		
3a	Aktér	Vyplní pole pro filtrování útoků.
3a1	Systém	Zobrazí útoky odpovídající filtru.
3b	Aktér	Stiskne tlačítko „Exportovat tabulku do excelu“
3b1	Systém	Otevře okno pro vybraní místa uložení souboru.
3b2	Aktér	Zvolí cílové místo souboru.
3b3	Systém	Uloží dokument do zvoleného místa.

3.2.13 Správa novinek

Správa novinek je přístupná v administrátorské části aplikace pro aktéry s rolí správce nebo admin. Po přesměrování na stránku má aktér přístupné funkce pro přidání, úpravu a mazání novinek.

Tabulka 13. Scénář případu užití Správa novinek

ID: UC013
Název: Správa novinek
Primární aktéři: Správce, Admin
Vedlejší aktér: Žádný
Vstupní podmínka: Uživatel je přihlášen a má přiřazenou roli Správce nebo Admina. Uživatel se nachází v administrátorské části.

Hlavní scénář:		
Krok	Aktér/Systém	Popis
1	Aktér	Klikne v navigační liště na tlačítko „Novinky“.
2	Systém	Zobrazí seznam novinek včetně tlačítek na správu novinek.
3	Aktér	Vybere z možností: Přidat, Editovat nebo Smazat novinku.
4	Systém	Načte stránku pro přidání, úpravu nebo smazání novinky.
5	Aktér	Provede požadovaný úkon a stiskne potvrzovací tlačítko.
6	Systém	Zobrazí informační hlášku.

3.2.14 Správa dat

Pro práci s daty musí být uživatel přihlášen jako správce nebo admin, v navigační liště je možné vybrat z možností pro správu epicentra, typu měkkého cíle, lokality k bydlišti, modus operandi, země, města nebo barvy grafu. Po přesměrování na požadovanou stránku je možné data přidávat, upravovat nebo mazat.

Tabulka 14. Scénář případu užití Správa dat

ID: UC014		
Název: Správa dat		
Primární aktéři: Správce, Admin		
Vedlejší aktér: Žádný		
Vstupní podmínka: Uživatel je přihlášen a má přiřazenou roli Správce nebo Admina. Uživatel se nachází v administrátorské části.		
Hlavní scénář:		
Krok	Aktér/Systém	Popis
1	Aktér	Najede v navigační liště na tlačítko „Práce s daty“ a vybere data, se kterými chce pracovat.
2	Systém	Zobrazí seznam zvolených dat včetně tlačítek pro práci s daty.
3	Aktér	Vybere z možností: Přidat, Editovat nebo Smazat.

4	Systém	Načte stránku pro přidání, úpravu nebo smazání zvolených dat.
5	Aktér	Provede požadovaný úkon a stiskne potvrzovací tlačítko.
6	Systém	Zobrazí informační hlášku.

3.2.15 Správa uživatelů

Správa uživatelů je umožněna pouze uživatelům s rolí admina. Po načtení stránky může admin filtrovat uživatele podle emailu, přidělovat role a ověřovat účty.

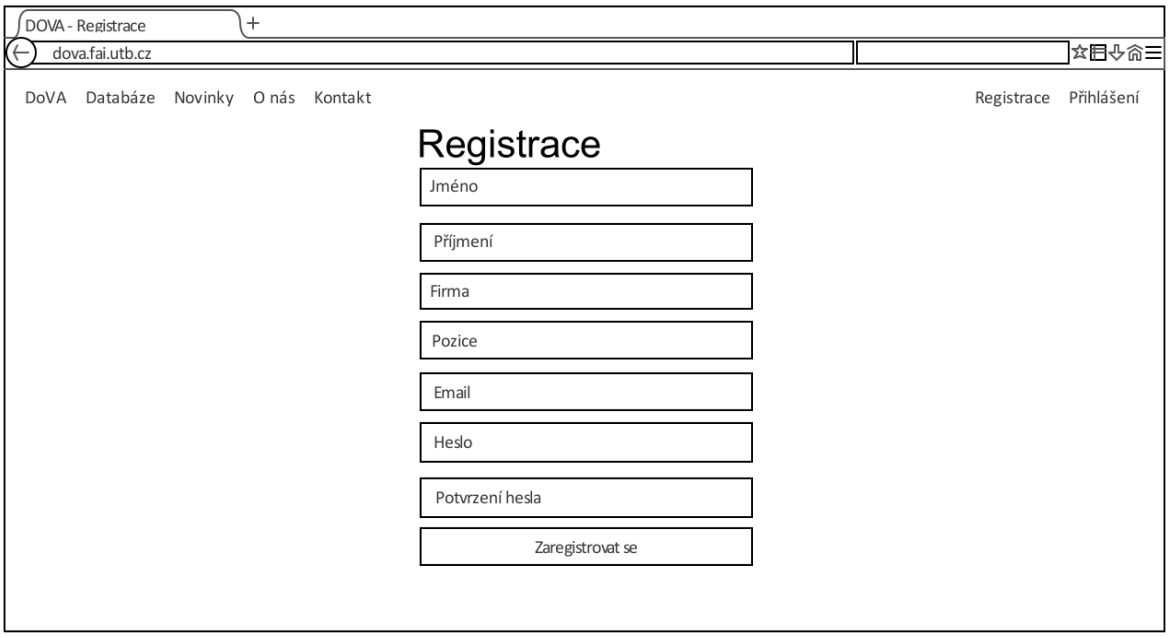
Tabulka 15. Scénář případu užití Správa uživatelů

ID: UC015		
Název: Správa uživatelů		
Primární aktér: Admin		
Vedlejší aktér: Žádný		
Vstupní podmínka: Uživatel je přihlášen a má přiřazenou roli Admina. Uživatel se nachází v administrátorské části.		
Hlavní scénář:		
Krok	Aktér/Systém	Popis
1	Aktér	Klikne v navigační liště na tlačítko „Uživatelé“.
2	Systém	Zobrazí seznam uživatelů.
3	Aktér	Zvolí uživatele pro úpravu.
4	Systém	Načte stránku pro úpravu uživatele.
5	Aktér	Ověří uživatele a přiřadí mu roli.
6	Systém	Provede změnu a zobrazí informační hlášku.
Alternativní scénář:		
3a	Aktér	Vyplní pole pro vyhledání uživatele podle emailu.
3a1	Systém	Zobrazí uživatele s odpovídajícím emailem.

3.3 Wireframe

Registrace

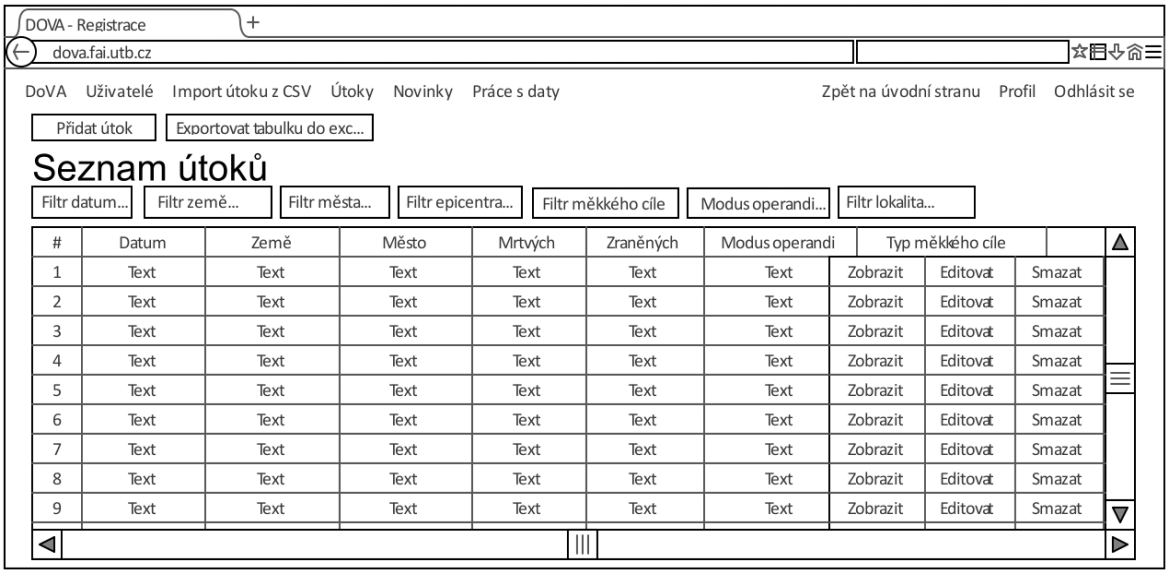
Pokud chce uživatel využívat pokročilejší funkce webové aplikace musí být registrován a jeho účet ověřen administrátorem. K tomuto účelu se využívá registrační formulář. Registrace je přístupná v horní navigační liště pod názvem „Registrace“. Zobrazení pro přihlášení je stejné jako registrace, obsahuje však pouze pole email a heslo.



