VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky

a komunikačních technologií

DIPLOMOVÁ PRÁCE

Brno, 2024

Bc. Tuan Ninh Nguyen

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

ÚSTAV TELEKOMUNIKACÍ
DEPARTMENT OF TELECOMMUNICATIONS

WEBOVÝ PROHLÍŽEČ PRO SENIORY
WEB BROWSER FOR SENIORS

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE — **Bc. Tuan Ninh Nguyen**
AUTHOR

VEDOUCÍ PRÁCE — **prof. Ing. Dan Komosný, Ph.D.**
SUPERVISOR

BRNO 2024

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

Diplomová práce

magisterský navazující studijní program **Informační bezpečnost**

Ústav telekomunikací

Student: Bc. Tuan Ninh Nguyen ***ID:*** 246483

Ročník: 2 ***Akademický rok:*** 2023/24

NÁZEV TÉMATU:

Webový prohlížeč pro seniory

POKYNY PRO VYPRACOVÁNÍ:

Vytvořte základní webový prohlížeč, který bude přizpůsobený pro seniory ve věkové skupině 90 let a více. Prohlížeč bude jednoduše ovladatelný. Implementujte ochranu proti podvodným (phishing) stránkám. Do prohlížeče integrujte podporu spolupráce s opatrovníkem seniora. Prohlížeč zhotovte v programovacím jazyce Python. Výsledky práce publikujte na repozitáři GitHub pod licencí MIT.

DOPORUČENÁ LITERATURA:

Podle pokynů vedoucího práce

Termín zadání: 5.2.2024 ***Termín odevzdání:*** 21.5.2024

Vedoucí práce: prof. Ing. Dan Komosný, Ph.D.

doc. Ing. Jan Hajný, Ph.D.
předseda rady studijního programu

Abstrakt

Diplomová práce se zabývá návrhem a implementací základního webového prohlížeče, který je přizpůsoben pro seniory ve věkové skupině 90 let a více. Je jednou z aplikací operačního systému pro seniory, který slouží pro usnadnění práce na počítači. Webový prohlížeč je vytvořen v jazyce Python. Umožňuje zvětšení textu, zobrazení webové stránky, zvukovou asistenci i ochranu proti podvodným stránkám (phishing). Prohlížeč je jednoduše ovladatelný. Každá událost v prohlížeči je zaznamenána do záznamu činnosti s různou úrovní pro vyhodnocení bezpečnostních rizik. Do webového prohlížeče je také implementováno odesílání zadaného textu na podvodné webové stránce opatrovníkovi seniora. Tím je zvýšena ochrana seniorů před podvodnými útoky. Výsledky práce jsou publikovány v repozitáři GitHub.

Klíčová slova

Webový prohlížeč, Senior, podvodná stránka, Phishing.

Abstract

The thesis deals with the design and implementation of a basic web browser that is adapted for seniors in the age group of 90 years and more. It is one of the applications of the operating system for the elderly, which is used to facilitate the work on the computer. The web browser is developed in Python. It allows text enlargement, web page display, voice assistance and protection against fraudulent sites (phishing). The browser is easy to use. Every event in the browser is logged to an activity record with different levels for security risk assessment. Sending the entered information to the guardian of the elderly person is also implemented in the web browser, which occurs if the senior launches a fraudulent web page. This increases the protection of seniors from fraudulent attacks. The results of this work are published in the GitHub repository.

Keywords

Web browser, Senior, fraudulent page, Phishing.

Bibliografická citace

NGUYEN, Tuan Ninh. Webový prohlížeč pro seniory [online]. Brno, 2024 [cit. 2024-04-25]. Dostupné z: https://www.vut.cz/studenti/zav-prace/detail/159213. Diplomová práce. Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací. Vedoucí práce Dan Komosný.

Prohlášení autora o původnosti díla

Jméno a příjmení studenta:	Bc. NGUYEN TUAN NINH
VUT ID studenta:	246483
Typ práce:	Diplomová práce
Akademický rok:	2023/2024
Téma závěrečné práce:	Webový prohlížeč pro seniory

Prohlašuji, že svou závěrečnou práci jsem vypracoval samostatně pod vedením vedoucí/ho závěrečné práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce. Jako autor uvedené závěrečné práce dále prohlašuji, že v souvislosti s vytvořením této závěrečné práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a jsem si plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č. 40/2009 Sb.

V Brně dne: 12. května 2024 .....

Podpis autora*

*Autor podepisuje pouze v tištěné verzi.

PODĚKOVÁNÍ

Rád bych poděkoval vedoucímu své diplomové práce, prof. Ing. Danu Komosnému, Ph.D., za vedení mého studia a podporu při konzultacích i při zpracování diplomové práce. Díky jeho pomoci jsem zvládl jednotlivé kroky směřující k výsledkům mé práce.

Neméně upřímně bych chtěl poděkovat své učitelce z Univerzity obrany v Brně, Mgr. Ludmile Koláčkové, Ph.D., za pomoc při studiu češtiny a svým rodičům i Hai Yen za podporu a motivaci v celém průběhu mého studia v zahraničí.

OBSAH

SEZNAM OBRÁZKŮ

Strana

SEZNAM TABULEK

Strana

SEZNAM VÝPISŮ

Strana

ÚVOD

S nástupem internetu došlo ke změnám v přístupu ke komunikaci a informacím, označovaným jako digitální revoluce. Tento jev ale není přínosný pro všechny uživatele informačních technologií. Zejména starší uživatelé se často ocitají v obtížné situaci kvůli rychlému technologickému pokroku. Proto vznikl projekt s názvem Senior Operating System, který by této kategorii uživatelů zjednodušil každodenní práci s počítačem. V tomto projektu je představen jednoduše ovladatelný webový prohlížeč pro seniory, vyvinutý v jazyce Python.

Webový prohlížeč umožňuje komfortní užívání a zaručuje uživatelskou bezpečnost při běžném používání služeb internetu. Zavádí tři klíčové funkce: zvětšení velikosti textu, zvukovou asistenci s podporou více jazyků a zabezpečení proti podvodné stránce, jejíž součástí je dynamická aktualizace databáze podvodných stránek. Poslední funkce spočívá v odeslání doplněné informace opatrovníkovi, že se uživatel pohyboval na podvodné stránce.

První funkce pomáhá těm, kteří mohou mít potíže se čtením, ale také poskytuje známou interakci pro ty, jejichž rodným jazykem není angličtina.

Druhá funkce zajišťuje, aby senioři byli chráněni proti podvodným útokům a vždy měli aktuální databázi podvodné stránky.

Poslední funkce představuje ochranu citlivých informací ve scénářích, kdy by uživatelé mohli neúmyslně ignorovat varování webového prohlížeče při připojení do podvodné webové stránky. Cílem této funkce není zasahovat do soukromí uživatele nebo získat soukromé a citlivé uživatelské informace, ale spíše fungovat jako pojistka pro zmírnění škod v případě ohrožení osobních údajů.

Diplomová práce obsahuje dvě části – teoretickou a praktickou. Je rozdělena do šesti kapitol, které shrnují základní informace o zkoumané problematice.

Kapitola 1 - Podvodné útoky - phishing - přináší základní informace o podvodném útoku, včetně charakteristického typu podvodného útoku a cíle podvodného útoku vůči seniorovi. Mimo to rovněž poskytuje způsoby detekce podvodných útoků.

Kapitola 2 - Přehled použitých nástrojů - je přehled nástrojů, které jsou používány k vytvoření webového prohlížeče. Kapitola 3 - Tvorba vlastního webového prohlížeče pro seniory - se zabývá konceptem návrhu a postupem tvorby vlastního webového prohlížeče pro seniory, jako jsou

zobrazení webové stránky, zvuková asistence, podpora více jazyků a další. Kapitola 4 - Zabezpečení webového prohlížeče pro seniory - a kapitola 5 - Pokročilé zabezpečení webového prohlížeče pro seniory - je věnována zabezpečním webového prohlížeče proti podvodné stránce, včetně zaznamenání události v webovém prohlížeči, dynamické aktualizace databáze podvodné stránky a další. Závěrečná kapitola 6 - Stažení a použití webového prohlížeče pro seniory - uvádí použití webového prohlížeče a způsob instalace webového prohlížeče.

Praktická část práce se věnuje naprogramování vlastního webového prohlížeče v jazyce Python, který je přizpůsoben pro seniory ve věkové skupině 90 let a více.

V závěru diplomové práce jsou shrnuty výsledky práce, popis řešené problematiky a jsou zde navrženy cíle pro možná vylepšení webového prohlížeče.

1. Podvodné útoky - phishing

Podvodné útoky - phishing představují významnou hrozbu pro kybernetickou bezpečnost a jsou součástí útoku sociálního inženýrství (social engineering attack), ve které se útočníci vydávají za důvěryhodné subjekty, aby tak osoby přiměli k poskytnutí citlivých osobních údajů, jako jsou údaje o pojištěných kartách, osobních identifikačních údajích, rodném čísle, bankovních údajích, účtu i hesle v sociálním médiu atd. [1]. Následky těchto útoků jsou nepředvídatelné, závisejí na cíli útočníků.

Úspěšný podvodný útok je značně závislý na psychologické manipulaci uživatelů. Útočníci využívají lidské slabosti, jako jsou důvěra a strach, aby přiměli oběti k rychlé reakci bez řádné kontroly. Například uživatel získá upozornění z e-mailu své banky, že bude jeho bankovní účet uzavřen za 24 hodin, pokud příjemce okamžitě neověří své osobní údaje kliknutím na uvedený odkaz.

Obvykle se podvodné útoky provádí prostřednictvím e-mailu, ale mohou se objevit i prostřednictvím jiných elektronických komunikačních kanálů [1]. Existují sociální média jako Facebook, Telegram nebo Twitter - rychlé zasílání zpráv, ve kterých sdílejí odkazy do podvodné webové stránky. Kvůli rozmanitým médiím je obtížné zajistit bezpečnosti proti podvodnému útoku - phishing. Uživatelé často kliknou na uvedený odkaz, který obsahuje dynamické vkládání přílohy, nebo stáhnou danou přílohu, která se zdá být legitimní, ale obsahuje škodlivý kód určený k získání identity uživatele nebo ohrožení dat. V některých případech jsou uživatelská data zašifrována kvůli stahování ransomware.

Podvodný útok by mohl být prováděn rozsáhle a škodlivě. Útočníci se mohou zaměřit na jednotlivce nebo společnosti na více úrovních. U jednotlivců mohou útočníci získat přímý přístup k bankovním účtům nebo občanskému průkazu, aby mohli provádět neoprávněné on-line nákupy i převádět finanční prostředky na své dočasné bankovní účty dříve, než si to oběť uvědomí. Kvůli nepoužití jejich osobních údajů je velmi obtížné zjistit, kdo je útočník.

Kromě předchozích případů mohou útočníci používat osobní údaje k tomu, aby si brali půjčky, páchali trestnou činnost nebo prováděli nezákonnou činnost pod jménem oběti.

U organizace by jediné narušení takovýmto útokem mohlo vést k ztrátě značné sumy peněz a ohrožení velkého množství citlivých osobních i organizačních údajů, což by mohlo mít dopad na

zákazníky, zaměstnance a provoz podniku. Po úspěšném útoku čelí organizace s významnou ztrátou důvěry zákazníků a dlouhodobou poškozením pověsti společnosti.

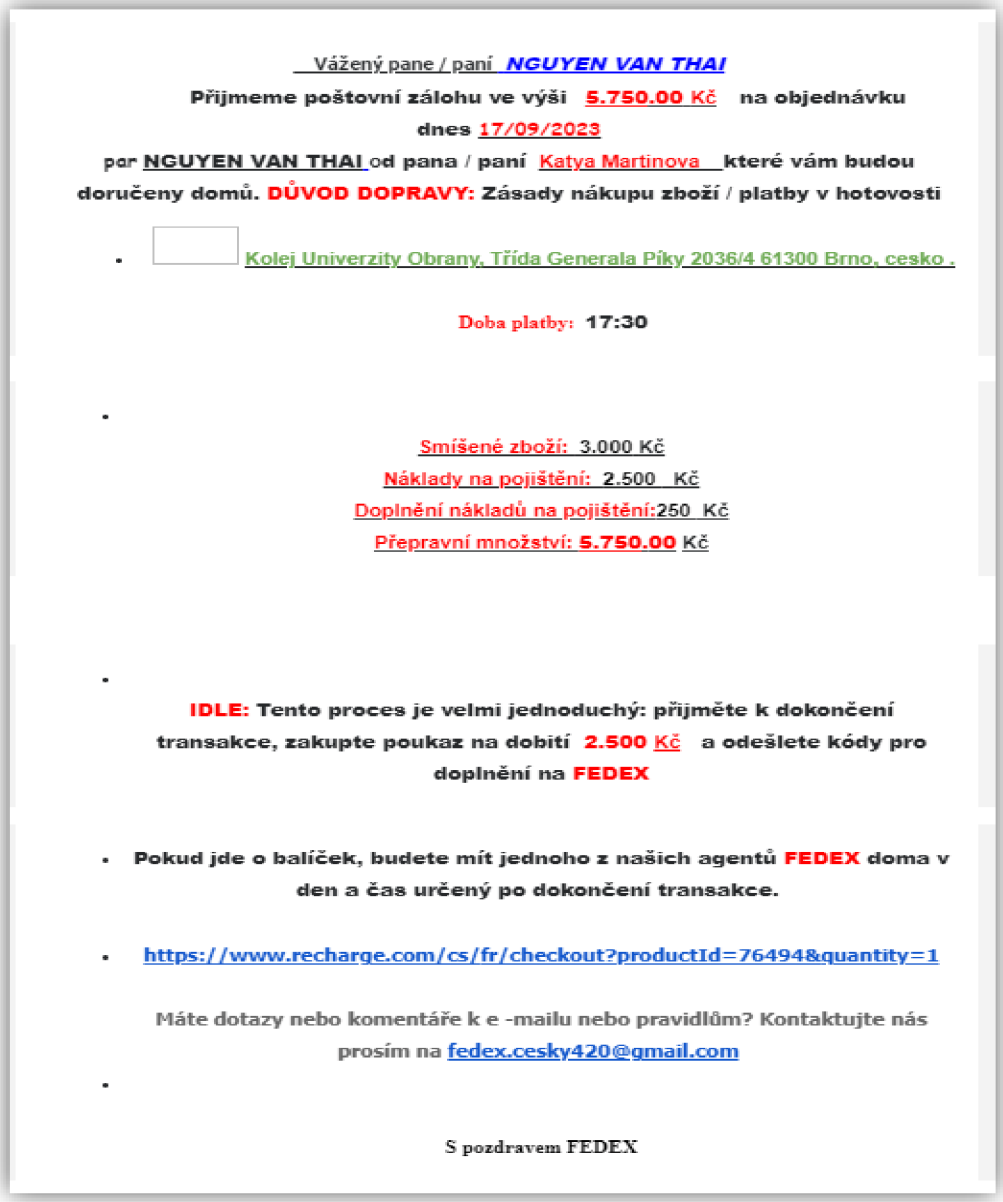
V následujících kapitolách je detailně představen podvodný útok. V kapitole 1.1 Typické typy podvodných útoků - jsou uvedeny charakteristické typy podvodných útoků, jako jsou phishing, vishing, smishing a další. Cíl podvodného útoku na seniory je popsán v kapitole 1.2 Cíle podvodného útoku na seniory a detekce podvodných útoku - je uveden v kapitole 1.3 Detekce podvodných útoků.

1.1 Typické typy podvodných útoků

Existuje mnoho typů podvodných útoků, které obsahují podvodnou stránku. Může to být e-mail phishing, spear phishing, whaling a další. V rámci této práce představíme pouze pět typických typů.

Podvodný útok – e-mail phishing

Podvodný útok – e-mail phishing nebo útok phishing přes e-mail představuje klamavou techniku, která je používána k tomu, aby útočníci jednotlivce přiměli k vyzrazení citlivých osobních informací [2]. Jedná se o nejstarší i nejčastější útok. Obrázek 1.1 zobrazí vlastní reálný podvodný útok přes e-mail, ve kterém útočník uložil uvedený odkaz pro dopravní platbu od organizace Fedex při objednávce.



Vážený pane / paní **NGUYEN VAN THAI**

Přijmeme poštovní zálohu ve výši 5.750.00 Kč na objednávku dnes 17/09/2023

par NGUYEN VAN THAI od pana / paní Katya Martinova které vám budou doručeny domů. DŮVOD DOPRAVY: Zásady nákupu zboží / platby v hotovosti

- Kolej Univerzity Obrany, Třída Generala Píky 2036/4 61300 Brno, cesko .

Doba platby: **17:30**

- Smíšené zboží: 3.000 Kč
  Náklady na pojištění: 2.500 Kč
  Doplnění nákladů na pojištění:250 Kč
  Přepravní množství: **5.750.00** Kč

- **IDLE: Tento proces je velmi jednoduchý: přijměte k dokončení transakce, zakupte poukaz na dobití 2.500 Kč a odešlete kódy pro doplnění na FEDEX**

- **Pokud jde o balíček, budete mít jednoho z našich agentů FEDEX doma v den a čas určený po dokončení transakce.**

- https://www.recharge.com/cs/fr/checkout?productId=76494&quantity=1

Máte dotazy nebo komentáře k e -mailu nebo pravidlům? Kontaktujte nás prosím na fedex.cesky420@gmail.com

S pozdravem FEDEX

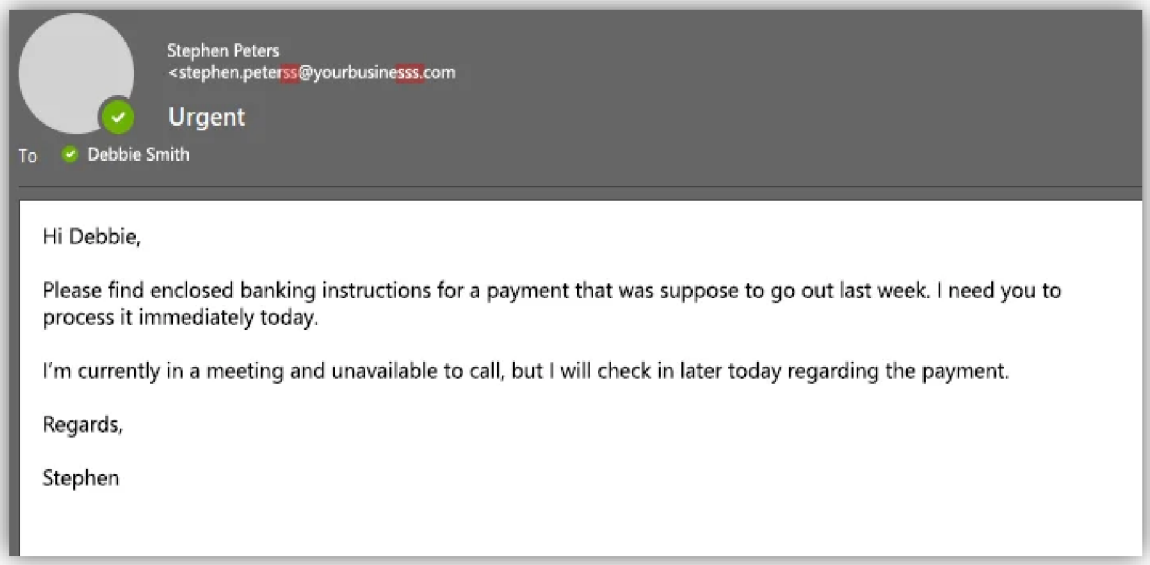
Obrázek 1.1: Vlastní reálný podvodný útok přes e-mail

Obvykle by šlo o zasílání e-mailů, které se tváří jako kdyby pocházely z důvěryhodných zdrojů, jako jsou poskytovatelé některé služby, například internetová služba nebo dopravní služba, banky nebo kolegové a přátelé.

E-mail od útočníků vyvolává pocit naléhavosti nebo poplachu, což by mohlo vést k finanční ztrátě, automatickému stahování malwaru do systému oběti, když klikne na odkaz v příloze a další.

Podvodný útok – whaling

Ve srovnání s jinými podvodnými útoky se podvodný útok whaling zaměří na vysoce postavené manažery, jako jsou vojenští velitelé, vedoucí pracovníci nebo známé osobnosti a další. Nejsou náhodné jako v podvodném útoku – phishing, obvykle jsou pečlivě naplánované a provedené. Zpravidla zahrnují důkladný průzkum, aby byla podvodná komunikace co nejpřesvědčivější. Kvůli tomu je velmi obtížné rozpoznat tento typ útoku. Reálná zpráva podvodného útoku – whaling je zobrazena v obrázku 1.2.



Obrázek 1.2: Zpráva od podvodného útoku - whaling [3]

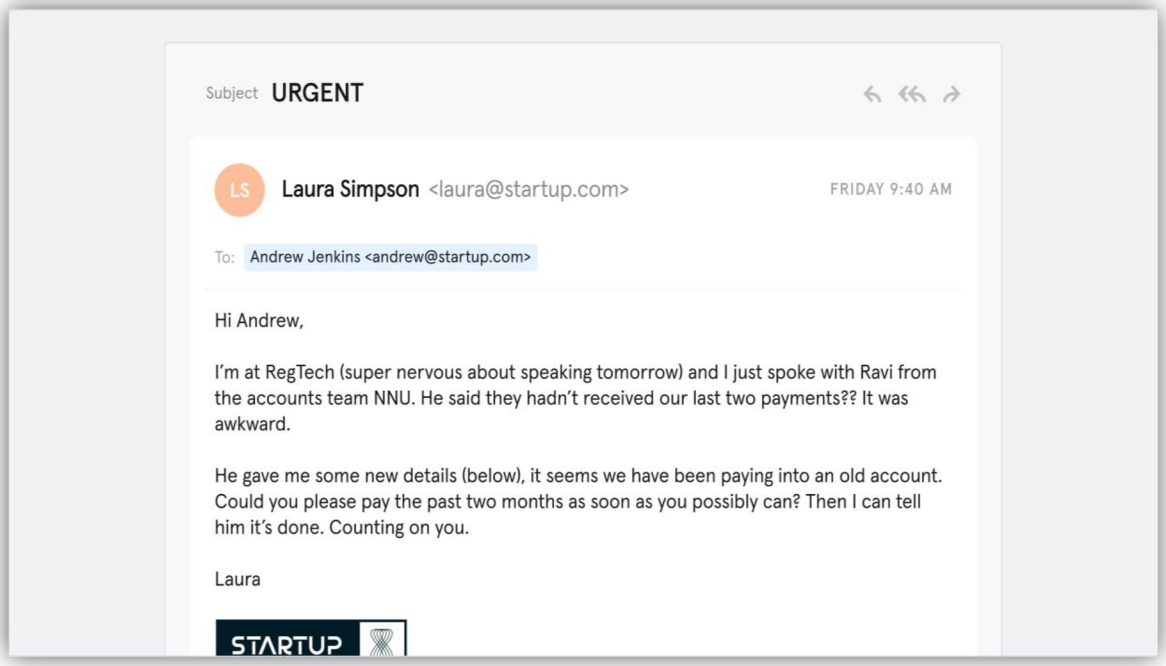
K napadení oběti vytvářejí útočníci e-maily, které se týkají konkrétní záležitost napodobující styl a tón korespondence, jakou cílová osoba očekává. Zahrnuje falšování známých e-mailových adres, používání záznamu organizace a napodobování stylu psaní nebo důvěryhodných kontaktů [4]. Také důsledky tohoto útoku mohou být závažné, včetně vysokých finančních ztrát nebo úniku velmi citlivých firemních dat.

Podvodný útok – spearphishing

Podvodný útok - spear phishing - je speciální útok, který se zaměřuje na konkrétní osoby nebo organizace. Podobně jako podvodný útok - whaling se využívá personalizované informace, díky čemuž jsou obtížně odlišitelné od legitimní komunikace a bývají velmi účinné. Proto je obvykle iniciována prostřednictvím elektronické komunikace jako e-mail. Obrázek 1.3 uvádí proces implementace toho podvodného útoku.

Obrázek 1.3: Proces implementace podvodného útoku - spearphishing [5]

K získání personalizované informace může být použito sledování cílových účtů na sociálních sítích, kde by osobní informace mohla být veřejná, úniků dat od různých předchozích útoků nebo zakoupení takové informace na černém trhu. Tato osobní informace útočníkům pomůže přesvědčivě napodobit známé subjekty. Cílem útoku je dosáhnout na přihlašovací údaje, jako je účet nebo heslo a stažení malwaru do systému oběti. Obrázek 1.4 zobrazuje jednu zprávu podvodného útoku – spearphishing.



Obrázek 1.4: Reálný podvodný útok - spearphishing [32]

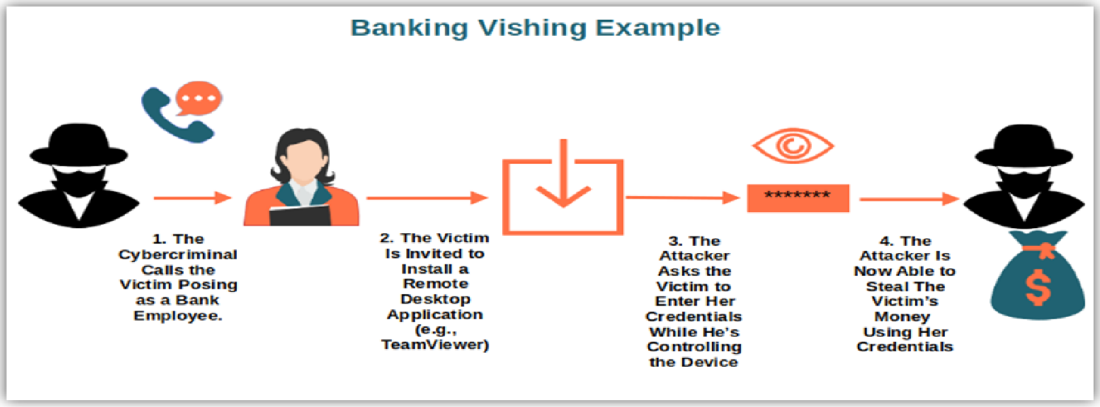
Podvodný útok – smishing

Podvodný útok - smishing nebo podvodný útok SMS phishing je metoda, která používá zasílání textových zpráv (SMS), které vypadají, jako by pocházely z důvěryhodných zdrojů jako banky, poskytovatelé některých služeb nebo vládní agentury [6]. Cílem je zveřejňování citlivých osobních údajů, jako jsou přihlašovací údaje, čísla kreditních karet nebo identifikovaný kód pro převod peněz přes banku a další. Navíc textová zpráva obsahuje stručnou strukturu, která by mohla omezit míru kontroly věnujícího příjemce, čímž se zvyšuje pravděpodobnost úspěšného podvodu. Obrázek 1.5 zobrazuje podvodnou textovou zprávu přes chytrý telefon.

Obrázek 1.5: Podvodná zpráva SMS přes chytrý telefon [7]

Podvodný útok – vishing

Podvodný útok - vishing nebo útok voice phishing je závažná kybernetická hrozba, která využívá telefonní službu k podvodnému vynucení důvěrných informací. Na rozdíl od tradičního typu podvodných útoků, který využívá sociální metodu komunikace, je podvodný útok - vishing prováděn prostřednictvím hlasových hovorů. Kromě toho mohou útočníci používat různé taktiky, včetně podvržení identifikace volajícího, který předstírá, že hovor přichází z uznávaného čísla nebo automatických hlasových zpráv, které přesměrují příjemce k zadání čísla účtu nebo hesla [6].



Obrázek 1.6: Proces implementace podvodného útoku - vishing [8]

1.2 Cíle podvodného útoku na seniory

V předchozí kapitole je uvedeno, že podvodný útok je významnou hrozbou pro všechny uživatele, kteří komunikují na internetu. Je pozorovatelný zejména u seniorů, protože jsou zranitelní v důsledku různých faktorů, včetně potenciálního nedostatku zkušeností s digitálními sítěmi a nízkými technologickými znalostmi [11]. Obvykle útočníci zneužívají důvěry a možné nízké znalosti seniorů o technologii, když jsou připojeni k internetu, aby získali osobní údaje a informace o finanční situaci uživatelů [9].

Závažné důsledky úspěšného podvodného útoku na seniory by mohly znamenat ztrátu uživatelské identity, ztrátu peněz z důchodu nebo narušení osobní bezpečnosti, což by mohlo být náročné vyřešit [10].

Kvůli tomu jsou bezpečné webové prohlížeče v souvislosti se seniory nezbytné proti uvedeným hrozbám. Webový prohlížeč by měl mít přísná bezpečnostní opatření, jako jsou varování při zobrazení podvodné webové stránky nebo automatické blokování škodlivých stránek, aby pomáhaly těm, kteří nejsou obeznámeni s technologií.

V rámci této diplomové práce vytváříme webový prohlížeč s ochranou proti podvodnému útoku. Obsahuje zvukové varování při zobrazení podvodné webové stránky i změnu barvy tlačítka na červenou barvu, která upoutá pozornost uživatelů. Na konci je každá činnost na webové stránce zaznamenána do záznamu činnosti pro vyhodnocení bezpečnostních rizik.

1.3 Detekce podvodných útoků

Pro rozpoznání podvodných útoků je nezbytné poznat jejich běžné znaky, které vedou k podezřelé komunikaci [12]. Některé znaky pro detekci podvodných útoků uvádí Tabulka 1.1.

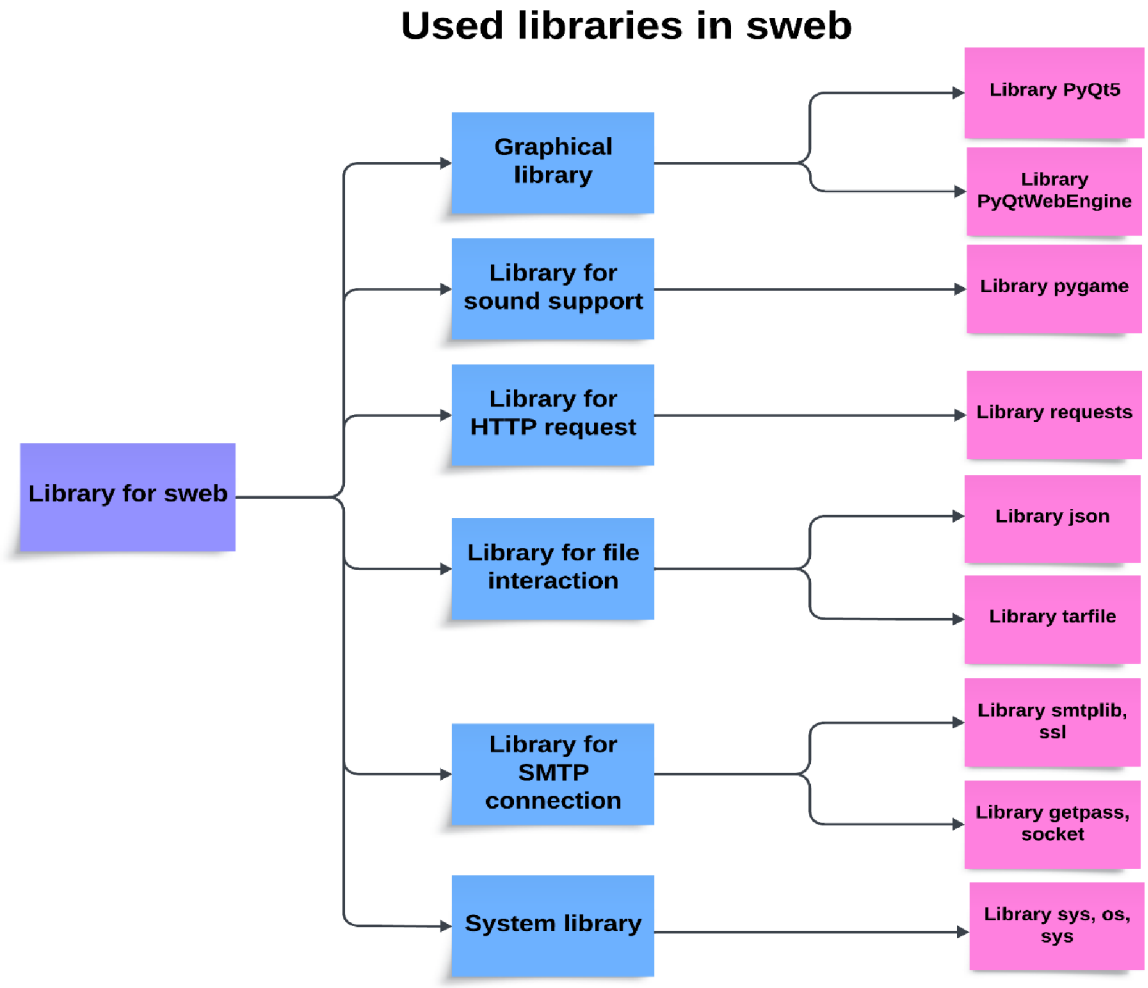
Tabulka 1.1: Detekce podvodných útoků

Běžné znaky	Popis
Podezřelé e-mailové adresy [1]	E-mailová adresa odesílatele by mohla mít překlepy nebo nesprávné znaky, kterými se liší od oficiálních adres. Například: fedex.cesky420@gmail.com, vut100@vut.cz,...

Obecný pozdrav	Obvykle používá obecný pozdrav místo jména, což znamená, že nebyl vytvořen osobně. Například: Ahoj, dobrý den pane/paní,...
Pravopisné a gramatické chyby	Organizace mají profesionální vysokostupňový psací standard pro komunikaci se svými zákazníky, pracovníky nebo společníky. Proto je e-mail plný chyb varovným signálem pro podvodný útok.
Pocit naléhavosti a hrozby	Často se jedná o falešný pocit naléhavosti nebo bezprostředního nebezpečí s cílem rychlého jednání bez řádné kontroly. Obvykle je to upozornění z banky nebo vládní agentury. Například: Bankovní karta bude blokována za 24 hodin, bankovní karta byla používána v zahraničí a potřebuje verifikaci,...
Neprofesionální design e-mailů [1]	Špatný design nebo nekvalitní obrázky by mohly být pokusem podvodného útoku. Například: Špatná struktura e-mailů, mnoho typů textu v jednom e-mailu, fotka není ostrá,...
Požadavek na osobní údaje	Legitimní organizace nikdy nepožaduje citlivé informace přes e-mail nebo telefonní hovor (heslo, údaje o bankovních účtech nebo identifikovaný kód pro verifikaci převodu peněz).
Neobvyklé přílohy nebo odkazy	E-mail může obsahovat odkazy, které vypadají legitimně, ale přesměruje na škodlivé podvodné stránky nebo obsahuje přílohu, ve které může infikovat systém malwarem, když je otevřená.
Nebezpečné adresy URL [1]	Bezpečná webová stránka má často https na začátku webové adresy URL. V případě chybí, pravděpodobně není legitimní.
Neshodné adresy URL	Najetí na jakýkoliv odkaz v e-mailu se v prohlížeči zobrazí skutečná adresa v dolní části. Pokud text odkazu neodpovídá zadané adrese URL, jedná se pravděpodobně o podvodný útok.

2. Přehled použitých nástrojů

V této kapitole jsou uvedeny použité nástroje pro vytvoření webového prohlížeče, jako jsou grafická knihovna, systémová knihovna, knihovna pro podporu zvuk, knihovna pro zpracování HTTP požadavku i odpovědi a další. Obrázek 2.1 zobrazuje přehled použitých nástrojů.



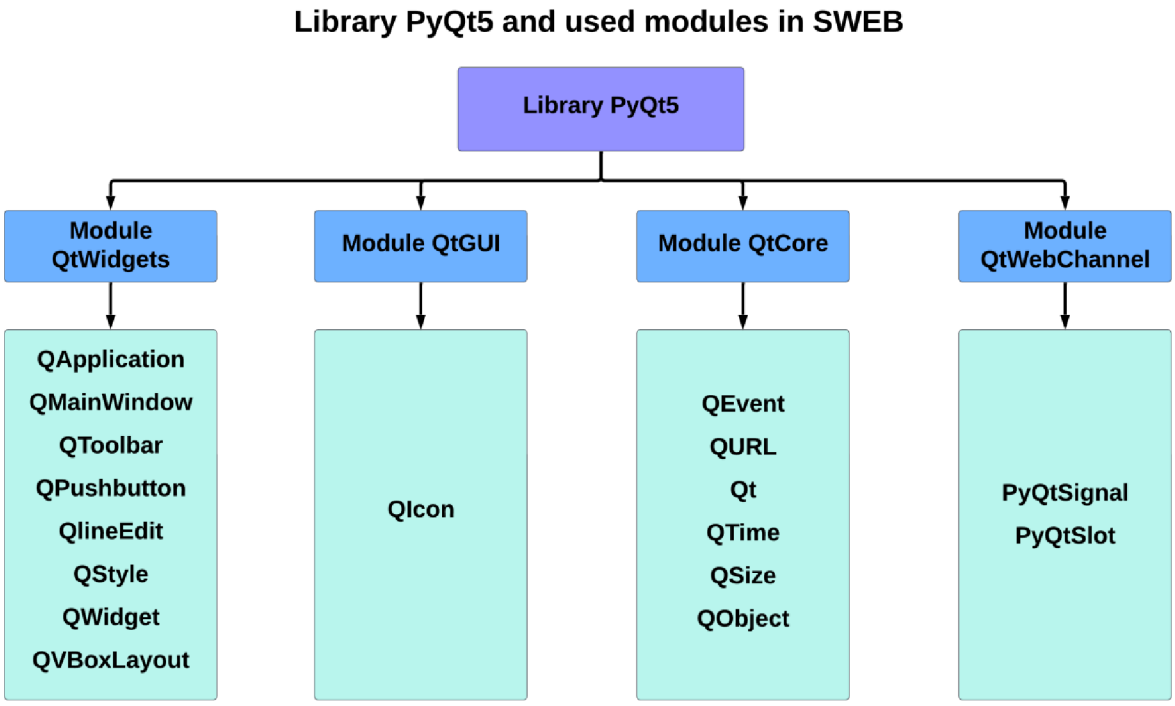
Obrázek 2.1: Přehled použitých nástrojů pro vytvoření swebu

2.1 Grafická knihovna

Grafická knihovna se slouží k vytvoření rozhraní webového prohlížeče pro seniory, zobrazení webového obsahu v prohlížeči, vytvoření vztahu mezi aplikačními prvky a další. V rámci této diplomové práce jsou používány knihovna PyQt5 a knihovna PyQtWebEngine.