Obrázek 3. Wireframe – registrace

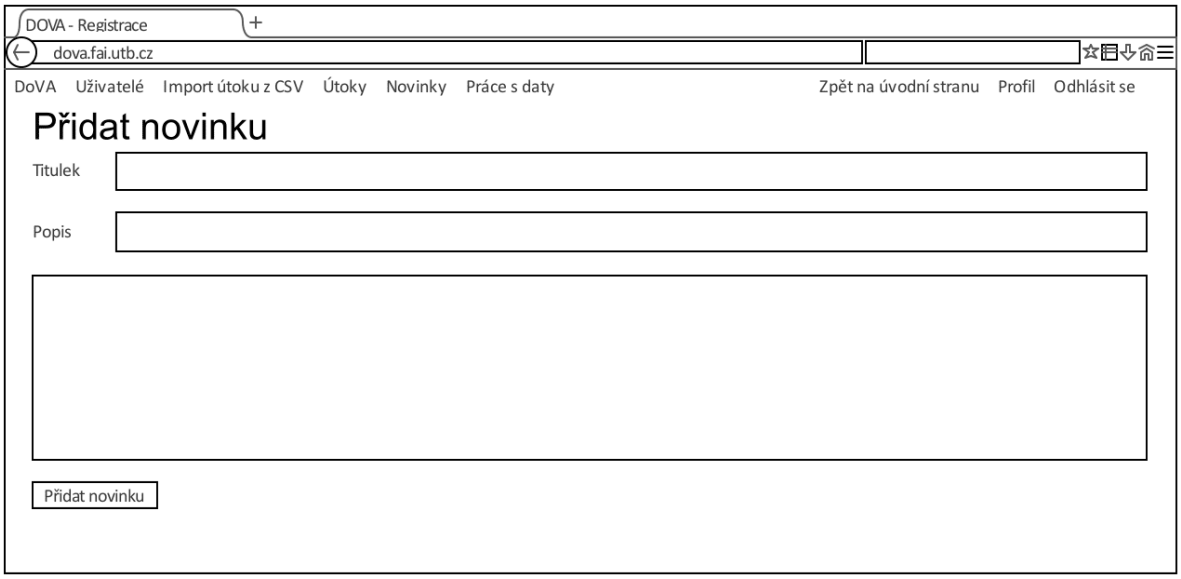
Uživatelské role správce a admina mají možnost přistupovat do administrátorské části aplikace, kde je možné zobrazení, přidávání a úprava dat. K ukázce jsou vytvořeny drátěné modely, které znázorňují vzhled administrátorské části aplikace.

Seznam útoků, přístupný v horní navigační liště jako „Útoky“, je důležitá část aplikace a ve svém zobrazení umožňuje přesměrování na přidání, úpravu, zobrazení a smazání útoků, dále obsahuje možnost filtrace dat nebo exportu tabulky do excelu. Z tohoto návrhu je možné vycházet při vytváření stránek pro správu všech dat ukládaných v databázi.



Obrázek 4. Wireframe – seznam útoků

K ukázce formulářů pro přidání je vytvořen drátěný model zobrazující stránku „Přidat novinku“. Jsou zde znázorněny pole pro vložení titulku, popisu a hlavní zprávy, kterou má novinka předat. Do přidání novinek vede cesta přes navigační lištu zvolit „Novinky“, po přesměrování vybrat „Přidat novinku“, následně se zobrazí zmiňovaný formulář.



Obrázek 5. Wireframe – přidat novinku

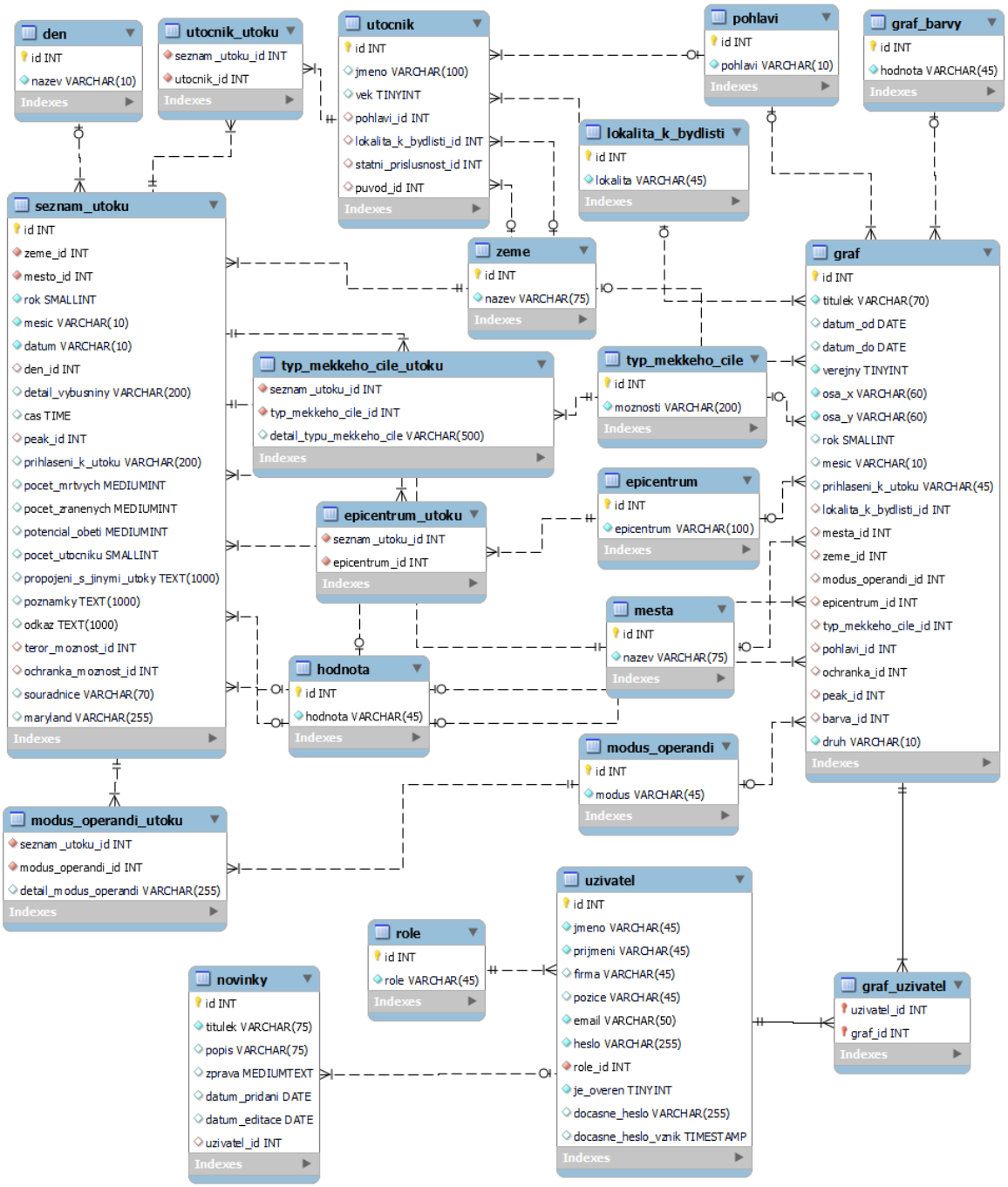
3.4 Databáze

Tato část je zaměřená na návrh databáze pro správu teroristických útoků. Databáze bude sloužit k ukládání a správě informací o teroristických útocích, grafech, uživatelích a novinkách. Návrh databáze je založen na původním seznamu útoků zaznamenávaného v excelové tabulce. Cílem databáze je poskytnout analytikům snadný přístup ke sdílenému uložišti útoků, grafů a novinek.

Hlavní částí databáze je tabulka seznam útoků, která obsahuje 6 povinných sloupců a 16 nepovinných sloupců. Některé ze sloupců obsahují hodnoty z jiných tabulek, proto mají přiřazené id hodnot z propojených tabulek, což zamezí vkládání duplicitních dat. K tabulce útoků jsou připojené tabulky: země, město, den a hodnota. Dále má seznam útoků připojené tabulky, které umožňují přiřadit k útoku jedno či více útočníků, typů měkkých cílů, epicenter a mody operandi. Tabulka útočník obsahuje jméno a věk útočníka, dále má připojeny tabulky pohlaví, země a lokalita k bydlišti, ze kterých uchovává id.

Další část databáze tvoří tabulka uživatel, která obsahuje sloupce jméno, příjmení, firma, pozice, email, heslo, stav ověření, dočasné heslo a datum jeho vzniku. Tabulka uživatel má přiřazenu tabulku rolí, novinky, které uživatel vytvořil a seznam vytvořených grafů.

Tabulka graf je svou velikostí podobná tabulce seznam útoků, z důvodu, že umožňuje uložit nejen titulek a základní osy grafu, ale i filtry na většinu sloupců z tabulky útoků. Tabulka grafů má přiřazeny tabulky s barvou grafu, pohlavím útočníka, lokalitou k bydlišti, zemí útoku, typem měkkého cíle, epicentrem, městem a modus útoku.



Obrázek 6. Návrh databáze

4 IMPLEMENTACE

4.1 Instalace webové aplikace

Instalace systému pro správu databáze teroristických je provedena na systému Ubuntu. V příkazovém řádku je znázorněna instalace a nastavení nástrojů potřebných pro fungování webové aplikace.