2.1.1 Knihovna PyQt5

Knihovna PyQt5 je klíčovým nástrojem při vývoji grafických uživatelských rozhraní (GUI) [13]. Kromě této knihovna je knihovna PyQtWebEngine používána k integraci webového obsahu do webového prohlížeče vytvořených pomocí knihovny PyQt5. Obě knihovny jsou detailně představeny v následující kapitole.



Obrázek 2.2: Knihovna PyQt5 a použité moduly v SWEB

Proti jiným knihovnám má knihovna PyQt5 tyto výhody:

- Pokročilá grafika a přizpůsobení: Podporuje pokročilou grafiku a přizpůsobení komponentu uživatelského rozhraní (UI) pomocí sady aplikačních prvků, což umožňuje navrhnout webový prohlížeč, který je intuitivní a známý pro seniory.
- Bohatá sada aplikačních prvků: Poskytuje mnoho aplikačních prvků, které lze použít k vytvoření funkčního a atraktivního uživatelského rozhraní. Je to důležité zejména pro seniory, protože lze přizpůsobit velké, snadno čitelné texty a tlačítka.

- Mechanismus signálů a slotů: Používá mechanismus signálů a slotů pro komunikaci mezi objekty, který pomáhá vytvářet interaktivní aplikaci. Toho lze využít ve webovém prohlížeči pro zpracování uživatelských činnosti, jako jsou kliknutí, vyplnění zadané adresy nebo přehrání zvuků.

- Integrace s webovými technologiemi: Obsahuje modul QtWebEngineWidgets, který umožňuje bezproblémové vkládání webového obsahu do webové aplikace. Modul QtWebEngine poskytuje prostředky pro prohlížení webových stránek bez samostatné instalace prohlížeče, což je klíčová část pro vytvoření webového prohlížeče [14].

2.1.1.1 Modul QtWidgets

Modul QtWidget je používán pro vytváření grafického uživatelského rozhraní (GUI). Poskytuje intuitivní sadu prvků uživatelského rozhraní (UI). Jeho význam spočívá v tom, že nabízí vysokou míru přizpůsobení, ale velmi jednoduché použití [18]. Proto by mohl vyhovovat potřebám starších uživatelů, jako jsou snadno čitelné texty a větší zobrazení tlačítka s danou připojenou navigací. V rámci této diplomové práce jsou některé třídy v tomto modulu používány, jako např. QApplication, QMainWindow, QToolbar, QPushButton a další. K instalaci tříd je používáno příkazem import. Výpis 2.1 zobrazí příkaz, který je používán ve webovém prohlížeči pro seniory.

Výpis 2.1: Import potřebných tříd z modulu QtWidgets

```
from PyQt5.QtWidgets import QLineEdit, QPushButton, QToolBar, QWidget
from PyQt5.QtWidgets import QMainWindow, QApplication, QStyle, QLabel,
QVBoxLayout
```

Třída QApplication

Třída QApplication je základem každé aplikace PyQt5, která spravuje hlavní nastavení a řídicí tok grafického uživatelského rozhraní (GUI) [19] a poskytuje nezbytnou infrastrukturu pro zpracování událostí (Event) a komunikaci s jinými aplikačními prvky. Což znamená, že zpracovává inicializaci i finalizaci aplikace, uživatelské činnosti v aplikaci a čistí úkoly při ukončení aplikace. Pro webový prohlížeč zaměřený na starší osoby ve skupině věku 80 a 90 let má velký význam pro zajištění toho, aby aplikace stále reagovala na interakce uživatelů [11].

Třída QMainWindow

Třída QMainWindow vytvoří hlavní okno aplikace, které je navrženo jako centrální okno připojující se všemi funkcemi standardních oken, včetně panelu "toolbar", panelu "statusbar" a centrální oblast, která by mohla obsahovat libovolné aplikační prvky. Pro seniory nabízí strukturovaný způsob uspořádání aplikačních prvků, který zajišťuje, že je uživatelské rozhraní snadno ovladatelné i pro uživatele s nižšími technickými znalostmi.

Třída QToolBar

Třída QToolbar je univerzální, může být přidána do hlavního okna pro rychlý přístup k nejčastěji používaným aplikačním prvkům nebo funkcím webové aplikace. Lze ji přizpůsobit specifickým potřebám starších uživatelů, jako jsou možnost ovládání sady aplikačních prvků pro lepší viditelnost. Umožňuje i změnit polohy panelu v hlavním okně aplikace, aby bylo lépe dosažitelné.

Třída QWidget

Třída QWidget slouží jako základní prvek pro vytváření grafického uživatelského rozhraní. Nabízí funkce pro správu tlačítek, oken zobrazení a dalších komponent grafického uživatelského rozhraní. Tato třída zapouzdřuje chování prvků uživatelského rozhraní a umožňuje přizpůsobení a uspořádání prvků v oknech aplikace.

Třída QPushButton, QStyle a QLabel

Třída QPushButton vytvoří jednoduché tlačítko, kterým lze provést akci stisknutím nebo kliknutím a další [20]. Jedná se o základní aplikační prvek při vytváření grafického uživatelského rozhraní, který uživatelům umožňuje jasně a přímo iniciovat akce. Na tlačítku by mohl být přidán text i ikona. Standardní ikona může být přizpůsobena pomocí třídy QStyle, která zajišťuje, že jsou vizuálně atraktivní a snadno rozpoznatelná pro starší osoby. Text může být přizpůsoben třídě QLabel, který poskytuje objasnění funkce tlačítka.

Trída QVBoxLayout

Zarovnání má zásadní význam pro jednoduché používání a čitelnost. Pomocí třídy QVBoxLayout by se ikona a text mohly ukládat vertikálně. Třídu QVBoxLayout lze přizpůsobit potřebám starších uživatelů a umísťovat nejpoužívanější tlačítka na vhodném místě.

Třída QLineEdit

U třídy QLineEdit se jedná o jednořádkové textové pole, do kterého by uživatelé mohli zadávat určený text [21]. Lze je nakonfigurovat pro různé případy použití, jako jsou doplněná pole hesla nebo textová pole pro vyhledávací dotazy.

V rámci této práce je používána pro vytvoření zadávací textové pole na webovou stránku, do které by se uživatelé chtěli zobrazit nebo pouze uvést dotaz.

2.1.1.2 Modul QtGUI

Modul QtGUI je základní modul pro vývoj grafických aplikačních prvků grafického uživatelského rozhraní [22]. V tomto modulu má třídu QIcon, která umožňuje vytvářet vlastní ikony a zlepšovat uživatelský zážitek při používání aplikace. Jeho schopnost škálovatelnosti zajišťuje přehlednost ikony nejen v jakékoli velikosti, což je zásadní pro staršího uživatele. Navíc umožňuje nastavení barevného kontrastu a velikosti pro různé úrovně zrakové ostrosti.

2.1.1.3 Modul QtCore

U modulu QtCore se jedná o mimografické uživatelské rozhraní (non-GUI), které je klíčové pro správu základní mechaniky aplikace [23]. Modul obsahuje nejen operaci se soubory, zpracování události, manipulaci s datem i časem, ale navíc i mechanismus signálů a slotů. Funkce modulu zajišťuje, že je webový prohlížeč stále interaktivní, což je klíčové při navrhování pro starší občany. Import potřebných tříd pro webový prohlížeč z toho modulu je uveden ve výpisu 2.2.

Výpis 2.2: Import použitých tříd z modulu QtCore

```
from PyQt5.QtCore import QEvent, QUrl, Qt, QTimer, QSize
from PyQt5.QtCore import pyqtSignal, QObject, pyqtSlot
```

Dále mechanismus signálů a slotů umožňuje vzájemnou komunikaci prvků v aplikaci. To je velmi důležité ve webovém prohlížeči, kde jsou běžné akce jako kliknutí na odkaz, odeslání formuláře nebo aktualizace stránky. V rámci této diplomové práce je používáno několik tříd z tohoto modulu, jako jsou QEvent, QUrl, Qt, PyQtSignal a další. Přehled použitých tříd z toho modulu je uveden v předchozím obrázku 2.1.

Třída QEvent

Třída QEvent je používána pro správu události v aplikaci a zachycení různých akcí uživatele, když komunikuje s aplikací [35]. Navíc jsou ještě používány ke spuštění příslušných reakcí. To je nezbytné pro zajištění dynamického a interaktivního zážitku u starších uživatelů, kteří se by mohli spoléhat na webový prohlížeč.

Třída QURL a třída Qt

Třída QURL umožňuje správně interpretovat a zpracovávat webové adresy URL. Pomocí této třídy by uživatelé mohli efektivně a bezpečně procházet webovou stránkou, což je nezbytné pro ochranu před podvodnou stránkou.

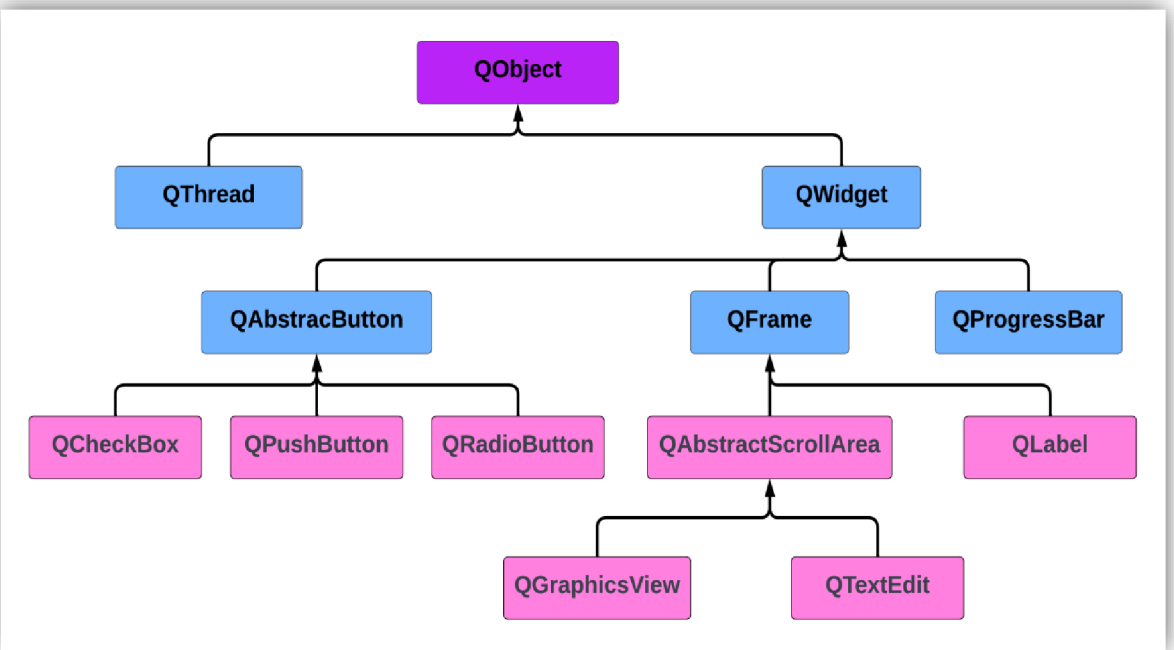
Třída Qt obsahuje globální identifikátor a pomocné funkce, které definují vlastnost objektů v aplikaci. Jsou používány v celé aplikaci, aby se zachovala konzistence chování a vzhledu aplikace. V rámci této diplomové práce je třída používána k odstranění standardního parametru hlavního okna.

Třída QTime a třída QSize

Třídy QTime a QSize poskytují funkce pro sledování i nastavení času a správu rozměrů oken a aplikačních prvků, čímž zajišťují, že aplikace je časově orientovaná a vizuálně uspořádaná. Obě těchto parametrů času a rozměrů oken jsou získány z uživatelského zařízení.

Třída QObject

Třída QObject je základní třída pro všechny objekty Qt, která umožňuje reagovat na různé události v aplikaci, například na akce uživatele, jako jsou reakce na vstupy uživatele a zachycení jejich vstupů [36]. Při vytváření hierarchií objektů QObject zjednodušuje správu a zajišťuje organizovanou strukturu komponent aplikace. Tento hierarchický systém je nezbytný pro uspořádání prvků ve webovém prohlížeči a je uveden v obrázku 2.3.



Obrázek 2.3: Hierarchický systém pro uspořádání prvků objektu Qobject [37]

2.1.1.4 Modul QtWebChannel

Modul QtWebChannel nabízí klíčovou schopností interagovat mezi aplikacemi Qt a jazyky HTML/Javascript, které běží ve webovém enginu. Základní mechanismus QtWebChannel zahrnuje vystavení tříd C++ odvozených od třídy QObject do HTML/JavaScript. Tím by se mohlo vytvořit obousměrný komunikační kanál, ve kterém mohou aplikace i webový obsah iniciovat interakce [38]. V této diplomové práci je používán k zachycování textu, který uživatele doplní do podvodné stránky po zvukovém varování. Tato funkce je prováděna změnou vlastnosti doplněné textové pole a zachycením signálu po ukončení doplnění.

Změna obsahu HTML, kterou poskytuje modul QtWebChannel, umožňuje dynamicky měnit obsah webové stránky zobrazené ve webovém prohlížeči. Možnost zvětšování velikosti textu je užitečná pro seniory zejména tím, že upravuje rozvrh pro zjednodušení navigace.

Navíc díky zachycování textového vstupu od uživatele do podvodné webové stránky může prohlížeč nabídnout funkce, jako jsou přizpůsobené možnosti vyhledání a prediktivní zadávání textu. Tyto funkce mohou zmírnit problémy na potíže s psaním.

Signál PyQtSignal

Signál PyQtSignal – jedná se o výkonnou funkci PyQt5, která umožňuje vytvářet komunikaci mezi jednotlivými objekty prohlížeče a navíc přizpůsobit vlastní signály. Tak zajišťuje aktualizaci a interakci webového prohlížeče v reálném čase [24]. Když by uživatelé kliknuli na tlačítko pro přechod na domovskou stránku nebo otevření nové karty, tato třída signálu zajistí, že tyto akce okamžitě vyvolají odpovídající reakce. Ještě lze využít k upozornění prohlížeče na provedení specifických akcí, jako je aktualizace zobrazení po dokončení načítání stránky nebo při zpřístupnění nového obsahu.

Signál pyqtSlot

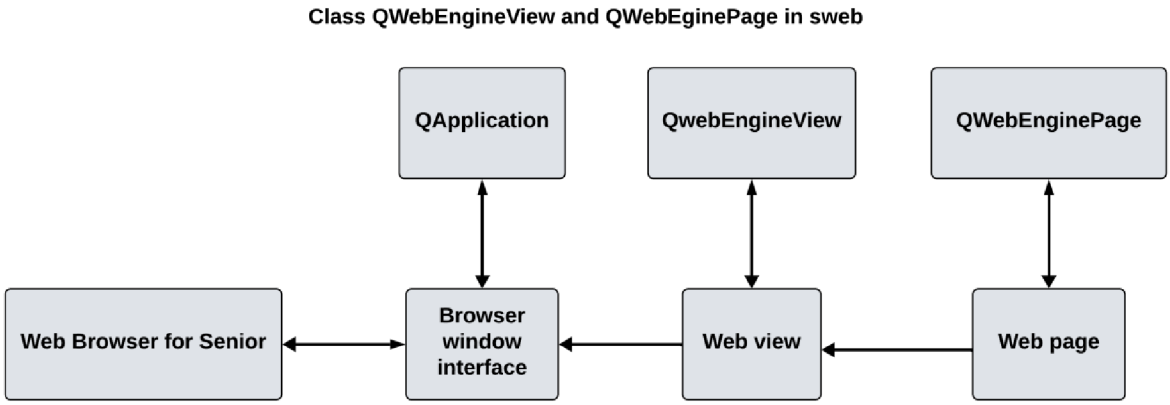
Signál pyqtSlot je navržen jako mechanismus signálů a slotů. Mechanismus funguje tím, že označuje funkce jako sloty, které potom lze připojit k signálům. S použitím pyqtSlot se zvyšuje nejen výkonnost, ale také bezpečnost aplikace. Ve webovém prohlížeči je tato přesnost důležitá.

2.1.2 Knihovna PyQtWebEngine

Knihovna PyQtWebEngine je navržena společností The Qt Company pro sadu vazeb jazyka Python. Tato knihovna poskytuje možnosti integrace webového obsahu do aplikací vytvořených pomocí knihovny PyQt5 a umožňuje bezproblémově vkládat webové stránky. Nabízí komplexní sadu funkcí, jako jsou funkce pro vykreslování webového obsahu, spouštění JavaScriptu a manipulaci s webovými prvky ve webové stránce. V rámci této diplomové práce je používán modul QtWebEngineWidget.

Modul QtWebEngineWidget

Modul QtWebEngineWidget poskytuje mnoho tříd pro vkládání webového obsahu do webové aplikace. Také je nezbytnou součástí pro vývoj moderních webových prohlížečů [15]. V rámci této diplomové práce jsou v tomto modulu používány dvě základní třídy - QWebEngineView a QwebEnginePage, které jsou uvedeny v obrázku 2.4.



Obrázek 2.4: Třída QWebEngineView a třída QWebEnginePage

Třída QWebEngineView

Třída QWebEngineView je důležitá třída, která je používána k zobrazení webových stránek nebo k načtení webového obsahu. Funguje jako kontejner, ve kterém se uloží webový obsah a poskytuje mnoho metod pro navigaci funkce vpřed nebo zpět v historii webové stránky, zvětšování nebo zmenšování a další typické způsoby interakce s webovou stránkou [16]. Pro seniory lze přizpůsobit tak, aby zobrazoval webový obsah i webové rozhraní s větším textem a jednoduššími navigačními ovládacími prvky, což zvyšuje použitelnost a čitelnost.

Třída QWebEnginePage

Třída QWebEnginePage oproti třídě QWebEngineView řídí chování webového obsahu. Představuje pouze jedno okno webové stránky a je zodpovědná za provádění čtení obsahu v souboru JavaScript a vykreslení webového obsahu. Ještě poskytuje několik způsobů pro kontrolu chování webových prvků a zpracování události (Event) související s webovou stránkou, jako

kliknutí na webový odkaz, stahování souborů [17]. Je nezbytná k tomu, aby umožňovala přepsat výchozí chování linek, které je klíčové pro ochranu seniorů před podvodnou stránkou a dalšími škodlivými aktivitami on-line.

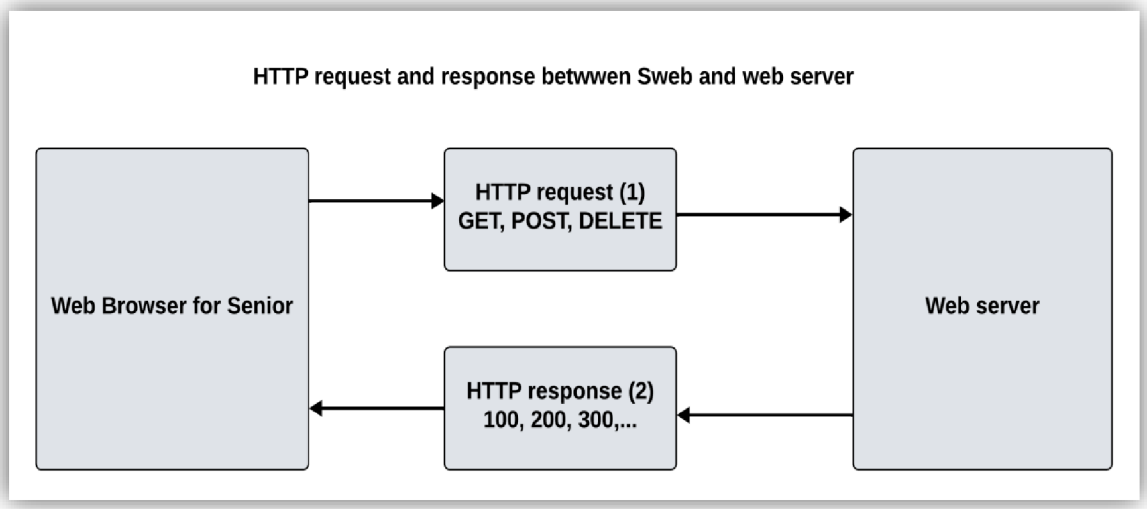
2.2 Knihovna pro podporu zvuku

Knihovna pygame je open-source knihovna, která je určená pro multimediální aplikaci v programovacím jazyce Python. Zjednodušuje vývoj webového prohlížeče pro seniory tím, že poskytuje moduly pro práci s grafikou a zvukem [25].

V rámci této diplomové práce je nutné pro přehrání zvuku, když uživatelé najedou myší na tlačítko i upozorňuje, že zobrazí podvodné webové stránky. Navíc pygame zahrnuje správu zvuku a podporuje různé zvukové formáty, které umožňují ovládání zvuku na pozadí ve webovém prohlížeči.

2.3 Knihovna pro zpracování požadavků a odpovědi HTTP

Knihovna requests je používána pro odesílání požadavků HTTP, která zjednodušuje proces zadávání požadavků do dané webové stránky a potom zpracování odpovědí webové stránky, aniž by bylo nutné ručně zpracovávat nebo odesílat data [39].



Obrázek 2.5: HTTP požadavek a odpověď mezi SWEB a serverem

Jedna z hlavních výhod knihovny je jednoduchost při provádění různých typů HTTP požadavků, jako jsou GET, POST, DELETE a další [26], jako jsou zobrazeny v obrázku 2.5.

2.4 Knihovna pro interakce se souborem

Při vývoji webového prohlížeče pro seniory je nutné zpracovat funkci s textovým souborem, souborem typu JSON a souborem typu TAR. Proto jsou knihovna JSON a knihovna tarfile používány.

Knihovna JSON

Knihovna json nabízí přímou metodu pro převod objektů v programovacím jazyce Python do správného formátu souboru JSON a dekódování dat JSON zpět do objektů Python. V projektu Senior Operating System jsou všechna konfigurační data uložena v souboru json, proto je tato knihovna velmi důležitá pro import dat do aplikace [30].

Knihovna tarfile

Knihovna tarfile je používána pro čtení, zápis a úpravu archivů tar v oblasti archivace a komprese souborů. Se schopností pracovat s různými typy souborů tar, jako jsou kompresní metoda gzip, LZMA, bzip2 a další umožňuje se zabývat správou souborů, archivací dat a provádění různých úkolů se souborem [31].

2.5 Knihovna pro vytvoření spojení se serverem SMTP

Knihovny smtplib a ssl usnadňují odesílání e-mailů přímo z webového prohlížeče a vytvářejí zabezpečená připojení do emailového serveru pro ochranu citlivých dat. K importu těchto knihoven se používá příkaz import ve výpisu 2.3.

Výpis 2.3: Import knihovny smtplib a ssl

```
import smtplib
import ssl, getpass, socket
from email.mime.text import MIMEText
from email.mime.multipart import MIMEMultipart
```

Knihovna smtplib

Knihovna smtplib slouží odesílání e-mailů pomocí protokolu SMTP (Simple Mail Transfer Protocol). Jeho význam spočívá v tom, že poskytuje přímou komunikační linku s uživateli a nabízí další funkci, které přesahují základní prohlížení webu [40]. V této diplomové práci je používána k upozorňování oprávněných uživatelů na nebezpečnostní události.

Knihovna ssl

Na druhou stranu je knihovna ssl nezbytná pro zabezpečení přenosu dat přes Internet. Používá se protokol SSL (Secure Sockets Layer) pro šifrování informací přenášených po síti, která zajišťuje, že veškerá data vyměňovaná mezi webovým prohlížečem a smtp servery zůstanou důvěrná a chráněná před zachycením nebo manipulací.

Knihovna getpass

Knihovna getpass pomáhá zajistit bezpečné zpracování citlivých informací, jako jsou uživatelské jméno, heslo a číslo platební karty. Je vhodná v tom, když senioři zadávají přihlašovací údaje do webového prohlížeče, lze ji používat k zakrytí zadávaných údaje na obrazovce. Ještě by mohla být používána pro získání aktuálního uživatelského jména v počítači, která umožňuje identifikovat uživatele.

Knihovna socket

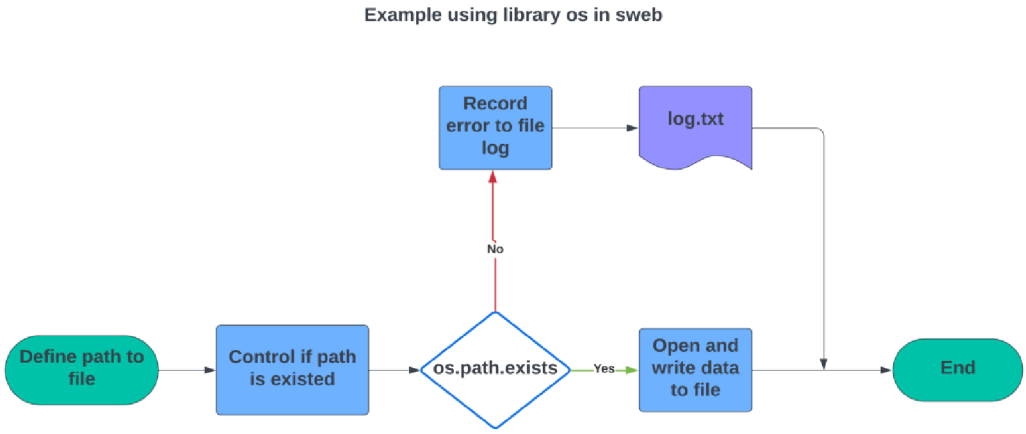
Knihovna socket tvoří základ síťové komunikace a poskytuje nástroj pro vytváření a správu síťových připojení, která jsou základem pro přístup k webovému obsahu. Ve webovém prohlížeči lze použít ke správě požadavků na webové servery a zpracování odpovědí.

2.6 Systémová knihovna

Systémová knihovna se slouží k poskytování základních funkcí s operačním systémem, uživatelským zařízením. V rámci této diplomové práce jsou knihovna os, knihovna sys a knihovna time používány.

Knihovna os

Knihovna os je používána pro interakci s operačním systémem, která zjednodušuje proces správy souborů a adresářů. Umožňuje aplikaci provádět operace, jako je čtení i zápis souborů, přejmenování a odstranění souborů a další. V rámci této práce používá třídu, která provádí čtení konfiguračních dat, čtení nebo zápis daných daty do textového souboru a další [27]. Konfigurační data jsou uložena v souboru json. Příklad použiti knihovny os je představen v obrázku 2.6.



Obrázek 2.6: Příklad použiti knihovny os

Knihovna sys

Knihovna sys slouží jako kritické rozhraní pro interpret programovacího jazyku Python a nabízí přístup k proměnným a funkcím v aplikaci. Jednou z primárních rolí této knihovny je poskytování informace o aktuálním stavu interpretu a nabízí argument příkazového řádku, označenému sys.argv. Tato funkce umožňuje vytvářet interaktivní aplikaci příkazového řádku [28].

Knihovna time

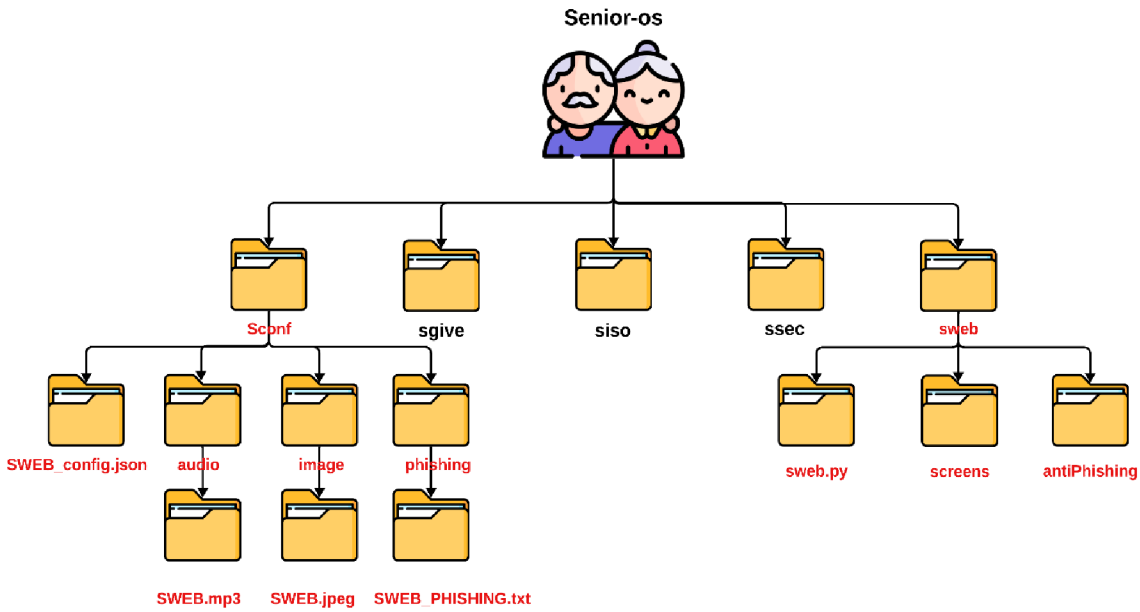
Knihovna time je nutná pro řízení a manipulaci s časem, která reprezentuje čas v různých časových formátech, nastavuje interval zpoždění mezi dvěma událostmi a převádí čas mezi různými formáty času. Navíc umožňuje operace časování s vysokým rozlišením, které jsou velmi důležité v této práci [29].

3. Tvorba vlastního webového prohlížeče pro seniory

V této kapitole je postupně popsán postup tvorby vlastního webového prohlížeče pro seniory. Kapitola 3.1 si představuje myšlenku a požadovaný výsledek v návrhu webového prohlížeče. Kapitola 3.2 pojednává o inicializaci konfigurace aplikace a v kapitole 3.3 je popsána metoda pro zobrazení webové stránky a vytvoření grafického uživatelského rozhraní. Dále je zvuková asistence a podpora více jazyků aplikace uvedena v kapitole 3.4 a kapitole 3,5. Na konci je metoda zvětšení velikosti zobrazeného textu webové stránky představena v kapitole 3.6.

3.1 Návrh webového prohlížeče pro seniory

Webový prohlížeč pro seniory je jedna aplikace z sady aplikacích v projektu, který je pojmenován operační systém pro seniory. Kromě webového prohlížeče obsahuje projekt ještě e-mailovou aplikaci, textový editor, obraz operačního systému a další. Více informace o projektu je uvedeno ve webové stránce https://github.com/forsenior/senior-os.

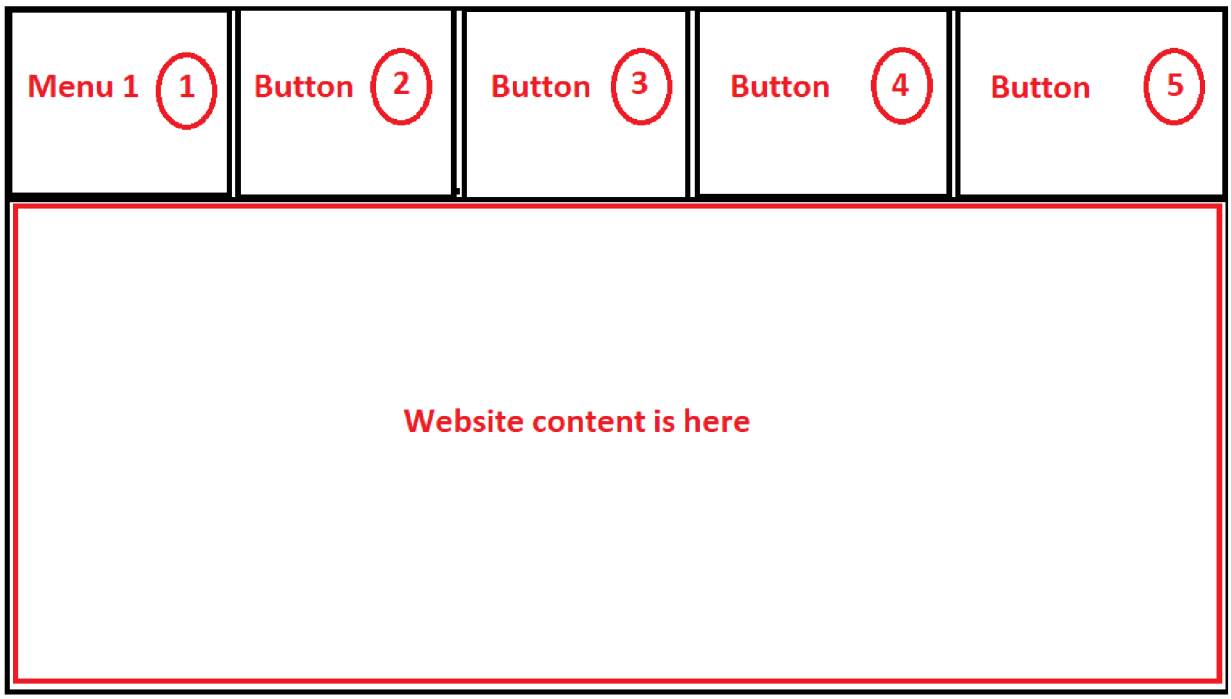


Obrázek 3.1: Složky a soubory webového prohlížeče v projektu senior-os

Obrázek 3.1 si představí umístění složky a souboru webového prohlížeče v projektu. Kvůli sady aplikací i efektivní vývoji aplikace v budoucnosti je konfigurační data všech aplikací uložena v adresáři sconf, jako je zobrazen v obrázku 3.1. Složka sconf obsahuje několik složek. Je

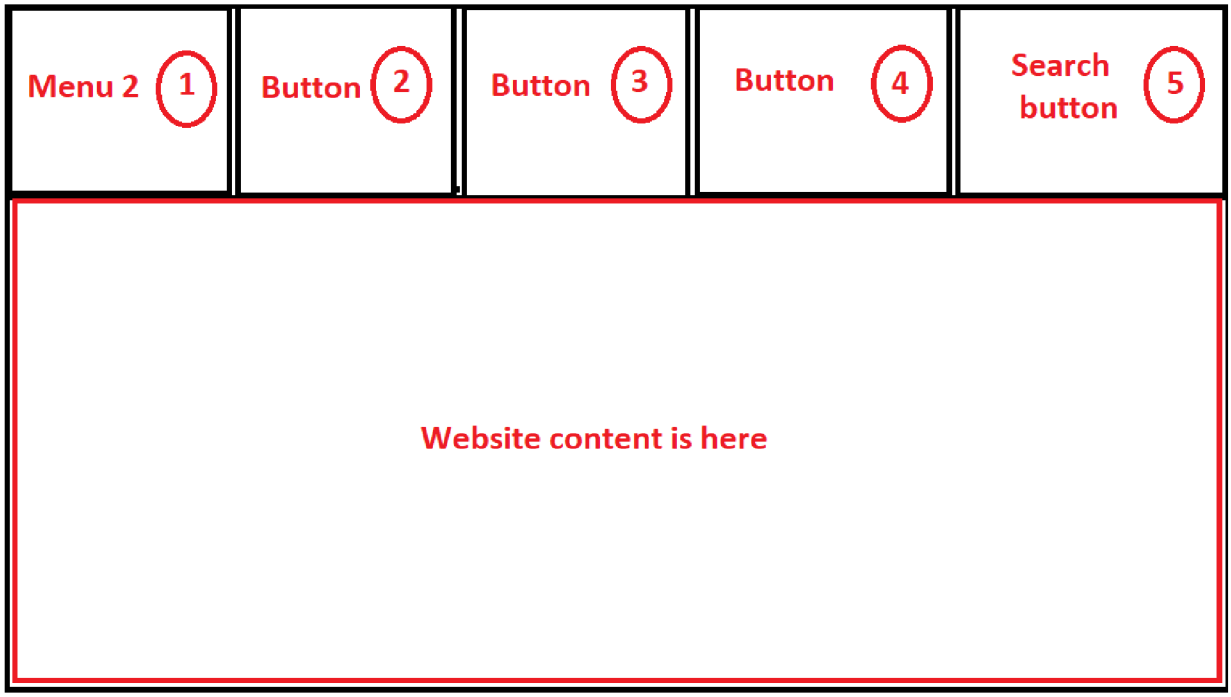
to složka pro zvuky hrající při najetí na tlačítko nebo při varování, složka pro obrázky zobrazených v tlačítku aplikace a složka, ve které je databáze podvodné stránky. Podrobná informace, která je uložena v konfiguračním souboru pro sweb, bude uvedena v další kapitole.

Předtím bylo už uvedeno, že je konfigurační soubor všech aplikací uložen ve stejné složce. Ale každá aplikace má vlastní složku, ve které jsou programovací soubory umístěny. V složce toto webového prohlížeče jsou hlavní programovací soubor, screenshoot z webového prohlížeče a potřebné soubory pro zabezpečení proti podvodné stránce. Kromě programovacího souboru je tam také soubor k popisu a použití prohlížeče, jako jsou soubor readme.md a textový soubor. V textovém souboru je požadavek na verze knihovny pro spuštění webového prohlížeče uveden a další.