Tabulka 16. Instalace webové aplikace – čerpáno z [25]

Příkaz	Popis
sudo apt update	Aktualizuje serverové balíčky na zařízení.
sudo apt install nginx	Nainstaluje nginx, na kterém poběží server. Po zadání příkazu je nutné souhlasit s instalací stisknutím tlačítek „y“ a „enter“.
sudo ufw app list	Výpis dostupných ufw firewall profilů.
sudo ufw allow 'Nginx HTTPS'	Proběhne povolení HTTPS provozu na portu 80.
sudo apt install mysql-server	Nainstaluje balíček, který umožní zprovoznění databáze. Po zadání příkazu je nutné souhlasit s instalací stisknutím tlačítek „y“ a „enter“.
sudo apt install php php-mysql php-intl php-curl php8.1-fpm	Nainstaluje balíčky potřebné pro fungování PHP aplikace. Po zadání příkazu je nutné souhlasit s instalací stisknutím tlačítek „y“ a „enter“.
	Je nutné přenést komprimovaný projekt databaze.zip a databázi databaze_teroristickych_utoku.sql do složky /var/www/.
cd /var/www/	Změní aktuální složku uživatele.
unzip databaze.zip	Rozbalí projekt a vznikne nová složka databaze_utoku v adresáři /var/www/

sudo chown -R www-data:www-data /var/www/databaze_utoku/ writable/cache	Změní oprávnění pro přístup do složky cache a jejích podsložek.
sudo chown -R www-data:www-data /var/www/databaze_utoku/ writable/session	Změní oprávnění pro přístup do složky session a jejích podsložek.
sudo mysql_secure_installation	Nejprve je zapotřebí vybrat stupeň zabezpečení hesla, v případě, že systém neumožní nastavení hesla, tak je nutné ukončit příkaz pomocí klávesové zkratky CTRL-C, zadat příkaz sudo mysql, poté nastavit heslo pomocí příkazu – „ALTER USER 'root'@'localhost' identified with mysql_native_password by 'noveHeslo';“ jakmile je heslo nastaveno, je třeba zadat do konzole příkaz - „exit“. Nyní je možné znovu zadat příkaz – „sudo mysql_ secure_installation“ a dokončit nastavovací proces.
sudo mysql – u root -p	Po provedení příkazu je nutné zadat heslo do databáze zvolené v předešlém kroku.
create database databaze_teroristickych_ utoku;	Provede vytvoření nové databáze.
exit	Příkaz pro opuštění úpravy databáze.
sudo mysql -u root -p databaze_teroristickych_utoku</var/www/databaze_utoku.sql	Proběhne import databáze z dodaného souboru na mysql server.
sudo nano /etc/nginx/sites-available/databaze_utoku	Otevře textový editor s názvem souboru, který bude při uložení vytvořen, v dalším kroku je popsáno nastavení potřebné pro spuštění a správné fungování systému.
server { listen 80; listen [::]:80;	Nastavení webového serveru pro HTTPS připojení.

server_name www.dova.fai.utb.cz;
return 301 $scheme://dova.fai.utb.cz$request_uri;
}
server {
listen 443 ssl http2;
listen [::]:443 ssl http2;
server_name dova.fai.utb.cz;
root /var/www/databaze_utoku;
index index.html index.php;
ssl_certificate /root/ssl/servercert.pem;
ssl_certificate_key /root/ssl/serverkey.pkey;
ssl_session_timeout 1d;
ssl_session_cache shared:MozSSL:10m;
ssl_session_tickets off;
ssl_protocols TLSv1.2 TLSv1.3;
ssl_ciphers ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384;
ssl_prefer_server_ciphers off;
add_header Strict-Transport-Security "max-age=63072000" always;
ssl_stapling on;
ssl_stapling_verify on;
ssl_trusted_certificate /root/ssl/chainECC2021.pem;
resolver 10.51.11.168;
}
	Důležité parametry:
	server_name – název domény.
	root – nastaví kořen dokumentu, nachází se zde webové soubory.
	ssl_certificate – cesta k souboru obsahující podepsaný certifikát.
	ssl_certificate_key – cesta k souboru obsahující privátní klíč.
	resolver – nastaví adresu pro překlad DNS jmen. Pokud není resolver nastaven, použije se resolver konfigurovaný v systému.

sudo ln -s /etc/nginx/sites-available/databaze_utoku /etc/nginx/sites-enabled/	Vytvoří link souboru vytvořeného v předešlém kroku.
sudo unlink /etc/nginx/sites-enabled/default	Zruší link souboru s přednastavením pro spuštění webové aplikace.
sudo systemctl reload nginx	Proběhne znovunačtení nginx a aplikuje se nový konfigurační soubor.

sudo nano /var/www/databaze_utoku/app/Config/App.php	V textovém editoru se otevře soubor pro úpravu základní domény. Je nutné vyhledat a nastavit „public $baseURL = 'http://localhost/';“. Následně změnu uložit.
sudo nano /var/www/databaze_utoku/app/Config/Database.php	V textovém editoru otevře soubor pro nastavení připojení k databázi. V části „public $default“ je nutné nastavit hodnotu „username“, která bude ukládat jméno uživatele databáze, v tomto případě je to „root“. Hodnota „password“ bude ukládat zvolené heslo uživatele „root“ a na závěr nastavit název databáze na řádku „database“ přiřadit „databaze_teroristickych_utoku“.
sudo apt install ssmpt	Provede instalaci balíčku ssmtp, je tak umožněno zasílání emailů.
sudo nano /var/www/databaze_utoku/app/Config/Email.php	Otevře textový editor pro úpravu konfiguračního souboru, který je přednastaven. Je možné změnit adresu smtp serveru nebo email.
sudo nano /var/www/databaze_utoku/app/Controllers/BaseController.php	Zde je zapotřebí ve funkci generovatEmail nastavit odesílací email.

Po dokončení instalace je zapotřebí nastavit v databázové tabulce „nastaveni“ hlavní email, na který budou chodit informační emaily o registraci nových uživatelů.

Pro přístup prvního uživatele do webové aplikace musí být v databázi ručně ověřen. Tuto změnu je možné provést v tabulce „uzivatel“, sloupec „je_overen“ nastavit na hodnotu „1“, popřípadě je možné změnit uživatelskou roli ve sloupci „role_id“.

4.2 Přenesení dat ze současného řešení

Pro přenesení dat ze současného řešení do vytvořeného systému je na základě požadavků zadavatele vytvořena funkce pro import z CSV souboru. Vzhledem k tomu, že jsou data uložena v excelovém souboru musí se nejprve převést do CSV souboru. Návod k provedení importu je popsán v kapitole 5.2.4 „Import útoku z CSV“. Samotná funkce nejprve ověří správnost formátu, následně soubor otevře a řádek po řádku prochází jednotlivé sloupce, které odděluje na základě středníků. Získaná data postupně ukládá do požadovaných tabulek a sloupců v databázi. Po provedení importu vypíše hlášku s počtem přidaných záznamů.

4.3 Implementace zabezpečení

Webová aplikace je zabezpečena proti SQL Injection a XSS. Šifrovaný přenos dat mezi webových serverem a prohlížečem uživatele zajišťuje protokol HTTPS. Uživatelská hesla jsou před vložením do databáze hashovaná, je k tomu využita PHP funkce password_hash. Přístup do jednotlivých částí aplikace je povolen na základě uživatelských rolí, do veřejných podstránek má přístup i nepřihlášený uživatel. Při přesměrování na podstránku s přístupem omezeným pro určité role proběhne kontrola uživatele.

Zabezpečení proti XSS zajišťuje PHP funkce „htmlspecialchars“. Toto zabezpečení je implementováno v controlleru aplikace. Funkce obdrží vstup od uživatele a zabezpečí části, které by mohly způsobit vložení skriptu.

```
'propojeniSUtoky'     => htmlspecialchars($this->request->getVar('propojeniSUtoky')),
'poznamky'      => htmlspecialchars($this->request->getVar('poznamky')),
'odkaz'     => htmlspecialchars($this->request->getVar('odkaz')),
'souradnice'      => htmlspecialchars($this->request->getVar('souradnice')),
'maryland'      => htmlspecialchars($this->request->getVar('maryland')),
```

Obrázek 7. Zabezpečení proti XSS

Pro ošetření vstupních dat je v modelu využívána funkce „osetriVstup($vstup). Pokud je vstupní parametr nenulový a nebyl zadán v číselném formátu proběhne ošetření proti SQL Injection. K tomuto účelu slouží zabudovaná funkce „escape()“, která uloží vstup v bezpečném formátu a zabalí jej do uvozovek, ty jsou následně odebrány použitím funkce „substr“.

```
function osetriVstup($vstup)
{
    if ($vstup == NULL) {
        return NULL;
    } else {
        if (is_numeric($vstup)) {
            return $vstup;
        } else {
            return substr($this->db->escape($vstup), 1, -1);
        }
    }
}
```

Obrázek 8. Funkce na ošetření vstupu

4.4 Testování funkčnosti a zabezpečení systému s uživateli

Před samotným testováním aplikace s uživateli bylo provedeno testování pro ověření, zda implementované zabezpečí funguje podle očekávání. Testování probíhalo na lokálním webovém serveru a byl ověřen přístup do jednotlivých částí webové aplikace na základě uživatelských rolí, ukládání hesel v databázi a kontrola odolnosti formulářů proti vložení SQL Injection a XSS. Kontrola byla provedena na celou webovou aplikaci. Pro ukázku jsou vytvořeny konkrétní testovací případy.

Testování přístupu do částí systému na základě uživatelských rolí bylo prováděno vyhledáváním adres, na které by aktuálně přihlášený uživatel neměl mít přístup. Pro ukázku jsou vytvořeny dva konkrétní testovací případy.

Tabulka 17. Testovací případ Zobrazení mapy bez přihlášení

ID: 001 Testovací případ: Zobrazení mapy útoků bez přihlášení
Vstupní podmínka: Žádná
Testovací kroky:

Krok	Popis
1	Vložit do vyhledávače adresu localhost/databaze_utoku/mapa.
2	Odeslat požadavek.
Očekávaný výsledek	Zobrazí se stránka „Přístup odepřen“.

Tabulka 18. Testovací případ Přesměrování do administrace s rolí uživatel

ID: 002 Testovací případ: Přesměrování do administrační části s rolí uživatel	
Vstupní podmínka: Přihlášení s rolí uživatel	
Testovací kroky:	
Krok	Popis
1	Vložit do vyhledávače adresu localhost/databaze_utoku/administrace.
2	Odeslat požadavek.
Očekávaný výsledek	Zobrazí se stránka „Přístup odepřen“.

Vložení SQL Injection přes vstupní formulář bylo provedeno jednotlivě na všechny formuláře. Pro znázornění byl vytvořen konkrétní testovací případ.

Tabulka 19. Testovací případ Vložení SQL Injection přes formulář

ID: 003 Testovací případ: SQL Injection vložená přes formulář pro přidání grafu	
Vstupní podmínka: Uživatel je přihlášen	
Testovací kroky:	
Krok	Popis
1	Zobrazit stránku pro přidání grafu.

2	Do pole titulek zadat: „název grafu; DROP TABLE epicentrum“ pro vložení SQL Injection.
3	Odeslat formulář.
Očekávaný výsledek	Je přidán graf. Tabulka epicentrum nebyla smazána.

Vložení XSS přes vstupní formulář bylo provedeno na všechny vstupní formuláře. Pro znázornění byl vytvořen konkrétní testovací případ.

Tabulka 20. Testovací případ Vložení XSS přes formulář

ID: 004 Testovací případ: XSS vložený přes formulář pro přidání grafu	
Vstupní podmínka: Uživatel je přihlášen	
Testovací kroky:	
Krok	Popis
1	Zobrazit stránku pro přidání grafu.
2	Do pole titulek zadat: *<script>alert("XSS")</script>* pro vložení XSS.
3	Odeslat formulář.
Očekávaný výsledek	Je přidán graf a uživatel je přesměrován na seznam grafů. Skript vložený do titulku grafu se neprovede.

Správnost formátu nově uloženého hesla ověřuje následující testovací případ.

Tabulka 21. Testovací případ Uložení hesla

ID: 005 Testovací případ: Uložení hesla
Vstupní podmínka: Žádná
Testovací kroky:

Krok	Popis
1	Zobrazit stránku pro registraci.
2	Vyplnit registrační formulář.
3	Odeslat registrační formulář.
4	Zobrazit záznamy v databázi.
Očekávaný výsledek	Uživatel má v databázi uložen hash hesla.

Testovací případy provedené na všechny části systému odpovídaly očekáváným výsledkům a během testování nedošlo k žádnému narušení systému. Byla tak prověřena a potvrzena správná funkčnost zabezpečení systému.

Následně se mohlo přejít na testování webové aplikace s uživateli, které probíhalo na sdíleném webovém serveru. Byli osloveni uživatelé a analytici, kteří budou s webovou aplikací nejvíce pracovat.

Cílem testování s uživateli bylo odhalit nedostatky a chyby systému, které vznikly při implementaci řešení. Uživatelé měli možnost ověřit správnou funkčnost systému z pohledu všech uživatelských rolí. Pro prvotní seznámení se systémem byl uživatelům poskytnut uživatelský manuál popisující fungování jednotlivých částí webové aplikace. Testování probíhalo přibližně 2 týdny a výsledek byl sepsán do textového dokumentu.

První problém se týkal zobrazování grafů. Po přidání většího množství grafů neodpovídaly názvy a hodnoty grafů zvoleným parametrům. Další nedostatek se týkal databáze, která byla při delší neaktivitě odpojena. Pro lepší využitelnost filtrů byl zaznamenán požadavek na nerozlišování diakritiky při zadávání hodnot do filtrů. Zbytek poznámek se týkal spíše drobností, mezi které patřily překlepy nebo přeuspořádání sloupců v tabulkách pro efektivnější čitelnost dat. Při uživatelském testování nebyl zjištěn žádný problém v zabezpečení systému. Všechny zmíněné poznámky byly opraveny a webová aplikace je tak připravena pro běžný provoz. Testování přineslo i řadu nápadů na budoucí rozšíření webové aplikace a může tak být považováno za úspěšné.

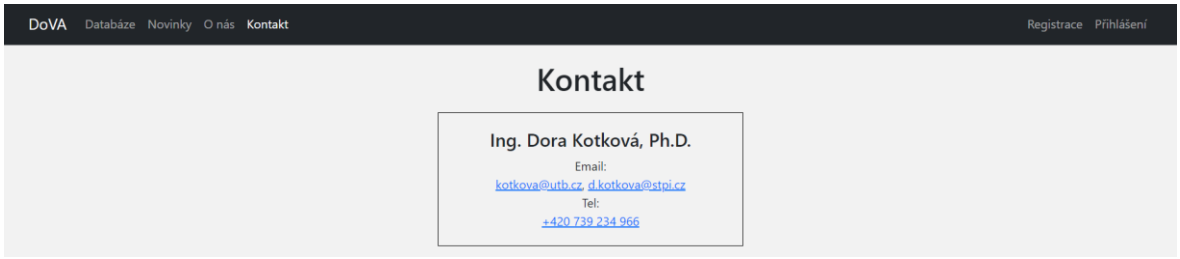
5 UŽIVATELSKÝ MANUÁL

V této části je znázorněná práce s webovou aplikací. Aplikace se skládá z 39 podstránek a dvou layoutů, které se dělí na uživatelskou a administrátorskou část. Funkce pro práci s databázovými tabulkami jsou založeny na podobném principu, proto budou k ukázce vybrány pouze některé.

5.1 Uživatelská část

Nepřihlášený uživatel má možnost zobrazení úvodní stránky, novinek, veřejných grafů, kontaktů a stránky „O nás“. Přihlášení uživatelé mají v uživatelské části navíc možnost pracovat s grafy a zobrazit mapu útoků.

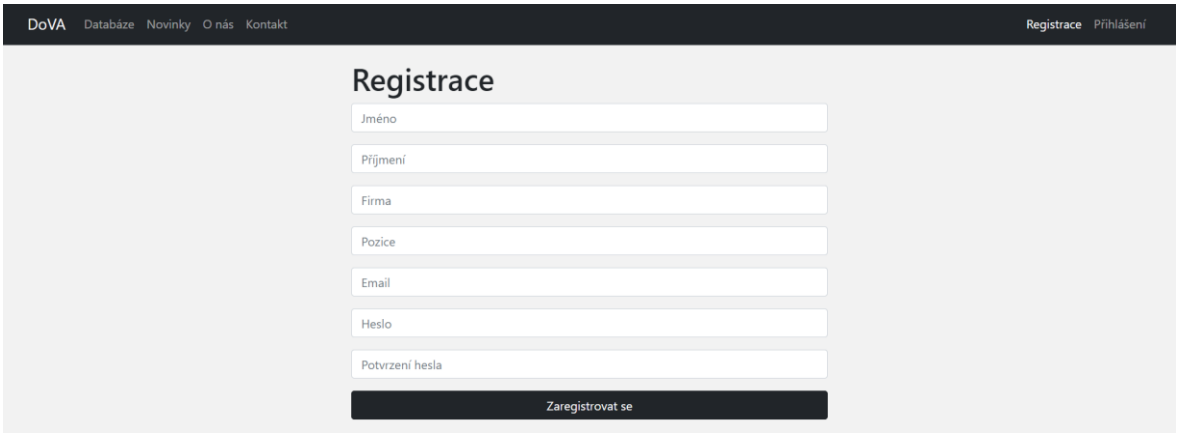
Obrázek 9. Webová aplikace – úvodní stránka



Obrázek 10. Webová aplikace – kontakt

5.1.1 Registrace

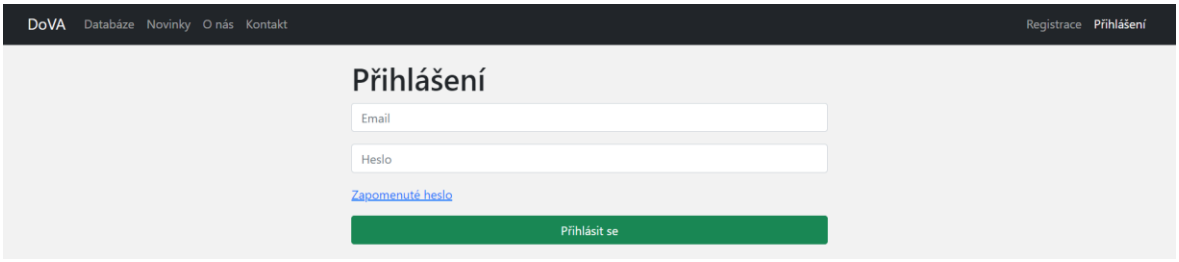
Před přihlášením do systému je nutné vyplnit registrační formulář, který je průchozí z navigační lišty jako „Registrace“. Po registraci musí uživatel vyčkat na ověření účtu adminem, následně je umožněno přihlášení.