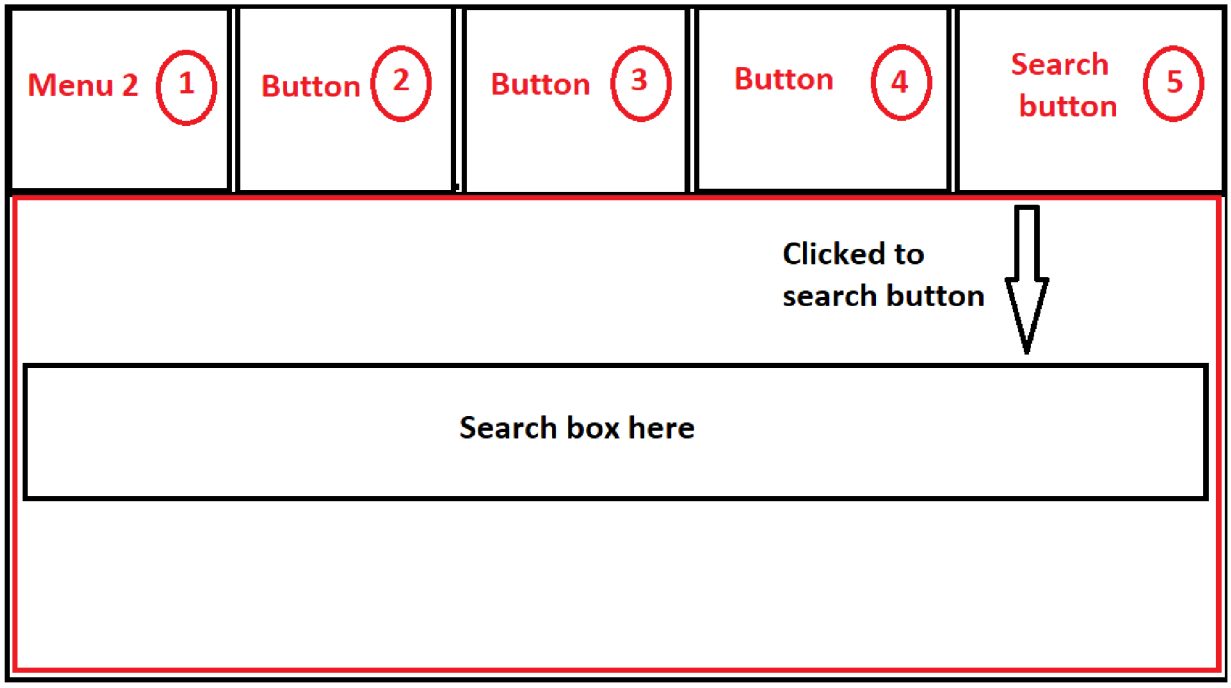
Obrázek 3.2: Návrh prvního menu

Webový prohlížeč pro seniory i jiná aplikace v projektu je navržen tak, že obsahuje dva hlavní menu, ale je pouze jeden menu zobrazen na rozhrání webového prohlížeče současně. Každý menu má čtyři tlačítka, které jsou prováděna na různou funkci. Jejich umístění je zobrazeno v obrázku 3.2. Uprostřed webového prohlížeče je místo pro uložení webového obsahu, ve kterém by uživatele mohly interagovat.



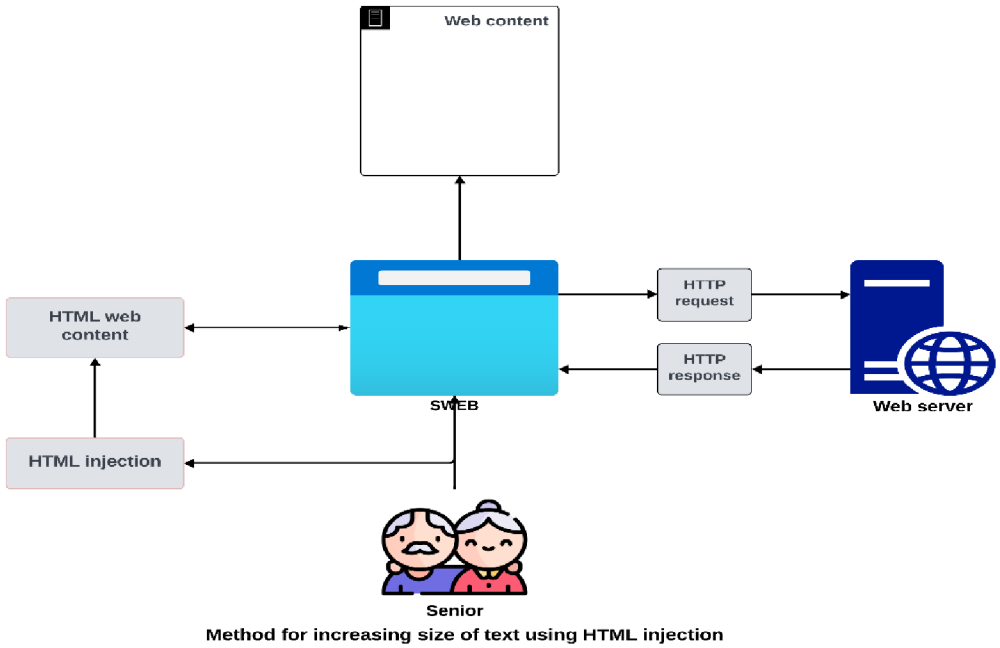
Obrázek 3.3: Návrh druhého menu

Dále menu 2 je navržen skoro podobně jako menu 1, pouze je funkce posledního tlačítka v rozdílu. Jedná se o tlačítko, po jeho kliknutí je zadávací pole zobrazeno. V zadávacím poli mohou uživatelé doplnit dotaz nebo připojenou webovou adresu, ke které by se chtěli připojit a dotazovat se, co by chtěli vědět.



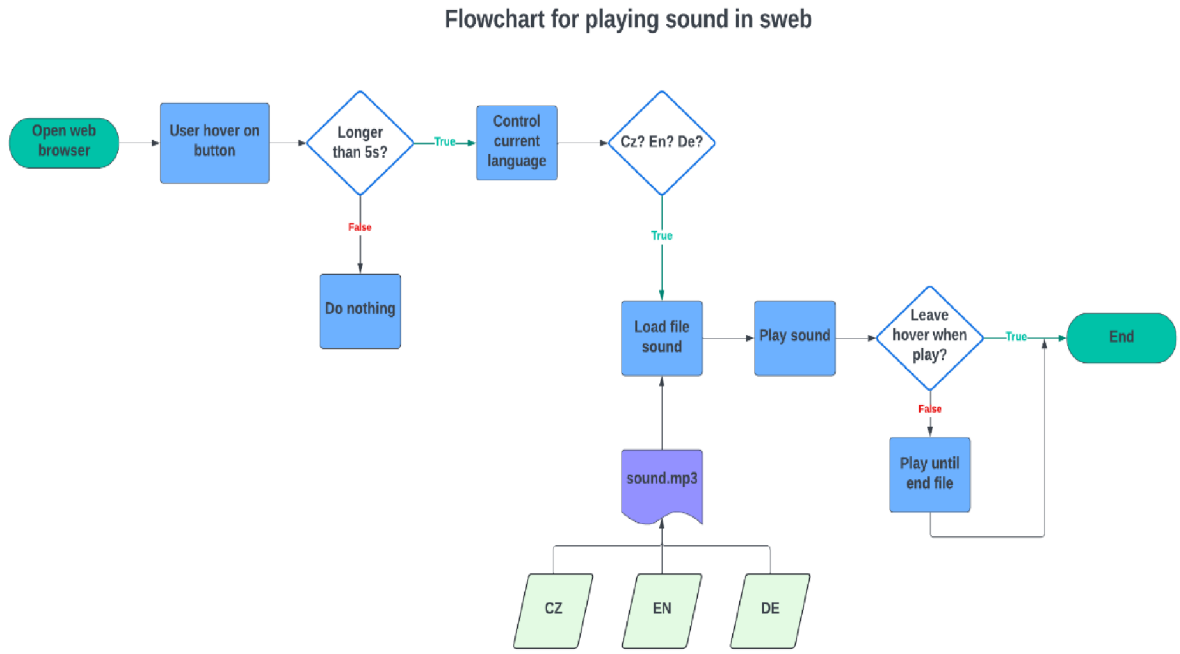
Obrázek 3.4: Vyhledávací pole ve webovém prohlížeči

Kdyby uživatel kliknul na vyhledávací tlačítko, webový obsah je zmizen a webový prohlížeč zobrazí pouze vyhledávací poli uprostřed, jako je uvedena v obrázku 3.4.



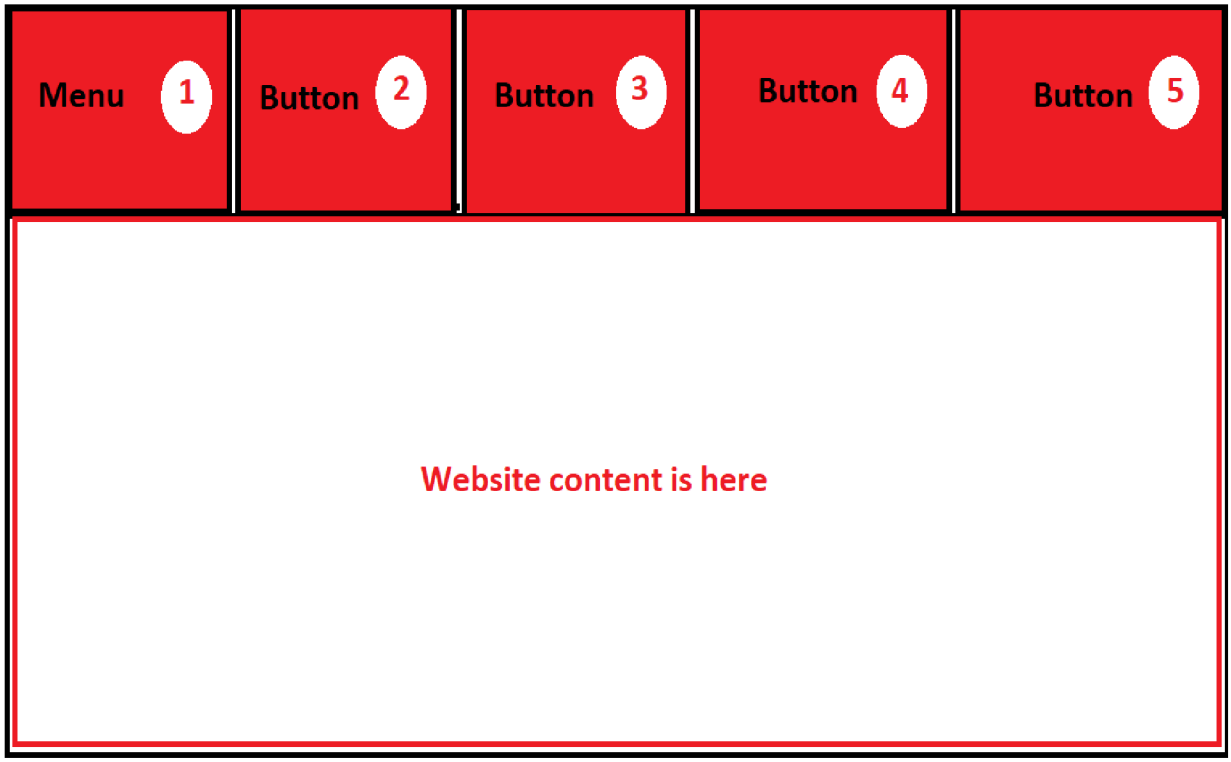
Obrázek 3.5: Metoda aplikování změny HTML pro zvětšení velikosti textu ve webovém obsahu

Pro seniory je nezbytné, že texty i ikony ve webovém prohlížeči jsou čitelné a dost velké. Velikost textu a ikonu v tlačítku lze inicializovat přímo v konfiguračním souboru sweb, potom je inicializovaná hodnota nastavena ve vytvoření tlačítka. Ale tedy existuje problém, že nelze přímo zvyšovat velikost textu webového obsahu v PyQt aplikaci. K řešení existujícího problému je metoda aplikování změny HTML používána, která je představena v obrázku 3.5.



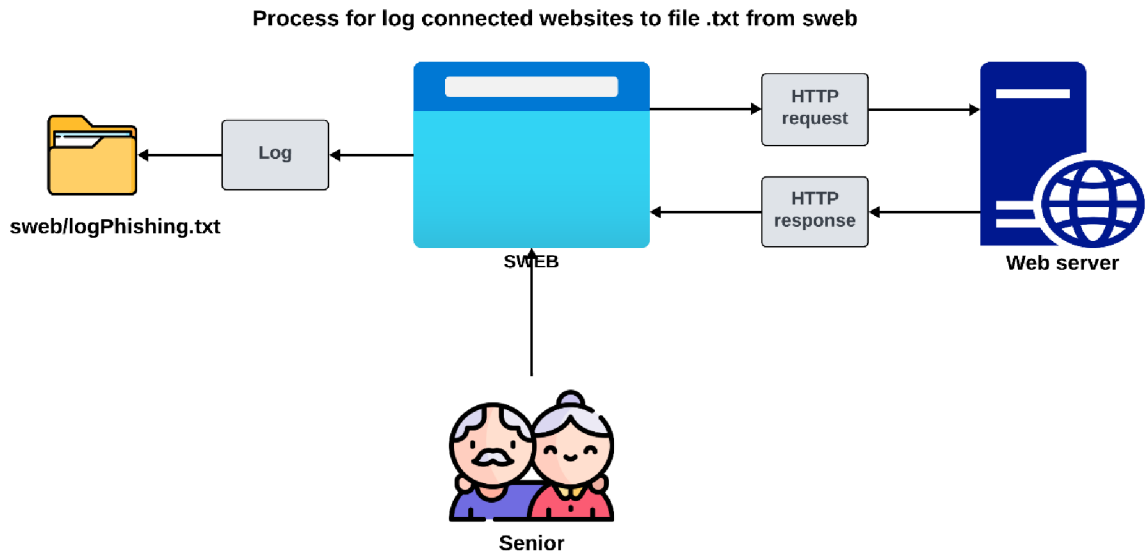
Obrázek 3.6: Diagram pro nahrání zvuku v swebu

Webový prohlížeč pro seniory je také navržen s podporou zvukové asistence. Tato funkce by mohla být velmi přínosná pro starší osoby, u nichž často dochází s věkem ke změnám, jako je zhoršení zraku. V rámci této diplomové práce jsou podporovány tři jazyky ve webovém prohlížeči (čeština, angličtina a němčina). Při najetí na tlačítko delší než 5 sekund, sweb nahraje zvuk, aby uživateli oznámil, jakou funkci má tlačítko nebo upozornění o bezpečnosti. Naopak nahrání zvuku končí při opuštění tlačítka. Zvukové soubory v různých jazycích jsou uloženy v adresáři sconf.



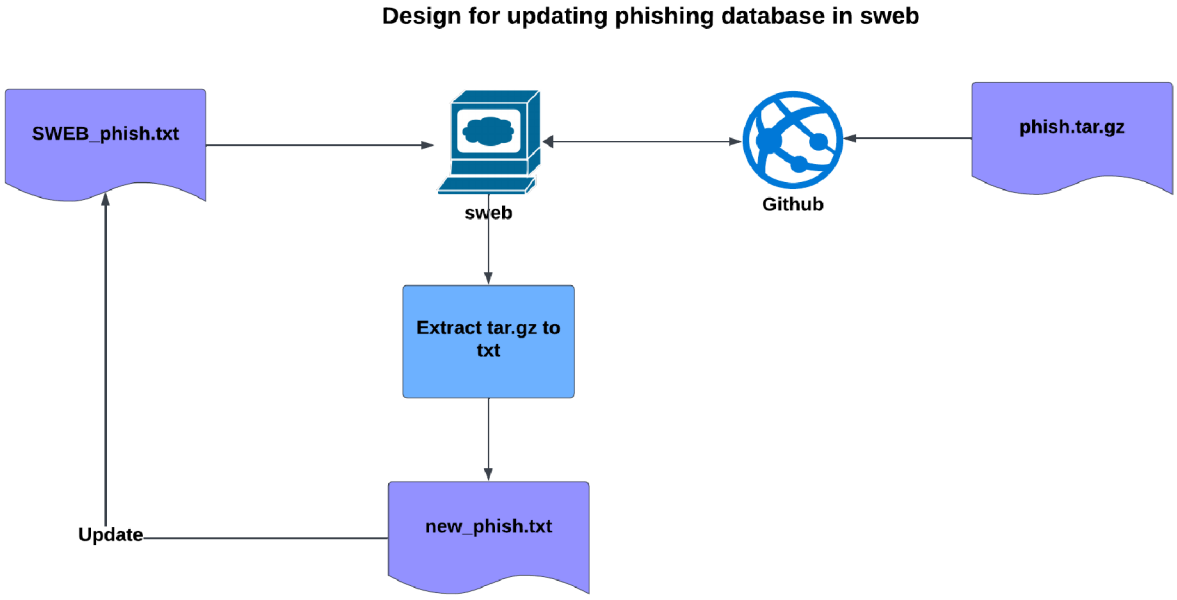
Obrázek 3.7: Rozhrání webového prohlížeče při připojení k podvodné stránce

K zabezpečení uživatele sweb podporuje bezpečnostní funkce proti podvodné stránce, jako jsou změna barvy tlačítka webového prohlížeče na červenou barvu, přehrání zvukového varování, ukládání činnosti do záznamu činnosti pro vyhodnocení bezpečnosti, když uživatel připojí k podvodné stránce. V obrázku 3.7 je zobrazeno rozhraní webového prohlížeče při připojení k podvodné stránce a proces záznamu činnosti webové stránky je uveden v obrázku 3.8.



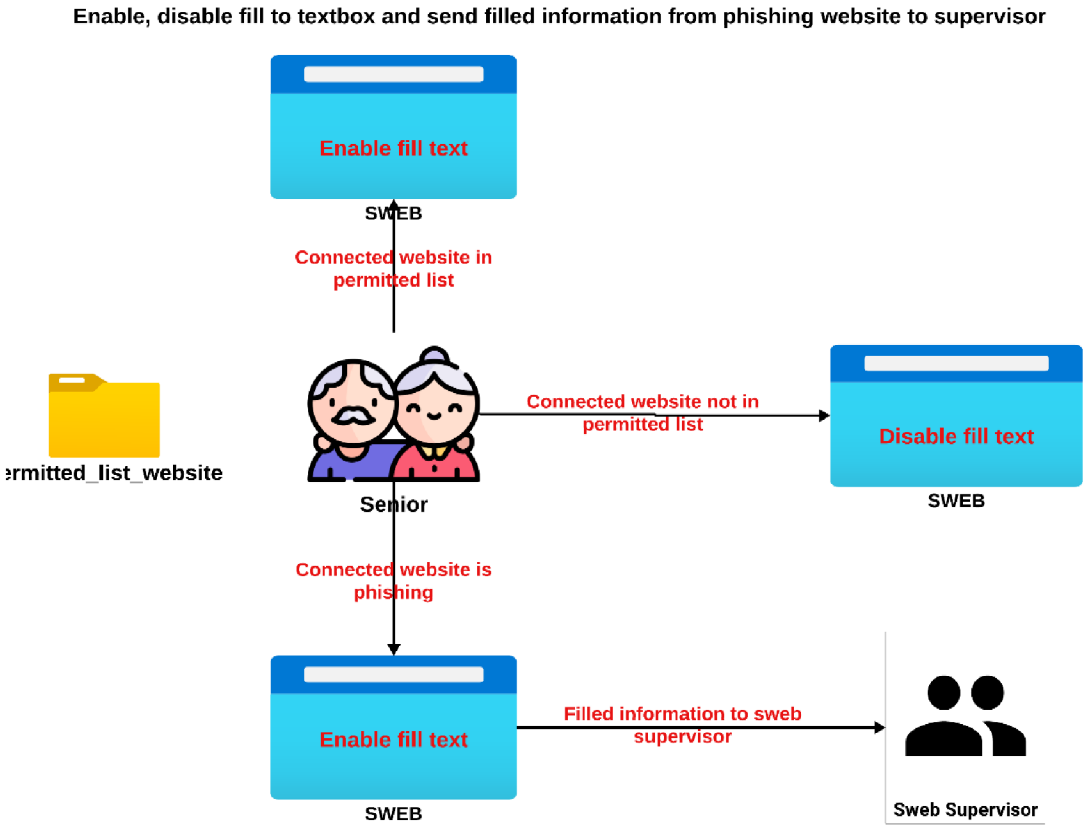
Obrázek 3.8: Proces záznamu činnosti webové stránky

Databáze podvodné stránky je aktualizována pravidelně při spuštění aplikace. Čas je vypočítán z poslední aktualizace. Návrh pro pravidelnou aktualizaci podvodné stránky je uveden v obrázku 3.9. V rámci této diplomové práce je aktualizována každé dva týdny.



Obrázek 3.9: Návrh pro pravidelnou aktualizaci podvodné stránky

Navíc webový prohlížeč definuje seznam povolené webové stránky, ve kterém by uživatelé mohli doplnit text. V případě, že není současná webová stránka v definovaném seznamu, doplnění textu není povolené. Na konci je doplněná informace od uživatele odeslána k opatrovníkovi, kdyby uživatelé doplnili vlastní informace do zadávacího pole v podvodné stránce. Seznam podvodné stránky je uložen v databázi podvodné stránky. Toto zabezpečení je uvedeno v obrázku 3.10.



Obrázek 3.10: Pokročilé zabezpečení proti podvodné stránce v sweb

3.2 Konfigurace aplikace

Poprvé je nutné inicializovat hlavní aplikaci, která zpracovává inicializaci, finalizaci aplikace a čistí všechny aplikační úkoly, když je aplikace ukončena. Tato funkce je prováděna pomocí třídy QApplication, která je uvedena v kapitole 2.1 Grafická knihovna. Ukázka inicializace aplikace a odvolání konfiguračními daty je uvedena ve výpisu 3.1.

Výpis 3.1: Inicializace aplikace a odvolání konfiguračními daty

```
qApplication = QApplication(sys.argv)
# If browser is opened in command terminal
input_url_from_terminal = sys.argv[1] if len(sys.argv) > 1 else
"https://seznam.cz"
# Load config data from JSON file
web_config = load_sweb_config_json()
template_config = load_template_config_json()
```

Webový prohlížeč umožňuje dva způsoby inicializace. První způsob inicializace je prováděn programovacím nástrojem, který podporuje spustit program ve programovacím jazyce Python. Druhý je spuštěn přes příkazový řádek použitím příkazu "python". Ukázka příkazu spouštění prohlížeče přes příkazový řádek je uveden ve výpisu 3.2.

Proměnná input_url_from_terminal je přiřazována doplněnou hodnotou URL jako argument příkazového řádku při spouštění skriptu Python. Aby získalo URL adresu zadanou uživatelem z terminálu, musí používat seznam sys.argv s hodnotou 1, což je první argument za jménem skriptu, kde se nachází doplněná URL adresa. Podmínka délky seznamu větší než jedna kontroluje, zda byl předán více než jeden argument do skriptu. Jestliže nebyla, to znamená, že je skript spuštěn bez zadání URL, proto bude input_url_from_terminal implicitně nastaven na hodnotu "https://seznam.cz". Spouštění prohlížeče přes příkazový řádek je velmi důležité, aby smail nebo jiné aplikace v projektu mohly zavolat sweb a zobrazit webovou stránku do sweb, pokud uživatel klikne na odkazy, které jsou v nich.

Výpis 3.2: Příkaz spouštění prohlížeče přes příkazový řádek

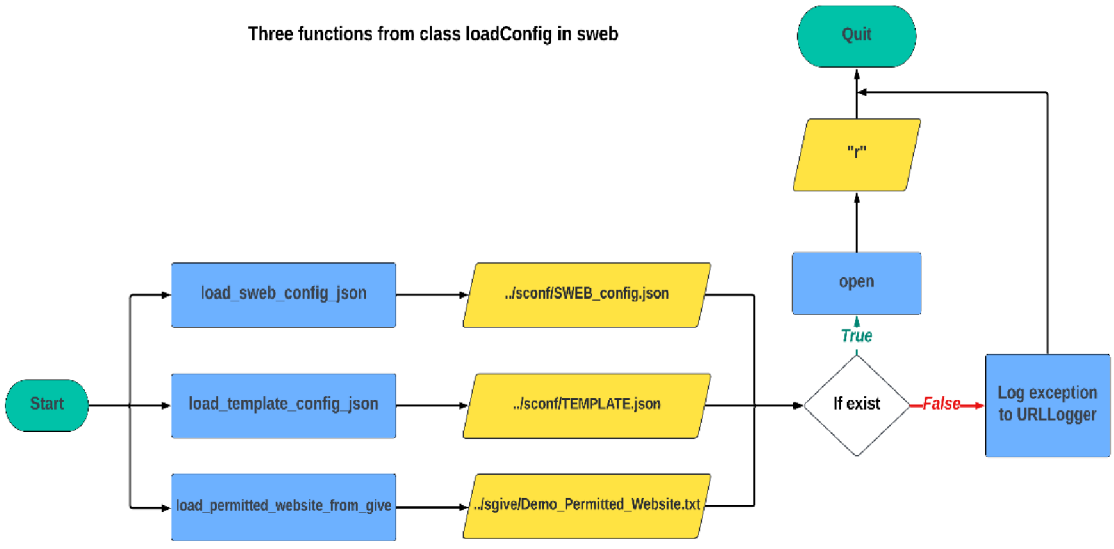
```
python main.py vutbr.cz
# Command for open in operating system FEDORA
python3 main.py vutbr.cz
```

Poté jsou počáteční konfigurační daty načteny spolu s inicializací aplikace, jako je konfigurační data odvolána ze dvou souborů json, které jsou uloženy v adresáři sconf. První soubor json je pojmenován TEMPLATE, je používán ve všech aplikacích projektu Senior Operation System, aby zajistil synchronizaci mezi všemi aplikacemi. Naopak je druhý soubor nastaven pouze pro vlastní webový prohlížeč, který je pojmenován SWEB_config, ve kterém se nachází informace pro jména tlačítka, cesty do souboru fotky i zvuků používaných ve webovém prohlížeči a další. K odvolání konfiguračních dat je využíváno vlastní třídou loadConfig.

Výpis 3.3: Načtení konfiguračního souboru aplikace

```
def load_sweb_config_json():
    # Exit when error occurs and print notification to log
    try:
        with open("../sconf/SWEB_config.json", "r",encoding='utf-8')
                                                        as open_file:
            language_database = json.load(open_file)
        open_file.close()
        return language_database
    except FileNotFoundError:
        print(f"Configuration file not found /sconf/SWEB_config.json")
    except json.JSONDecodeError:
        print(f"Error parsing JSON file: /sconf/SWEB_config.json")
```

Ve třídě loadConfig jsou tři funkce, které jsou pojmenovány load_template_config_json, load_sweb_config_json a load_permitted_website_from_sgive. Jedna z nich je zobrazena ve výpisu 3.3. První funkce load_template_config_json je používána pro načtení konfigurační daty ze souboru TEMPLATE a druhá pro načtení ze souboru SWEB_config. Poslední funkce načte povolené webové stránky, které jsou aplikovány definovanou HTML změnou (bude uvedeno v příští kapitole). Povolené webové stránky jsou uloženy v adresáři sgive.



Obrázek 3.11: Tři funkce ve třídě loadConfig

Ještě ve třídě je operace se soubory integrována s kontrolou chyb pomocí struktury try-except pro zpracování výjimek. Nejprve zkusí otevřít soubor se vstupní cestou k souboru, metodou “r”, kódování UTF-8 určené, což znamená, že soubor je kódován ve tvaru UTF-8. Potom načte

všechna konfigurační data příkazem load a dokonce je vrátí pomocí příkazu return. Jsou zachyceny dvě výjimky, jako jsou FileNotFoundError a JSONDecodeError. První výjimka je FileNotFoundError, která nastane, pokud soubor json v zadaném adresáři neexistuje. Druhá je JSONDecodeError, která nastane, pokud obsah souboru nemá platnou formu souboru JSON.

Výpis 3.4: Zobrazení aplikace v celoobrazovkovém režimu

```
main_window.show_app_full_screen()
self.setWindowFlags(Qt.CustomizeWindowHint)
self.showFullScreen()
```

Aby bylo hlavní okno aplikace zobrazeno celoobrazovkově (nemá žádné záhlaví, tlačítko pro minimalizace, ukončení ani možnost přesunu) je nutné nastavit specifické příznaky oken a zobrazit aplikaci v celoobrazovkovém režimu. Příkazy pro tuto funkci jsou uvedeny ve výpisu 3.4. Metoda obsahuje celkem dva kroky. Poprvé nastavuje příznak oken na hodnotu CustomizeWindowHint, která přizpůsobí chování okna a odstraní standardní ovládací prvky okna, jako jsou tlačítko pro minimalizace, ukončení a další. Potom používá metodu showFullScreen pro zobrazení hlavního okna v celoobrazovkovém režimu.

3.3 Zobrazení webové stránky a vytvoření grafického uživatelského rozhraní

V této kapitole je postupně uveden způsob zobrazení webové stránky a metoda pro vytvoření grafického uživatelského rozhraní.

3.3.1 Zobrazení webové stránky

Vytvoření prvků pro zobrazení webového obsahu provádí pomocí třídy QwebEngineView jako je uvedena ve výpisu 3.5, která umožňuje vložit webový prohlížeč do webové aplikace. Webová aplikace je vytvořena třídou QApplication. Webový prohlížeč obsahuje pouze standardní webový obsah.

Výpis 3.5: Vytvoření prvků pro zobrazení webového obsahu

```
self.main_browser = QWebEngineView()
# Set cutstom page to open new page in the same browser
self.my_custom_page = MyWebEnginePage(self.main_browser)
```

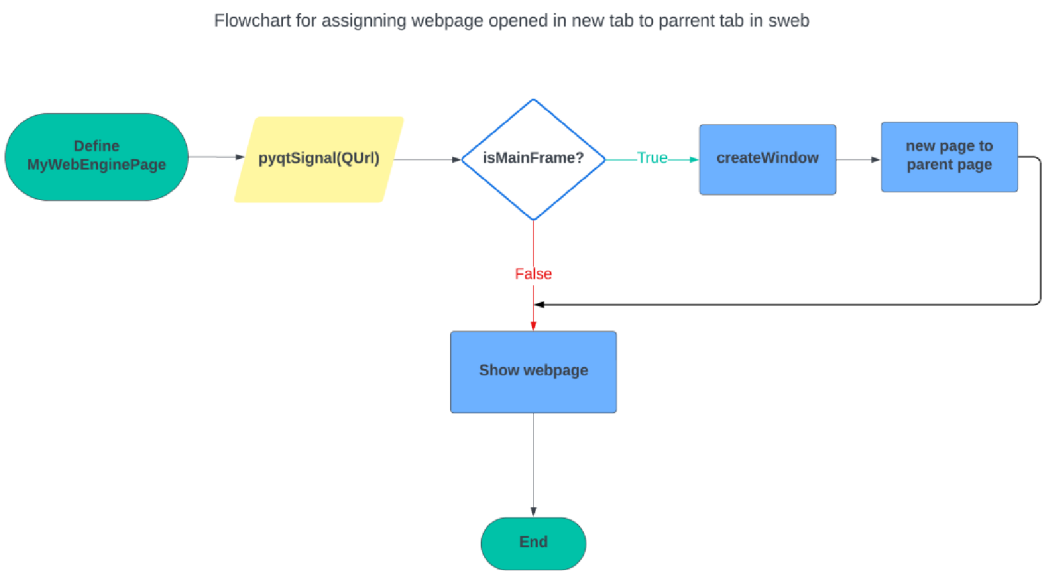
Dále je webový obsah v prohlížeči přizpůsoben na konkrétní chování vlastní třídou MyWebEnginePage. Tato třída má pouze jeden vstupní parametr, jedná se o hodnotu webového prohlížeče vytvořeného třídou QWebEngineView.

Výpis 3.6: Přizpůsobení standardního chování webového obsahu

```
class MyWebEnginePage(QWebEnginePage):
    # Define a signal that will carry a URL as its argument
    urlChangedSignal = pyqtSignal(QUrl)
    def __init__(self, parent=None):
        super().__init__(parent)
        # Create a channel for recording filling text when user fill text in
phishing page
        self.channel = QWebChannel(self)
        self.setWebChannel(self.channel)
    def acceptNavigationRequest(self, url, _type, isMainFrame):
        # Ensure only modifying behavior for clicked links
        if _type == QWebEnginePage.NavigationTypeLinkClicked and isMainFrame:
            # Navigate to the url
            self.urlChangedSignal.emit(url)
            # Tell the view that handled this navigation request
            return False
        # Return True for all other navigation requests
        return True
    def createWindow(self, _type):
        # Create a new instance of MyWebEnginePage for the new window request
        new_page = MyWebEnginePage(self)
        new_page.urlChangedSignal.connect(self.urlChangedSignal.emit)
        return new_page
```

V některé webové stránce je webový odkaz nastaven hodnotou “about=_blank” jako výchozí hodnota. To znamená, že je každé kliknutí na odkaz přesměrováno na nové různé okno. Ale to není výhoda pro třídu QWebEngineView, protože je navržena tak, aby vždy zobrazovala webový obsah stránky pouze v jednom okně. Kvůli tomu je nezbytné odstranit výchozí chování webového prohlížeče a spravovat více instancí QWebEngineView, aby byly zobrazeny pouze v jedné instanci. Ukázka na vlastní třídu MyWebEnginePage je uvedena ve výpisu 3.6.

Vlastní třída MyWebEnginePage umožňuje vlastní zpracování navigačních požadavků, které jsou inicializovány z webového obsahu stránky, zejména při kliknutí na odkazy.



Obrázek 3.12: Vývojový diagram pro přiřazení nové stránky do současného okna

Nejprve je vlastní signál deklarovaný pomocí třídy pyqtSignal s hodnotou QUrl. Oba jsou uvedeny v předchozí kapitole. Signál je zachycen třídou QUrl. Kdykoliv jsou signály splněny určité dané podmínky, oznamuje další části aplikace. Metoda __init__ definuje počáteční konstruktor s argumentem "parent=None" používající ke správě paměti a vytváření hierarchií aplikačních prvků. Potom je nutné přebírat metodu acceptNavigationRequest z třídy QwebEnginePage. Kdykoli se objeví jakýkoliv navigační požadavek ve webovém obsahu prohlížeče, je volána metoda NavigationTypeLinkClicked, jako je kliknutí na webový odkaz. U hodnoty "isMainFrame" se jedná o hlavní oblast obsahu webové stránky. Metoda acceptNavigationRequest má dvě vrácené hodnoty. První hodnota je "True", že je navigační požadavek pro hlavní okno stránky, typický jako kliknutí na odkaz, který vede na novou stránku, tak metoda nahradí aktuální obsah hlavní stránky obsahem nové stránky. Druhá hodnota je "False", že je navigační požadavek sloužící k načtení obsahu v určitém okně webové stránky bez změny celého obsahu stránky. Kvůli tomu je hodnota "False" používána pro řešení webového odkazu se chováním otevírající v novém okně. Vývojový digram pro tuto metodu je představen v obrázku 3.12.

Ještě je instance třídy QwebChannel vytvořena, která je detailně popsán ve předchozí kapitole. Třída je určena k usnadnění komunikace mezi Qt aplikacemi a JavaScript běžícími

ve webovém enginu. S parametrem “self” je naznačeno, že QwebChannel má stejnou dobu životnosti jako objekt, ve kterém je vytvářen. V této práci je QwebEnginePage, které je schopno zobrazovat webový obsah. Dále je nastaveno s metodou setWebChannel, která slouží k přiřazení QwebChannel webovému obsahu. S vstupním parametrem “self.channel” určuje, že bude používat dříve vytvořenou instanci QwebChannel pro tuto komunikaci.

Potom je nezbytné přizpůsobit metodu createWindow od třídy QWebEnginePage. Je určena ke zpracování navigačních požadavků na vytvoření nových webových stránek, jako je kliknutí na odkaz, který požaduje otevření v novém okně webového prohlížeče. Metoda je definována s parametrem “_type”, který je obvykle představen typem okna nebo webovou stránkou, která je požadována k otevření. V metodě je vytvořena nová instance třídy MyWebEnginePage, která umožňuje přizpůsobit vlastní chování na této nové webové instanci. Se vstupním parametrem “self” zajistí, že je aktuální webová stránka nastavena jako “parent” nové stránky. Metoda “emit” s parametrem “self” vyvolá vysílání signálu “urlChangedSignal” v aktuální stránce, která umožňuje “parent” webové stránce reagovat na události, které se nastanou na nové stránce.

Na konci je problém zobrazení webového obsahu v novém okně řešen s přizpůsobením obou metod acceptNavigationRequest a createWindow z třídy QWebEnginePage.

3.3.2 Zobrazení webové stránky v chytrém telefonu

Pro změnu uživatelského agenta webového zobrazení, zvláště pro změnu zobrazení webového obsahu ve webovém prohlížeči mezi chytrým telefonem a počítačem je používána metoda setUserAgent, která se použije na instanci my_custom_page. Metoda setUserAgent je uvedena v následujícím výpisu 3.7.

Výpis 3.7: Metoda setUserAgent

```
mobile_user_agent = "Mozilla/5.0 (iPhone; CPU iPhone OS 15_0 like Mac
OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/15.0
Mobile/15E148 Safari/604.1"
self.my_custom_page.setUserAgent(mobile_user_agent)

def setUserAgent(self, user_agent):
    self.profile().setHttpUserAgent(user_agent)
```

Proměnná mobile_user_agent je textový řetězec, který definuje uživatelský agent. Ten sděluje webové stránce, že webový požadavek přichází ze Safari na iPhonu v systému IOS 15.0, jádru

AppleWebKit/605.1.15. Potom je webová stránka definovaná s předchozí definovanou proměnnou uživatelského agenta. Proto bude jakákoli webová stránka načtená ve webovém prohlížeči zacházet jako z mobilního zařízení a webový server vrátí obsah optimalizovaný pro mobilní zařízení. Na konci je profil QwebEngine nastaven hlavičkou HTTP User-Agent pomocí metodě setHttpUserAgent, kterou bude webový prohlížeč používat pro všechny následující požadavky HTTP do webového serveru.

Výpis 3.8: Signál connect a nastavení výchozí stránky

```
self.custom_page.urlChangedSignal.connect(self.on_url_changed_my_custom_page)
self.main_browser.setPage(self.my_custom_page)
self.setCentralWidget(self.main_browser)
# Check if input URL is contained HTTP or HTTPS
if input_url_from_terminal.startswith("https") or
input_url_from_terminal.startswith("http"):
    self.main_browser.setUrl(QUrl(input_url_from_terminal))
else:
    self.main_browser.setUrl(QUrl("http://" + input_url_from_terminal))
```

Webová stránka na prohlížeči je nastavena přizpůsobenou webovou stránkou ve předchozím kroku, která je zobrazena uprostřed aplikace pomocí metody setCentralWidget jako uveden ve výpisu 3.8.