Obrázek 11. Webová aplikace – registrace

5.1.2 Přihlášení

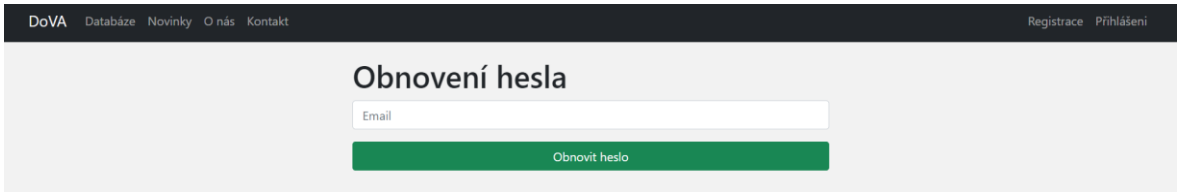
Jakmile uživatel obdrží email oznamující ověření účtu, může přejít k přihlášení, které je průchozí z navigační lišty. Zpřístupněné části systému závisí na uživatelské roli.



Obrázek 12. Webová aplikace – přihlášení

5.1.3 Obnovení hesla

V případě zapomenutí hesla má uživatel možnost použít funkci obnovení hesla, která je průchozí ze stránky pro přihlášení. Po vyplnění formuláře obdrží uživatel email s náhodně vygenerovaným dočasným heslem, které je funkční 24 hodin. Je tedy nutné provést po přihlášení změnu dočasného hesla.



Obrázek 13. Webová aplikace – obnovení hesla

5.1.4 Změna hesla

Po úspěšném přihlášení se uživateli v horní navigaci zobrazí možnost „Profil“, na kterou je i přesměrován a pomocí formuláře má možnost provést změnu hesla.

Obrázek 14. Webová aplikace – změna hesla

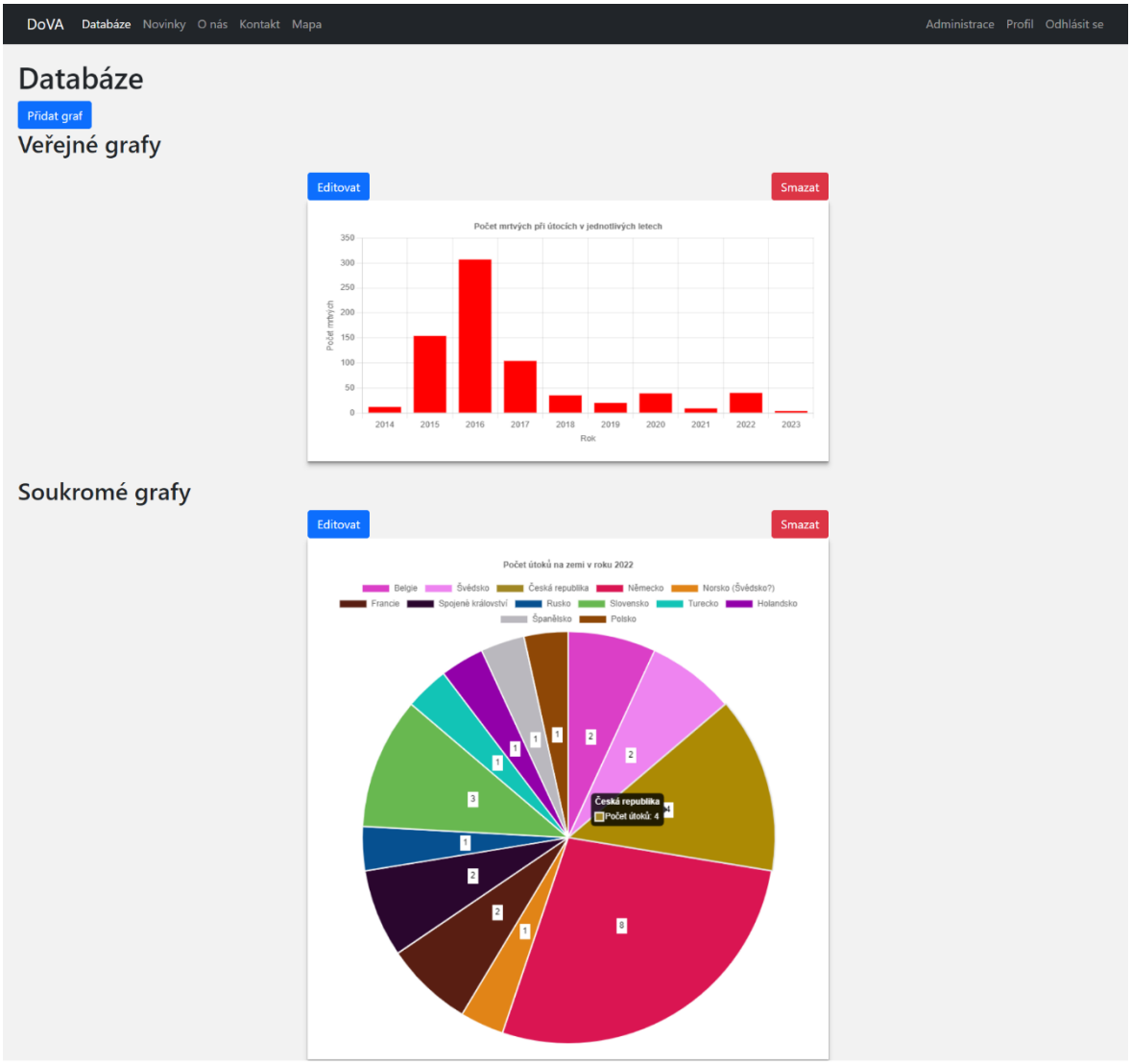
5.1.5 Změna údajů

Přihlášený uživatel má v sekci „Profil“ možnost změnit své jméno, příjmení, firmu, pozici a email

Obrázek 15. Webová aplikace – změna údajů

5.1.6 Práce s grafy

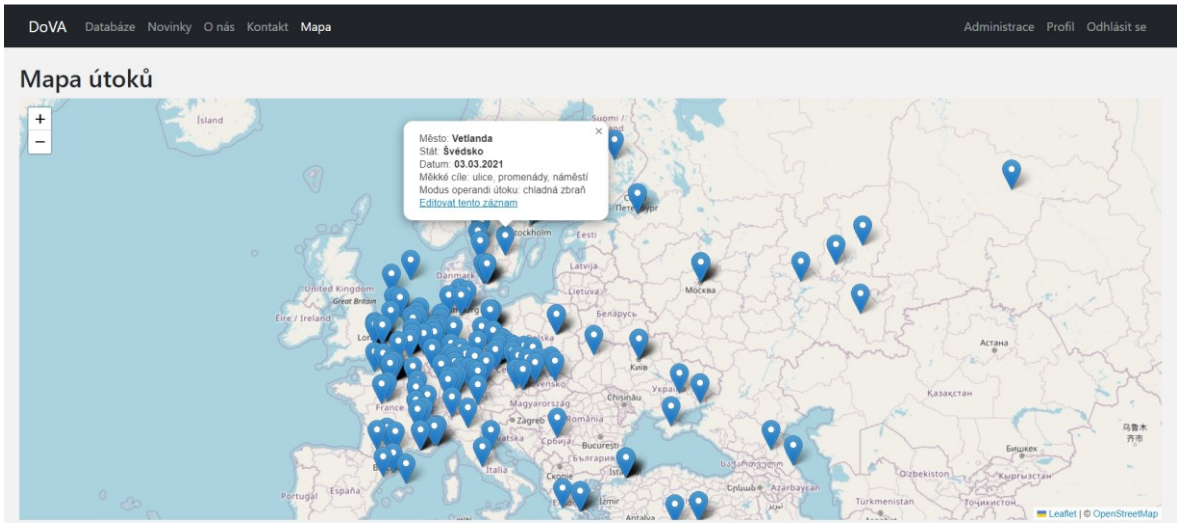
V navigační liště pod odkazem „Databáze“ má přihlášený uživatel možnost přidávat, upravovat a mazat grafy, nepřihlášený uživatel uvidí pouze grafy veřejné. Formulář pro přidání grafu se zobrazí po stisknutí tlačítka „Přidat graf“. Vytváření grafu umožňuje zadat název, osu Y, která může zobrazovat počet útoků, zraněných nebo mrtvých. Na ose X je možné zobrazit země, města, roky, měsíce, datum, den, epicentrum, modus operandi nebo lokality. Graf může být soukromý nebo veřejný a je možné zobrazit graf sloupcový nebo koláčový, následně je možné vybrat z široké řady nepovinných filtrů.



Obrázek 16. Webová aplikace – zobrazení grafů

5.1.7 Zobrazení mapy

Na mapu s útoky má přistup pouze přihlášený uživatel, je generovaná na základě souřadnic zadaných u útoků. Mapu je možné různě polohovat a při rozkliknutí označeného místa se zobrazí základní popis útoku, správce nebo admin mají navíc možnost prokliku na editaci záznamu.

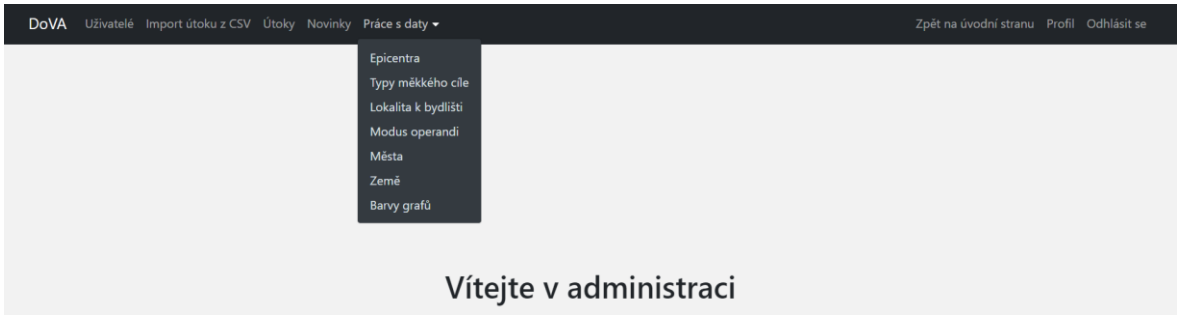


Obrázek 17. Webová aplikace – zobrazení mapy

5.2 Administrátorská část

Tato část je přístupná pouze roli „Admin“ a „Správce“. Admin bude mít navíc možnosti spravovat uživatele, ověřit uživatele, změnit uživatelskou roli a smazat uživatele.

Po přesměrování do administrace budou mít správce a admin k dispozici navigační lištu, která umožňuje přejít na úpravu požadované kategorie. Po zvolení kategorie se zobrazí seznam záznamů. Záznamy je možné přidávat, upravovat, mazat, popřípadě filtrovat.



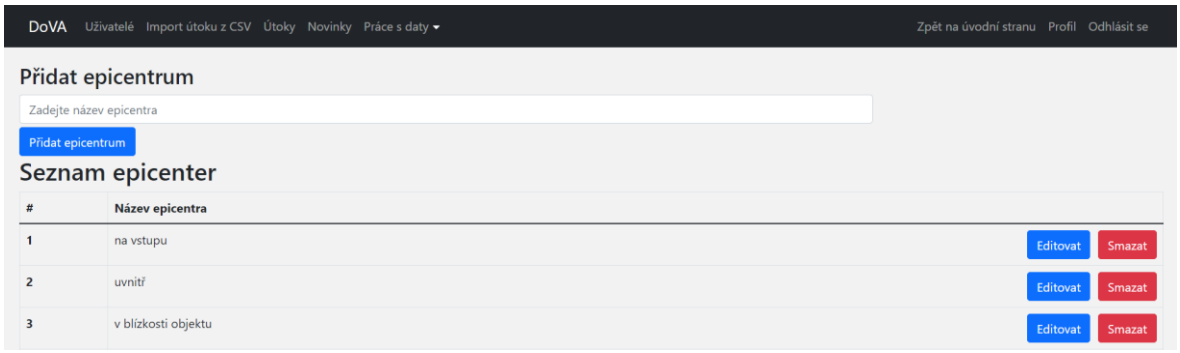
Obrázek 18. Webová aplikace – správa dat

5.2.1 Práce s daty

Práce s daty se skládá z prvků, které obsahují pouze název a tvoří je epicentra, typy měkkého cíle, lokalita k bydlišti, modus operandi, města, země a barvy grafů. Demonstrace funkcí bude znázorněna na stránce epicenter, na stejném principu fungují i ostatní zmíněné kategorie.

5.2.1.1 Přidání záznamu

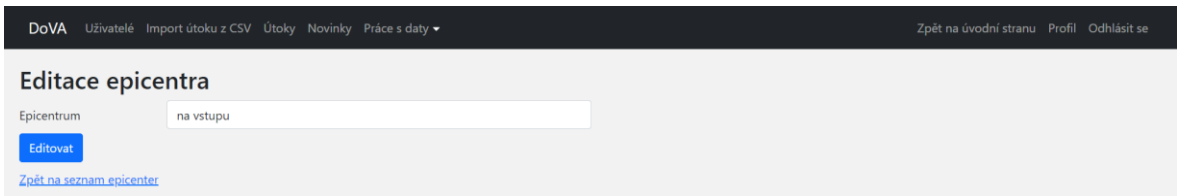
V horní části se nachází formulář pro přidání nového záznamu, který je nutné vyplnit a následně odeslat stisknutím tlačítka pro přidání.



Obrázek 19. Webová aplikace – seznam epicenter

5.2.1.2 Úprava záznamu

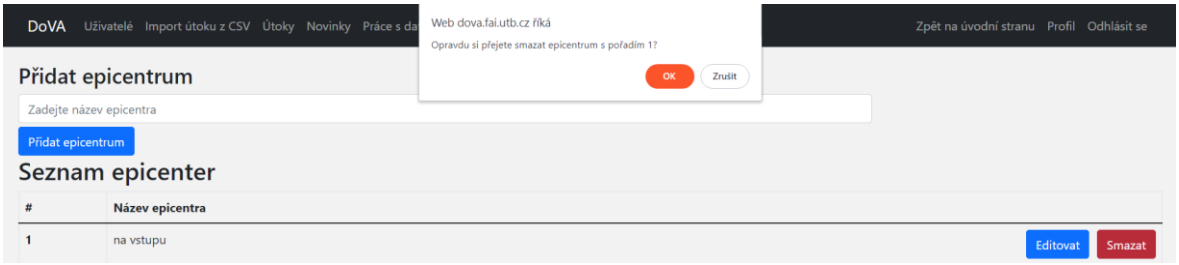
V seznamu najdeme požadovaný záznam a stiskneme tlačítko „Editovat“, následně systém zobrazí záznam na nové stránce, kde můžeme provést úpravu.



Obrázek 20. Webová aplikace – úprava epicentra

5.2.1.3 Odebrání záznamu

V seznamu najdeme požadovaný záznam, stiskneme tlačítko „Smazat“, následně se zobrazí potvrzovací okno, aby nedošlo k nechtěnému smazání.



Obrázek 21. Webová aplikace – odebrání epicentra

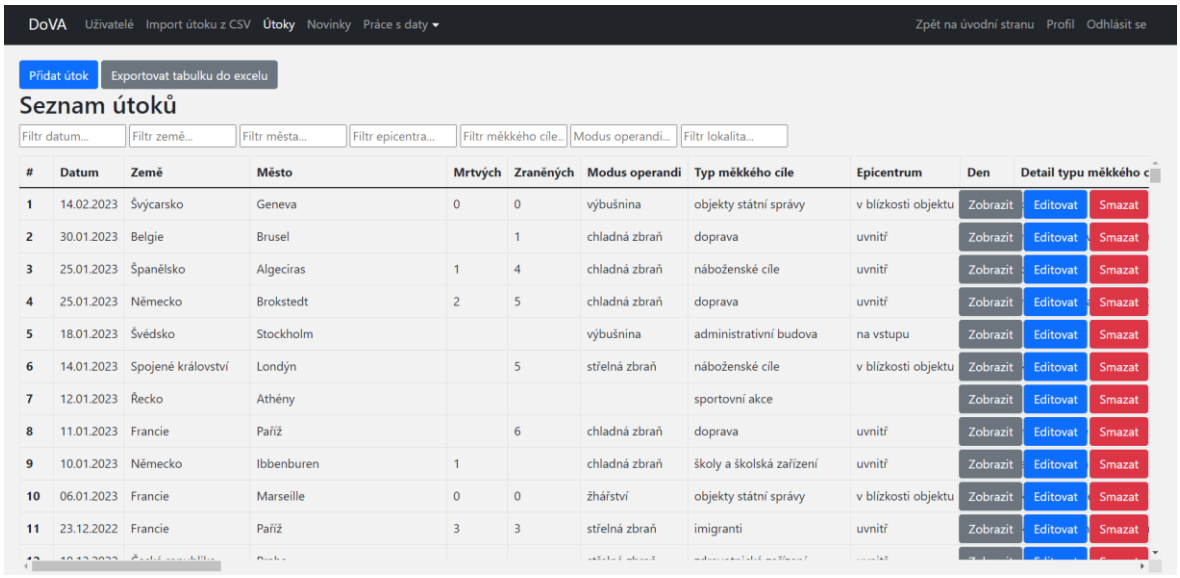
5.2.2 Správa útoků

Správa útoků je možná po stisknutí tlačítka „Útoky“ v navigační liště. Po načtení stránky se zobrazí seznam útoků. Útoky je možné filtrovat podle data, země, města, epicentra, typu měkkého cíle, modu operandi a lokality. Ve vrchní části se nachází tlačítka pro přidání útoku a export tabulky do excelu. Vypsané útoky mají tlačítka pro přesměrování na zobrazení, úpravu a smazání útoku.

Po stisknutí tlačítka „Přidat útok“ se zobrazí formulář, který umožní zadat všechny hodnoty útoku. Povinné pole jsou označeny hvězdičkou, zbytek je volitelný. Pro přidání detailu modu operandi a typu měkkého cíle je nutné zakliknout nejdříve prvek, ke kterému bude detail patřit. Formulář pro přidání útočníka se zobrazí po stisknutí tlačítka „Přidat útočníka“, který se nachází ve spodní části stránky.

Export tabulky se spustí po stisknutí tlačítka, následně je možné vyplnit název a cestu k souboru. Při filtraci dat se provede export záznamů zobrazených v tabulce.