Výchozí hodnota webové stránky se jedná o webové stránce seznam.cz. Při každém kliknutí uživatele na webový odkaz ve webovém prohlížeči je signál zachycen metodou connect, která přesměruje na vlastní metodu on_url_changed_my_custom_page. V této metodě načte novou adresu URL pomocí metodě setURL se vstupním parametrem url. Proto je webový prohlížeč přesměrován na novou adresu po kliknutí.

3.3.3 Vytvoření grafického uživatelského rozhrání

Cílem diplomové práce je vytváření webového prohlížeče pro starší osoby. Proto je nezbytné zajistit, aby všichni senioři mohli snadno číst, interagovat s aplikací, jako jsou velká tlačítka, ikony i jasné texty včetně hlasové asistence i více podporovaných jazyků. Tak napomůže uživatelům ke spokojenosti, a to i těm, pro které není angličtina mateřským jazykem.

3.3.3.1 Přidání aplikačních prvků

V souboru TEMPLATE.json adresáře sconf jsou uloženy konfigurační parametry o grafickém uživatelském rozhraní, jako je počet menu, počet tlačítek a další, které jsou uvedeny ve výpisu 3.9. V projektu Senior Operating System má prohlížeč celkem 2 tlačítka menu. Každé menu obsahuje 4 tlačítka.

Výpis 3.9: Konfigurační parametry o grafickém uživatelském rozhraní

```
"GUI_template": {
        "num_of_menu_buttons": 2,
        "num_of_opt_on_frame": 4,
        "padx_value": 5,
        "height_divisor": 4.5,
        "width_divisor": 5
    }
```

K vytváření tlačítka je používána třída QPushButton, která je uvedena v předchozí kapitole. Všechna tlačítka na webovém prohlížeči splní následující pravidlo, že mají pouze text nebo pouze ikonu na tlačítku, což znamená, že v případě, že má text, nesmí mít ikonu a naopak. Text je přidán do tlačítka pomocí třídy QLabel a ikona je přidána třídou QIcon. Oba - text i ikona - jsou ovládány třídou QVBoxLayout pro jednoduché řízení.

Výpis 3.10: Metoda pro získání signálu kliknutí a změny standardního kurzoru

```
self.menu1WWW1.clicked.connect(self.navigate_www1)
self.menu1WWW1.setCursor(Qt.PointingHandCursor)
self.menu_1_toolbar.addWidget(self.menu1WWW1)
```

Pro získání signálu každého kliknutí na webový odkaz je používána metoda clicked od tlačítka třídy QPushButton, jako je zobrazena ve výpisu 3.10. Signál je vždy emitován, kdykoliv uživatel klikne na tlačítko. Navíc je metoda connect používána k propojení signálu se slotem. V tomto případě, když je vyslán signál kliknutí, metoda connect je volána. Ještě je standardní kurzor zobrazen na ruku, když je ukazatel myši nad jakýmkoliv tlačítkem. To se provádí metodou setCursor s hodnotou PointingHandCursor z třídy Qt. Na konci je tlačítko přidáno do aplikačního prvku menu pomocí metody addWidget od třídy QToolbar. Informace pro všechna menu i tlačítka je uvedena v tabulce 3.1.

Tabulka 3.1: Ovládání aplikační stránky

Jméno tlačítka	Text	Ikon	Signál po kliknutí	Popis
Menu 1	Ano	Ne	Self.toggle_toolbar	Přepínání na menu 2
Exit	Ne	Ano	Self.close	Ukončení aplikace
Back	Ne	Ano	Self.browser.back	Vrátí zpět do předchozí webové stránky
WWW 1	Ne	Ano	Self.navigate_www1	Přesměrování na webovou stránku www.edition.cnn.com
WWW 2	Ne	Ano	Self.navigate_www2	Přesměrování na webovou stránku www.irozhlas.cz
Menu 2	Ano	Ne	Self.toggle_toolbar	Přepínání na menu 1
WWW 3	Ne	Ano	Self.navigate_www3	Přesměrování na webovou stránku www.google.com
WWW 4	Ne	Ano	Self.navigate_www4	Přesměrování na webovou stránku www.aktualne.cz
WWW 5	Ne	Ano	Self.navigate_www5	Přesměrování na webovou stránku www.denik.cz
Address	Ano	Ne	Self.toggle_url_toobar	Zobrazení zadávací pole URL, ve které by uživatelé mohli žádat připojenou adresu.

Všechna tlačítka jsou uložena v jednotlivém toolbar pro snadnou správu. Příkazy pro přidání textu a ikonu do tlačítka jsou uvedeny ve výpisu 3.11.

Výpis 3.11: Příkazy pro přidání textu a ikonu do tlačítka

```
menu1WWW1_icon = QIcon(self.path_to_image_www1)
menu1WWW1_label = QLabel(self.menu1WWW1)
menu1WWW1_label.setPixmap(menu1WWW1_icon.pixmap(QSize(int(self.buttons
_width_info/(1.5)),int(self.buttons_height_info/(1.5)))))
menu1WWW1_layout.addWidget(menu1WWW1_label)
# Align icon in the center
menu1WWW1_layout.setAlignment(menu1WWW1_label,Qt.AlignCenter)
```

3.3.3.2 Přepínání mezi dvěma menu

K přepínání mezi menu 1 a menu 2 slouží vlastní metoda toggle_between_toolbar, která přepíná dvě menu v grafickém uživatelském rozhraní aplikace. Tato metoda je uvedena ve výpisu 3.12.

Výpis 3.12: Metoda pro přepínání mezi dvěma menu

```
# Method use for disable menu when click to another menu
def toggle_between_toolbar(self):
    # Toggle visibility of toolbars
    if self.menu_1_toolbar.isVisible():
        self.menu_1_toolbar.setVisible(False)
        self.menu_2_toolbar.setVisible(True)
    else:
        self.menu_2_toolbar.setVisible(False)
        self.menu_1_toolbar.setVisible(True)
```

Se vstupním parametrem self je webová aplikace odkazována. Menu 1 je zobrazeno jako výchozí grafické rozhraní. Naopak je menu 2 nastaveno jako neviditelné nebo pod menu 1. K nastavení viditelnosti stačí přizpůsobit metodu isVisible od třídy QToolbar. Metoda má celkem dvě hodnoty, jako jsou True (nastavena na viditelnou) a False (nastavena na neviditelnou). Kdykoli aplikace získá signál kliknutí na menu, metoda zkontroluje, od kterého menu je, a provádí přepínání mezi dvěma menu.

Výpis 3.13: Přiřazení metody toggle_between_toolbar na tlačítko

```
self.menu1_button.clicked.connect(self.toggle_between_toolbar)
```

Metoda toggle_between_toolbar je pak přiřazena na tlačítko pomocí metody clicked a connect. Způsob přiřazení je uveden ve výpisu 3.13.

3.3.3.3 Vytvoření zadávací pole URL

Dále je zadávací pole URL vytvořeno třídou QLineEdit. Třída je výhodná na vytvoření zadávací pole pro zadávání webových adres nebo dotazu, protože má pouze jednořádkový textový vstup. Včetně metody setAlignment pro nastavení zarovnání textu uvnitř zadávací pole URL s hodnotou AlignCenter od třídy Qt zajišťuje doplněný text, který je vždy na středu zadávacího pole.

Výpis 3.14: Vytvoření a nastavení stylů pro zadávací textové pole URL

```
# Create a URL bar
self.url_bar = QLineEdit()
self.url_bar.setAlignment(Qt.AlignCenter)
# Change the parameter of URL bar
self.url_bar.setStyleSheet(f"""
    QToolBar {{
        background-color: {self.color_info_menu};
    }}
    QLineEdit {{
        border: 2px solid black;
        height: {self.buttons_height_info}px;
        font-family: {self.font_family_info};
        font-size: {int(self.buttons_height_info/3)}px;
        font-weight: {self.font_weight_info};
        background-color: {self.color_info_app};
    }}
""")
# When text of URL is changed, check for URL Phishing
self.url_bar.returnPressed.connect(self.navigate_to_url)
```

Ještě je nezbytné definovat vlastní styl pro zadávací pole URL. Je prováděno metodou setStyleSheet [33], která umožňuje nastavit různé textové i barevné vlastnosti, jako jsou nastavení barvy, výšky, textové rodiny i velikost písma a další. Nastavené hodnoty jsou uvedeny ve výpisu 3.14. Dokonce metoda returnPressed třídy QLineEdit spojuje s vlastní metodou navigate_to_url. Signál je vždy emitován, kdykoli uživatel stiskne klávesou Enter, zatímco třída QLineEdit má fokus.

Metoda navigate_to_url je pravděpodobně zodpovědná za zpracování logiky navigace na webovou adresu URL. Logika je zpracována krok za krokem. Nejprve je nutné získat doplněnou adresu URL ze zadávacího pole URL. Tato funkce je prováděna pomocí metody text a strip. První metodou text získá zadaný text a druhá metoda strip odstraní počáteční nebo koncové bílé znaky, což je používáno pro vyčištění uživatelského vstupu.

Potom je nezbytné zkontrolovat hodnotu zadanou uživatelem. V případě, že zadaný text neobsahuje žádnou tečku ".", předpokládá, že zadaný text není webovou adresou URL, ale jen vyhledávacím textem. Proto ji upraví na webovou adresu URL s vyhledávačem Google. Tato funkce je prováděna pomocí textového dotazu "https://www.google.com/search?q=" se zkratkou "q" na konci, což znamená "question" v angličtině. Potom se ujistí, že webová adresa URL má protokol. Zkontroluje, zda text obsahuje "://", který je součást protokolu HTTP jako "http://" nebo protokolu HTTPS jako "https://". Pokud protokol nemá, předepíše adresu "https://", přičemž se používá zabezpečené připojení HTTPS. Na konci odstraní koncové znaky "/" pomocí logické matematiky [:-1] a přejde na novou webovou adresu URL metodou setURL od třídy QUrl.

3.3.3.4 Přizpůsobení vlastnosti tlačítka

Informace o velikosti výšky a šířky je přizpůsobena vlastní třídou GetHeightAndWidthFromScreen. Třída dynamicky vypočítá velikost na základě velikosti uživatelského monitoru. Používá se knihovna screeninfo, která umožňuje načíst umístění a velikost fyzických obrazovek. Se vstupní hodnotou 0 je určena k výběru primárního monitoru. Ukázka třídy GetHeightAndWidthFromScreen je uvedena ve výpisu 3.15.

Výpis 3.15: Ukázka třídy GetHeightAndWidthFromScreen

```
class GetMonitorHeightAndWidth:
    def __init__(self):
        # 0 = Get the first monitor
        monitor = get_monitors()[num_of_monitor]
        screen_width, screen_height = monitor.width, monitor.height
        self.button_height = screen_height / height_divisor
        # Number of button on menu = numberOfOptions + 1
        total_padding = (num_option_on_frame)*padding
        # Calculate width for button
        self.button_width = math.floor((screen_width-
                                total_padding)/width_divisor) - padding
```

Výška i šířka tlačítka se vypočítá vydělením obrazovky podle dané hodnoty "divisor". Tento dělitel je pravděpodobně definován v souboru TEMPLATE.json adresáře sconf pro synchronizaci s jinými aplikací v projektu Senior Operating System. Proto se výška tlačítka rovná vydělením výšky monitoru hodnotou dělitele výšky. Na požadavek jednoduché čitelnosti odpovídá prázdnou mezerou mezi dvěma tlačítky. Hodnota velikosti je také definována v souboru TEMPLATE.json.

Šířka tlačítka se vypočítá podle následující rovnice: (Šířka monitoru – počet tlačítka * šířka tlačítka) / dělitel šířky. Dokonce je takto získána flexibilní hodnota výšky a šířky tlačítka.

Výpis 3.16: Nastavené parametry tlačítka ve výchozím stavu

```
QToolBar {{
      background-color: {self.color_info_menu};
          }}
QPushButton {{
      border: 1px solid black;
      background-color: {self.color_info_button_unselected};
      font-size: {self.font_size_info}px;
      font-weight: {self.font_weight_info};
      font-family: {self.font_family_info};
      width: {self.buttons_width_info}px;
      height: {self.buttons_height_info}px;
             }}
QPushButton:hover {{
      background-color: {self.color_info_button_selected};
             }}
QPushButton QLabel {{
      font-size: {self.font_size_info}px;
      font-weight: {self.font_weight_info};
      font-family: {self.font_family_info};
             }}
```

Vlastnost tlačítka je nastavena metodou setStyleSheet. Metoda umožňuje nastavit barvu, barvu při najetí na tlačítko, velikost i rodina textu, text vytvořený z třídy QLabel a další. Nastavené hodnoty jsou uvedeny v tabulce 3.2.

Tabulka 3.2: Vlastnost a hodnota nastavené na tlačítko

Vlastnost	**Popis**	**Hodnota**
Border	Hranice tlačítka.	Velikost: 1px. Typ: solid. Barva: black.
Background color	Barva tlačítka, když není vybraná.	#e5e5e5 – šedý.
Hover color	Barva tlačítka, když je vybraná.	#00ff00 – zelená.

Font size	Velikost písma.	36px.
Font weight	Váha písma.	Bold – tučně.
Font family	Třída pásma.	Helvetica.
Width	Šířka tlačítka.	Podle výpočtu ve třídě GetMonitorHeightAndWidth.
Height	Výška tlačítka.	Podle výpočtu ve třídě GetMonitorHeightAndWidth.

Vlastní třída GetHeightAndWidthFromScreen je používána k získání velikosti výšky a šířky, která je nastavena na tlačítka webového prohlížeče. Jeho velikost je flexibilní a vypočítá se podle uživatelského monitoru knihovnou screeninfo. Potom je nutné přizpůsobit vlastnosti tlačítka pomocí metody setStyleSheet se získanou hodnotou.

3.4 Zvuková asistence

Zvuková asistence do webového prohlížeče by mohla být velmi přínosná pro starší osoby, u nichž často dochází s věkem ke změnám, jako je zhoršení zraku (proto je pro ně obtížné čtení).

Výpis 3.17: Metoda pro přehrání zvuku

```
# QpushButton can be set HoverLeave and HoverEnter event with "widget"
# Play sound when usesr hovers on button longer than 5 seconds
def setup_hover_sound_value(self, input_widget,
hover_time,path_to_sound):
    # Using Qtimer to set clock
    input_widget.hover_timer = QTimer()
    input_widget.hover_timer.setInterval(hover_time)
    # Run only one times when hover
    input_widget.hover_timer.setSingleShot(True)
    input_widget.hover_timer.timeout.connect(lambda:
                              self.play_sound_for_button(path_to_sound))
    # Install event to widget -> Event is comefrom eventFilter
    input_widget.installEventFilter(self)
```

Nejprve je metoda setup_hover_sound_value vytvořena, která obsahuje funkce přehrání zvuku při najetí na dané tlačítko. Metoda má celkem 4 vstupní parametry: self, input_widget, doba při najetí a cesta do zvukového souboru, jako uvedeny ve výpisu 3.17. Parametr self je zkratka pro hlavní aplikaci a parametr input_widget se jedná o dané tlačítko. Doba při najetí je

definována v souboru TEMPLATE.json adresáře sconf a cesta do zvukového souboru je uložena v souboru SWEB_config.json taky adresáře sconf.

K vytváření i nastavení specifického intervalu pro časové odpočítávání se používá třídu QTimer. Pomocí metodě setInterval je doba při najetí uložena do časovače QTimer, který se odpočítává od dané vstupní doby. Navíc metoda setSingleShot je nastavena se hodnotou True, která zajišťuje, že se časovač spustí pouze jednou za událost najetí. Kdykoli vyprší časovač, spouští funkci play_sound_for_button, která přehrává zvuk. Tato funkce je prováděna metodou timeout.connect. Na konci metoda installEventFilter umožňuje začít zpracovávat události najetí prostřednictvím metody eventFilter.

Výpis 3.18: Zpracování události najetí na dané tlačítko

```
# Set event for leave and enter button -> Using only with QpushButton
def eventFilter(self, watched, event):
    if event.type() == QEvent.HoverEnter:
       watched.hover_timer.start()
    elif event.type() == QEvent.HoverLeave:
       watched.hover_timer.stop()
       # Stop sound immediately
       self.stop_sound_for_button()
    return super().eventFilter(watched, event)
```

Metoda eventFilter je nezbytná zpracovat události najetí na dané tlačítko. Metoda slouží k zachycení událostí předtím, než je doplněna daném požadavkem. Má pouze tří vstupní parametry, jako jsou self, watched, event. Parametr watched odkazuje na tlačítko, ke kterému se událost vztahuje. Parametr Event je objekt, který obsahuje podrobnosti o události, které se nastaly. Události HoverEnter a HoverLeave od třídy QEvent se vyskytuje, kdykoli ukazatel myši vstoupí a opouští do daného tlačítka. Je časovač aktivní metodou start a pasivní metodou stop. Aktivní i pasivní stav časovače umožňuje zbránit akci, která by se mohla nastat po najetí. Navíc je pasivní stav připojen s metodou stop_sound_for_button, která je navržen tak, aby zastavil jakýkoliv zvuk po opuštění tlačítka, který by mohl být přehráván v důsledku najetí a zabrání pádu prohlížeče. Ve výpisu 3.19 je ukázka metody stop_sound_for_button.

Výpis 3.19: Metoda stop_sound_for_button pro zastavení zvuku.

```
def stop_sound_for_button(self):
   if self.sound_mixer_control_for_button:
      self.sound_mixer_control_for_button.stop()
      self.sound_mixer_control_for_button = None
```

Metoda play_sound_for_button je sloužena pro přehrání zvuku z dané adresy k zvukovému souboru. Tato funkce je prováděna knihovnou pygame, jako je uvedeno ve výpisu 3.20. Nejprve metoda zkontroluje, zda zvukový soubor na dané adrese existuje. Jestliže neexistuje, oznámí textové oznámení "Sound file not found" v konzoli. Naopak se používá metodu mixer.sound k načtení zvukového souboru a poté jej přehraje. Jakékoli výjimky během tohoto procesu jsou dokonce zachyceny a vypsány v konzoli.

Výpis 3.20: Metoda play_sound_for_button

```
def play_sound_for_button(self, path_to_sound):
    # Ensure the file exists before playing it
    if not os.path.exists(path_to_sound):
        print(f"Sound file not found: {path_to_sound}")
        return
    try:
        # Load and play the sound file
        self.sound_mixer_control_for_button = pygame.mixer.Sound(path_to_sound)
        self.sound_mixer_control_for_button.play()
    except Exception as exc:
        print(f"Failed to play sound: {str(exc)}")
```

Souhrnně metoda setup_hover_sound zajišťuje funkci, při které se přehraje zvuk, když uživatel vstoupí do tlačítka po nastavenou dobu. Zvuk se okamžitě zastaví, pokud tlačítko opustí. Metoda je užitečná pro vylepšení interakce se staršími osobami.

3.5 Podpora více jazyků aplikace

Vlastní třída Translator je navržena tak, aby zvládala jazykové překlady. Poskytuje jednoduchý způsob, jak implementovat podporu více jazyků do webové aplikace. Výpis 3.21 zobrazí ukázku vlastní třídu Translator.

Výpis 3.21: Vlastní třída pro podporu více jazyků

```
class Translator:
    def __init__(self):
        self.language_config_database = load_sweb_config_json()
        # Default shortcut for language
        self.language_keys = ["cz","en","de"]
        self.current_language_in_browser =
               self.language_config_database["language"]["default_language"]
        # Set current language is CZ =0 , EN = 1, DE = 2
        if(self.current_language_in_browser) == "cz":
            self.current_language_index = 0
        elif self.current_language_in_browser == "en":
            self.current_language_index = 1
        else:
            self.current_language_index = 2
```

Třída načítá jazykové konfigurační daty, přepíná mezi jednotlivými jazyky a načítá překlady textu i zvuku z konfiguračního souboru. Přeložené texty i cesty do zvukového souboru v různém jazyce jsou uloženy ve souboru SWEB_config.json adresáře sconf.

V rámci této diplomové práce podporuje webový prohlížeč pouze tři různé jazyky, jako jsou čeština, angličtina a němčina. Výchozí jazyk ve webovém prohlížeči je načtena ze souboru SWEB_config.json, který je nastaven na angličtinu. Instruktor __init__ definuje seznam jazykových kódů, jako jsou zkratka “cz” pro češtinu, zkratka “en” pro angličtinu a zkratka “de” pro němčinu. Potom je jazykový index používán, který určuje aktuální jazyk a slouží ke snadnému přepínání mezi jednotlivými jazyky.

Metoda toggle_language zvýší jazykový index pro přepínání na další jazyk v jazykovém seznamu. Pokud jazykový index překročí počet dostupných jazyků, je nastaven zpět na nulu, čímž se efektivně prochází jednotlivé jazyky. V metodě je parametr current_language je pravidelně aktualizován, aby se projevil nový jazyk po přepnutí.

Tabulka 3.3: Překlad ovládacího prvku

Jméno tlačítka	**Čeština**	**Angličtina**	**Němčina**
Menu 1	Menu 1	Menu 1	Menü 1
Menu 2	Menu 2	Menu 2	Menü 2
Address	My page	Moje stránka	Meine Seite

Aktuální text a cesta do zvukového souboru jsou načtena z konfiguračního souboru SWEB_config adresáře sconf a jsou aktualizovány do každého tlačítka v aplikaci pomocí metodě get_translated_text a get_translated_audio. Nejprve je nutné vytvořit klíč pomocí zkratce aktuálního jazyka, který je získán z parametru current_languge a vstoupit název daného tlačítka. Vytvořený klíč má následující textovou formu "sweb_{zkratka_jazyka}_{jméno_tlačítka}". Potom načte hodnotu z konfiguračního souboru podle klíče a klíčové hodnoty, jako jsou řetězcový text "text" pro text a řetězcový text "audio" pro zvuk. Výsledek metody vrátí přeložený text a cesta ke zvukovému souboru, pokud byl nalezen. V opačném případě vrátí zprávu, že překlad nebyl nalezen. Přeložený text je uveden v tabulce 3.3.

Výpis 3.22: Aktualizace textu a zvuku ve webovém prohlížeči

```
# Method for get current language and update default language in app
# If translate button is clicked, change to other language and audio
def toggle_supported_language(self):
   self.language_translator.toggle_supported_language()
   self.update_ui_text()
   self.update_ui_audio()
```

Jedna instance třídy Translator je odvozena ve třídě MyBrowser, která je pojmenována lang_translator. Ve třídě MyBrowser také obsahuje metodu toggle_language, která je používána k aktualizaci textu a zvuku, když uživatel změní jazyk webového prohlížeče. Je metoda připojena se dvěma metody, jako jsou metodu update_ui_text pro aktualizaci textu všech tlačítka v prohlížeči a metoda update_ui_audio pro aktualizaci zvuku.

Stručně zajišťuje třída Translator aktualizaci textu a zvukového souboru pro všechna tlačítka na webovém prohlížeči. Webový prohlížeč podporuje pouze tři různé jazyky, jako jsou čeština, angličtina a němčina. Výchozí jazyk je nastaven na angličtiny. Je nezbytná pro uživatele, jejichž mateřským jazykem není angličtina.

3.6 Zvětšení velikosti zobrazeného textu webové stránky

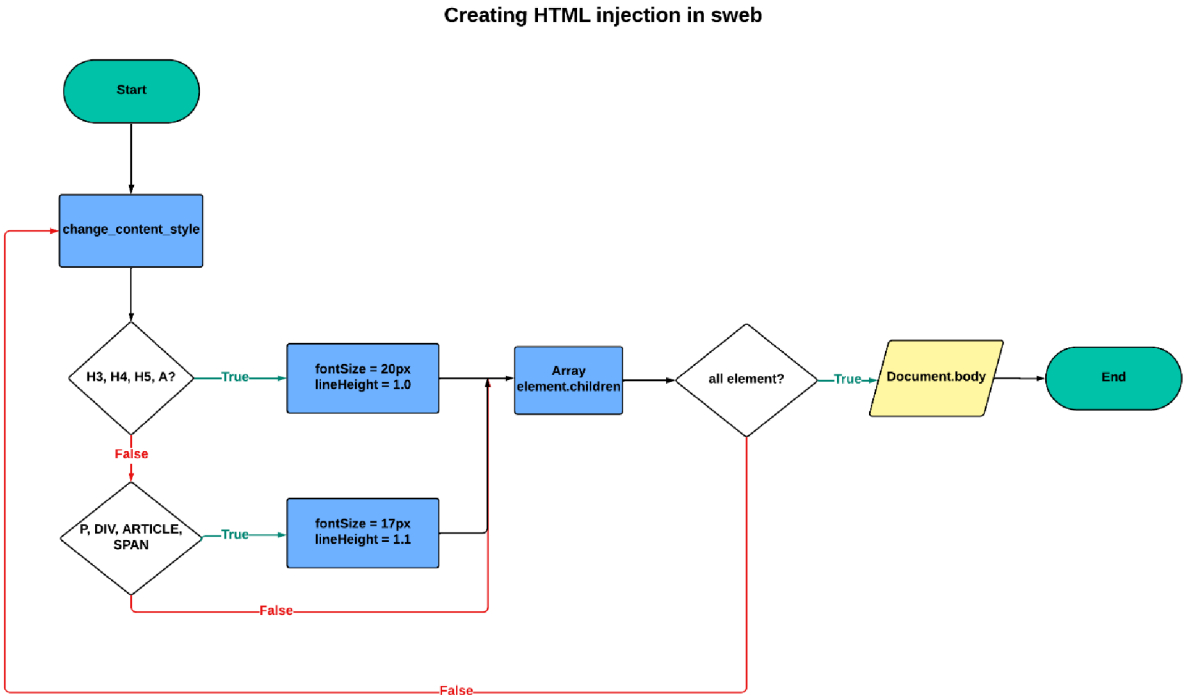
Nastavení velikosti písma na webové stránce pro lepší čitelnost se jedná o významnou funkci pro starší uživatele. Ale vzhledem k zapouzdřené povaze webového obsahu a rozdílu mezi prohlížečem a styly webové stránky není možná přímo upravovat styl webové stránky z rozhraní prohlížeče sweb. Proto jsou metody jako změna obsahu HTML [41] a změna zvětšení faktoru používány v této diplomové práci.

Poprvé je metoda změny obsahu HTML používána. Tato metoda zahrnuje spuštění vlastního JavaScriptu v aktuální webové stránky za vlastním účelem, jako jsou přímé úpravy jejích zobrazených stylů a interakčních funkcí. Proto by se mohla zaměřit na konkrétní prvky a upravit jejich velikost písma. Ukázka vlastní změna obsahu HTML pro zvětšení velikosti textu webové stránky je uvedena ve výpisu 3.23.

Výpis 3.23: Vlastní změna obsahu HTML pro zvětšení velikosti textu webové stránky

```
<!-- Create a function to change content style-->
var change_content_style = function(element) {
    <!-- Method includes will return value in UPPERCASE>
    if (['H3', 'H4', 'H5', 'A'].includes(element.tagName)) {
        <!-- Header with bigger size-->
        element.style.fontSize = '20px';
        element.style.lineHeight = '1.0';
    }
    <!-- Method includes will return value in UPPERCASE>
    else if (['P', 'DIV', 'ARTICLE',
'SPAN'].includes(element.tagName)) {
        <!-- Content with smaller size>
        element.style.fontSize = '17px';
        element.style.lineHeight = '1.1';
    }
    Array.from(element.children).forEach(change_content_style);
}
change_content_style(document.body);
```

Hlavní funkce změny obsahu HTML se jedná o funkci change_content_style. Funkce prochází DOM webové stránky (Document Object Model) a selektivně mění styly prvků s začátkem document.body. Tento přístup zajišťuje, že úpravy jsou komplexní a ovlivňují celý webový obsah prezentovaný uživateli.



Obrázek 3.13: Definice změny obsahu HTML pro zvětšení velikosti textu

Změna obsahu HTML ve výpisu 3.23 rozlišuje mezi prvky záhlaví, jako jsou “H3”, “H4”, “H5”, “A” a textovými prvky těla, jako jsou “P”, “DIV”, “ARTICLE”, “SPAN”. Toto rozlišení umožňuje nastavit různé styly pro různé prvky, které zlepšují uživatelskou čitelnost. Prvky záhlaví jsou zvýrazněny větší velikostí písma s hodnotou 20px a výškou řádku 1,0. Zatímco prvky textu těla jsou mírně zvětšeny na hodnotu 17px s výškou řádku 1,1, aby se zlepšila přehlednost textu. Detailní postup je představen v obrázku 3.13.

Funkce Array.from(element.children).forEach(change_content_style) iteruje přes všechny prvky DOM uzlu převedením kolekce “children” uzlu DOM na pole. Pro každý prvek v definované poli provede vlastní funkci change_content_style. Tím, že změna obsahu HTML vyvolá funkci change_content_style na každém potomkovi. To zajistí, že definované změny stylu budou aplikovány nejen na počáteční uzel, ale taky na všechny potomní prvky, čímž se dosáhne komplexní úpravy stylu webové stránky.

Výpis 3.24: Metoda runJavaScript pro spuštění změny obsahu HTML

```
self.main_browser.page().runJavaScript(injection_javasript)
```

Po denifonání parametru změny obsahu HTML je metoda page() volána na objektu main_browser. Tato metoda vrací objekt QWebEnginePage, který představuje webovou stránku aktuálně načtenou v sweb. Třída QWebEnginePage poskytuje různé metody pro interakci s webovým obsahem. V tomto sweb je metoda runJavaScript používána, která obsahuje platný kód JavaScriptu. Platný kód je uložen ve proměnné injection_javascript. Proto asynchronně provede kód JavaScriptu na webové stránce, což umožňuje dynamickou úpravu obsahu a chování stránky na základě skriptu.

Dále je metoda setZoomFactor je používána pro zvětšení velikosti zobrazení webové stránky. Je výkonná metoda, která umožňuje ovládat úroveň zvětšení webového obsahu. Se zadáním zvětšení faktoru většího než 1,0 se webový obsah zvětší. Nejen text, ale i obrázky a další prvky jsou větší. To je užitečné zejména pro starší uživatele.

Výpis 3.25: Metoda zvětšení faktoru

```
self.main_browser.setZoomFactor(1.5)
```

Použití faktoru je nastaveno s hodnotou 1,5. To znamená, že každý prvek obsahu webové stránky, včetně textu, obrázků je zvětšen na 150 % původní velikosti. Použití self s hodnotou main_browser naznačuje, že tato instance prohlížeče je primární součástí aplikace.

Závěrem lze říci, že přímá manipulace se styly webových stránek v sweb představuje problém. Proto metody jako změna obsahu HTML a úprava zvětšení faktoru nabízejí účinné zlepšení čitelnosti textu ve webovém prohlížeči založeném na knihovnu PyQt. Tyto metody přizpůsobuje různým potřebám uživatelů, včetně seniorů a zlepší tak jejich zážitek z prohlížení swebu.

4. Zabezpečení webového prohlížeče pro seniory

Webový prohlížeč pro seniory by měl obsahovat spolehlivá bezpečnostní opatření, která identifikují podvodné stránky a blokují nebo upozorňují uživatele na možná rizika. V rámci této diplomové práce je zabezpečen tak, že uživatele identifikuje a upozorňuje, kdykoli zobrazí podvodné webové stránky, která je uložena v databázi podvodné stránky, změní původní barvu tlačítka na červenou barvu, zaznamená každé činnosti z aplikace do záznamu činnosti. Dokonce aktualizuje pravidelně databázi podvodné webové stránky za každé 2 týdny, která zajišťuje ochranu ve webovém prohlížeči. Tyto předchozí funkce jsou prováděny třemi vlastními třídy, jsou URLBlocker, URLLogger a UpdatePhishingTXT.

Kapitola 4.1 si představí základní způsob ochrany proti podvodné stránce ve webovém prohlížeči. Dále je zaznamenání činnosti webové stránky ve webovém prohlížeči uvedeno v kapitole 4.2. Na konci je popsána aktualizace databáze podvodné stránky v katpitole 4.3.

4.1 Ochrana proti podvodné stránce

V této podkapitole je postupně popsán způsob ochrany proti podvodné stránce ve webovém prohlížeči.

Výpis 4.1: Zachycení změny adresy URL a metoda connect

```
self.main_browser.urlChanged.connect(self.security_against_phishing)
```

Metoda urlChanged je poskytována webovým prohlížečem. Pomocí hodnoty self.main_browser je zachycena, kdykoli se aktuální adresa URL ve webovém prohlížeči změní. K tomu by mohlo dojít, když uživatel přejde na novou stránku, klikne webový odkaz ve webovém obsahu, doplní webovou adresu nebo vyhledávaný text do zadávacího pole, která vede k načtení nové adresy URL. K připojení signálu ke slotu je také používána metoda connect. To znamená, že kdykoliv je signál zachycen prohlížečem, slot je prováděn. Slot v tomto příkazu je metoda security_again_phishing.

Výpis 4.2: Kontrola webové adresy URL od webového prohlížeče

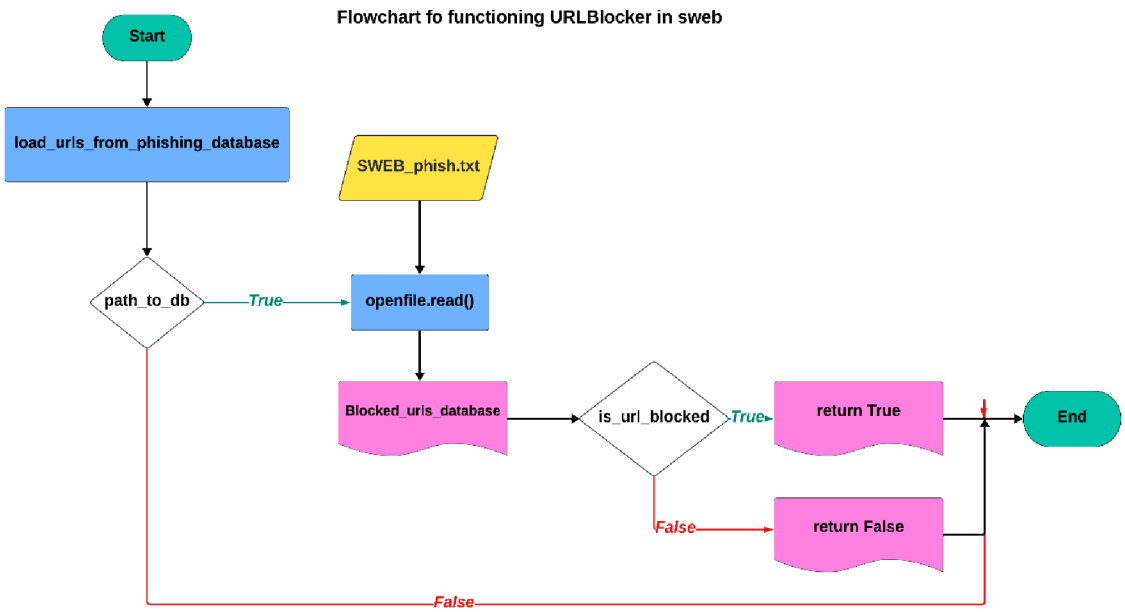
```
def security_against_phishing(self,qurl):
    url_in_browser_value = qurl.toString()
    if url_in_browser_value.endswith('/'):
       if self.url_blocker.is_url_blocked(url_in_browser_value):
           self.toggle_phishing_webpage = True
           self.play_sound_for_button(self.path_to_alert_phishing_music)
           # Log with level 5 when connected to phishing
           self.url_logger.log_blocked_url('WEBBROWSER', 5, 'main<security>',
                     f'Connection to Phishing server {url_in_browser_value}')
           # Set red colour for connect to phishing
           self.menu_1_toolbar.setStyleSheet(self.phishing_style_toolbar())
           self.menu_2_toolbar.setStyleSheet(self.phishing_style_toolbar())
           # Connect to URL after entering
           self.main_browser.setUrl(QUrl(url_in_browser_value))
        else:
           self.toggle_phishing_webpage = False
           # Set default style for toolbar
           self.menu_1_toolbar.setStyleSheet(self.default_style_toolbar())
           self.menu_2_toolbar.setStyleSheet(self.default_style_toolbar())
           # Log with LEVEL 6 INFORMATIONAL
           self.url_logger.log_blocked_url('WEBBROWSER', 6, 'main<security>',
                                    f'Connection to {url_in_browser_value}')
           # Connect to URL after entering
           self.main_browser.setUrl(QUrl(url_in_browser_value))
```

Metoda security_again_phishing obsahuje logiku pro kontrolu nové webové adresy URL a je uvedena ve výpisu 4.2. Je navržena tak, aby analyzovala adresy URL, na které prohlížeč přechází, zda je adresa URL považována za bezpečnou nebo potenciálně podvodnou webovou stránku. K tomu nejprve zkontroluje, že adresa URL obsahuje textový řetězec “about:blank”, což je obvykle prázdná stránka. Pokud neobsahuje, pokračuje na další logiky. Naopak se metoda okamžitě vrátí s hodnotou False a končí. Proto není zaznamenáváno do záznamu činnosti. Potom je nutné kontrolovat, zda webová adresa URL obsahuje textový řetězec “google.com”, který je předpokládaná na bezpečnou webovou stránku, tak kontrola podvodné stránky se obejde a pouze zaznamenává webovou adresu URL do záznamu činnosti. Na konci zkontroluje, zda je adresa URL blokována metodou url_blocked od třídy URLBlocker.

Výpis 4.3: Správa podvodných stránek

```
class URLBlocker:
    def __init__(self, paths_to_db):
        self.blocked_urls_database = set()
        self.load_urls_from_phishing_database(paths_to_db)
    def load_urls_from_phishing_database(self,path):
        with open(path,"r") as openfile:
           if openfile is not None:
              content  = openfile.read()
              reading_url = content.strip().split('\n')
              self.blocked_urls_database.update(reading_url)
    def is_url_blocked(self, input_url):
        for blocked_url in self.blocked_urls_database:
           if blocked_url in input_url:
              return True
        return False
```

Třída URLBlocker je určena ke správě podvodných stránek, která je uložena v databázi podvodné stránky SWEB_PHISH_1.txt adresáře sconf/phish. Ukázka této třídy je zobrazena ve výpisu 4.3. Nejprve je seznam podvodných adres URL inicializován jako prázdná množina určující k uložení adres URL z databáze podvodných stránek. Tato funkce je prováděna hodnotou set bez inicializačního parametru. Potom je nutné otevřít databázi podvodných stránek v specifické cestě v režimu čtení podle hodnoty “r”. Cesta k databázi je uložena v souboru SWEB_config.json adresáře sconf. Metoda load_url_from_txt přečte celý obsah databáze, odstraní počáteční i koncové bílé znaky “\n” pomocí metodě strip. Poté obsah rozdělí na samostatné řádky, přičemž se považuje za samostatnou adresu URL. Na konci je blokovaná adresa URL aktualizována do blokového seznamu metodou update, jako je představena v obrázku 4.1.



Obrázek 4.1: Vývojový diagram pro třídu URLBlocker

Metoda is_url_blocked je navržena tak, aby určila, zda by daná adresa URL byla považována za adresu podvodné stránky. Metoda má pouze jeden vstupní parametr url, který je získán signálem urlChanged od webového prohlížeče. Iteruje každou podvodnou adresu URL v seznamu a zkontroluje, zda je podřetězec vstupní adresy URL. Metoda vrátí hodnotu True, když by byla adresa obou URL shodná a zablokována. Naopak vrátí hodnotu False.

Souhrnně třída URLBlocker poskytuje funkce pro udržování seznamu podvodných adres URL, které by měly být blokovány. Seznam je získán v databázi podvodných stránek SWEB_PHISH_1 adresáře sconf/phish. Třída ještě nabízí metodu pro kontrolu, zda je daná adresa URL součástí tohoto seznamu. Funkce třídy je velmi užitečná pro zabezpečení webového prohlížeče proti podvodné stránce pro seniory. Obsahuje flexibilní způsob hledání - že hledá podvodnou adresu URL v seznamu jako podřetězec v rámci dané adresy URL.

4.2 Zaznamenání události ve webovém prohlížeči

Jakékoli události v prohlížeči jsou zaznamenány s cílem vyhodnocení bezpečnostních rizik. V rámci této diplomové práce je zvláště užitečné zaznamenávání takových událostí, jako jsou zobrazení podvodné webové stránky, existence chyby při inicializaci webového prohlížeče a

během spuštění metod v prohlížeči, nefungování zaznamenávání a další. Je tato funkce prováděna vlastní třídou URLLogger.

Tabulka 4.1: Záznam události při prohlížení webu aplikace

Úrovně	Úroveň logování	Popis
2	CRITICAL	Aplikace nepracuje
5	NOTICE	Přistupuje do phishingové webové stránky
6	INFORMATIONAL	Přistupuje do navštívené webové stránky

Ve třídě URLLogger je nastaven seznam úrovní zaznamenávání obsahující celkem 8 úrovní [34], jako jsou EMERGENCY, ALERT, CRITICAL, ERROR, a další. Ale stačí 3 úrovně pro webový prohlížeč, které jsou uvedeny v tabulce 4.1.

Výpis 4.4: Počáteční konstruktor od třídy URLLogger

```
class URLLogger:
    def __init__(self):
        # 7 security levels for logging
        self.severity_log_levels = ["EMERGENCY", "ALERT", "CRITICAL",
"ERROR", "WARNING", "NOTICE", "INFORMATIONAL", "DEBUGGING"]
        self.log_file_name = "logPhishing.txt"
        self._init_()
    def _init_(self):
        try:
            with open(self.log_file_name, 'r') as open_file:
                open_file.readline()
        except FileNotFoundError:
            with open(self.log_file_name, 'w', encoding="utf-8") as
                                                        open_file:
                open_file.write("Logging phishing URL from Browser\n")
```

Nejprve je nutné definovat počáteční parametr souboru log, ve kterém ukládá název souboru, do kterého se logování zapisuje. V případě, že není žádný název souboru zadán, je nastaven na výchozí hodnotu “logPhishing.txt”. Konstruktor _init_ je volán k inicializaci souboru log, který je uveden ve výpisu 4.4. Kdyby existoval soubor, pouze otevři v režimu čtení s hodnotou “r”. Naopak vytvoří nový soubor se zadaným názvem log v režimu zápisu s hodnotou “w” a zapíše úvodní řádek na začátku souboru.

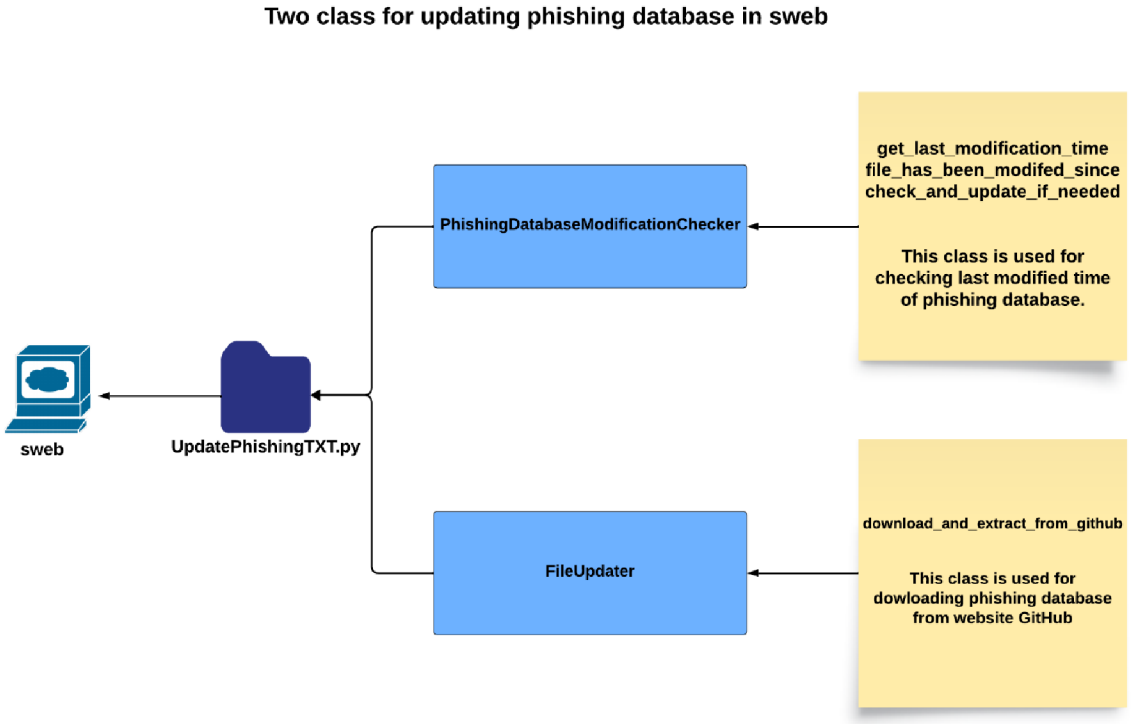
Na konci je nutné provádět formátování a zápis záznamu do textového souboru log. K zajištění aktuálního času je používáno časové razítko knihovny datetime. Zase vytvoří řetězec

záznamu, otevře textový soubor v režimu “a - open for writing” a zapíše řetězec záznamu do následovaného nového řádku na konci souboru. Tím je zajištěno, že je každý řetězec záznamu přidán do souboru, aniž by došlo k přepsání existujícího obsahu.

Třída URLLogger poskytuje jednoduchý způsob zaznamenávání jakýchkoliv událostí ve webovém prohlížeči do záznamu činnosti. Tato funkce je nutná, aby sledovalo potenciální bezpečnostní hrozby, aktivity uživatelů a chování prohlížeče v aplikaci. Záznamy lze použít ještě pro účely analýzy, ladění nebo auditu.

4.3 Aktualizace databáze podvodné stránky

Pravidelná aktualizace databáze podvodné stránky pro webový prohlížeč je nezbytná. Existuje pro to mnoho důvodů, jako udržování účinnosti webového prohlížeče, ochrana uživatele proti vývoji hrozeb a další, protože podvodníci vytvářejí neustále nové webové stránky a používají různé strategie, aby se vyhnuli odhalení.



Obrázek 4.2: Návrh třídy pro aktualizaci podvodné stránky

Ještě pravidelná aktualizace zajišťuje, že databáze vždy obsahuje nejnovější známé podvodné adresy URL, což zvyšuje schopnost účinně chránit uživatele. Tato funkce je prováděna svou vlastní třídou PhishingDatabaseModificationChecker a FileUpdater, jako jsou představeny v obrázku 4.2.

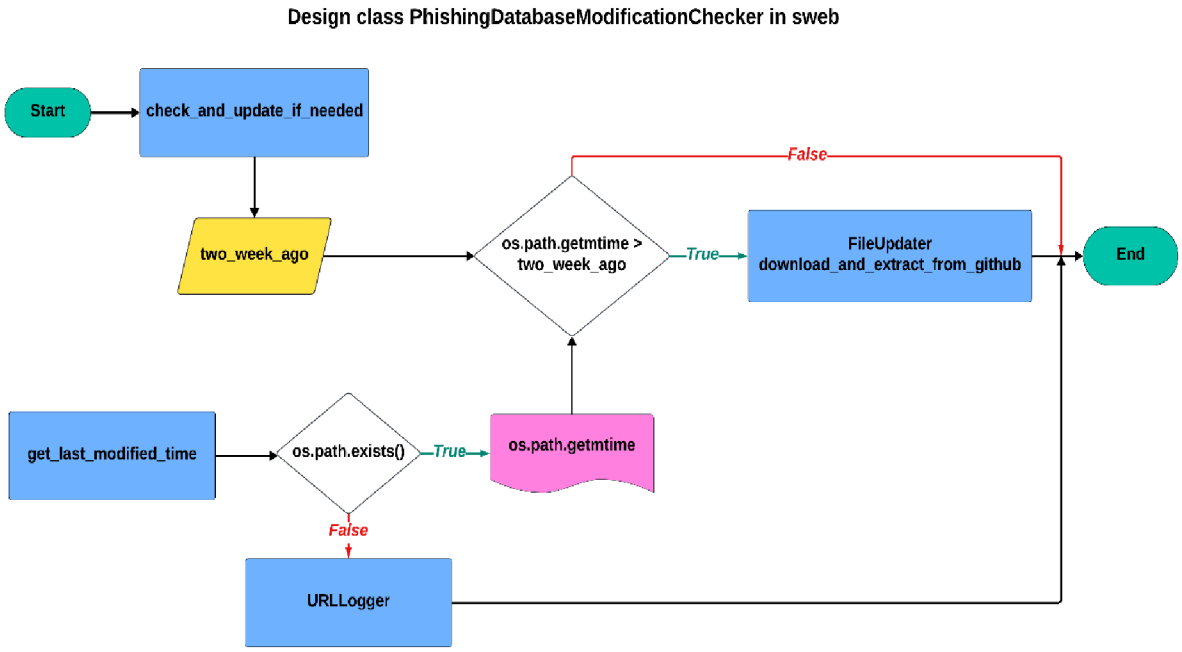
4.3.1 Inicializace kontroly času poslední modifikace databáze

Třída PhishingDatabaseModificationChecker je navržena pro monitorování databáze podvodné stránky a v případě potřeby jej aktualizuje. Integruje několik metod, včetně kontroly času poslední modifikace databáze a aktualizace databáze ze vzdáleného zdroje. V rámci této diplomové práce je vzdálený zdroj na webové stránce GitHub.

Výpis 4.5: Inicializace nové třídy PhishingDatabaseModificationChecker

```
class PhishingDatabaseModificationChecker:
   def __init__(self,my_config_data,input_from_main_url_logger):
     self.url_logger = input_from_main_url_logger
     self.path_to_phishing_database =
                       my_config_data["phishing_database"]["path"]
     url_to_tar_github =
my_config_data["phishing_database"]["path_to_tar_github"]
     self.database_updater = FileUpdater(url_to_tar_github,
          self.path_to_phishing_database,self.url_logger)
```

Nejprve je třída PhishingDatabaseModificationChecker inicializována konstruktorem __init__, který je uveden ve výpisu 4.5. Konstruktor má celkem tři vstupní parametry, jako jsou self, konfigurační data a logger. Self je zkratka pro celou webovou aplikaci. Konfigurační data obsahují cestu k databázi podvodné stránky a webovou adresu URL ke vzdálenému souboru typu tar.gz obsahujícího aktuální databázi podvodné stránky. Návrh této třídy je představen v obrázku 4.3.



Obrázek 4.3: Třída pro kontrolu času poslední modifikace podvodné databáze

Konfigurační data jsou uložena v souboru SWEB_config adresáře sconf. Parametr logger je používána k zaznamenání chyby do textového souboru log, kdykoliv chyba nastane při získání poslední modifikace času.

Potom je jedna instance třídy FileUpdater inicializována se vstupní cestou webové adresy URL ke vzdálenému souboru typu tar.gz, který je dostupný na webové stránce GitHub. Tato instance je pravděpodobně zodpovědná za stahování a extrakci databáze podvodné stránky.

Výpis 4.6: Získání poslední časové modifikace databáze podvodné stránky

```
def get_last_modification_time(self):
    # Returns as a datetime object.
    # Check if the file is existed
    if not os.path.exists(self.path_to_phishing_database):
        raise FileNotFoundError(self.url_logger.log_blocked_url('WEBBROWSER',
2, 'UpdatePhishingTXT', f'File path not found {self.file_path_to_txt}'))
    else:
        # Get the last modificated time
        last_update_time = os.path.getmtime(self.path_to_phishing_database)
        # Using fromtimestamp to change it to Calender
        return datetime.fromtimestamp(last_update_time)
```

Třída get_last_modification_time je určena k získání poslední časové modifikace textového souboru phishing a vrácení času ve formě objektu datetime. Ukázka této třídy je zobrazena ve

výpisu 4.6. Potom zkontroluje existenci zadané databáze podvodné stránky použitím metody path.exists knihovny os. Pokud databáze neexistuje, vyvolá výjimku FileNotFoundError.

Navíc zaznamená tuto chybovou událost pomocí parametru logger se textovou zprávou úrovně CRITICAL oznamující, že cesta k databázi nebyla nalezena. Naopak, pokud databáze existuje, zjistí čas jeho poslední modifikace pomocí metody path.getmtime třídy os, který vrací modifikovaný čas jako časové razítko. Potom je časové razítko převedeno na objekt datetime pomocí metody fromtimestamp.

Výpis 4.7: Kontrola poslední modifikace databáze je větší než dva týdny

```
# Returns True if modified after check_time, False otherwise.
def file_has_been_modified_since(self, compared_time):
    return self.get_last_modification_time() > compared_time
```

Poslední modifikace databáze podvodné stránky se porovnává s porovnávaným časem v metodě file_has_been_modified_since. V rámci této práce se porovnávaný čas rovná dvě týdny. Pokud modifikovaný interval není větší než dvě týdny, tak vrací hodnotu False, což znamená, že nebyla databáze změněna za dva týdny. Naopak metoda vrací hodnotu True.

Výpis 4.8: Metoda přístupu k aktualizaci databáze

```
def check_and_update_if_needed(self):
    two_weeks_ago = datetime.now() - timedelta(weeks=2)
    if not self.file_has_been_modified_since(two_weeks_ago):
        self.database_updater.download_and_extract_from_github()
```

Medota check_and_update_if_needed ve výpisu 4.8 inicializuje hodnotu času před dvěma týdny od aktuálního času pomocí metody datetime.now a timedelta s hodnotou dvou týdnů. Jestliže je získána hodnota True od metody file_has_been_modified_since, spustí proces aktualizace voláním metody download_and_extract od třídy FileUpdater.

Na shrnutí, třída PhishingDatabaseModificationChecker slouží k automatizaci procesu kontroly, zda je databáze podvodné stránky nutno aktualizovat, kdy byl naposledy změněn. Pokud nebyla aktualizována v posledních dvou týdnech, spustí se proces aktualizace, aby se zajistila aktuálnost databáze. Pro udržování aktuální bezpečnosti webového prohlížeče je důležité mít nejnovější seznam podvodných stránek.

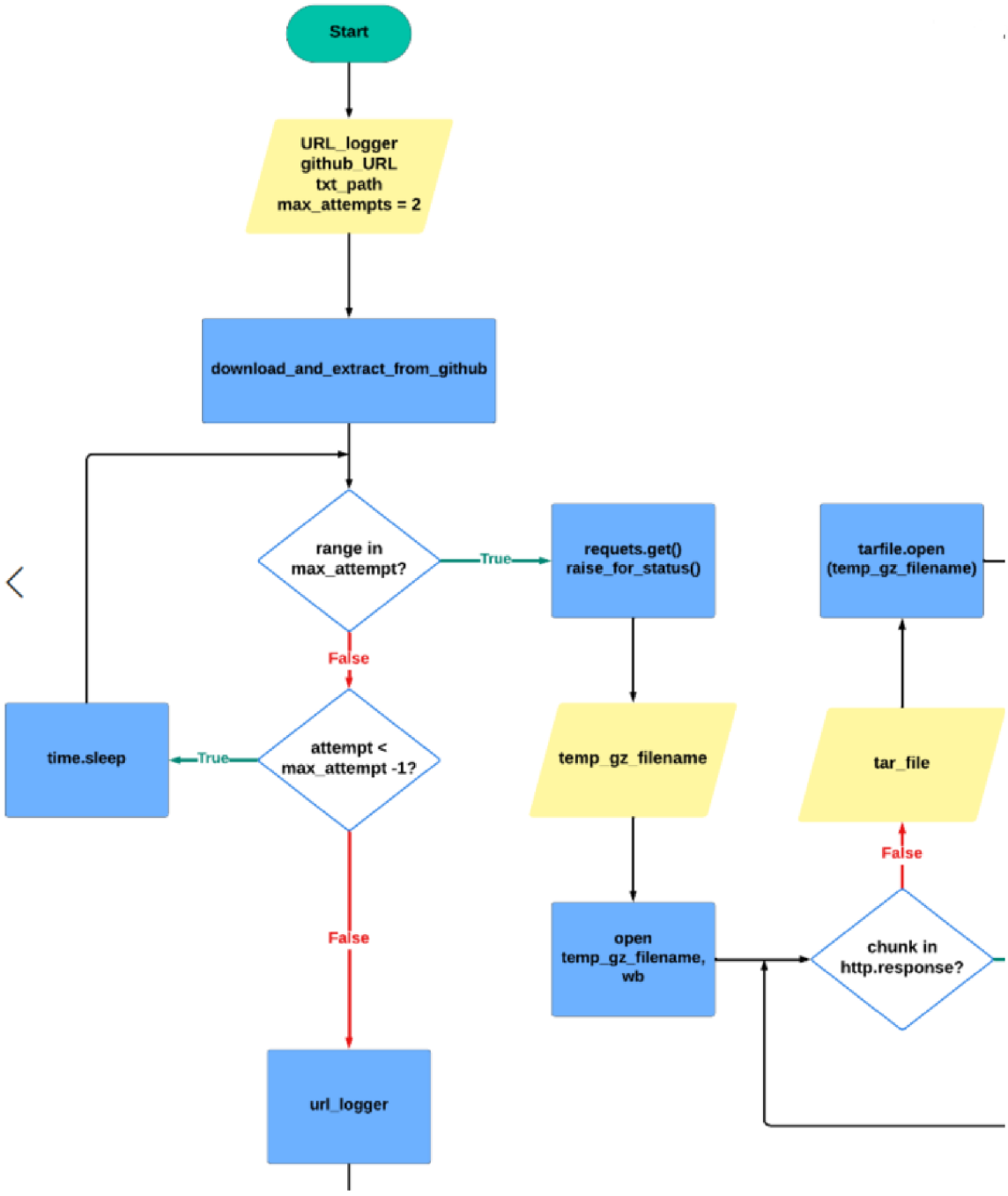
4.3.2 Stažení databáze podvodné stránky

Třída FileUpdate je navržena pro stahování a aktualizaci databáze podvodné stránky konkrétně ze vzdálené webové stránky GitHub. Ve třídě je současně metoda pro zpracování stahování souboru tar.gz ze vzdáleného zdroje, metoda pro extrakci obsahu souboru .tar.gz do databáze podvodné stránky a správa chyb během procesu pomocí třídě URLLogger.

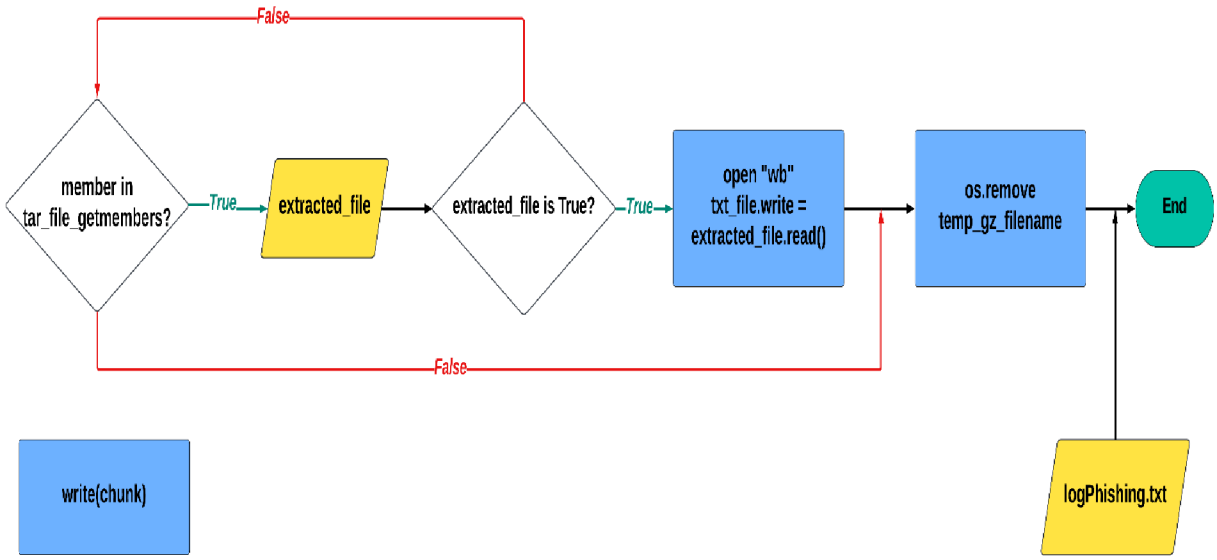
Výpis 4.9: Třída FileUpdater pro stažení databáze

```
class FileUpdater:
    def __init__(self, github_url, path_to_database,input_url_logger):
        self.url_logger = input_url_logger
        self.github_url = github_url
        self.txt_path = path_to_database
        self.max_attempts = 2
        # Set delay after redirect HTTP
        self.delay_betwween_attempts = 0.1
```

Třída FileUpdater je inicializována konstruktorem __init__, jako je uveden ve výpisu 4.9. Konstruktor má celkem 4 vstupní parametry, jako jsou self, cesta k souboru tar.gz na webové stránce GitHub a cesta k databázi podvodné stránky. Parametr self je zkratka pro celou aplikaci. Cesta k souboru typu .tar.gz na webové stránce GitHub a cesta k databázi podvodné stránky jsou získány ze třídy PhishingDatabaseModificationChecker. Obě cesty jsou uloženy v souboru SWEB_config.json adresáře sconf. Vývojový diagram pro tuto třídu je představen v obrázku 4.4 a obrázku 4.5.



Obrázek 4.4: Diagram pro třídu na uložení a aktualizaci databáze podvodné stránky - první část



Obrázek 4.5: Diagram pro třídu na uložení a aktualizaci databáze podvodné stránky - druhá část

Potom je nutné inicializovat dvě hodnoty max_attempts a delay_between_attempts, které zajistí úspěšné vytvoření dočasného souboru typu .tar.gz pro aktualizaci databáze podvodné stránky. Dočasný soubor typu .tar.gz je uveden v dalším kroku. Hodnota max_attempts označí počet pokusů, od kterých se aplikace pokusí stáhnout v případě neúspěchu stahování. Ještě je uvedena hodnota delay_between_attempts dobou zpoždění mezi dvěma pokusy o opakování.

Výpis 4.10: Metoda stahování a extrakce

```
def download_and_extract_from_github(self):
    for attempt in range(self.max_attempts):
       try:
          # Connect to file_github and download
          http_response = requests.get(self.github_url, stream=True)
          # HTTPError object if an error has occurred during the process.
          http_response.raise_for_status()
          # Set file temp
          temp_gz_filename = "downloaded_phishing_database_temp.tar.gz"
          # Write to file temp
          with open(temp_gz_filename, "wb") as temp_file:
              for chunk in http_response.iter_content(chunk_size=1024):
                  temp_file.write(chunk)
        except (requests.ConnectionError, requests.HTTPError) as excep:
          if attempt < self.max_attempts -1:
              # Wait for the specified delay before retrying
              time.sleep(self.delay_betwween_attempts)
          else:
              self.url_logger.log_blocked_url("WEBBROWSER", 2,
                 "UpdatePhishingTXT", f'Can not update SWEB_PHISHING_1.txt')
```

Metoda download_and_extract je používána ke stahování a rozbalení obsahu souboru na webové stránce GitHub do databáze podvodné stránky. Tato metoda je zobrazena ve výpisu 4.10. Metoda obsahuje zpracování chyb a logické opakování pokusu pomocí metody try catch. Proces stahování je prováděn metodou get knihovny requests, která odešle požadavek HTTP GET na danou webovou cestu. V tomto případě je cesta do webové stránky GitHub. Metoda má dva vstupní parametry, jako jsou cesta k souboru typu .tar.gz na webové stránce GitHub a argument stream=True. Argument stream=True je používán ke stahování dat po každé části, což je užitečné pro zpracování velkých souborů.

Po odesílání požadavku HTTP GET je nutné zpracovat chybu, která by mohla nastat při stahování. Metoda raise_for_status zkontroluje, zda byl požadavek HTTP GET úspěšný. V této metodě vyvolá výjimku ConnectionError a HTTPError a existující chyba je zaznamenána do textového souboru log se stupni CRITICAL, pokud HTTPError vrátil stavový kód 4XX nebo 5XX, což je chyba. Proto je zajištěno, že proces pokračuje pouze, když by získal úspěšné odpovědi se stavovým kódem 200. Potom je dočasný soubor typu tar.gz inicializován k dočasnému uložení stažených dat. Metoda open se hodnotou “wb” (Write-binary) je nutná pro zápis binárních dat, jako je soubor tar.gz v této práci. Každá uložená část má nastavenou velikost 1024 bajtů a zapíše se do dočasného souboru pomocí atributu iter_chunk a write.

Výpis 4.11: Otevření, zapíše soubor a odstranění dočasného souboru tar.gz

```
try:
    with tarfile.open(temp_gz_filename, "r") as tar_file:
        for member in tar_file.getmembers():
            extracted_file = tar_file.extractfile(member)
            if extracted_file:
                with open(self.txt_path, "wb") as txt_file:
                    txt_file.write(extracted_file.read())
    # Remove file temp
    os.remove(temp_gz_filename)
    # Break for if the first HTTP is succeed
    Break
except tarfile.ReadError:
    self.url_logger.log_blocked_url('WEBBROWSER', 2,
'UpdatePhishingTXT', f'Can not open and write file tar
                                    {temp_gz_filename}')
```

Na konci je dočasný soubor otevřen s hodnotou “r” knihovny tarfile. Vyvolá výjimku ReadError a chyba je zaznamenána do souboru log se stupni CRITICAL, pokud by se nemohl otevřit.

Metoda extractfile extrahuje každý člen souboru tar.gz. Tato metoda má dvě vrácené hodnoty, první se jedná o objekt, když je soubor. Druhá hodnota je “None”, když není soubor. Potom podmínka kontroluje, zda je objekt souboru a otevře databázi podvodné stránky v režimu zápisu v binárním formátu “wb”. Zde se zapíše obsah dočasného souboru do databáze podvodné stránky. Po dokončení extrakce je nutné odstranit dočasný soubor pomocí metody remove od knihovny os, který zajistí, aby dočasný soubor nezabíral místo na disku po extrakci svého obsahu. Tato metoda je stručně popsána ve výpisu 4.11.

Stručně třída FileUpdater poskytuje metodu pro stahování souboru typu .tar.gz na webové stránky GitHub a aktualizaci databáze podvodné stránky. Je užitečná pro udržování aktuální databáze podvodné stránky pro bezpečnost webového prohlížeče. Po aktualizaci databáze následuje odstranění dočasného souboru typu .tar.gz. Třída obsahuje zpracování chyb, aby byla zajištěna spolehlivost procesu aktualizace.

5. Pokročilé zabezpečení webového prohlížeče pro seniory

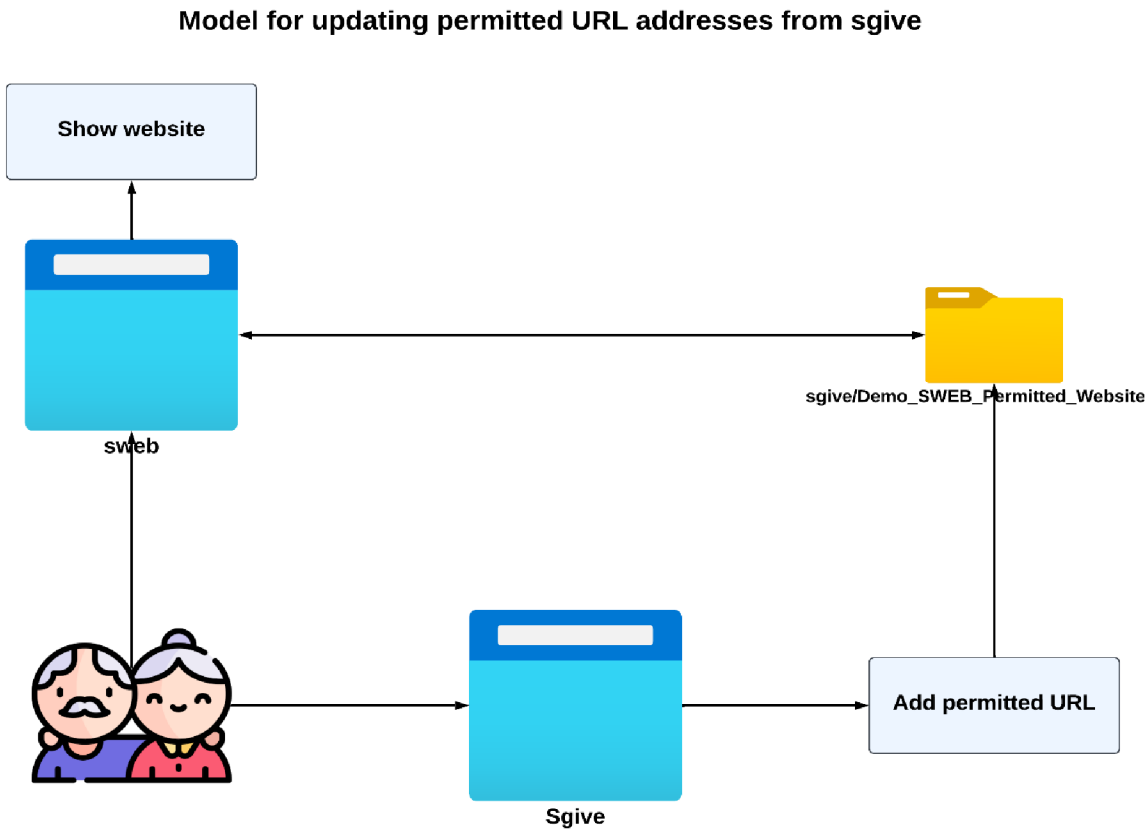
Předchozí kapitola 4 přinesla ž představení základní metody pro zabezpečení uživatele proti podvodné stránce.

Tato kapitola uvede bezpečnostní opatření, která zabrání zneužití osobních údajů. Jedním z takových opatření je prevence zadávání textu na webových stránkách. Tato funkce zakazuje uživatelům neúmyslné zadávání citlivých údajů, jako jsou hesla, osobní identifikační čísla, emailová informace, bankovní karta do formulářů umístěných na webových stránkách. Kdyby se uživatelé připojili do podvodné stránky, která je definována v databázi podvodných webových stránek, sweb zaznamená zadané informace od uživatele a tyto zaznamenané informace jsou bezpečně odesílány k opatrovníkovi. Toto pokročilé zabezpečení je uvedeno v obrázku 3.10.

Kapitola 5.1 definuje metodu pro vytvoření seznamu povolených webových stránek, v nichž je povoleno doplnit text do zadávacího pole. V kapitole 5.2 je představen způsob zákazu doplnění textu do nepovolené webové stránky. Dále kapitola 5.3 uvede metodu pro zaznamenání doplněné informace od uživatele do podvodné stránky. Kapitola 5.4 pojednává o odeslání získané uživatelské informace od podvodné stránky k opatrovníkovi.

5.1 Definování povolené webové stránky

K zvýšení bezpečnosti webového prohlížeče pro seniory je definování souboru důvěryhodných webových stránek používáno. Tato metoda spočívá v tom, že uživatele ukládají své důvěryhodné URL do databáze povolené stránky. V rámci této diplomové práce je tato databáze pojmenován Demo_SWEB_Permitted_Websites.txt a je uložena v adresáři sgive. Aplikace sgive umožňuje uživatelovi pravidelně aktualizovat své povolené webové stránky. Aktualizace může být přímé z rozhrání aplikace sgive, jako je zobrazena v obrázku 5.1.



Obrázek 5.1: Model pro aktualizaci povolené webové stránky

Pro načtení všech povolených webových stránek v databázi je používána metoda load_permitted_website_from_sgive, jak je uvedeno ve výpisu 5.1. Tato metoda je inicializována ve třídě loadConfig.

Výpis 5.1: Metoda načtení povolených webových stránek na doplnění textu

```
def load_permitted_website_from_sgive():
  permitted_website_list = set()
  # Exit when error occurs and print notification to log
  try:
    with open("../sgive/Demo_SWEB_Permitted_Websites.txt", 'r') as open_file:
        content  = open_file.read()
        reading_website = content.strip().split('\n')
        permitted_website_list.update(reading_website)
    open_file.close
    return permitted_website_list
  except FileNotFoundError:
    print(f"Configuration file not found: {open_file}")
```

Metoda umožňuje webovému prohlížeči selektivně povolit zadávání textu pouze na povolených webových stránkách, které byly ověřeny a považovány za bezpečné stránky. Také jsou povolené webové stránky možné přidány uživatelem podle jejich potřeby. Když uživatele připojí na webovou stránku, sweb porovná současnou adresu URL s každou adresou URL v databázi povolené webové stránky, jako je uvedeno ve výpisu 5.2. Pokud je nalezena shoda, sweb zapne doplnění do textového pole, která umožní komunikovat s webovou stránkou. Naopak je komunikace zakázána.

Výpis 5.2: Metoda pro volání databáze povelené webové stránky

```
permitted_website_list = load_permitted_website_from_sgive()
# Check if it is permitted website
check_result = any(permitted_website in url_in_browser_value for
                    permitted_website in permitted_website_list)
```

Tato metoda nejen zvyšuje zabezpečení, ale také nabízí možnost přizpůsobení, která umožňuje uživatelům nebo správcům vytvořit databáze povolených webových stránek. Implementace této metody zachovává snadné používání, čímž zajišťuje, že se senioři mohou bezpečně zapojit do digitálního světa.

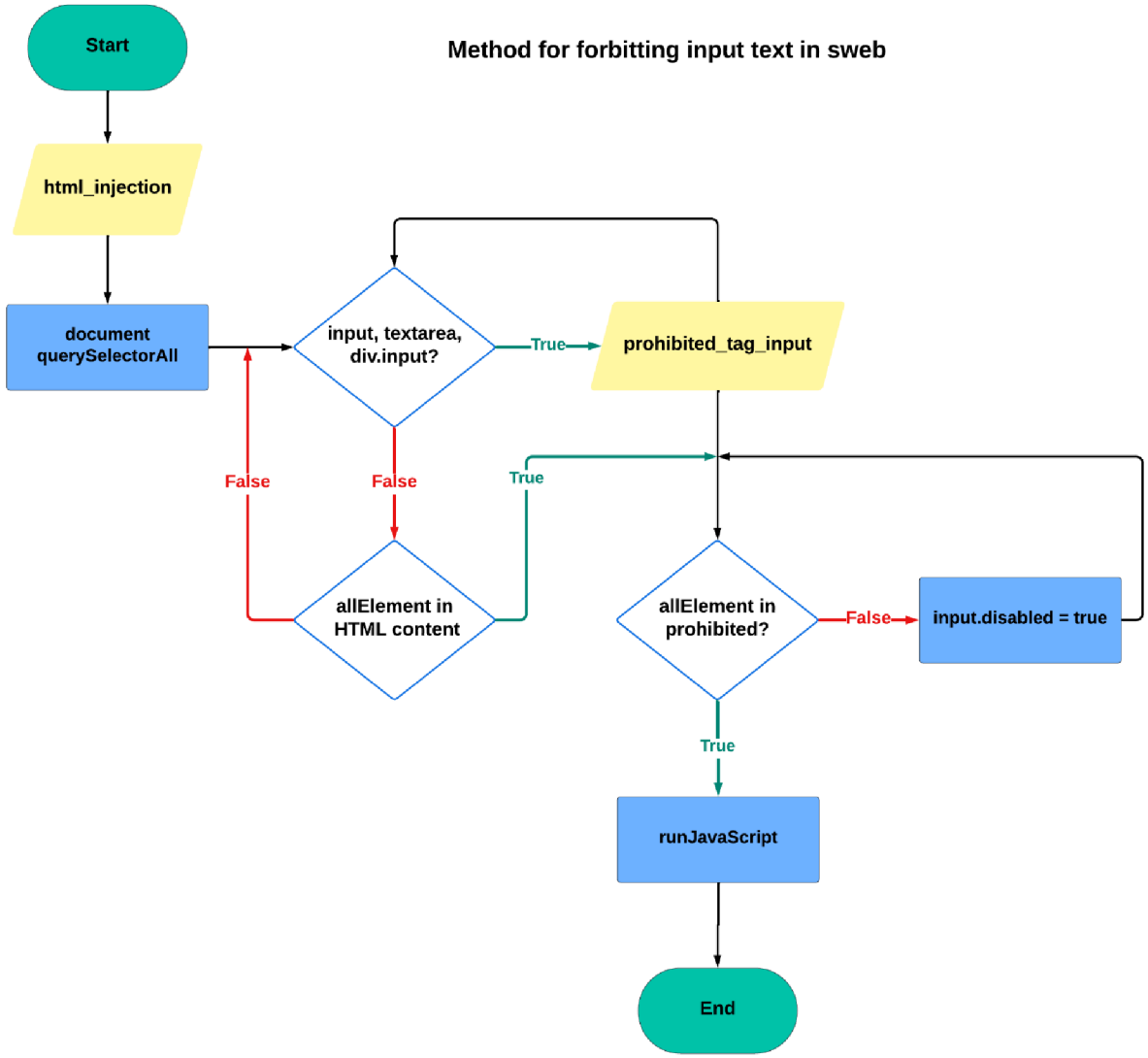
5.2 Zákaz doplnění textu

Zákaz doplnění textu do webové stránky účinně omezuje zadávání osobních údajů, jako jsou přihlašovací údaje, platební údaje a kontaktní údaje na webových stránkách, které by mohly být škodlivé nebo kompromitované. Povolené webové stránky jsou výslovně definovaných v důvěryhodném seznamu. Když se uživatel pokusí o interakci s webovou stránkou, která není rozpoznána v seznamu, sweb automaticky zakáže pole pro zadávání textu, čímž zabrání možnosti získání citlivých údajů neoprávněnými subjekty.