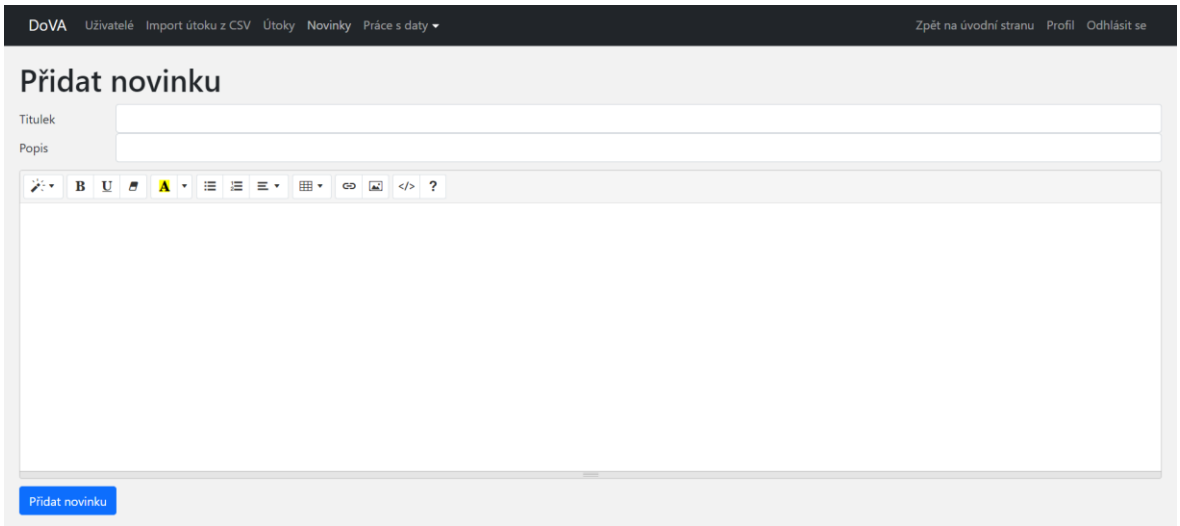
V seznamu útoku jsou 3 tlačítka. Tlačítko „Zobrazit“ přesměruje na detail útoku, ve kterém jsou vypsány pouze vyplněné hodnoty. Tlačítko „Editovat“ zobrazí formulář s informacemi o útoku, které je možné následně změnit. Tlačítko „Smazat“ zobrazí potvrzovací okno, které umožní smazání záznamu.



Obrázek 22. Webová aplikace – seznam útoků

5.2.3 Správa novinek

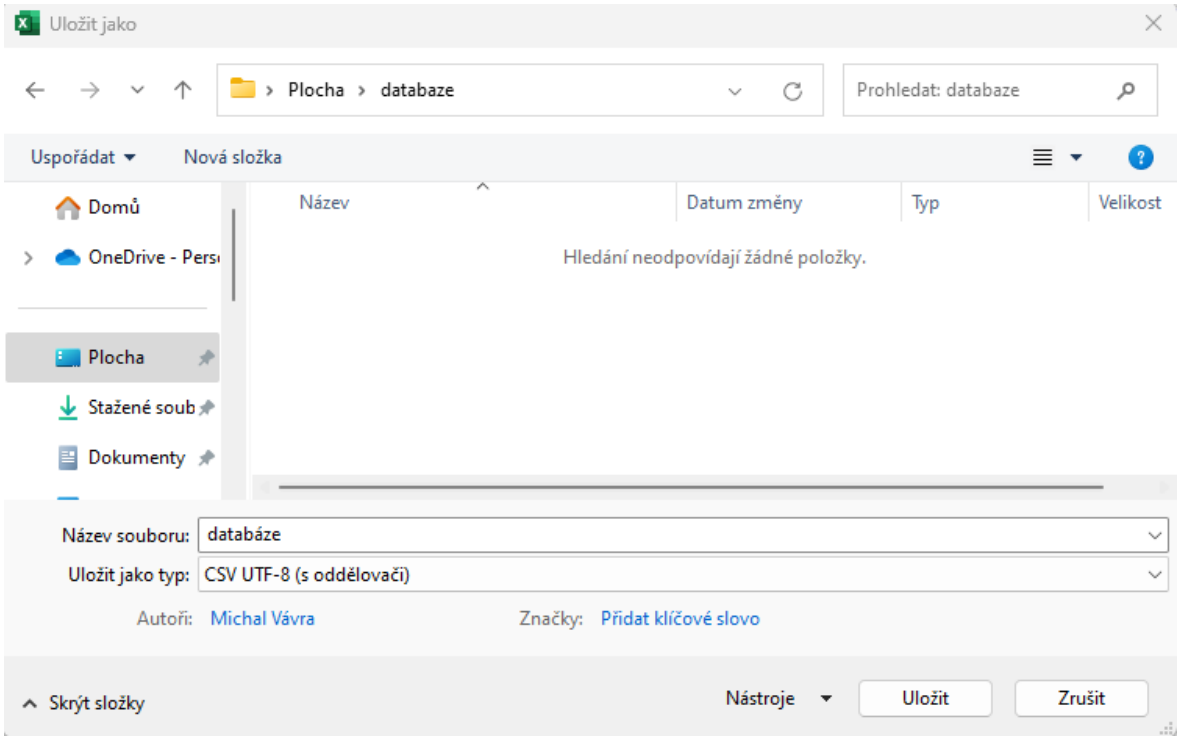
Stránka pro správu novinek se zobrazí po zvolení možnosti „Novinky“ v navigační liště. Vzhled této stránky obsahuje seznam novinek s tlačítky pro jejich správu. Formulář pro přidání novinky obsahuje povinné pole „titulek“, následně je možné vyplnit popis a vytvořit vlastní vzhled stránky, který se provádí v textovém editoru použitím html elementů.



Obrázek 23. Webová aplikace – přidat novinku

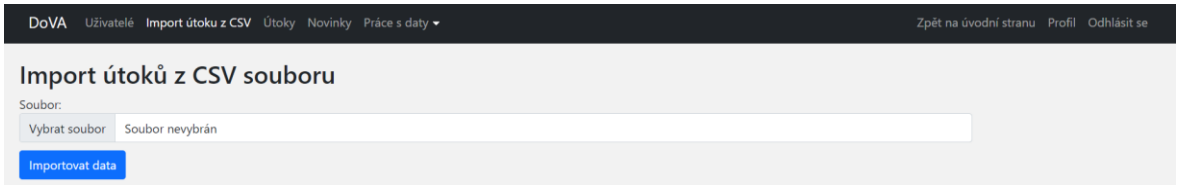
5.2.4 Import útoku z CSV

Před provedením importu je nutné uložit soubor jako typ .csv a zachovat správné pořadí sloupců. Pro uložení dat v CSV formátu je zapotřebí otevřít excelový sešit s útoky, zvolit možnost „soubor“ → „uložit jako“ → „procházet“ → zadat název souboru a v části „Uložit jako typ“ zvolit možnost „CSV UTF-8 (s oddělovači)“ → „uložit“.



Obrázek. Uložení CSV souboru

V tuto chvíli je soubor připraven a může být v části „Import útoku z CSV“ nahrán do databáze útoků.

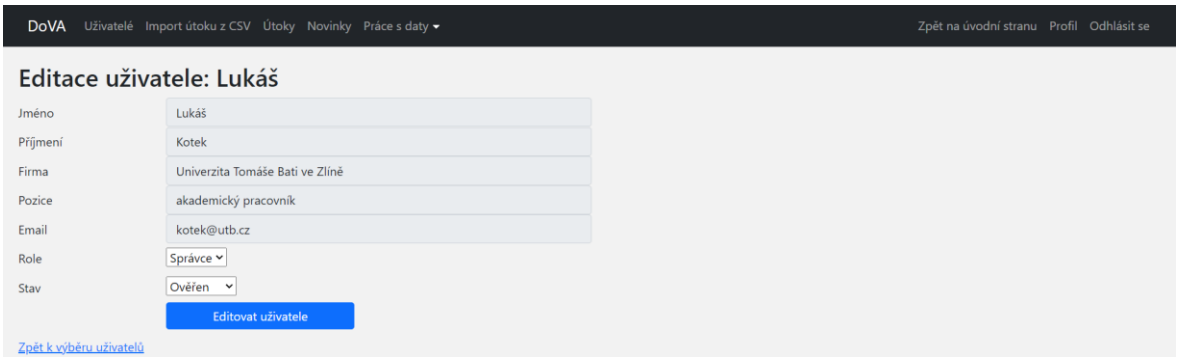


Obrázek 24. Webová aplikace – import útoku

5.2.5 Práce s uživateli

Tato část je přístupná pouze adminům. Seznam uživatelů se otevře po kliknutí na možnost „Uživatele“ v navigační liště. Uživatele je možné filtrovat podle emailu, tlačítko „Editovat“ umožní ověření uživatele a změnu jeho role. Poslední funkcí je smazání uživatele.

Obrázek 25. Webová aplikace – seznam uživatelů



Obrázek 26. Webová aplikace – změna role uživatele

ZÁVĚR

Hlavním cílem bakalářské práce bylo navrhnout a implementovat systém pro správu databáze teroristických útoku. Systém byl vytvořen na základě požadavků stanovených zadavatelem.