Výpis 5.3: Změna obsahu HTML pro zákaz doplnění textu do webové stránky

```
<!-- Declare tags for prohibiting input text to textfill-->
var prohibited_tag_input = document.querySelectorAll('input, textarea,
div.input');
<!-- Disable input field in webpage-->
prohibited_tag_input.forEach(function(input) {
    <!-- True == input value is disabled-->
    input.disabled = true;
});
```

K zákazu doplnění textu do podvodné stránky je metoda změny obsahu HTML používána. Její nastavené parametry jsou uvedeny ve výpisu 5.3. Metoda je prováděna výběrem konkrétních prvků webové stránky, které obvykle přijímají uživatelský vstup, jako jsou element “input”, “textarea” a “div” s třídou “input”. Metoda document.querySelectorAll si vybere všechny prvky na webové stránce, které odpovídají předchozím zadaným selektorům a vrací seznam uzlů obsahující všechny prvky, které splňují definovaná kritéria. Potom metoda forEach je volána na získaném seznamu uzlů.



Obrázek 5.2: Vývojový diagram pro zákaz doplnění textu v swebu

Pro každý prvek v seznamu se provede funkce a nastaví jeho vlastnost input.disabled na hodnotu “true”. To znamená, že by uživatelé nemohly doplnit i integrovat s definovanými prvky, čímž se tyto prvky stávají neaktivními. Vývojový diagram pro tuto metodu je zobrazen v obrázku 5.2.

5.3 Zaznamenání doplněné uživatelské informace

Zaznamenání doplněné uživatelské informace v podvodné stránce se jedná o zájem ochrany citlivých informací pro uživatele, zejména ve scénářích, kdy by uživatele mohly neúmyslně ignorovat varování při připojení do podvodné webové stránky. Cílem této funkce není zasahovat do soukromí uživatele nebo získat soukromé a citlivé uživatelské informace, ale spíše funguje jako pojistka pro zmírnění škod v případě ohrožení osobních údajů. Jako by byly na podvodné webové stránce zadány přihlašovací údaje nebo finanční informace, mohly by být okamžitě zahájeny reakce a oznámení k uživatelovi, jako je změna heslo nebo upozornění finančních institucí. Což by snížilo riziko krádeže identity i finančního podvodu.

Výpis 5.4: Změna obsahu HTML pro zaznamenání doplněné uživatelské informace

```
var script = document.createElement('script');
<!-- Define and call script qtwebchannel-->
script.src = 'qrc:///qtwebchannel/qwebchannel.js';
script.onload = function() {
   new QWebChannel(qt.webChannelTransport, function(channel) {
      window.notification_fill_text = channel.objects.notification_fill_text;
      <!-- Elements for capturing text are defined HERE!!!-->
      document.querySelectorAll('input[type="text"], input[type="email"],
input[type="search"], input[type="password"], input[type="tel"],
input[type="url"],input[enterkeyhint="search"],
textarea').forEach(function(element) {
          element.addEventListener('change', function() {
             var data = {value: element.value, url: window.location.href};
             <!-- Parse text to channel in type of JSON text-->
             window.notification_fill_text.receiveData(JSON.stringify(data));
             });
         });
     });
};
```

Metoda pro zaznamenání doplněné uživatelské informace do podvodné stránky je představena ve výpisu 5.4. V tomto swebu je metoda změny obsahu HTML používána. Jedná se o metodu dynamického přidávání nového prvku “script” na webovou stránku, který je načten souborem QtWebChannel, v této situaci je soubor qwebchannel.js. Toto nastavení usnadňuje komunikaci

mezi webovým obsahem typu JavaScript a aplikací PyQt. Nejenže zachytí vstupní data uživatele z různých formulářových prvků, ale také odesílá získaná data zpět do aplikace PyQt ke zpracování. Její vývojový diagram je zobrazen v obrázku 5.3.

Obrázek 5.3: Diagram pro zaznamenání uživatelské informace v sweb

Poprvé je nutné vytvořit nový skript “script” a jeho atribut “src” se nastaví na hodnotu “qrc:///qtwebchannel/qwebchannel.js”, ve kterém je soubor QtWebChannel Javascript umístěno. Tento soubor je nezbytný pro navázání komunikace mezi obsahem webové stránky a aplikací PyQt. Kdyby byl vytvořený skript načten pomocí atributu script.onload, zpětná funkce inicializuje kanál QWebChannel. Inicializovaný kanál umožňuje obsah webové stránky komunikovat s objekty swebu.

Vytvořený kanál QWebChannel vyžaduje dva argumenty, jako jsou qt.webChannelTransport a function(channel). První argument určuje transportní mechanismus, který je QWebChannel používán k posílání zpráv. Druhý argument je funkce zpětného volání, která se zavolá, jakmile je kanál úspěšně vytvořen. Slouží jako inicializační nebo nastavovací blok, ve kterém lze přistupovat k objektům zpřístupněným prostřednictvím QWebChannel a pracovat s nimi. Kanál je detailně uveden v obrázku 5.3.

Ve funkci zpětného volání je získán odkaz na objekt, který je vystaven v swebu, jako je zobrazeno ve výpisu 5.4, že je pojmenován notification_fill_text. Tento objekt je určen k odesílání získaných dat z webové stránky do aplikace. Potom si vybere všechny prvky formuláře, které by mohly obsahovat uživatelský zadaný text, jako jsou element “input” s různých typů nebo element “textarea”. Tato funkce je prováděna pomocí metody document.querySelectorAll. Každý prvek z těchto definovaných prvků je prováděn událostí addEventListener s argumentem “change”, který se spustí, když uživatel změní obsah vstupního prvku.

Výpis 5.5: Připojení vytvořeného skriptu

```
document.head.appendChild(script);
```

Při výskytu události změny obsahu předchozího definovaného prvku se vytvoří datový objekt, který zachycuje aktuální hodnotu pomocí element.value a adresu URL aktuální stránky pomocí window.location.href. Tento datový objekt je zpracován do řetězce JSON pomocí funkce JSON.stringify. Potom je získaný řetězec JSON odeslán do swebu prostřednictvím metody window.notification_fill_text.receiveData. V tomto swebu se získaný řetězec JSON jedná o textovou doplněnou hodnotu, její typ a adresu podvodné webové stránky. Využívaná metoda receiveData bude uvedena v další kapitole. Nakonec se vytvořený skript připojí k dokumentu s hodnotou “head”, čímž se zajistí spuštění skriptu a nastavení pro zachycení a odeslání vstupních dat. Příkaz připojení vytvořeného skriptu je uveden ve výpisu 5.5.

5.4 Odeslání doplněné uživatelské informace k opatrovníkovi

Po zaznamenání doplněné uživatelské informace v podvodné stránce je nutné odesílat získané informace k opatrovníkovi. Tato metoda se slouží k ochraně uživatelů před bezprostředními hrozbami, které představují podvodné útoky a je prováděna vlastní třídou NotificationFillTextToPhishing. Třída NotificationFullTextToPhishing je představena ve výpisu 5.6.

Výpis 5.6: Třída NotificationFillTextToPhishing

```
class NotificationFillTextToPhishing(QObject):
    @pyqtSlot(str)
    def receiveData(self, received_data):
```

Vytvořená třída je inicializována se vstupní třídou QObject, což je základní třída pro všechny objekty, které by se mohly účastnit na systému signálů a slotů. Třída QObject je uvedena v obrázku 2.3. Pomocí příkazu @pyqtSlot označuje metodu jako slot, který lze připojit k signálu. Sloty v tomto případě jsou funkce, které jsou volány v reakci na vyslání signálu, konkrétně jsou zaznamenání doplněné uživatelské informace od podvodné stránky. Vstupní hodnota "str" určuje, že tento slot očekává jeden argument typu string.

Dále je metoda receiveData definována pro příjem zachycených dat. V předchozí kapitole 5.3 Zaznamenání doplněné uživatelské informace - bylo už uvedeno, že parametr received_data je řetězec ve formátu JSON, který obsahuje textovou doplněnou hodnotu, její typ a adresu podvodné webové stránky.

Výpis 5.7: Rozebrání získané informace z formátu JSON

```
parsing_data = json.loads(received_data)
input_text = parsing_data.get('value')
connected_phishing_url = parsing_data.get('url')
computer_username = getpass.getuser()
computer_devicename = socket.gethostname()
current_time = datetime.now().strftime('%Y-%m-%d %H:%M:%S')
```

Uvnitř metody receiveData je přijatý řetězec rozebrán z formátu JSON do slovníku Pythonu pomocí funkce json.loads(). Tato funkce transformuje řetězec JSON na objekt jazyka Python, což usnadňuje práci s daty. Funkce je představena ve výpisu 5.7. Získaná data jsou následně zpracována do jednotlivých dat pomocí metody get s hodnotou klíče. Kromě těchto dat je

inicializováno uživatelské přihlašovací jméno, počítačové jméno a současný čas. Tyto všechny předchozí informace jsou odeslány k opatrovníkovi na ochranu uživatele. Formát odeslaných informací k opatrovníkovi je uveden v následujícím výpisu 5.8.

Výpis 5.8: Formát odeslaných informací k opatrovníkovi

```
*****Data received from sWEB when user filled text in phishing
website*****
        - Device name: {computer_devicename}
        - User name: {computer_username}
        - Website: {connected_phishing_url}
        - Time: {current_time}
        - Filled text: {input_text}
```

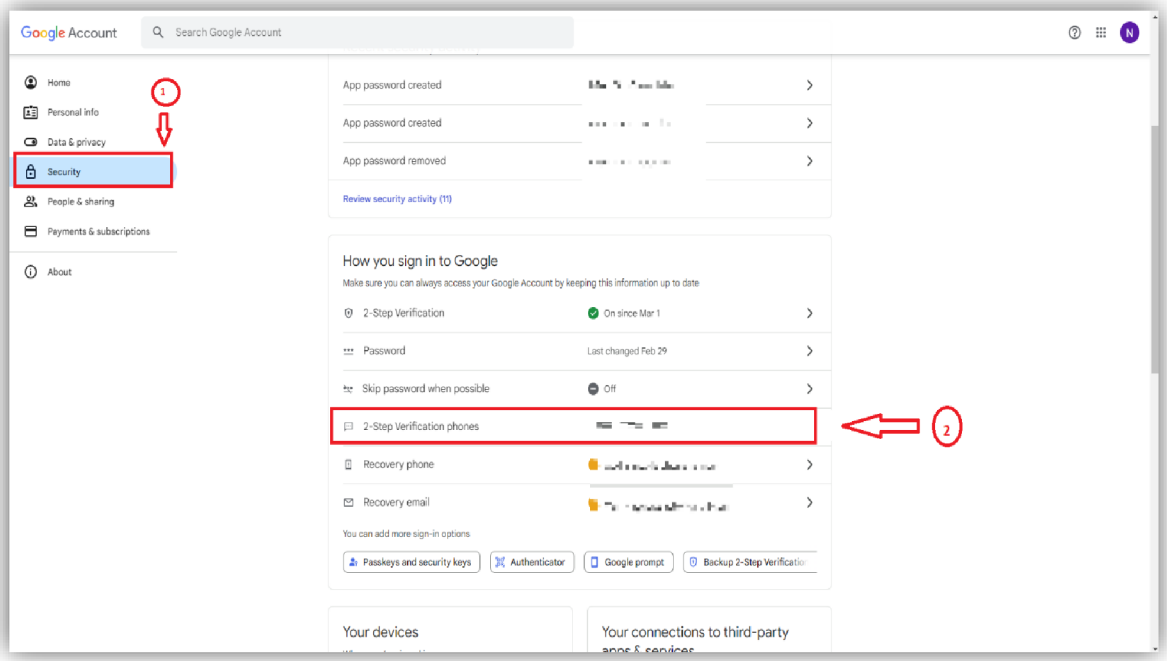
Po inicializaci formátu odeslaných informací je funkce send_email určena k přenosu e-mailů, která využívá protokol SMTP. Funkce začíná načtením potřebných údajů o konfiguraci e-mailu z definovaného konfiguračního souboru JSON, který je pojmenován názvem SWEB_config.json. Tento soubor je uložen v adresáři sconf. Zahrnuje e-mailovou adresu odesílatele, heslo odesílatele, e-mailovou adresu příjemce, předmět e-mailu, adresu serveru SMTP a port SMTP. Tyto konfigurace jsou nezbytné pro navázání spojení s e-mailovým serverem a zajištění správného adresování a odeslání e-mailu. Uložené konfigurační hodnoty pro navázání spojení přes protokol SMTP jsou představeny v tabulce 5.1.

Tabulka 5.1: Konfigurační hodnoty pro metodu send_email

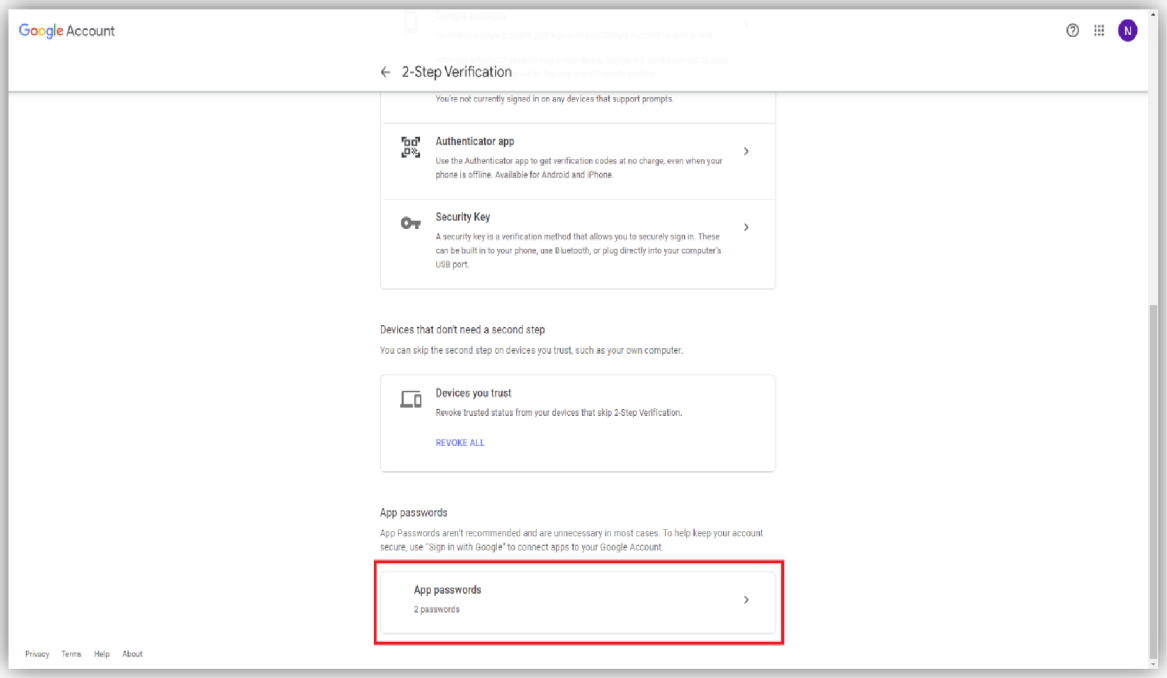
Proměnná	**Hodnota**	**Popis**
Sender_mail	ninhtestmagisterwork11111@gmail.com	E-mailová adresa odesílatele.
Sender_password	txhs bgkh aiga jnjc	Heslo odesílatele.
Receiver_mail	nguoiyeuvtv@gmail.com	E-mailová adresa opatrovníkovi.
Subject	User's filling data	Předmět e-mailu.
SMTP_server	Smtp.gmail.com	Adresa serveru gmail.
SMTP_port	587	Číslo portu SMTP

Heslo odesílatele v tabulce 5.1 není přihlašovací heslo odesílatele, ale je heslo třetí strany ze služby gmail. Často je označované jako heslo aplikace, které je vyžadováno pro vyšší

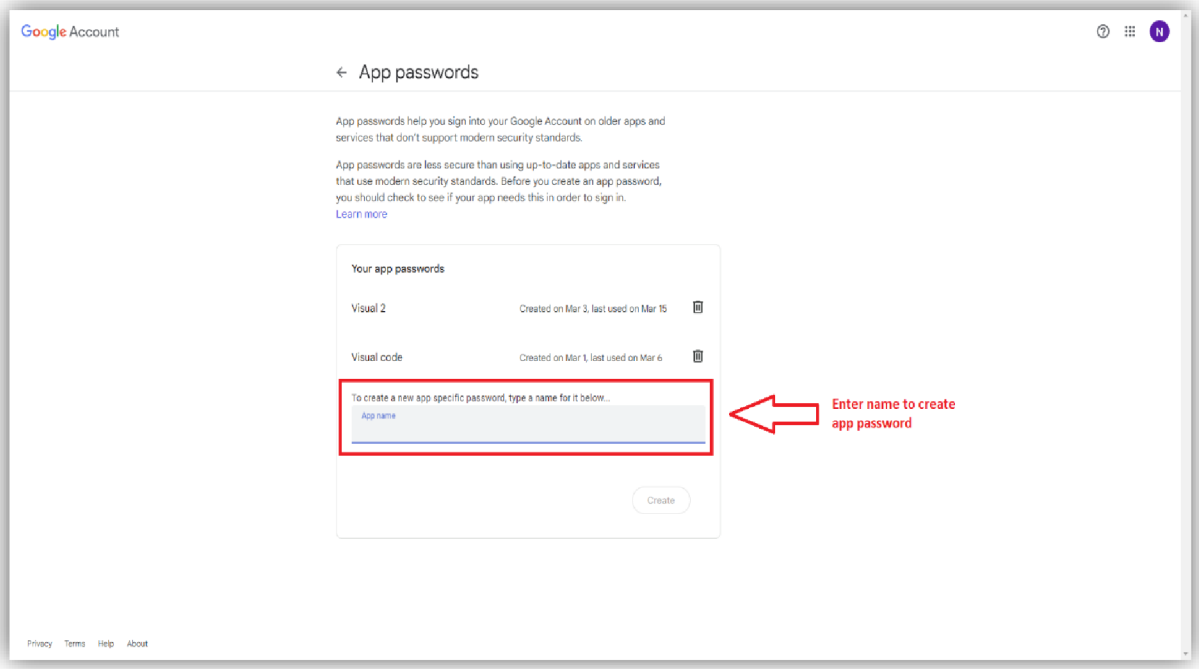
zabezpečení. Společnost Google toto vynucuje, aby poskytla další vrstvu ochrany. Hesla aplikací umožňují méně zabezpečeným aplikacím přistupovat k účtu Google pomocí jedinečného hesla, čímž se izoluje riziko pro konkrétní aplikaci. Tento přístup zajišťuje, že heslo hlavního účtu zůstane bezpečně v případě prozrazení hesla a heslo aplikace lze snadno zrušit. K vytvoření hesla aplikace je nutné si přihlásit do webové stránky GoogleAccount použitím hlavního účtu a hesla. Nyní je kliknutí na možnost „spravovat přístup třetích stran", heslo aplikace. Postup vytvoření je uveden v následujícím obrázku.



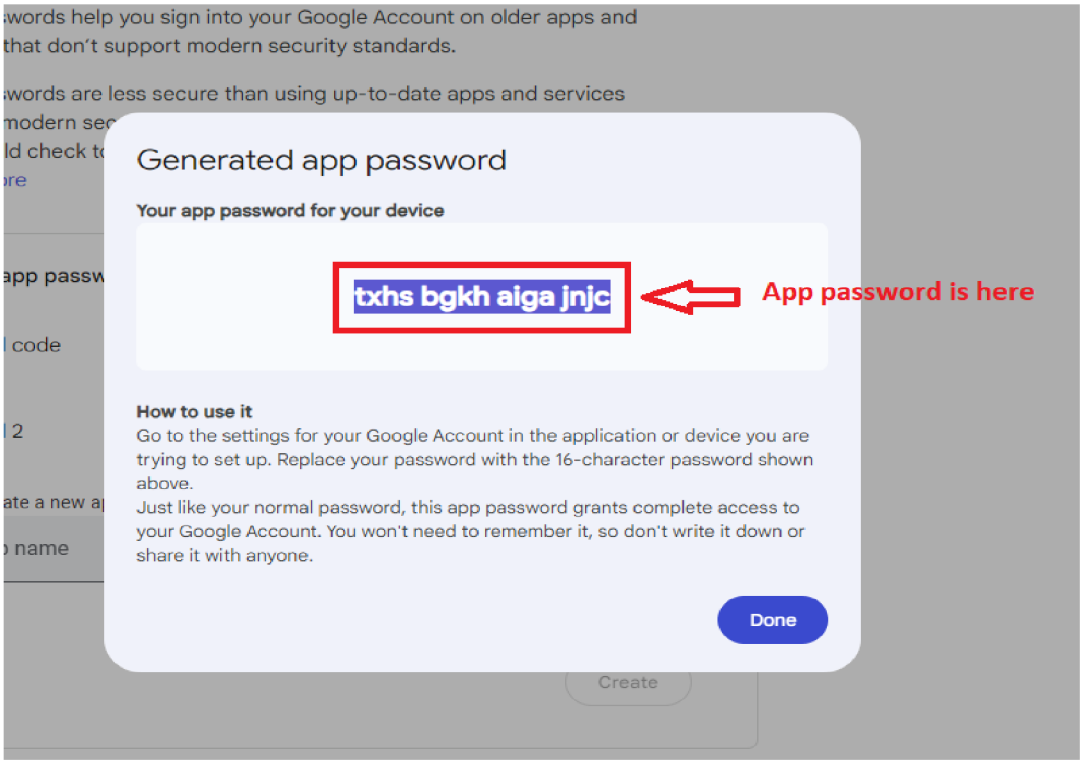
Obrázek 5.4: Přístup k nastavení bezpečnosti



Obrázek 5.5: Přístup k nastavení hesla aplikace



Obrázek 5.6: Vytvoření hesla aplikace

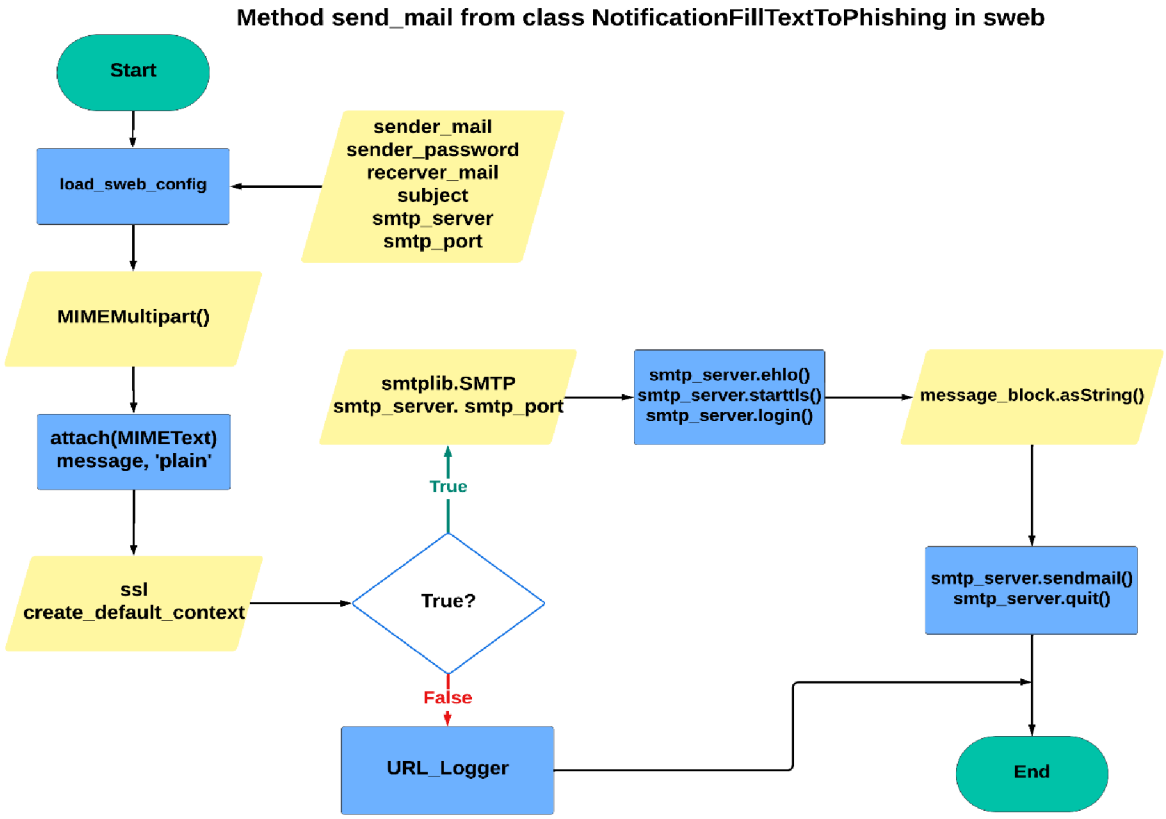


Obrázek 5.7: Heslo aplikace používaných v swebu

Výpis 5.9: Vytvoření e-mailové zprávy

```
message_block = MIMEMultipart()
message_block['From'] = sender_mail
message_block['To'] = receiver_mail
message_block['Subject'] = subject
message_block.attach(MIMEText(message_to_receiver, 'plain'))
ssl_context = ssl.create_default_context()
```

Ve výpisu 5.9 se jedná o vytvoření e-mailové zprávy pomocí třídy MIMEMultipart a MIMEText. Tato funkce nastavuje základní součásti e-mailové zprávy, včetně adresy odesílatele, adresy příjemce, e-mailového předmětu a e-mailového těla. E-mailové tělo bylo inicializováno ve výpisu 5.8. Třída MIMEMultipart slouží k vytváření e-mailových zpráv, které mohou obsahovat více částí. Druhá třída je MIMEText, která představuje textový obsah e-mailu. V tomto swebu obsahuje dva argumenty. První argument je skutečné tělo e-mailů a druhý argument "plain" určuje typ e-mailového těla jako prostý text, což znamená, že e-mail neobsahuje HTML ani jiné formátování. Detailní informace je zobrazena v obrázku 5.8.



Obrázek 5.8: Vývojový diagram metoda send_email

Funkce ssl.create_default_context() inicializuje nový kontext SSL s výchozím nastavením. Tato funkce zajistí, že připojení k serveru SMTP bude bezpečnostně šifrované.

Výpis 5.10: Odesílání vytvořené zprávy k opatrovníkovi

```
try:
    smtp_server = smtplib.SMTP(smtp_server, smtp_port)
    smtp_server.ehlo()
    smtp_server.starttls(context=ssl_context)
    smtp_server.ehlo()
    smtp_server.login(sender_mail, sender_password)
    text = message_block.as_string()
    smtp_server.sendmail(sender_mail, receiver_mail, text)
    smtp_server.quit()
    print("Email sent successfully!!!")
except Exception as excep:
    url_logger = URLLogger()
    # Log with level 2 - CRITICAL
    url_logger.log_blocked_url('WEBBROWSER', 5, 'main <security>',
f'Not success to sending user filling text from phishing webpage to
Authorized people')
```

K odeslání e-mailových zpráv do zadaného SMTP serveru je nutná inicializace připojení. Tato funkce je prováděna pomocí třídy smtplib se dvěma vstupními parametry. Jsou jméno serveru a číslo portu, které jsou uvedeny v tabulce 5.1. Tímto krokem se vytvoří základní spojení potřebné pro odeslání e-mailu.

Potom je pozdrav EHLO volitelně odeslán k SMTP serveru. Tento pozdrav zahájí komunikaci mezi SMTP klientem a SMTP serverem. Ještě zajistí, že jsou oba připraveni zahájit proces přenosu e-mailu. Metoda starttls aktualizuje vytvořené připojení na použití protokolu TLS, který zajišťuje šifrování přenosu e-mailu.

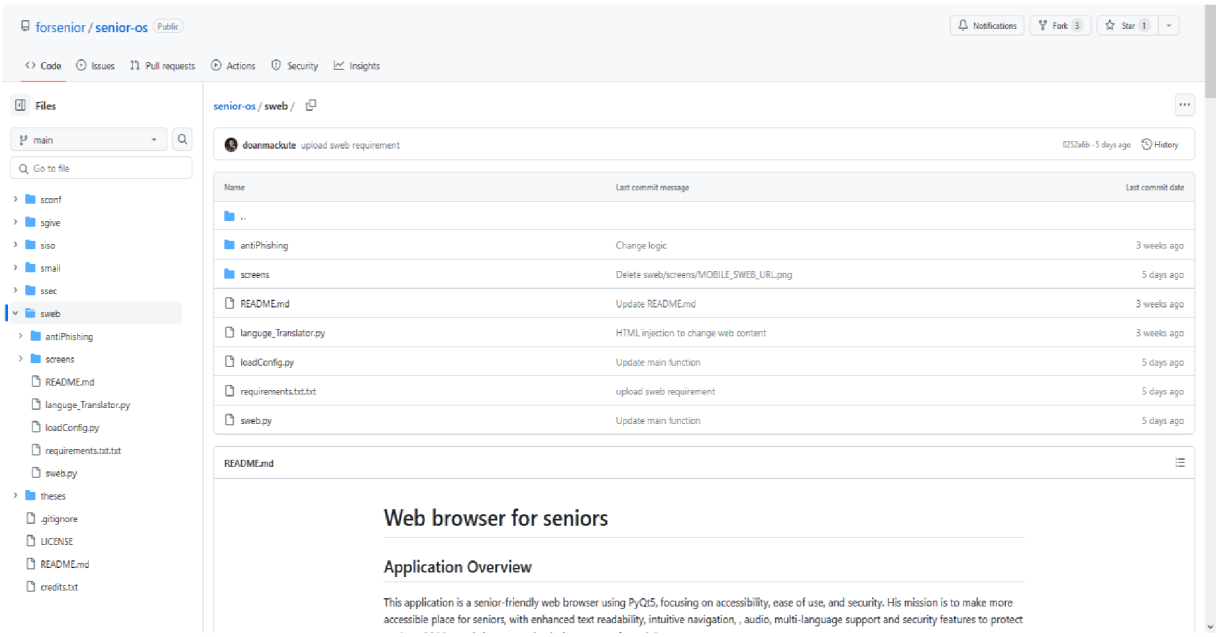
Na konci se přihlásí k serveru SMTP pomocí e-mailové adresy a heslo odesílatele, které jsou inicializovány v předchozím kroku. Funkce přihlášení je prováděna pomocí metody sendmail, jako je uvedena v obrázku 5.8. Vytvořené spojení se serverem SMTP je uzavřeno pomocí smtp_server.quit. Ještě zachytí blok except všechny výjimky, které se objeví během procesu odesílání e-mailu. Inicializuje instanci URLLogger a zaznamená chybovou zprávu s úrovně "NOTICE" do zaznamenaného textového souboru pro opravu chybových funkčností webového prohlížeče.

6. Stažení a použití webového prohlížeče pro seniory

V této kapitole je detailně představeno stažení kódu a použití webového prohlížeče pro seniory. Kapitola 6.1 uvede způsob stažení zdrojového kódu z webové stránky GitHub, ve které je projekt operačního systému pro seniory zveřejněn. Dále si kapitola 6.2 představí proces instalace knihoven a spuštění aplikace, jako jsou způsob instalace v operačním systému Windows, Fedora, metoda pro převod souboru Python do souboru typu .exe a spuštění webového prohlížeče. Použití webového prohlížeče pro seniory uvedeno v kapitole 6.3.

6.1 Stažení kódu z webové stránky GitHub

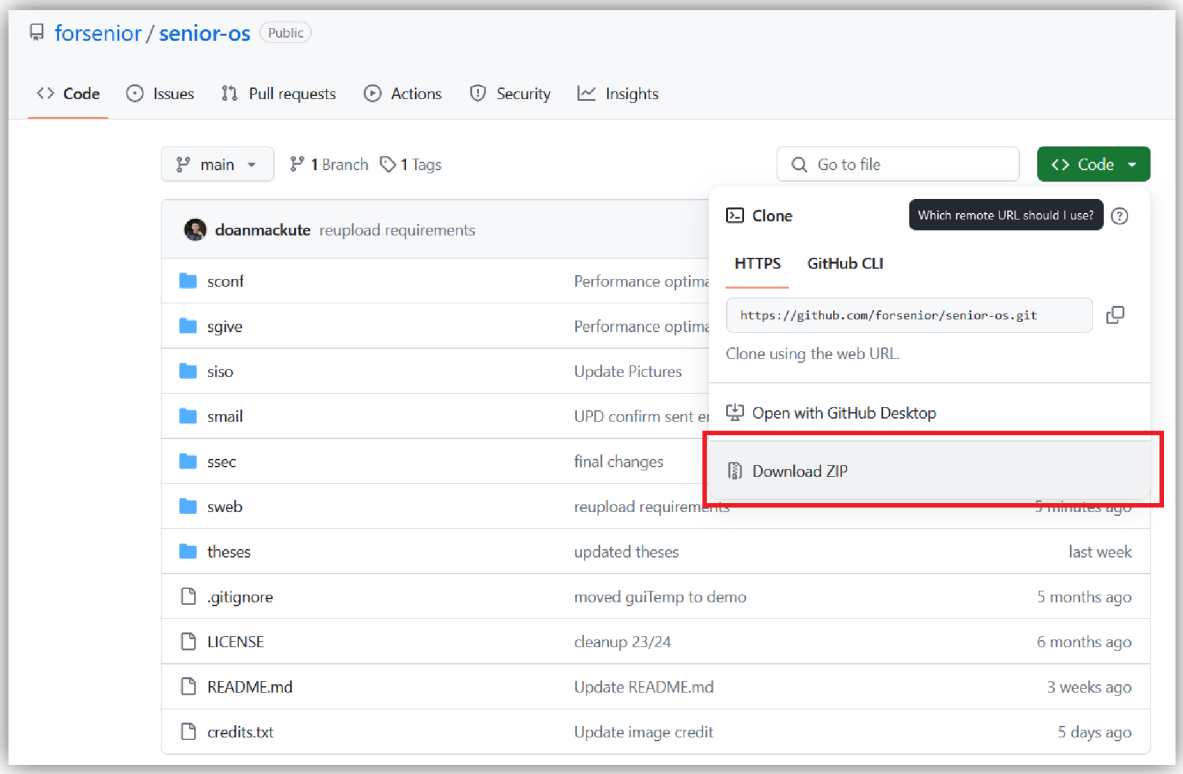
Nejprve je nutné stáhnout zdrojový kód, který je dostupný na webové stránce GitHub.



Obrázek 6.1: Struktura adresáře sweb v projektu senior-os

Výsledky této diplomové práce jsou zveřejněny na webové stránce GitHub pod licencí MIT, konkrétně pod organizací forsenior v repozitáři senior-os (Senior Operating System) v adresáři sweb. Adresář sweb obsahuje programový kód webového prohlížeče pro seniory, snímky obrazovky v adresáři screens a adresář antiPhishing, které slouží k ochraně uživatele proti podvodné stránce - phishing a k zaznamenávání činnosti i chyby ve spuštění aplikace, návod použití webového prohlížeče v souboru README.md a požadavek na využívané knihovny.

Odkaz do projektu Senior Operating System je uveden: https://github.com/forsenior/senior-os/tree/main. Struktura adresáře sweb je zobrazena v obrázku 6.1.



Obrázek 6.2: Přímá instalace operačního systému pro seniory

Instalace webového prohlížeče lze nainstalovat samostatně. Ale realizace probíhá primárně s celým operačním systémem pro seniory, protože počáteční konfigurační data pro všechny aplikace a konfigurační data webového prohlížeče jsou uložena v adresáři sconf, který je mimo adresáře sweb. Instalace kompletního operačního systému včetně všech aplikací by mohla být prováděna dvěma způsoby. První způsob je možné snadno provádět tak, že přímo nainstaluje ve webové stránce Github s předchozím odkazem do projektu Senior Operating System. Způsob přímé instalace je uveden v obrázku 6.2. Stačí kliknout na zobrazení kódu a tlačítko Download ZIP.

Výpis 6.1: Instalace v rozhraní příkazového řádku CLI

```
[ninhnguyentuan@fedora ~]$ sudo -i
[sudo] password for ninhnguyentuan:
[root@fedora ~]# wget https://github.com/forsenior/senior-os/tree/main
--2023-12-07 21:20:54--  https://github.com/forsenior/senior-os/tree/main
Resolving github.com (github.com)... 140.82.121.3
Connecting to github.com (github.com)|140.82.121.3|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]
Saving to: 'main.1'
```

Druhý způsob lze provádět přes rozhraní příkazového řádku CLI, protože byl operační systém pro seniory vyvinut v Linuxové distribuci, konkrétně Fedora. V tomto způsobu stačí otevřít terminál a spustit příkaz wget s předchozím odkazem do projektu Senior Operating System. Ukázka příkazu pro instalaci je uvedena ve výpisu 6.1.

Stažený soubor z obou způsobů je v typu zip, protože je nutné dekomprimovat jej do daného adresáře. Po dekompresi je projekt se všemi aplikacemi k dispozici.

6.2 Instalace knihoven a spuštění aplikace

V rámci této diplomové práce je používáno několik knihoven, které je možné uložit příkazem v rozhraní příkazového řádku (CLI), jako jsou PyQt5, PyQtWebEngine, screeninfo, pygame, requests, PyQt5Designer a další. PyQt5Designer je nutné použít v případě, že zajistí drag-and-drop rozhraní pro návrh grafického uživatelského rozhraní (GUI). Příkazy pro instalaci knihoven v operačním systému Fedora i Linux jsou uvedeny ve výpisu 6.2.

Výpis 6.2: Instalace knihoven v operačním systému Fedora, Linux

```
# Install required Python packages with dnf if using Fedora
sudo dnf install python3
sudo dnf install python3-qt5
sudo dnf install python3-qt5-webengine
sudo dnf install python3-pygame
pip3 install screeninfo
pip3 install yagmail
```

Kromě toho je webový prohlížeč pro seniory také navržen pro uživatele, kteří současně používají jiný operační systém než Fedora, Linux. Proto je vhodný pro operační systém Windows, který je používán největším počtem uživatelů. Příkazy pro instalaci knihoven v operačním systému Windows jsou představeny ve výpisu 6.3.

Výpis 6.3: Instalace knihoven v operačním systému Windows

```
# Install required Python packages in command prompt
pip install PyQt5
pip install PyQtWebEngine
pip install screeninfo
pip install PyQt5Designer
pip install pygame
pip install requests
pip install yagmail
```

V této fázi vývoje webového prohlížeče pro seniory není verze používaných knihoven pravidelně aktualizována. To znamená, že jejich verze je pořád stejná od začátku vývoje. Různé verze by mohly někdy způsobit špatné spuštění aplikace, ale k tomu nedochází často. Proto je požadavek pro spuštění webového prohlížeč uveden ve výpisu 6.4.

Výpis 6.4: Požadavky na verzi knihovny pro spuštění webového prohlížeče

```
python == 3.12.0
pyqt5 == 5.15.10
pyqtwebengine == 5.15.6
screeninfo == 0.8.1
pygame == 2.5.2
requests == 2.31.0
yagmail == 0.15.293
```

Pro kontrolu verze používané knihovny je používán příkaz pip show v příkazovém řádku. Příklad na kontrolu verze knihovny pyqt5 je představen ve výpisu 6.5. Pro ostatní knihovny je využíván stejným způsobem.

Výpis 6.5: Zobrazení verze knihovny pyqt5

```
C:\Users\nguoi>pip show pyqt5
Name: PyQt5
Version: 5.15.10
Summary: Python bindings for the Qt cross platform application toolkit
Home-page: https://www.riverbankcomputing.com/software/pyqt/
Author: Riverbank Computing Limited
Author-email: info@riverbankcomputing.com
License: GPL v3
Location: C:\Users\nguoi\AppData\Roaming\Python\Python312\site-
packages
Requires: PyQt5-Qt5, PyQt5-sip
Required-by: PyQtWebEngine
```

Po instalaci všech použitých knihoven je webový prohlížeč pro seniory dostupný k použití. Spuštění uložené aplikace je jednoduché pro programátory, kteří se často zabývají

programováním a interpretují programovací kód. Webový prohlížeč lze spustit přímo z příkazového řádku nebo používat programovací nástroj Visual Code.

Výpis 6.6: Spuštění webového prohlížeče v příkazovém řádku

```
D:\senior-os-main\sweb>python sweb.py
pygame 2.5.2 (SDL 2.28.3, Python 3.12.0)
Hello from the pygame community.
https://www.pygame.org/contribute.html
Warning: QT_DEVICE_PIXEL_RATIO is deprecated. Instead use:
   QT_AUTO_SCREEN_SCALE_FACTOR to enable platform plugin controlled
per-screen factors.
   QT_SCREEN_SCALE_FACTORS to set per-screen DPI.
   QT_SCALE_FACTOR to set the application global scale factor.
```

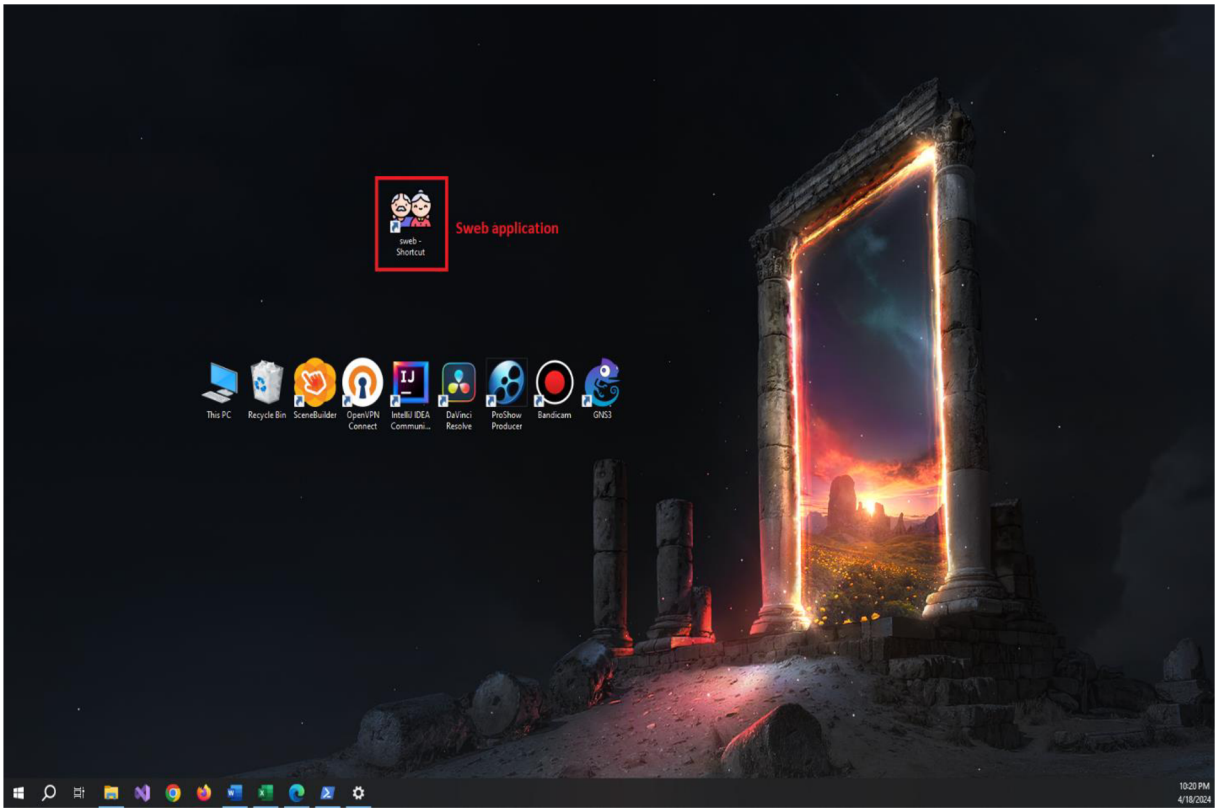
Jedná se o problém pro seniory, kteří nemají znalosti o programování a jsou zmateni při interakci s technikou. Je pro ně velmi obtížné, aby používali příkazový řádek nebo programovací nástroj při každém spuštění, kdyby chtěli číst novou zprávu nebo si prohlížet webové stránky. K řešení existujícího problému je používána metoda vytvoření souboru typu .exe, která vytvoří aplikační rozhraní a aplikace může být spuštěna při jednom kliknutí. Toto řešení je nezbytné a jednoduché pro seniory, protože od nich nevyžaduje žádné znalosti o programování.

V této diplomové práci je nástroj PyInstaller [41] používán k převodu skriptu Python do souboru .exe. Je představen ve výpisu 6.7.

Výpis 6.7: Převod skriptu Python do souboru .exe v PowerShell

```
PS C:\Users\nguoi\Downloads\senior-os-main1\senior-os-main\sweb> pip install
pyinstaller
PS C:\Users\nguoi\Downloads\senior-os-main1\senior-os-main\sweb> python -m
PyInstaller --onefile -w sweb.py
472 INFO: PyInstaller: 6.4.0, contrib hooks: 2024.1
472 INFO: Python: 3.12.0
527 INFO: Platform: Windows-10-10.0.19045-SP0
528 INFO: wrote C:\Users\nguoi\Downloads\senior-os-main1\senior-os-
main\sweb\sweb.spec
543 INFO: Extending PYTHONPATH with paths
['C:\\Users\\nguoi\\Downloads\\senior-os-main1\\senior-os-main\\sweb']
pygame 2.5.2 (SDL 2.28.3, Python 3.12.0)
Hello from the pygame community. https://www.pygame.org/contribute.html
1141 INFO: checking Analysis
1142 INFO: Building Analysis because Analysis-00.toc is non existent
...
118773 INFO: Building PYZ (ZlibArchive) C:\Users\nguoi\Downloads\senior-os-
main1\senior-os-main\sweb\build\sweb\PYZ-00.pyz
119558 INFO: Building PYZ (ZlibArchive) C:\Users\nguoi\Downloads\senior-os-
main1\senior-os-main\sweb\build\sweb\PYZ-00.pyz completed successfully.
119650 INFO: checking PKG
119650 INFO: Building PKG because PKG-00.toc is non existent
119651 INFO: Building PKG (CArchive) sweb.pkg
167351 INFO: Building PKG (CArchive) sweb.pkg completed successfully.
167408 INFO: Bootloader C:\Users\nguoi\AppData\Roaming\Python\Python312\site-
packages\PyInstaller\bootloader\Windows-64bit-intel\runw.exe
167408 INFO: Bootloader C:\Users\nguoi\AppData\Roaming\Python\Python312\site-
packages\PyInstaller\bootloader\Windows-64bit-intel\runw.exe
167408 INFO: checking EXE
167409 INFO: Building EXE because EXE-00.toc is non existent
167409 INFO: Building EXE from EXE-00.toc
167421 INFO: Copying bootloader EXE to C:\Users\nguoi\Downloads\senior-os-
main1\senior-os-main\sweb\dist\sweb.exe
167662 INFO: Copying icon to EXE
167777 INFO: Copying 0 resources to EXE
167778 INFO: Embedding manifest in EXE
167912 INFO: Appending PKG archive to EXE
168195 INFO: Fixing EXE headers
181725 INFO: Building EXE from EXE-00.toc completed successfully.
```

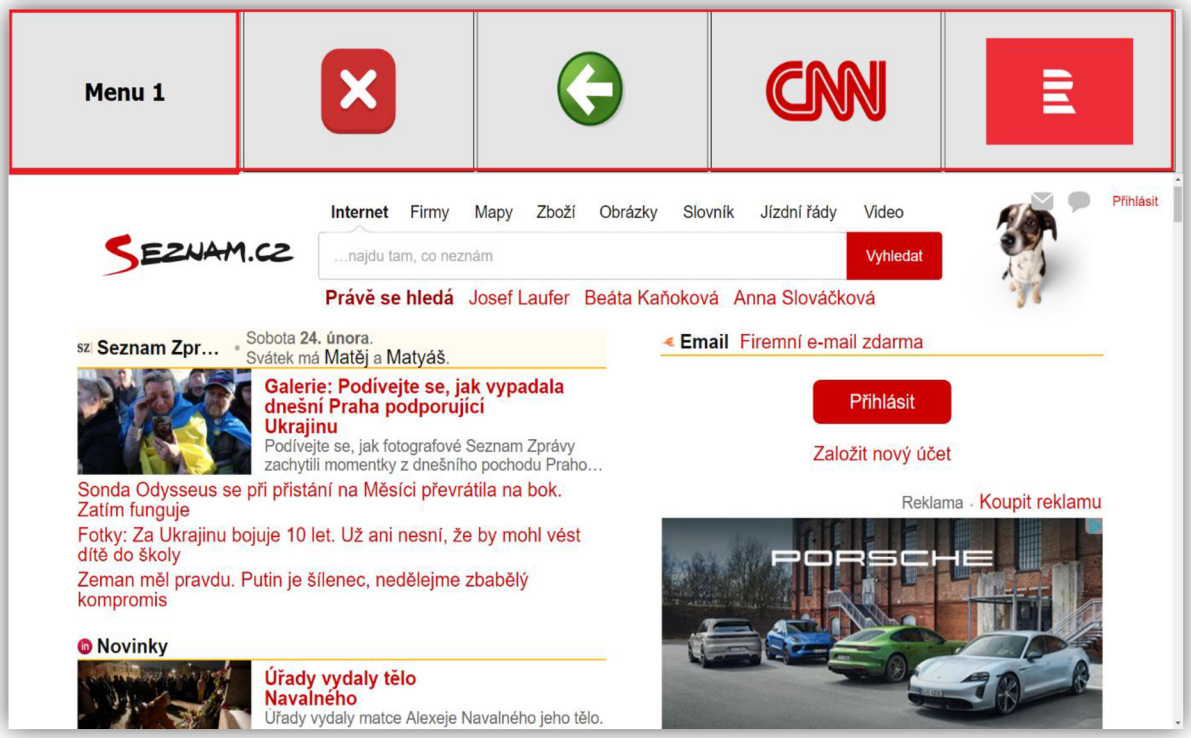
Proces převodu vytvoří jednu novou složku, ve které je soubor typu .exe umístěn. V tomto případě je soubor sweb.exe. Na konci je nutné nechat soubor sweb.exe do adresáře sweb, protože je tam hlavní spuštěný program a vytvořit zástupce aplikace do hlavního rozhraní Windows, ve kterém by uživatelé mohli přímo spustit kliknutím na aplikační ikonu.



Obrázek 6.3: Zástupce aplikace sweb z rozhraní uživatele

6.3 Použití webového prohlížeče pro seniory

V této kapitole jsou stručně představeny funkce a grafické rozhraní webového prohlížeče pro seniory, který byl vytvořen pro předkládanou diplomovou práci. Cílem vytvoření webového prohlížeče je přizpůsobení pro seniory ve věkové skupině 90 let a více. Proto je webový prohlížeč jednoduše ovladatelný. Celá aplikace je napsána v programovacím jazyce Python s knihovnou PyQt5 a další.



Obrázek 6.4: Menu 1 a webová stránka www.seznam.cz

Jako výchozí webová stránka po zatížení aplikace byla zvolena webová stránka www.seznam.cz podporující mnoho mezinárodních jazyků a obsahující vždy aktuální zprávy. Potom je obsah webové stránky také zvětšen, aby byl vhodný pro staršího uživatele. To zvyšuje použitelnost a čitelnost webové stránky. Ukázka zobrazení webové stránky www.seznam.cz je zobrazena v obrázku 6.4.

Obrázek 6.5: Menu 1 a webová stránka www.seznam.cz v chytrém telefonu

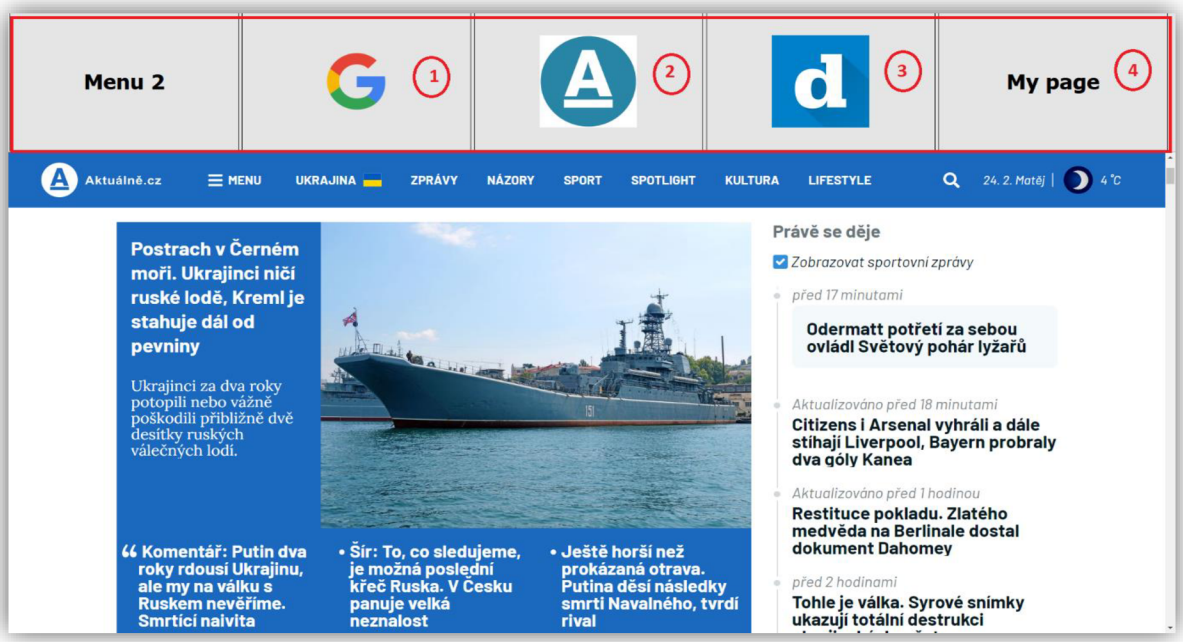
Webový prohlížeč pro seniory taky umožňuje zobrazení webové stránky v chytrém telefonu. Tato funkce uživateli poskytuje více způsobů zobrazení, které je vhodné. Rozhraní menu 1 a obsah webové stránky www.seznam.cz v chytrém telefonu je představeno v obrázku 6.5.

Aplikace má celkem dvě hlavní menu, každé z nich obsahuje 4 tlačítka. Dvě menu i všechna tlačítka jsou navržena s velkou a flexibilní velikostí, která je vypočítána podle hlavního okna monitoru uživatele. Obsahuje velké ikony nebo texty, které poskytují objasnění jejich jednoduché funkce.

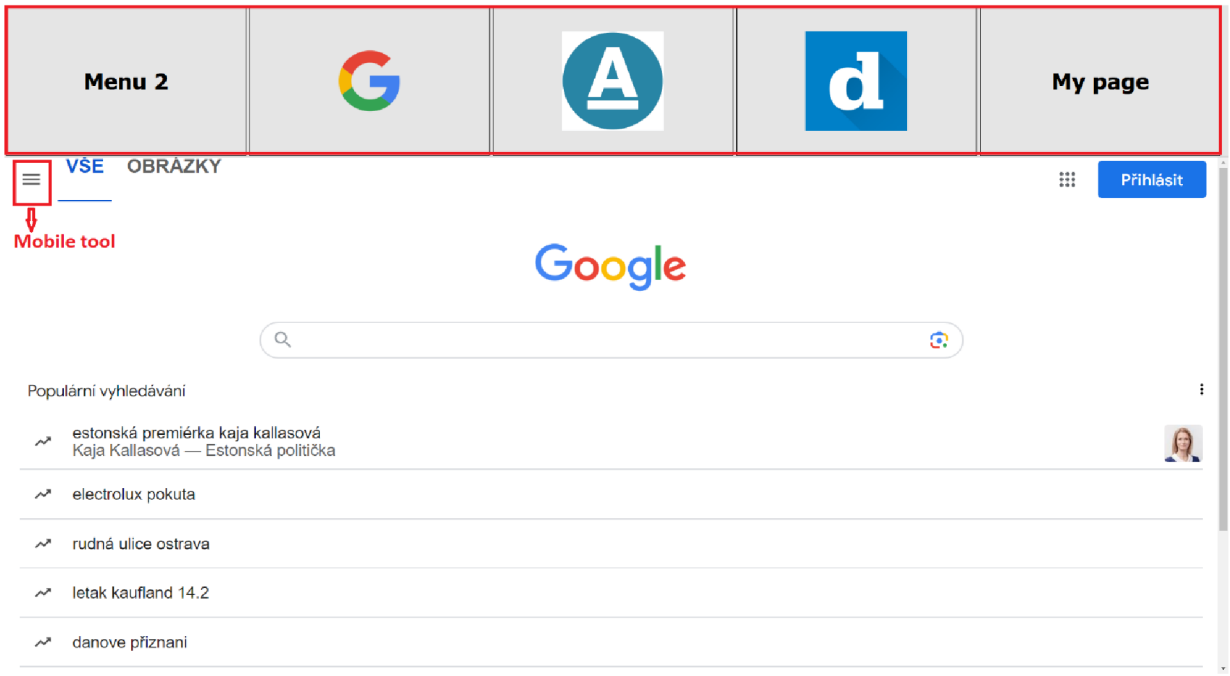
Tlačítka jsou integrována se svou vlastní navigací po kliknutí uživatele, jako jsou zobrazení webové stránky pro čtení zprávy, funkce připojení do webové stránky www.google.com pro doplnění dotazu, funkce zpět, funkce ukončení aplikace a dokonce zadávací textové pole, když je stránka s novinkami mimo seznam.

Menu 1 je první menu, zahrnující následující funkce, jako jsou dokončení aplikace, funkce zpět do předchozí webové stránky a zobrazení některé webové stránky s novinkami. V menu 1

jsou zvoleny novinky www.edition.cnn.com a www.irozhlas.cz. Po kliknutí na první menu se zobrazí druhé menu.

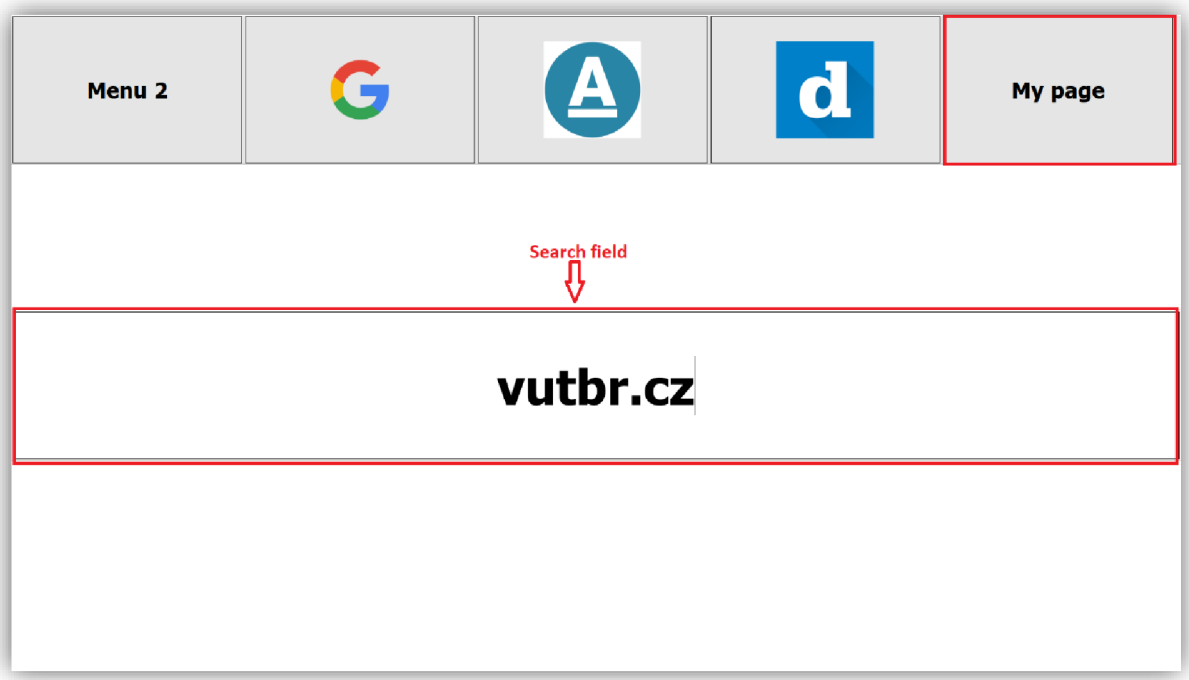


Obrázek 6.6: Menu 2

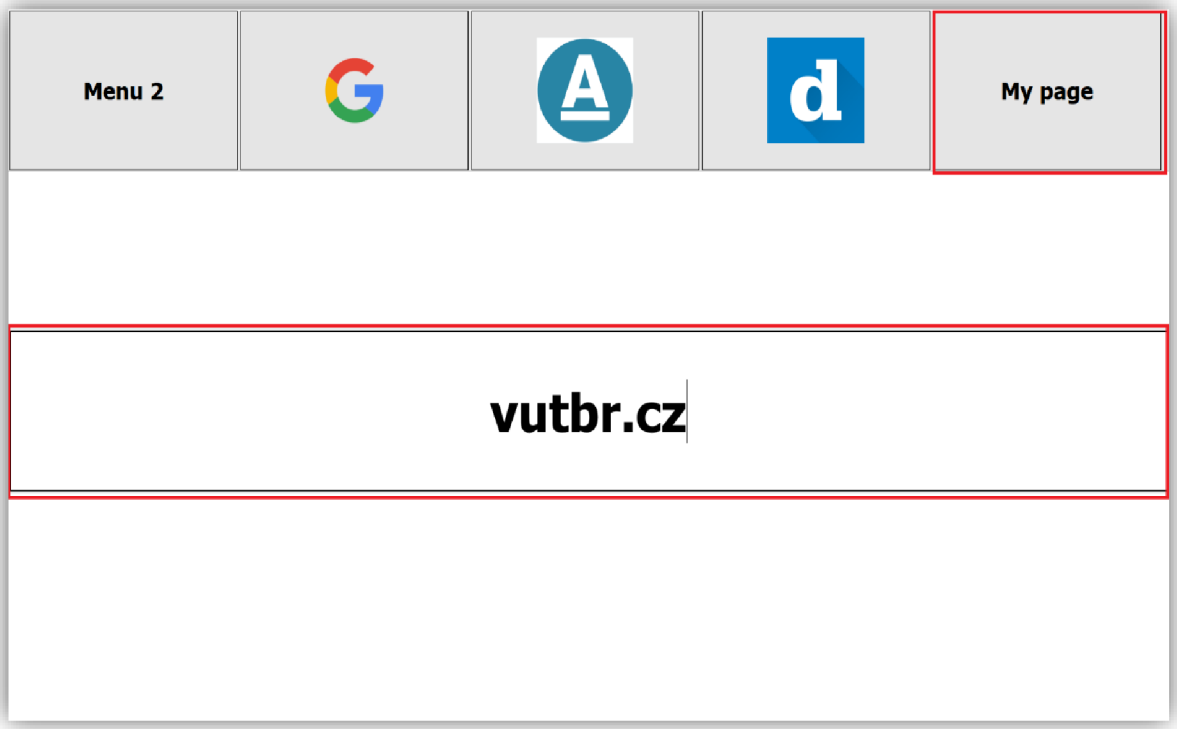


Obrázek 6.7: Menu 2 v chytrém telefonu

Na druhém menu je zobrazení webové stránky www.google.com pro doplnění dotazu, zobrazení některých webových stránek s novinkami a dokonce zadávací textové pole, jako je zobrazeno v obrázku 6.6 a obrázku 6.7. V menu 2 jsou zvoleny www.aktualne.cz a www.denik.cz pro čtení novinek. Při kliknutí na zadání vlastní webové stránky URL se zobrazí pouze zadávací textové pole uprostřed aplikace (to zajišťuje, aby senioři nebyli příliš zmateni). Zadávací textové pole je zobrazeno v obrázku 6.8.

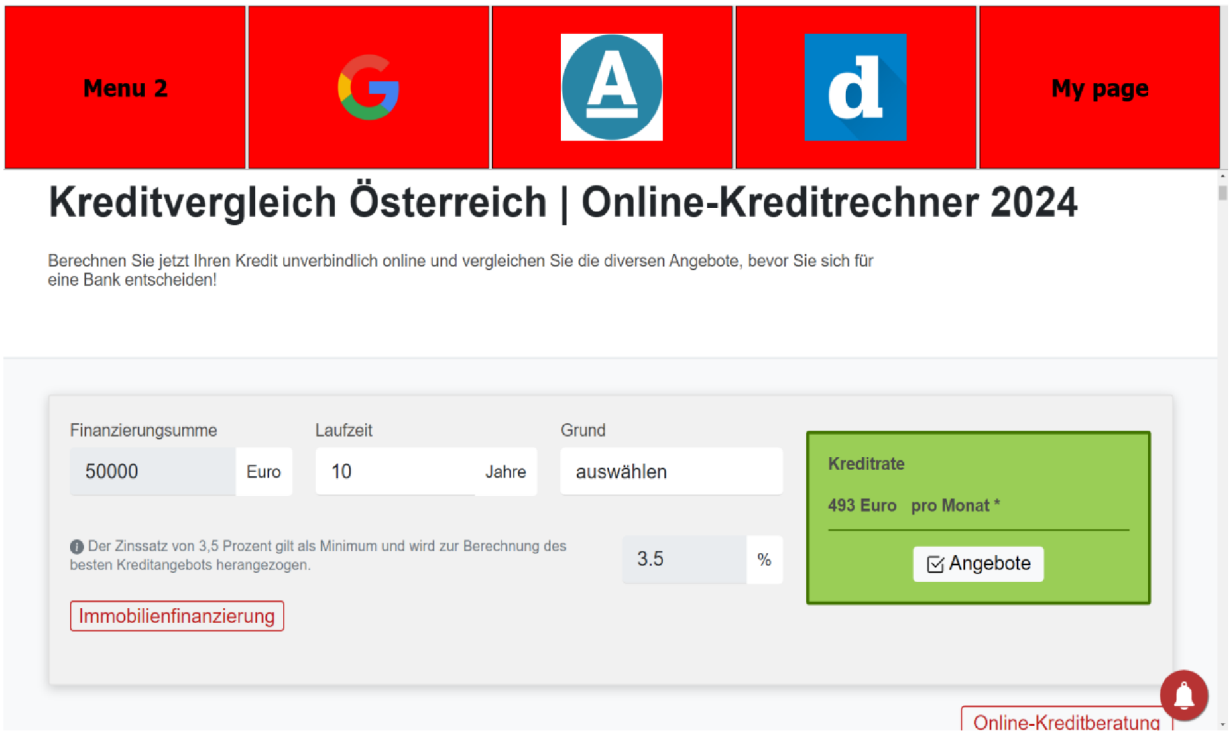


Obrázek 6.8: Zadávací textové pole URL

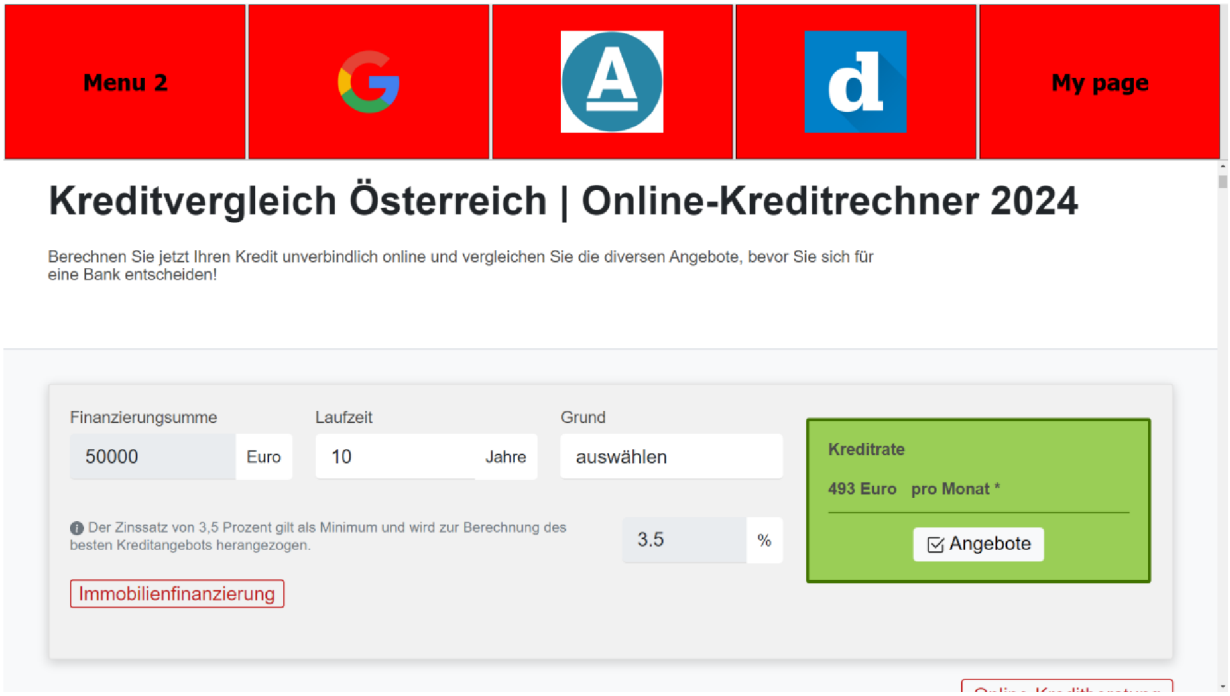


Obrázek 6.9: Zadávací textové pole URL v chytrém telefonu

Pro seniory je ještě nezbytné, aby webový prohlížeč měl ochranu proti podvodné stránce. Kdyby uživatelé zobrazili jakékoli podvodné stránky, které jsou uloženy v databázi podvodné stránky, všechna menu i tlačítka změní původní barvu na červenou barvu a zároveň se přehraje zvuk upozornění „Pozor, tato webová stránka není bezpečná" v české verzi. Obrázek 6.10 a Obrázek 6.11 zobrazují rozhraní aplikace, v případě, že zobrazí podvodnou stránku.



Obrázek 6.10: Webový prohlížeč při připojení do podvodné stránky



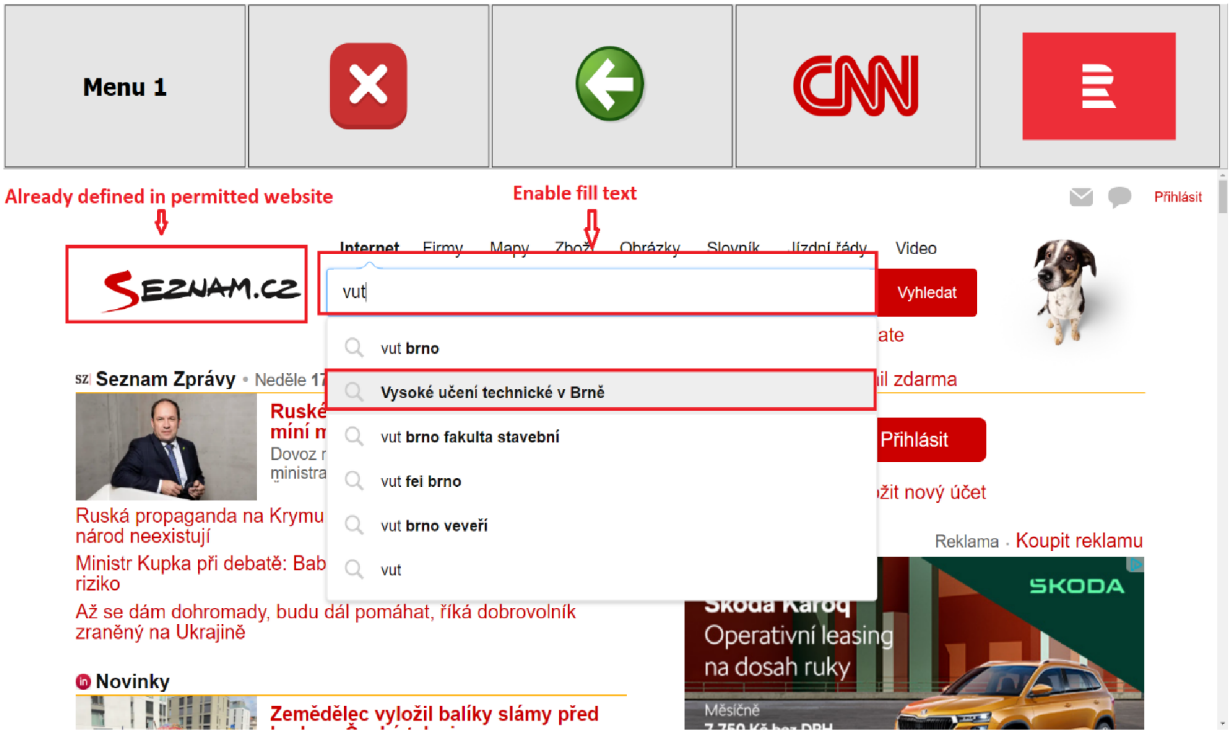
Obrázek 6.11: Webový prohlížeč při připojení do podvodné stránky v chytrém telefonu

Barva je obnovena na původní hodnotu, pouze pokud uživatel zobrazí jinou webovou stránku, která není v databázi podvodné stránky. Protože webový prohlížeč vždy zkontroluje adresu webové stránky po každém kliknutí na odkaz, zda je nebo není v databázi podvodné stránky. Aby bylo zajištěno, že není databáze podvodné stránky zastaralá, je aktualizována každé dva týdny od poslední aktualizace při spuštění webového prohlížeče. Kromě předchozí funkce má webový prohlížeč také přehrání zvuku, když uživatelé najedou na jakékoliv tlačítko déle než 5 sekund. To zlepšuje jejich uživatelský zážitek.