V teoretické části byla provedena rešerše existujících řešení, specifikace požadavků na webovou aplikaci, ze které byl stanoven a popsán postup pro navržení webové aplikace. V poslední části byly popsány použité technologie.

Praktická část zachycuje návrh aplikace skládající se z modelu případů užití, ke kterému jsou vytvořeny konkrétní scénáře, následně je navržen wireframe a databáze systému. Po návrhu webové aplikace následuje její implementace, která zahrnuje popis instalace webové aplikace, způsob přenesení dat ze současného řešení do nového systému, zabezpečení aplikace a testování s koncovými uživateli. Poslední částí bakalářské práce je uživatelský manuál, který zachycuje vzhled a fungování systému.

Webová aplikace umožňuje analytikům jednoduchou obsluhu databáze. Přihlášení do systému je umožněno pouze uživatelům ověřeným adminem a přístup k jednotlivým funkcím závisí na uživatelské roli.

SEZNAM POUŽITÉ LITERATURY

[1] Lekce 1 - Úvod do UML. itnetwork.cz - Učíme národ IT [online]. Copyright © 2023 itnetwork.cz. Veškerý obsah webu [cit. 05.03.2023]. Dostupné z: https://www.itnetwork.cz/navrh/uml/uml-uvod-historie-vyznam-a-diagramy

[2] Overview of the GTD. Home | START.umd.edu [online]. Copyright © 2009 [cit. 05.03.2023]. Dostupné z: https://www.start.umd.edu/gtd/about/

[3] Incident Summary for GTDID: 202012310017. Home | START.umd.edu [online]. Copyright © 2009 [cit. 16.03.2023]. Dostupné z: https://www.start.umd.edu/gtd/search/IncidentSummary.aspx?gtdid=202012310017

[4] WebML – proces vývoje webové aplikace (specifikace požadavků) | Interval.cz. Interval.cz | Svět Internetu, Technologií a Bezpečnosti [online]. Copyright © [cit. 25.03.2023]. Dostupné z: https://www.interval.cz/clanky/webml-proces-vyvoje-webove-aplikace-specifikace-pozadavku/

[5] Funkční požadavky - PM Consulting. PM Consulting - Projektové řízení, změny, agile, management 3.0, týmy [online]. Copyright © PM Consulting [cit. 25.03.2023]. Dostupné z: https://www.pmconsulting.cz/slovnikovy-pojem/funkcni-pozadavky/

[6] Nefunkční požadavky - PM Consulting. PM Consulting - Projektové řízení, změny, agile, management 3.0, týmy [online]. Copyright © PM Consulting [cit. 02.04.2023]. Dostupné z: https://www.pmconsulting.cz/slovnikovy-pojem/nefunkcni-pozadavky/

[7] Use-Case Model - Javatpoint. Tutorials List - Javatpoint [online]. Copyright © Copyright 2011 [cit. 04.04.2023]. Dostupné z: https://www.javatpoint.com/use-case-model

[8] Lekce 3 - UML - Use Case Specifikace. itnetwork.cz - Učíme národ IT [online]. Copyright © 2023 itnetwork.cz. Veškerý obsah webu [cit. 10.04.2023]. Dostupné z: https://www.itnetwork.cz/navrh/uml/uml-use-case-specifikace-diagram

[9] What Are Wireframes? | Balsamiq Wireframing Academy [online]. [cit. 11.04.2023]. Dostupné z: https://balsamiq.com/learn/articles/what-are-wireframes

[10] Database Structure and Design Tutorial | Lucidchart. [online]. Copyright © [cit. 11.04.2023]. Dostupné z: https://www.lucidchart.com/pages/database-diagram/database-design

[11] SQL Injection | OWASP Foundation. OWASP Foundation, the Open Source Foundation for Application Security | OWASP Foundation [online]. [cit. 11.04.2023]. Dostupné z: https://owasp.org/www-community/attacks/SQL_Injection

[12] Cross Site Scripting (XSS) | OWASP Foundation. OWASP Foundation, the Open Source Foundation for Application Security | OWASP Foundation [online]. [cit. 11.04.2023]. Dostupné z: https://owasp.org/www-community/attacks/xss/

[13] What is end-user testing? How does end-user testing work? | Disbug Blog. Disbug - Capture bugs with clarity [online]. Copyright © Disbug 2021 [cit. 11.04.2023]. Dostupné z: https://disbug.io/en/blog/end-user-testing

[14] PHP: What is PHP? - Manual. PHP: Hypertext Preprocessor [online]. [cit. 12.04.2023]. Dostupné z: https://www.php.net/manual/en/intro-whatis.php

[15] What is MySQL? | DigitalOcean. DigitalOcean | The Cloud for Builders [online]. Copyright © 2023 DigitalOcean, LLC. All rights reserved. [cit. 12.04.2023]. Dostupné z: https://www.digitalocean.com/community/tutorials/what-is-mysql

[16] What is CodeIgniter? | How IT Work | Scope & Skill | Feature & Advantage. EDUCBA | Best Online Training & Video Courses Certification [online]. Copyright © 2023 [cit. 14.04.2023]. Dostupné z: https://www.educba.com/what-is-codeigniter/

[17] MVC Framework Introduction - GeeksforGeeks. GeeksforGeeks | A computer science portal for geeks [online]. [cit. 14.04.2023]. Dostupné z: https://www.geeksforgeeks.org/mvc-framework-introduction/

[18] Introduction to HTML. W3Schools Online Web Tutorials [online]. [cit. 15.04.2023]. Dostupné z: https://www.w3schools.com/html/html_intro.asp

[19] What is CSS - javatpoint. Tutorials List - Javatpoint [online]. Copyright © Copyright 2011 [cit. 16.04.2023]. Dostupné z: https://www.javatpoint.com/what-is-css

[20] What is Bootstrap - JavaTpoint. Tutorials List - Javatpoint [online]. [cit. 16.04.2023]. Dostupné z: https://www.javatpoint.com/what-is-bootstrap

[21] JavaScript pro začátečníky: co to je a jak funguje. WEB & MOBILE DEVELOPMENT AGENCY | Rascasone [online]. Copyright © [cit. 20.04.2023]. Dostupné z: https://www.rascasone.com/cs/blog/co-je-javascript-pro-zacatecniky

[22] What is Visual Studio Code?. Educative: Interactive Courses for Software Developers [online]. Copyright ©2023 Educative, Inc. All rights reserved [cit. 20.04.2023]. Dostupné z: https://www.educative.io/answers/what-is-visual-studio-code

[23] MySQL Workbench - javatpoint. Tutorials List - Javatpoint [online]. Copyright © Copyright 2011 [cit. 22.04.2023]. Dostupné z: https://www.javatpoint.com/mysql-workbench

[24] Full Lifecycle Modeling for Business, Software and Systems | Sparx Systems. UML modeling tools for Business, Software, Systems and Architecture [online]. [cit. 22.04.2023]. Dostupné z: https://sparxsystems.com/products/ea/index.html

[25] How To Install Linux, Nginx, MySQL, PHP (LEMP stack) on Ubuntu 22.04 | DigitalOcean. DigitalOcean | The Cloud for Builders [online]. Copyright © 2023 DigitalOcean, LLC. All rights reserved. [cit. 03.05.2023]. Dostupné z: https://www.digitalocean.com/community/tutorials/how-to-install-linux-nginx-mysql-php-lemp-stack-on-ubuntu-22-04

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

CSV	Comma-Separated Values
XSS	Cross-Site Scripting
SQL	Structured Query Language
PHP	Hypertext Preprocessor
HTML	Hypertext Markup Language
MVC	Model View Controller
HTTPS	HyperText Transfer Protocol Secure
DNS	Domain Name System

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHA P I: HODNOCENÍ ZADAVATELE APLIKACE

Aplikace pro správu databáze teroristických útoků je nástroj sloužící pro práci s daty týkajících se násilných útoků v Evropě, Turecku a evropské části Ruska od roku 2014. Potřeba databáze vyvstala z našeho několikaletého výzkumu měkkých cílů, násilných útoků, a to zejména jejich trendů, způsobů útoků na ně, počtu mrtvých a zraněných a mnoho dalších podrobností, které jsou pro náš výzkum nezbytné. Samotná databáze byla představena v rámci několika projektů, které jsme vedli, nebo na nich spolupracovali, a v mnoha publikačních výstupech. S narůstajícím počtem útoků se databáze stala nepřehlednou a práce s ní byla časově náročná. Proto vyvstala potřeba vytvořit předkládanou aplikaci, která by tento problém vyřešila a umožnila nám (např. na konferencích) rychle generovat grafy nebo třídit informace podle nastavených filtrů. Po podrobných testech našeho analytického týmu ohledně praktického využití aplikace lze konstatovat, že aplikace plně naplňuje naše potřeby, je velmi přehledná, intuitivní, umožňuje podrobnou práci s daty, jako je filtrování, editování, samozřejmě také mazání a export. Velkým přínosem je také geografické znázornění útoků na mapě, kde jsou zobrazeny kromě míst také základní informace o útoku, jako je např. místo, datum, modus operandi. Celkově aplikaci hodnotím velmi kladně a spolupráce se studentem byla na výborné úrovni. Ke všem připomínkám přistupoval odpovědně a snažil se vše vyřešit k naší úplné spokojenosti.