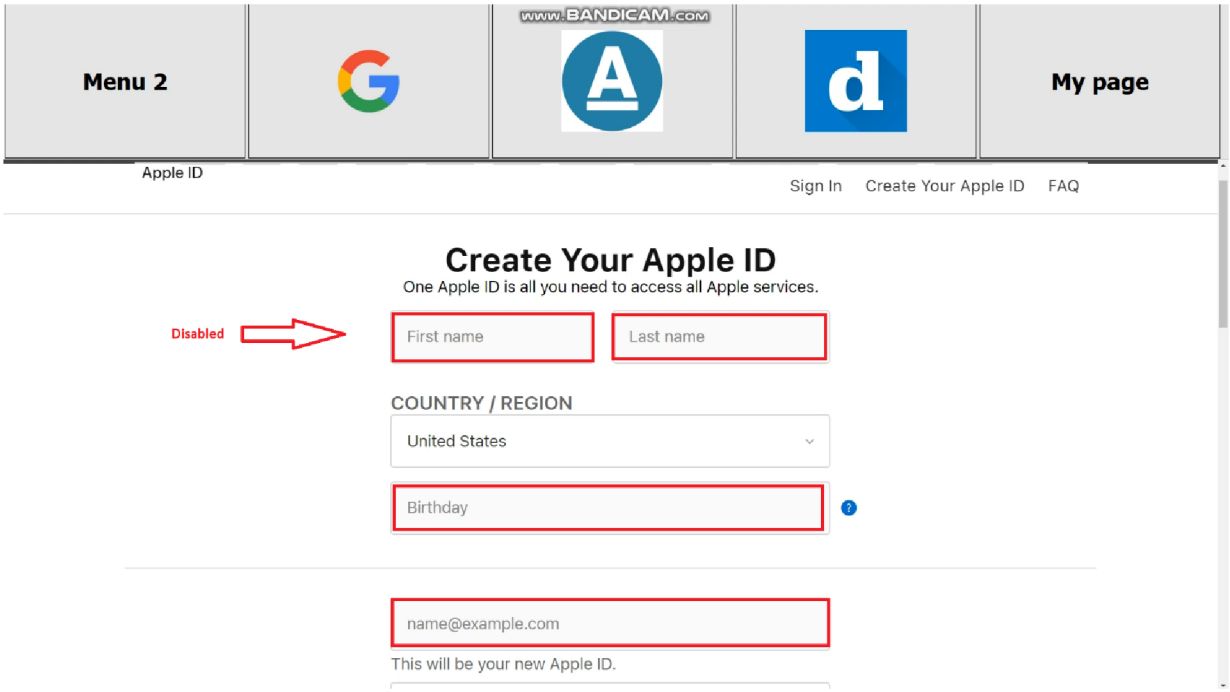
Výpis 6.8: Zaznamenání zobrazení do textového souboru log

```
2023-10-27 23:08:45 : WEBBROWSER-CRITICAL -> main <security> : Application
did not work
2023-10-27 23:09:39 : WEBBROWSER-INFORMATIONAL -> main <security> :
Connection to https://ct24.ceskatelevize.cz
2023-10-28 19:23:10 : WEBBROWSER-NOTICE -> main <security> : Connection to
Phishing server https://symposiumhotels.com
2023-11-05 19:22:02 : WEBBROWSER-NOTICE -> main <security> : Connection to
Phishing server https://alliedpayments.ca
2023-11-05 19:22:20 : WEBBROWSER-NOTICE -> main <security> : Connection to
Phishing server https://suntrust-onlinebanking.blogspot.com
2024-02-24 23:53:50 : WEBBROWSER-INFORMATIONAL -> main <security> :
Connection to https://www.brandbucket.com/names
2024-02-24 23:53:56 : WEBBROWSER-NOTICE -> main <security> : Connection to
Phishing server https://buzzdept.com
2024-02-24 23:53:57 : WEBBROWSER-INFORMATIONAL -> main <security> :
Connection to https://www.brandbucket.com/names/buzzdept?source=ext
2024-02-24 23:54:50 : WEBBROWSER-INFORMATIONAL -> main <security> :
Connection to https://www.seznam.cz/
2024-02-24 23:54:54 : WEBBROWSER-NOTICE -> main <security> : Connection to
Phishing server https://www.finanz.at/konto/
2024-02-24 23:55:43 : WEBBROWSER-INFORMATIONAL -> main <security> :
Connection to https://www.seznam.cz/
2024-02-24 23:55:56 : WEBBROWSER-NOTICE -> main <security> : Connection to
Phishing server https://www.finanz.at/#google_vignette
2024-02-24 23:56:00 : WEBBROWSER-NOTICE -> main <security> : Connection to
Phishing server https://www.finanz.at/trading/
2024-02-24 23:56:09 : WEBBROWSER-NOTICE -> main <security> : Connection to
Phishing server https://www.finanz.at/konto/
2024-03-01 20:57:58 : WEBBROWSER-NOTICE -> main <security> : Connection to
Phishing server https://bestveganmakeup.com/contact/
2024-03-01 21:31:32 : WEBBROWSER-INFORMATIONAL -> main <security> :
Connection to https://www.seznam.cz/
2024-03-01 21:33:11 : WEBBROWSER-NOTICE -> main <security> : Connection to
Phishing server https://bestveganmakeup.com/contact/
2024-03-01 21:33:27 : WEBBROWSER-INFORMATIONAL -> main <security> :
Connection to https://www.google.com/
2024-03-01 21:33:36 : WEBBROWSER-INFORMATIONAL -> main <security> :
Connection to https://www.google.com/search?q=seznam
2024-03-01 21:33:43 : WEBBROWSER-INFORMATIONAL -> main <security> :
Connection to https://www.seznam.cz/
```

Každá činnost webové stránky je zaznamenána do záznamu činnosti, který je používán pro vyhodnocení bezpečnostních rizik, aby pravidelně zlepšoval bezpečnost na prohlížeči. Každý záznam je uložen ve strukturovaném textu s více úrovněmi. Čím nižší úrovně, tím vyšší nebezpečí. Pokud by nefungoval prohlížeč, je to také zaznamenáno do textového souboru log. Ukázka souboru log je uveden ve výpisu 6.8.



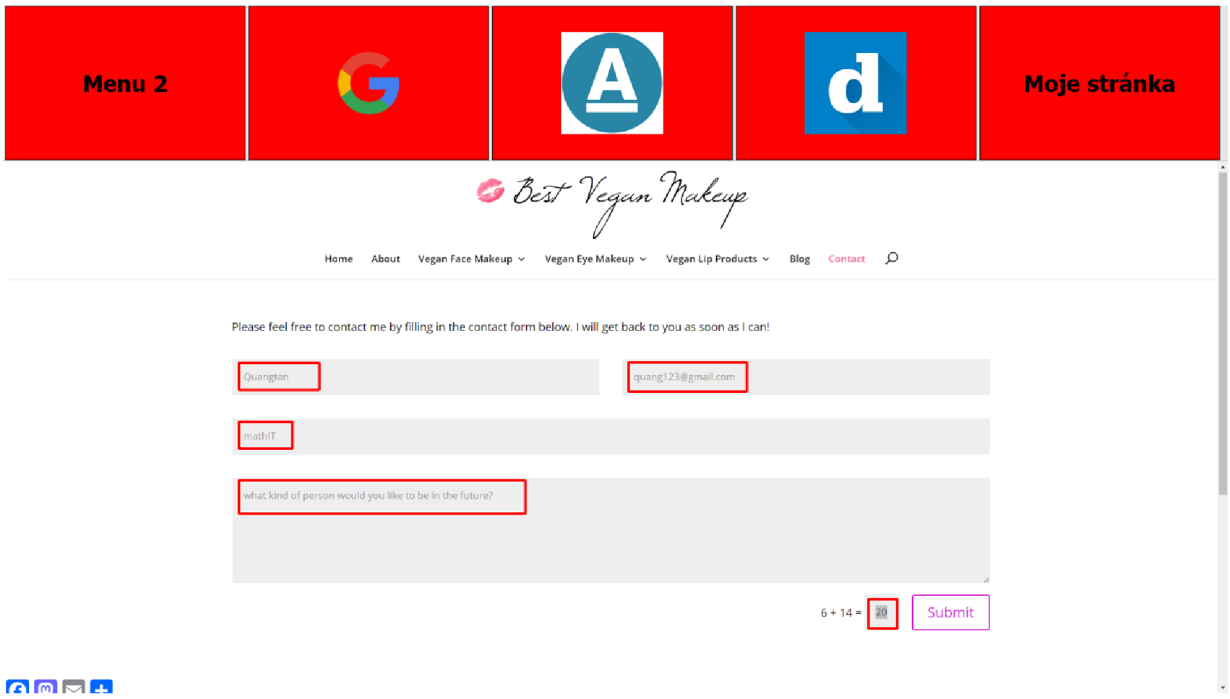
Obrázek 6.12: Povolení doplnění textu do textového pole



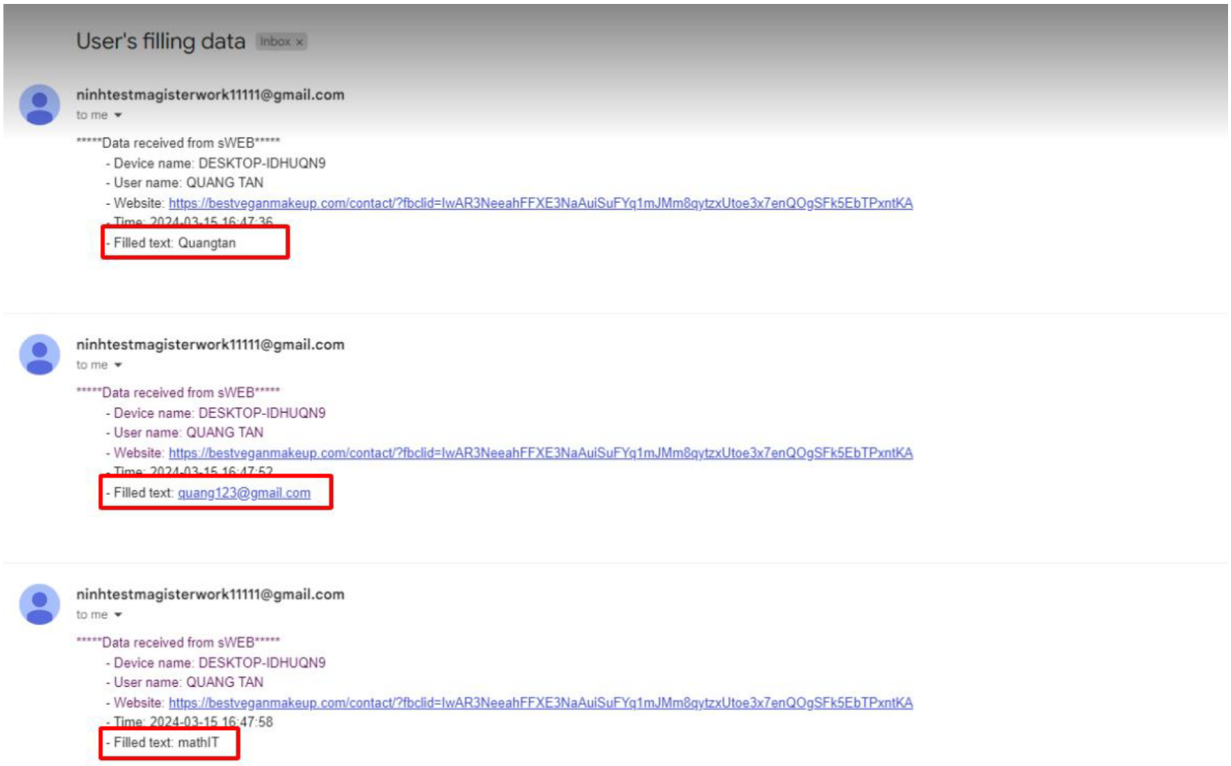
Obrázek 6.13: Zákaz doplnění textu do textového pole

Navíc poskytuje webový prohlížeč pro seniory metodu pro povolení a zakázaní vyplňování textu do vyhledávacího nebo textového formuláře z webového obsahu. Tato metoda zakazuje uživatelům neúmyslné zadávání citlivých údajů, jako jsou hesla, osobní identifikační čísla, e-mailová informace, bankovní číslo. Povolené webové stránky jsou definovány v textovém souboru a mohou být pravidelně aktualizovány podle uživatelského požadavku. Jeden příklad je uveden v obrázku 6.12 a obrázku 6.13. Stránka seznam.cz je definována v souboru povolené webové stránky, aby uživatel mohl doplnit text do pole pro zadávání textu. Jinak není stránka appleid.apple.com definována, uživatel může otevřít pole pro zadávání textu, ale doplnění textu do pole je zakázáno.

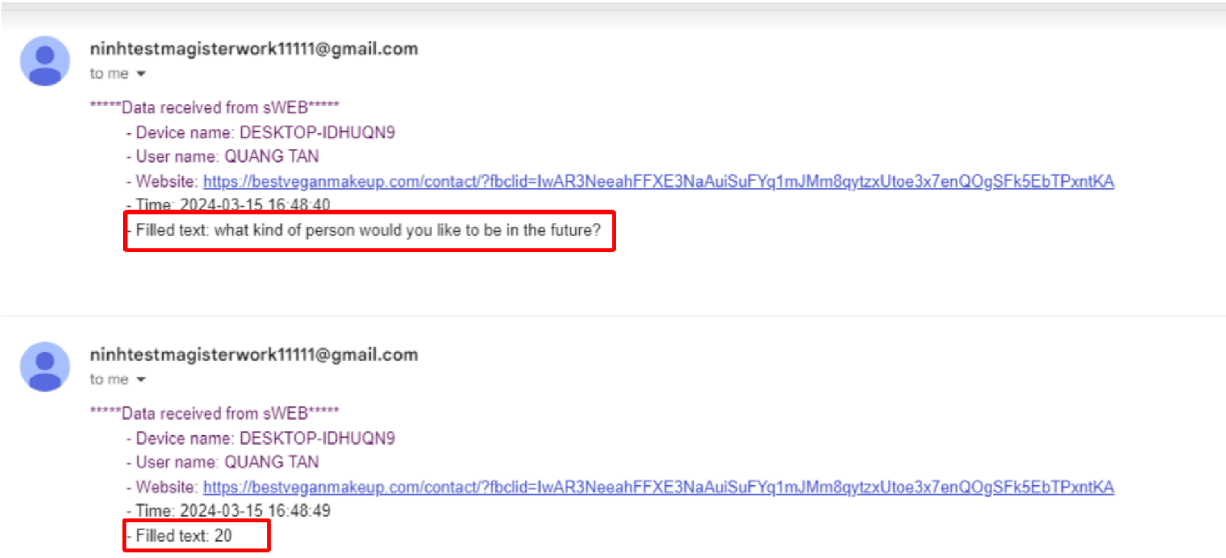
Na konci jsou zaznamenávány uživatelské informace do podvodné stránky. Jedná se o zájem ochrany citlivých informací zejména ve scénářích, kdy by uživatelé mohli neúmyslně ignorovat varování při připojení do podvodné webové stránky. Cílem této funkce není zasahovat do soukromí uživatele nebo získat soukromé a citlivé uživatelské informace, ale spíše funguje jako pojistka pro zmírnění škod v případě ohrožení osobních údajů. Následující informace byla získána při testování třetí osoby od uživatele a je detailně představena v následujícím obrázku.



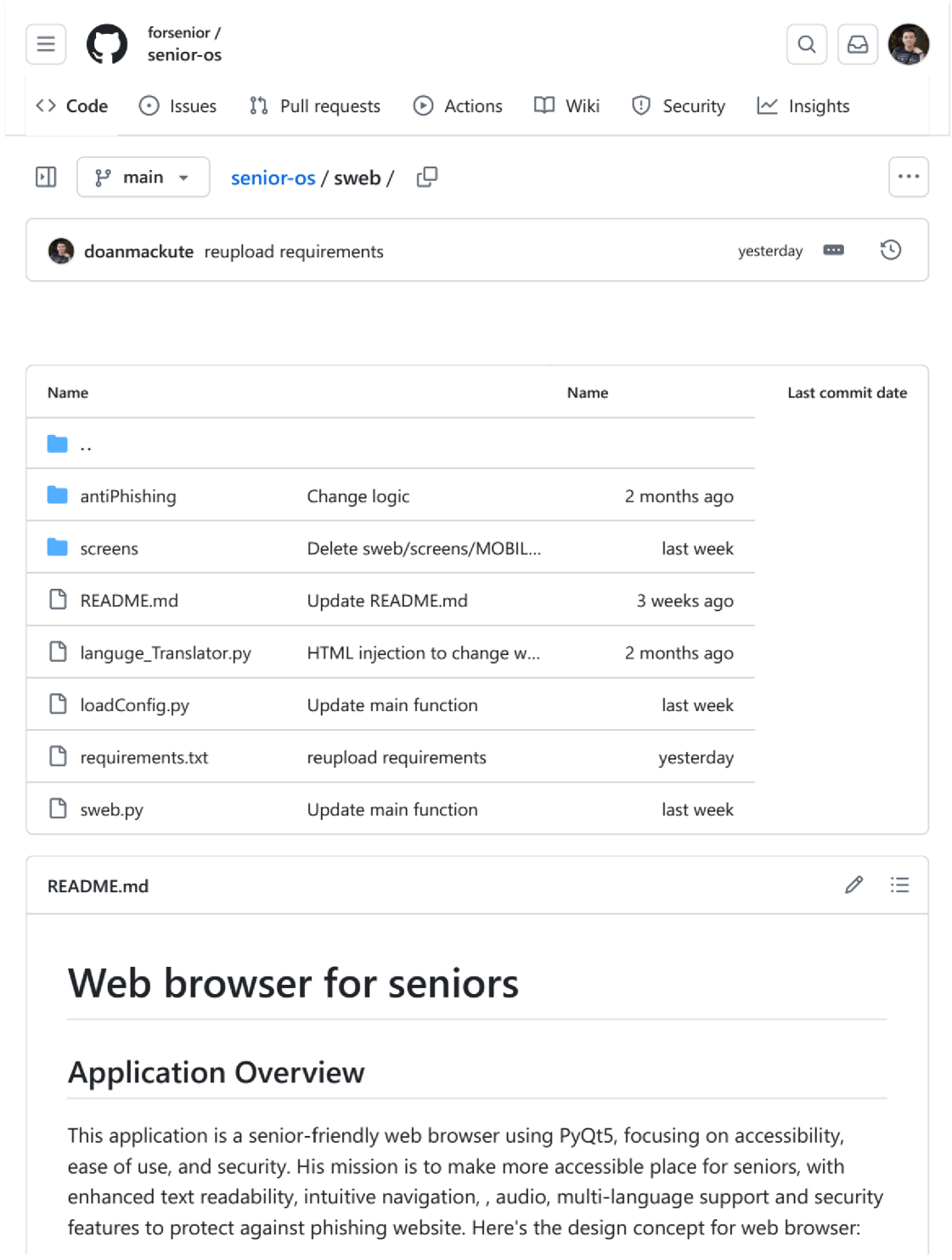
Obrázek 6.14: Doplnění informace do podvodné stránky



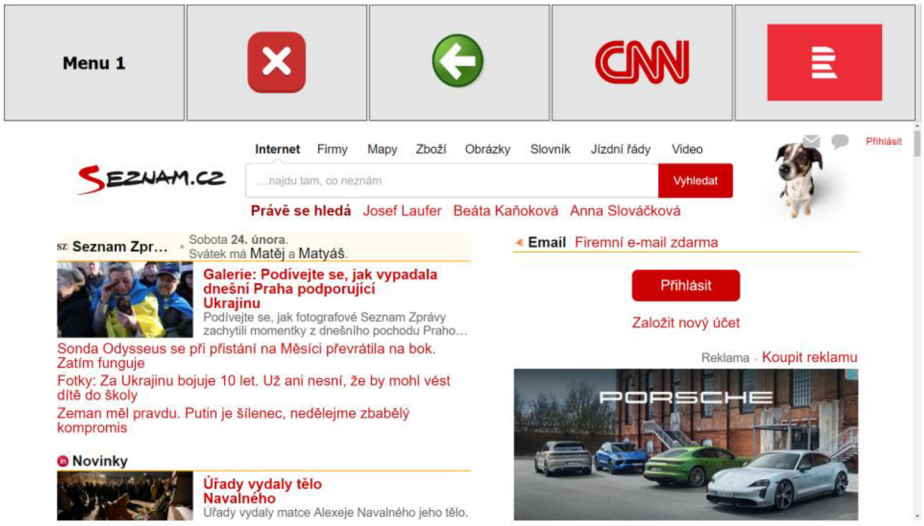
Obrázek 6.15: Získaná informace u opatrovníka



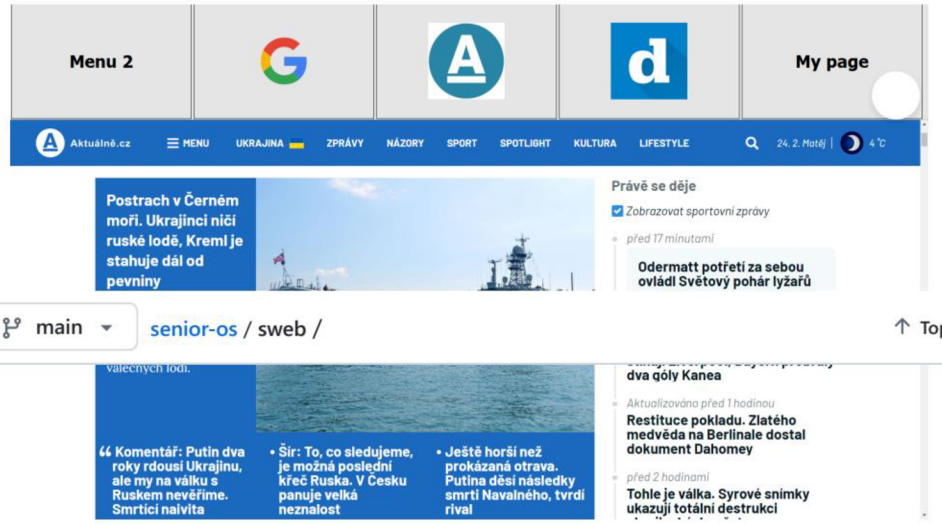
Obrázek 6.16: Další získaná informace u opatrovníka


forsenior / senior-os
Code
Issues
Pull requests
Actions
Wiki
Security
Insights
main
senior-os / sweb /
doanmackute reupload requirements
yesterday
Name
Name
Last commit date
..
antiPhishing Change logic 2 months ago
screens Delete sweb/screens/MOBIL... last week
README.md Update README.md 3 weeks ago
languge_Translator.py HTML injection to change w... 2 months ago
loadConfig.py Update main function last week
requirements.txt reupload requirements yesterday
sweb.py Update main function last week
README.md
Web browser for seniors
Application Overview
This application is a senior-friendly web browser using PyQt5, focusing on accessibility, ease of use, and security. His mission is to make more accessible place for seniors, with enhanced text readability, intuitive navigation, , audio, multi-language support and security features to protect against phishing website. Here's the design concept for web browser:

- Menu 1

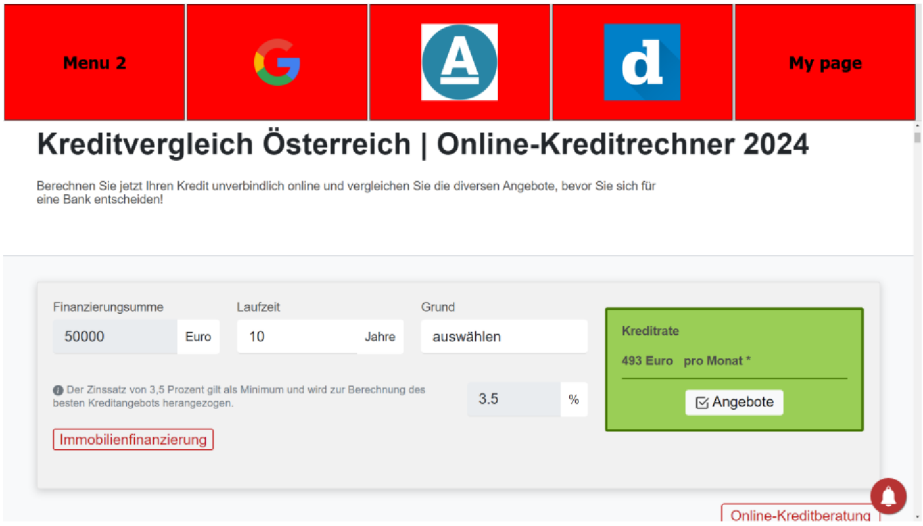


- Menu 2



main senior-os / sweb / Top

- Warning when connect to phishing webpage these are installed from phishing database



Our Design

- We believe the Internet should be accessible to everyone, regardless of age. Our browser empowers seniors with user-friendly tools, making the online world an enjoyable space to explore.
- Věříme, že by Internet měl být přístupný všem bez ohledu na věk. Náš prohlížeč poskytuje seniorům uživatelské přívětivé nástroje, díky nimž je online svět příjemným prostorem k objevování.
- Wir glauben, dass das Internet für jeden zugänglich sein sollte, unabhängig vom Alter. Unser Browser stellt Senioren benutzerfreundliche Tools zur Verfügung und macht die Online-Welt zu einem angenehmen Ort zum Erkunden.

Key Features

- Clear and Large Buttons: Easy navigation with large for essential functions.
- Readable Text: Enhanced text size not only in the buttons but also in the content of webpage.
- Audible support: Sound support for button interactions whenever users hover on the buttons longer than 5s.
- Support multiple languages: Available in English, Czech, and Deutsch.
- Security Against Phishing Webpage: Identify and alert users about potential phishing websites.
- Activity Logging: Logs browsing activity to a text file for security purposes.

Installation

!!!Ensure you have Python3 or pip installed on your system. Follow these steps to set up Web Browser in FEDORA operating system:

```
# Clone the project repository
git clone https://github.com/forsenior/senior-os

# Navigate to the project directory
cd sweb

# Install required Python packages with dnf if using Fedora
sudo dnf install python3
sudo dnf install python3-qt5
sudo dnf install python3-qt5-webengine
sudo dnf install python3-pygame
pip3 install screeninfo
pip3 install yagmail

# Run the browser
python3 sweb.py
```

Follow these steps to set up Web Browser in WINDOWS operating system:

```
# Clone the project repository
git clone https://github.com/forsenior/senior-os

# Navigate to the project directory
cd sweb

# Install required Python packages in command prompt
pip install PyQt5
pip install PyQtWebEngine
pip install screeninfo
pip install PyQt5Designer
pip install pygame
pip install requests
pip install yagmail

# Run the browser from terminal
python sweb.py [Your visited website]
```

Usage

ZÁVĚR

Předkládaná diplomová práce s názvem *Webový prohlížeč pro seniory* se zabývá implementací základního webového prohlížeče, který je přizpůsoben pro seniory ve věkové skupině 90 let a více. Implementace prohlížeče je lehce ovladatelná a slouží pro usnadnění každodenní práce na počítači.

Diplomová práce se skládá ze dvou částí – teoretické a praktické.

V teoretické části práce jsou detailně popsány typy podvodných útoků - phishing, smishing a vishing s jejich charakteristickým rysy. Jsou zde uvedeny i možné způsoby podvodných útoků na seniory a dále je popsán způsob detekce podvodných stránek. Dále je uveden přehled použitých nástrojů ve webovém prohlížeči, jako jsou grafická knihovna, knihovna pro podporu zvuku, knihovna pro zpracování požadavků a odpovědi HTTP, knihovna pro interakce se souborem, knihovna pro vytvoření spojení se serverem SMTP a systémová knihovna, včetně jejich tříd.

Praktická část práce se věnuje naprogramování vlastního webového prohlížeče v jazyce Python, který je přizpůsoben pro seniory ve věkové skupině 90 let a více. Umožňuje způsob zobrazení webové stránky v počítači i chytrém telefonu. Prohlížeč obsahuje funkce vícejazyčného překladu aplikace, zvukové asistence, ochranu proti podvodné stránce, přehrání výstražného zvuku i změnu barvy tlačítka. Ta se mění na červenou barvu, pokud uživatel zobrazí podvodnou stránku - phishing, která je uložena v databázi podvodných stránek.

Prohlížeč pomocí úprav HTML provádí zvětšení velikosti textu pro jeho lepší čtení seniorem.

Zabezpečení uživatele je rozděleno do tří kategorií. V první kategorii je povoleno doplnit informace do formuláře ve webovém obsahu, jehož webová adresa je definována v souboru povolené webové stránky.

Druhá kategorie se zaměřuje na povolení webové stránky. Pokud by nebyla webová stránka v souboru povolené stránky, doplnění do textového pole webového obsahu by bylo zakázáno. V poslední kategorii zabezpečení se jedná o odeslání doplněné informace od uživatele k opatrovníkovi. K tomu dojde, jestliže se senior připojí do podvodné stránky, neúmyslně ignoruje varování od webového prohlížeče a doplní své informace do textového pole.

Zde je nutno zdůraznit, že cílem této funkce není zasahovat do soukromí uživatele nebo získat soukromé a citlivé uživatelské informace, ale spíše fungovat jako pojistka pro zmírnění škod v případě ohrožení osobních údajů.

Databáze podvodných stránek je automaticky aktualizována každé dva týdny, což zajistí, aby byl prohlížeč vždy aktuální a obsahoval i nejnovější známé podvodné adresy URL, což zvyšuje schopnost účinně chránit uživatele.

Mimo to jsou texty a ikony na každém tlačítku zobrazeny v dostatečné velikosti, aby zlepšovaly uživatelský zážitek. Na konci jsou všechny přístupy k webové stránce zaznamenány do záznamu činnosti pro vyhodnocení bezpečnostních rizik.

Výsledek zhotoveného programového kódu webového prohlížeče je dostupný na webové stránce GitHub. Jeho odkaz je zde: https://github.com/forsenior/senior-os/tree/main/sweb.

LITERATURA

[1] *Phishing: Detection, Analysis And Prevention.* Ms Amrita Mitra [cit. 2023-11-23]

[2] *Phishing Exposed.* Lance James [cit. 2023-11-23]

[3] *What is Whaling Phishing?* [online]. Kyle Chin [cit. 2023-11-23]. Dostupné z https://www.aztechit.co.uk/blog/what-is-whaling-phishing

[4] *Whaling attack (whaling phishing)* [online]. Ben Lutkevich [cit. 2023-11-23]. Dostupné z https://www.techtarget.com/searchsecurity/definition/whaling

[5] *How Spear Phishing (Targeted Scam) Detection Works* [online]. Saul Harvey DVM [cit. 2023-11-23]. Dostupné z https://en.naneedigital.com/article/how_spear_phishing_targeted_scam_detection_works

[6] *19 Most Common Types of Phishing Attacks in 2023* [online]. Kyle Chin [cit. 2023-11-23]. Dostupné z https://www.upguard.com/blog/types-of-phishing-attacks

[7] *ÚTOKY PŘES E-MAILY, SMS NEBO TELEFON (PHISHING)* [online]. Bezpecnejsi ostrava [cit. 2023-11-23]. Dostupné z https://bezpecnejsi.ostrava.cz/situace/internet/phishing-utoky-pres-zpravy/

[8] *What Is Voice Phishing? A Vishing Definition and Meaning* [online]. Savvy Security [cit. 2023-11-23]. Dostupné z https://cheapsslsecurity.com/blog/what-is-voice-phishing-vishing-definition-meaning/

[9] *5 Cyber Scams Targeting Seniors* [online]. Diane Amato [cit. 2023-11-23]. Dostupné z https://www.rbcroyalbank.com/en-ca/my-money-matters/money-academy/cyber-security/understanding-cyber-security/5-cyber-scams-targeting-seniors/

[10] *How this 77-year-old widow lost $661,000 in a common tech scam: 'I realized I had been defrauded of everything'* [online]. Greg Iacurci [cit. 2023-11-23]. Dostupné z https://www.cnbc.com/2023/10/08/how-one-retired-woman-lost-her-life-savings-in-a-common-elder-fraud-scheme.html

[11] *IT'S PHISHING GRANDMA, NOT FISHING: WEB AND TECH GUIDE FOR SENIORS.* Maria T [cit. 2023-11-23]

[12] *Protect yourself from phishing* [online]. Microsoft [cit. 2023-11-23]. Dostupné z https://support.microsoft.com/en-us/windows/protect-yourself-from-phishing-0c7ea947-ba98-3bd9-7184-430e1f860a44

[13] *Create GUI Applications with Python & Qt5 (PyQt5 Edition): The hands-on guide to making apps with Python.* Dr Martin Fitzpatrik [cit. 2023-11-23]

[14] *PyQt vs. Tkinter — Which Should You Choose for Your Next GUI Project?* [online]. Martin Fitzpatrick [cit. 2023-11-23]. Dostupné z https://www.pythonguis.com/faq/pyqt-vs-tkinter/

[15] *PyqtWebEngine* [online]. Riverbank computing [cit. 2023-11-23]. Dostupné z https://pypi.org/project/PyQtWebEngine/

[16] *QWebEngineView* [online]. The Qt company [cit. 2023-11-23]. Dostupné z https://doc.qt.io/qtforpython-5/PySide2/QtWebEngineWidgets/QWebEngineView.html

[17] *QWebEnginePage* [online]. The Qt company [cit. 2023-11-23]. Dostupné z https://doc.qt.io/qtforpython-5/PySide2/QtWebEngineWidgets/QWebEnginePage.html

[18] *QWidget* [online]. The Qt company [cit. 2023-11-23]. Dostupné z https://doc.qt.io/qtforpython-5/PySide2/QtWidgets/QWidget.html

[19] *QApplication* [online]. The Qt company [cit. 2023-11-23]. Dostupné z https://doc.qt.io/qtforpython-5/PySide2/QtWidgets/QApplication.html

[20] *QPushButton* [online]. The Qt company [cit. 2023-11-23]. Dostupné z https://doc.qt.io/qtforpython-5/PySide2/QtWidgets/QPushButton.html

[21] *QLineEdit* [online]. The Qt company [cit. 2023-11-23]. Dostupné z https://doc.qt.io/qtforpython-5/PySide2/QtWidgets/QLineEdit.html

[22] *QtGui* [online]. Riverbank computing [cit. 2023-11-23]. Dostupné z https://docs.huihoo.com/pyqt/PyQt5/QtGui.html

[23] *QtCore* [online]. Riverbank computing [cit. 2023-11-23]. Dostupné z https://docs.huihoo.com/pyqt/PyQt5/QtCore.html

[24] *Python PyQt5.QtCore.pyqtSignal() Examples* [online]. Program creek [cit. 2023-11-23]. Dostupné z https://www.programcreek.com/python/example/99609/PyQt5.QtCore.pyqtSignal

[25] *Pygame* [online]. Pypi [cit. 2023-11-23]. Dostupné z https://pypi.org/project/pygame/

[26] *Requests* [online]. Pypi [cit. 2023-11-23]. Dostupné z https://pypi.org/project/requests/

[27] *Os* [online]. Python Software Foundation [cit. 2023-11-23]. Dostupné z https://docs.python.org/3/library/os.html

[28] *Sys — System-specific parameters and functions* [online]. Python Software Foundation [cit. 2023-11-23]. Dostupné z https://docs.python.org/3/library/sys.html

[29] *Time — Time access and conversions* [online]. Python Software Foundation [cit. 2023-11-23]. Dostupné z https://docs.python.org/3/library/time.html

[30] *Json — JSON encoder and decoder* [online]. Python Software Foundation [cit. 2023-11-23]. Dostupné z https://docs.python.org/3/library/json.html

[31] *Tarfile — Read and write tar archive files* [online]. Python Software Foundation [cit. 2023-11-23]. Dostupné z https://docs.python.org/3/library/tarfile.html

[32] *Phishing vs Spear Phishing: Phishing and Spear Phishing Examples* [online]. Tessian [cit. 2023-11-23]. Dostupné z https://en.naneedigital.com/article/how_spear_phishing_targeted_scam_detection_works

[33] *Qt Style Sheets Examples* [online]. The Qt company [cit. 2023-11-23]. Dostupné z

https://doc.qt.io/qt-6/stylesheet-examples.html

[34] *Logging and Log Management: The Authoritative Guide to Understanding the Concepts Surrounding Logging and Log Management*. Anton Chuvakin Ph.D. Stony Brook University Stony Brook NY [cit. 2023-11-23]

[35] *QEvent* [online]. The Qt company [cit. 2024-04-15]. Dostupné z https://doc.qt.io/qtforpython-5/PySide2/QtCore/QEvent.html#

[36] *QObject class* [online]. The Qt company [cit. 2024-04-15]. Dostupné z https://doc.qt.io/qt-6/qobject.html

[37] *Qt for Beginners* [online]. The Qt company [cit. 2024-04-15]. Dostupné z https://wiki.qt.io/Qt_for_Beginners

[38] *QWebChannel* [online]. The Qt company [cit. 2024-04-15]. Dostupné z https://doc.qt.io/qtforpython-5/PySide2/QtWebChannel/QWebChannel.html

[39] *Request 2.31.0* [online]. Pypi.org [cit. 2024-04-15]. Dostupné z https://pypi.org/project/requests/

[40] *SMTP protocol client* [online]. python [cit. 2024-04-15]. Dostupné z https://docs.python.org/3/library/smtplib.html

[41] *Attacking Web Applications With Python: Exploiting Web Forms and Requests* [online]. srinivas [cit. 2024-04-15]. Dostupné z https://www.infosecinstitute.com/resources/secure-coding/attacking-web-applications-with-python-exploiting-web-forms-and-requests/

[42] *Understanding PyInstaller Hooks* [online]. pyinstaller [cit. 2024-04-15]. Dostupné z https://pyinstaller.org/en/stable/hooks.html

SEZNAM POUŽITÝCH ZKRATEK A ZNAČEK

GUI	Graphical User Interface
UI	User Interface
URL	Uniform Resource Locator
SMS	Short Message Service
BUT	Brno University of Technology
FEKT	Faculty of Electrical Engineering and Communication
UTF-8	Unicode Transformation Format
JSON	JavaScript Object Notation
HTML	HyperText Markup Language
CSS	Cascading Style Sheets
CLI	Command Line Interface
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure