SLOVENSKÁ TECHNICKÁ UNIVERZITA V BRATISLAVE
FAKULTA ELEKTROTECHNIKY A INFORMATIKY

ÚVOD DO POČÍTAČOVEJ BEZPEČNOSTI
ZADANIE Č.4 - DOCHÁDZKOVÝ SYSTÉM

Adrián Somor, Samuel Gibala, Matúš Kornhauser, Ľuboš Likó, Peter Barnas

1 Registrácia a prihlasovanie používateľov

1.1 Implementácia registrácie a prihlásenia používateľov

V systéme bola implementovaná registrácia nových používateľov pomocou používateľského mena, emailu a hesla a rovnako možnosť prihlásenia sa pre existujúcich používateľov. Po validácii vstupných údajov popísaných nižšie je implementované ukladanie a porovnávanie hesla pomocou *Bcrypt* funkcionality.

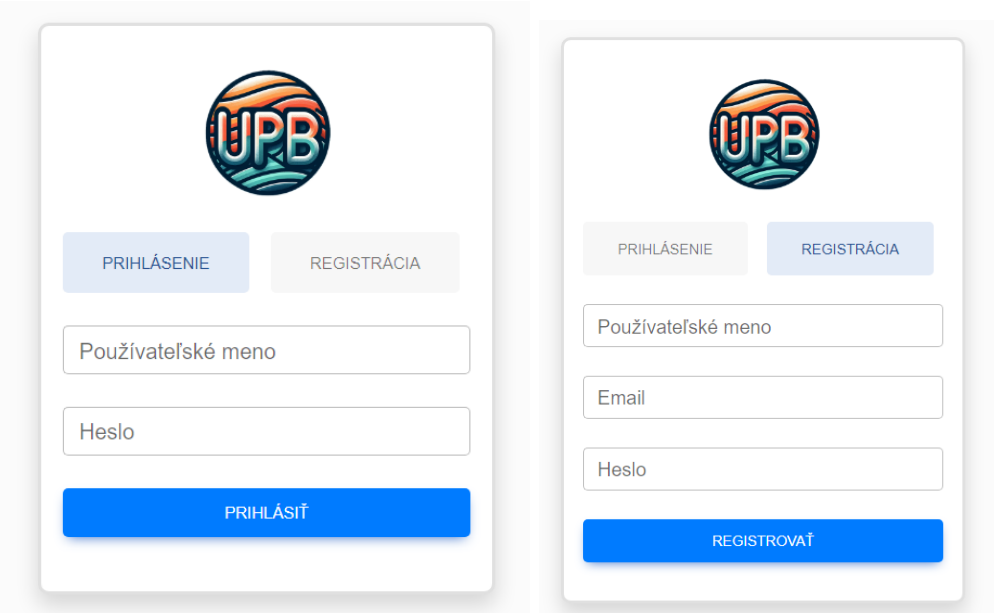
Bcrypt je kryptografická *hash* funkcia určená na *hashovanie* hesiel a ich bezpečné ukladanie na backende aplikácií spôsobom, ktorý je menej náchylný na kybernetické útoky založené na slovníkoch. Vytvorili ju v roku 1999 Niels Provos a David Mazières, pričom ako základ použili šifrovací algoritmus *Blowfish*. *Bcrypt* vykonáva komplexný proces *hashovania*, počas ktorého sa heslo používateľa transformuje na vlákno znakov pevnej dĺžky. Používa jednosmernú *hashovaciu* funkciu, čo znamená, že po *zahashovaní* hesla ho nemožno vrátiť do pôvodnej podoby. Zakaždým, keď sa používateľ prihlási do svojho účtu, *bcrypt* porovná novú hodnotu *hash* s verziou uloženou v pamäti systému, aby skontroloval, či sa heslá zhodujú. Namiesto jednoduchého *hashovania* daného hesla *bcrypt* pridáva náhodný údaj, nazývaný *salt* , aby vytvoril jedinečný *hash*, ktorý je takmer nemožné prelomiť automatickým odhadom počas útokov *hash* slovníkom a hrubou silou. *Bcrypt* vyniká medzi ostatnými *hashovacími* algoritmami aj tým, že používa *cost factor*. Pomocou neho môžete určiť počet iterácií hesla a kôl *hashovania*, ktoré sa majú vykonať, čím sa zvýši množstvo času, úsilia a výpočtových zdrojov potrebných na výpočet konečnej hodnoty *hash*. *Cost factor*. robí z *bcrypt* pomalý algoritmus, ktorý potrebuje podstatne viac času na vytvorenie *hash* kľúča, čím sa z neho stáva bezpečný nástroj na ukladanie hesiel.[1]

Pre potreby *hashovania* hesla pri ukladaní do databázy bola použitá funkcia *generate_password_hash(password, rounds=None, prefix=None)*. Táto funkcia generuje *hash* hesla pomocou *bcrypt*. Zadaním *rounds* sa nastaví parameter *log_rounds* funkcie *bcrypt.gensalt()*, ktorý určuje zložitosť *saltu*. Predvolená hodnota je 12. Zadaním prefixu sa nastaví parameter *prefix* funkcie *bcrypt.gensalt()*, ktorý určuje verziu algoritmu použitého na vytvorenie *hashu*.[2]

Na overenie hesla bola použitá funkcia *check_password_hash(pw_hash, password)*, ktorá testuje *hash* hesla oproti kandidátovi na heslo. Kandidát na heslo sa najprv *zahashuje* a následne sa v konštantnom čase porovná s existujúcim *hashom*. Návratová hodnota je buď *True*, alebo *False*.[2]

Zabezpečenie komunikácie medzi klientom a serverom pri prihlasovaní a registrácii

bolo zabezpečené asymetrickým šifrovaním. Po validácii vstupov na *frontende* je získaný verejný kľúč zo servera. Vložené údaje sú následne zašifrované získaným verejným kľúčom a poslané na server. Tento si po získaní odšifruje vlastným súkromným kľúčom prijaté údaje a ak prebehne validácia korektne, vykoná potrebné kroky.



Obr. 1: Obrazovka s kartami prihlásenia a registrácie

1.2 Šifrovanie

Webová aplikácia využíva šifrovanie AES (Advanced Encryption Standard). Pri registrácií alebo prihlásení sa pre používateľa vygeneruje jedinečný kľúč. Vygenerovaný kľúč sa pred poslaním na server zašifruje RSA verejným kľúčom servera. Server následne odšifruje tento kľúč a pri úspešnom vykonaní zaregistruje kľúč a inicializačný vektor pre daného používateľa a používateľ si uloží tieto údaje do cookies. Po tomto čase je používateľ odhlásený. Ak chce používateľ zapísať dochádzku alebo vytvoriť export, musí sa overiť kľúč používateľa. Tento kľúč je viazaný na session prihláseného používateľa, to znamená, že údaje môže upravovať len oprávnený používateľ. Server overuje kľúč používateľa a potvrdzuje jeho pravosť. Následne sa po úspešnom overení kľúča zaznamenajú zmenené údaje. Cookies majú nastavenú dobu expirácie na dve hodiny, čo znamená, že ak používateľ bude prihlásený dlhšie ako 2 hodiny a vykoná úpravy v systéme, systém ho automaticky odhlási a bude sa musieť prihlásiť znovu, aby sa vytvoril nový kľúč.

1.3 Bezpečný prenos údajov client-server

Prenos údajov z klienta na server je zabezpečený pomocou vygenerovaného kľúča používateľa zašifrovaným RSA verejným kľúčom servera. Pri zlyhaní overenia je používateľ odhlásený z aplikácie.

1.4 Bezpečný prenos údajov server-client

Prenos údajov zo serveru na klienta je zabezpečený pomocou vygenerovaného kľúča servera zašifrovaným RSA verejným kľúčom používateľa. Pri zlyhaní overenia je používateľ odhlásený z aplikácie.

1.5 Používatelia v databáze

Pre účel testovania sa v databáze nachádzajú používatelia user1, user2, user3 s heslom `"Aaa1234."`. Títo používatelia majú vytvorené náhodné záznamy dochádzky pre mesiace 10/2023 a 11/2023.

1.6 Aplikácia

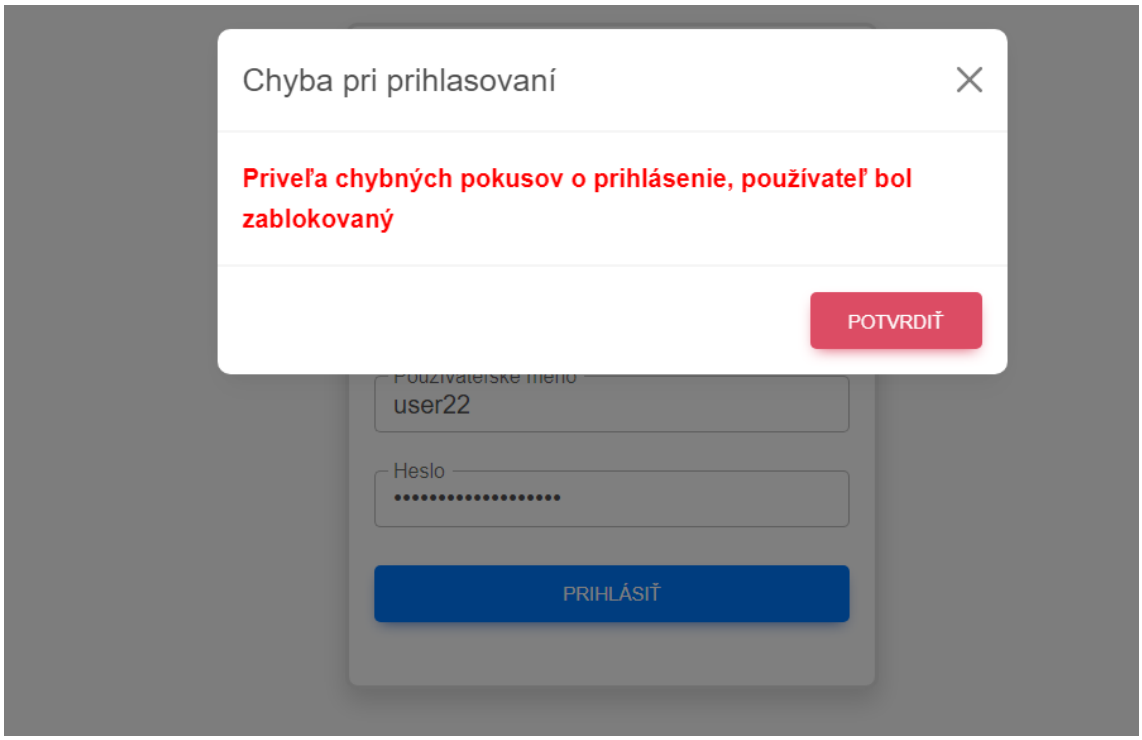
Aplikácia beží na porte 5001.

1.7 Časový rozostup pri prihlasovaní

V systéme bola implementovaná ochrana pred *brute-force* útokom spôsobom zablokovania používateľa. Ak používateľ zadá bezprostredne po sebe 5-krát nesprávne heslo, je jeho konto zablokované na 5 minút a v priebehu tohto mu nie je umožnené prihlásiť sa. Pri tomto môže nastať viacero situácií, ktoré boli identifikované a riešené:

- Po uplynutí časového limitu 5 minút má používateľ k dispozícii ďalších 5 pokusov na vloženie hesla.
- Po uplynutí 24 hodín od posledného zadania nesprávneho hesla sa pokusy nulujú a používateľ má opäť k dispozícii 5 pokusov.
- Ak používateľ zadá správne heslo, počet nesprávnych pokusov je vynulovaný

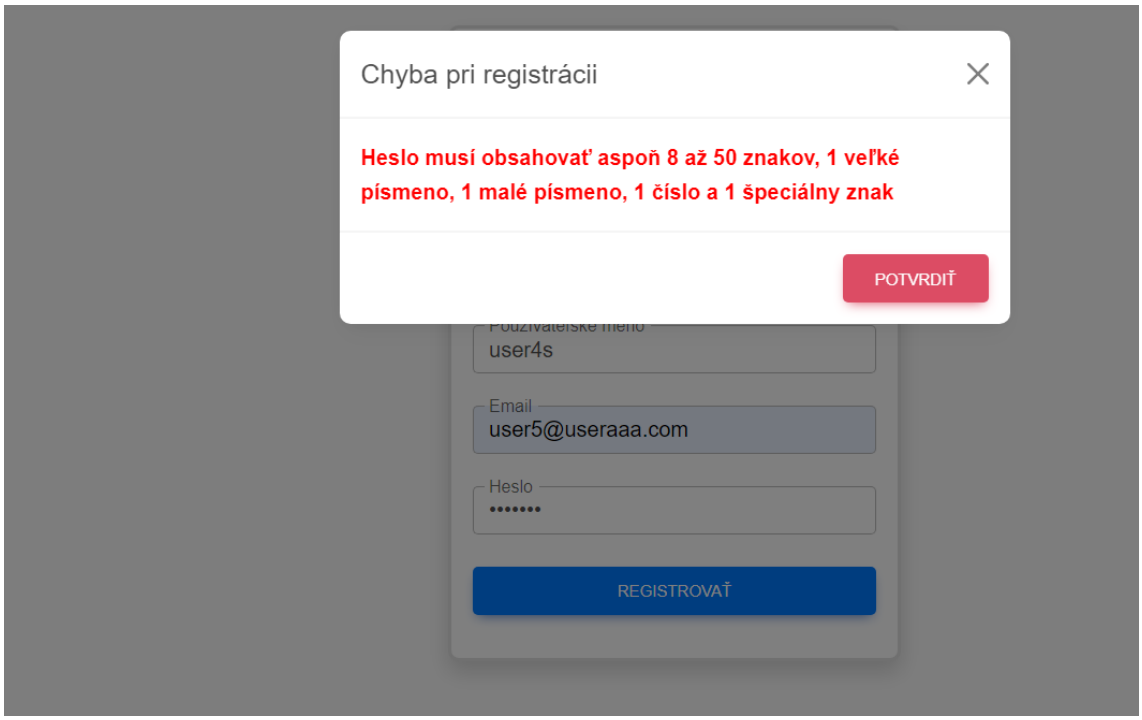
Po dosiahnutí 5 nesprávnych pokusov o prihlásenie je používateľ informovaný o zablokovaní jeho konta informáciou zobrazenou na obrázku 2.



Obr. 2: Zablokovanie účtu používateľa

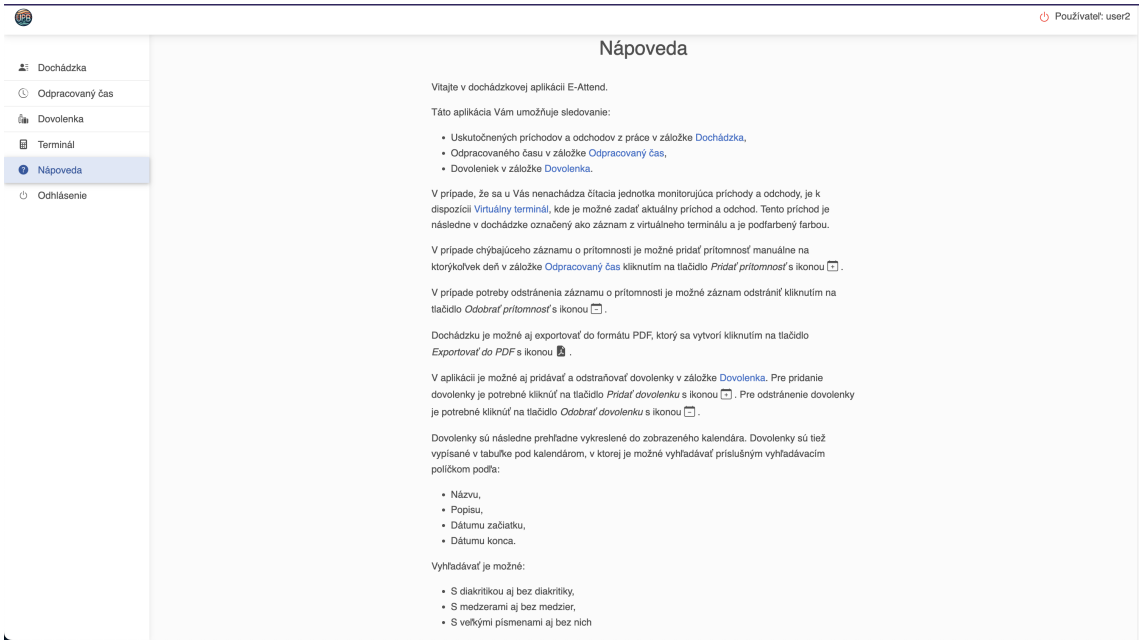
1.8 Kontrola zložitosti hesla

Heslo zadané pri registrácií musí obsahovať aspoň jedno veľké písmeno, malé písmeno, číslo a špeciálny znak. Dĺžka hesla musí byť minimálne 8 znakov a maximálne 50. Heslo sa pri registrácii kontroluje, či sa nenachádza v slovníku 100 000 ľahko uhádnuteľných hesiel. Ak nie sú všetky spomenuté podmienky splnené súčasne, registrácia nebude povolená. Na obrázku 3. môžeme vidieť chybové hlásenie pre nesplnenie požiadaviek na heslo.



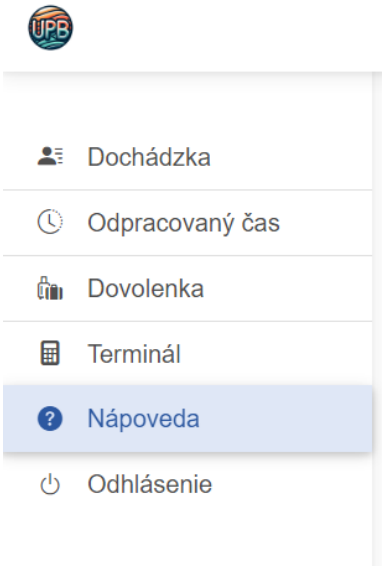
Obr. 3: Nesprávny formát hesla

2 Funkcionalita aplikácie



Obr. 4: Úvodná obrazovka po prihlásení - Nápoveda

Po prihlásení používateľa do systému sa mu zobrazí úvodná obrazovka, ktorú môžeme vidieť na obrázku 4. Nachádza sa na nej návod, popisujúci orientáciu a prácu v prostredí aplikácie.

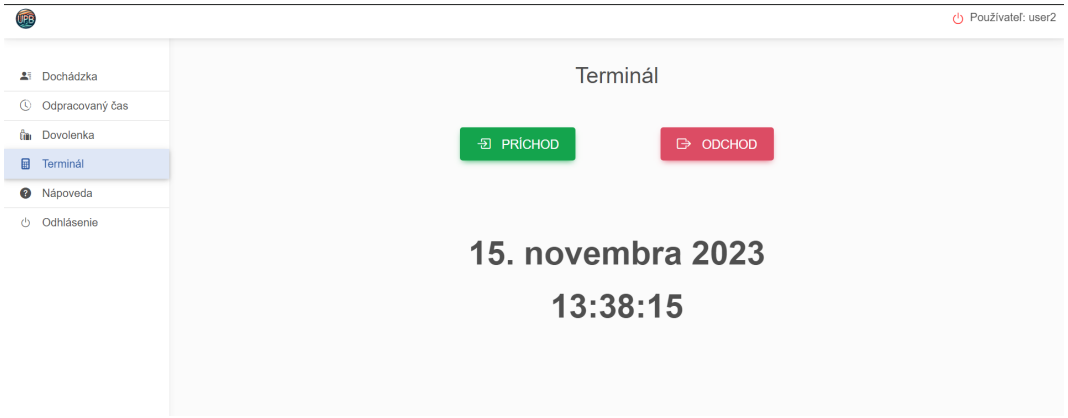


Obr. 5: Navigačný panel

Na ľavej strane sa nachádza menu, ktoré môžeme vidieť na obrázku 5.

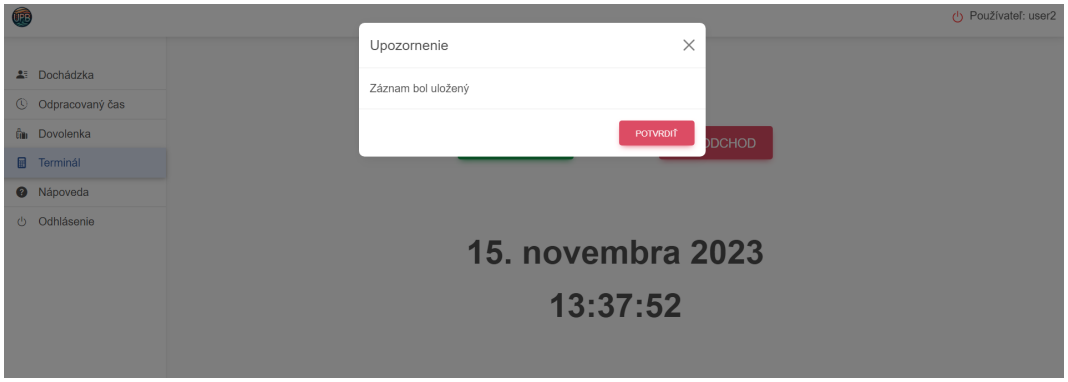
2.1 Virtuálny terminál

Prejdením na záložku *Terminál* sa nám zobrazia tlačidlá *Príchod* a *Odchod* ako môžeme vidieť na obrázku 6. Táto záložka slúži na zadanie príchodu a odchodu v práci.



Obr. 6: Virtuálny terminál

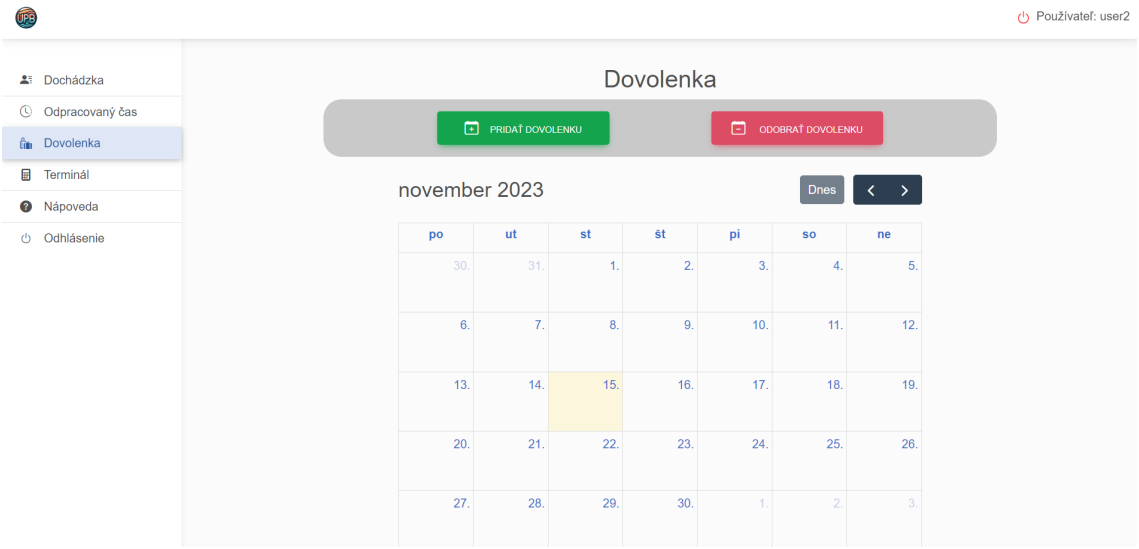
Po stlačení tlačidla príchod sa nám automaticky uloží do databázy aktuálny čas príchodu. Pri úspešnom vykonaní nám vyskočí okno s potvrdením, že pridanie bolo správne vykonané. Okno môžeme vidieť na obrázku 7. Pri zadaní odchodu naskočí rovnaké okno oznamujúce, že záznam bol správne zapísaný.



Obr. 7: Uloženie záznamu

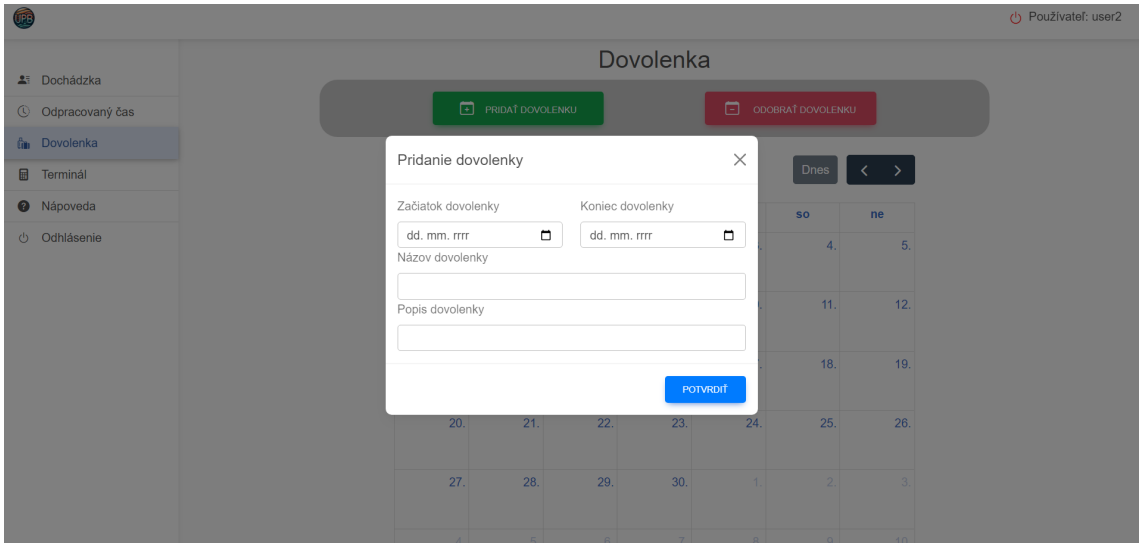
2.2 Dovolenka

Po prejdení na záložku *Dovolenka* sa nám zobrazí kalendár s dovolenkami a tlačidlá na pridanie a odobratie dovolenky ako môžeme vidieť na obrázku 8.

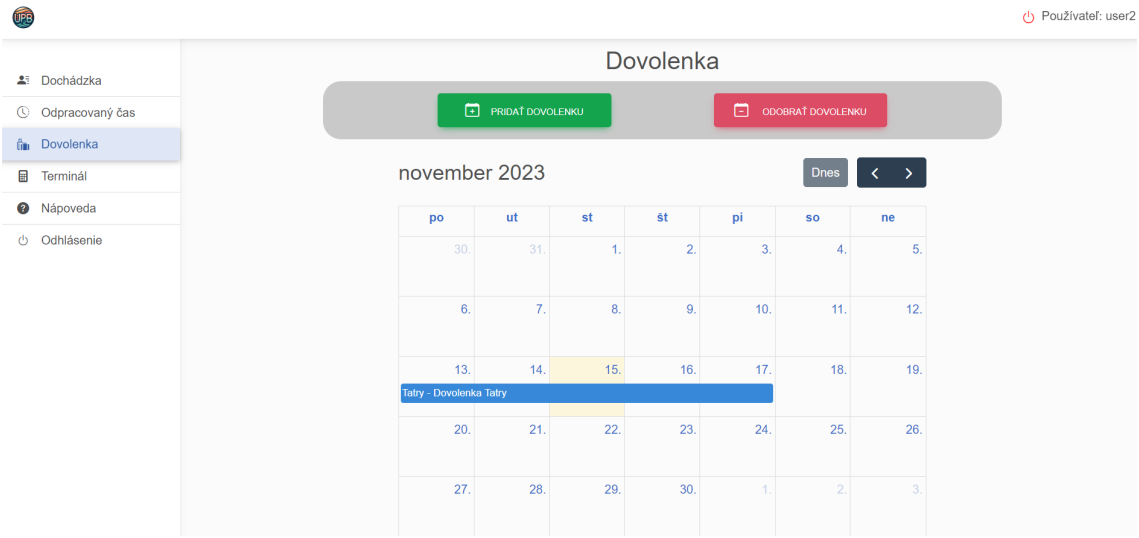


Obr. 8: Dovolenka

Po stlačení tlačidla pridanie dovolenky sa nám zobrazí okno, do ktorého sa zadáva dátum dovolenky začiatok a koniec, názov dovolenky a popis dovolenky ako môžeme vidieť na obrázku 9. Pri vyplnení daného okna sa dovolenka pridá do kalendára, čo môžeme vidieť na obrázku 10. Pri nezadní dátumu, názvu alebo popisu dovolenky, vyskočí okno s upozornením, že dovolenka nebola správne vyplnená a takýto záznam sa neuloží.

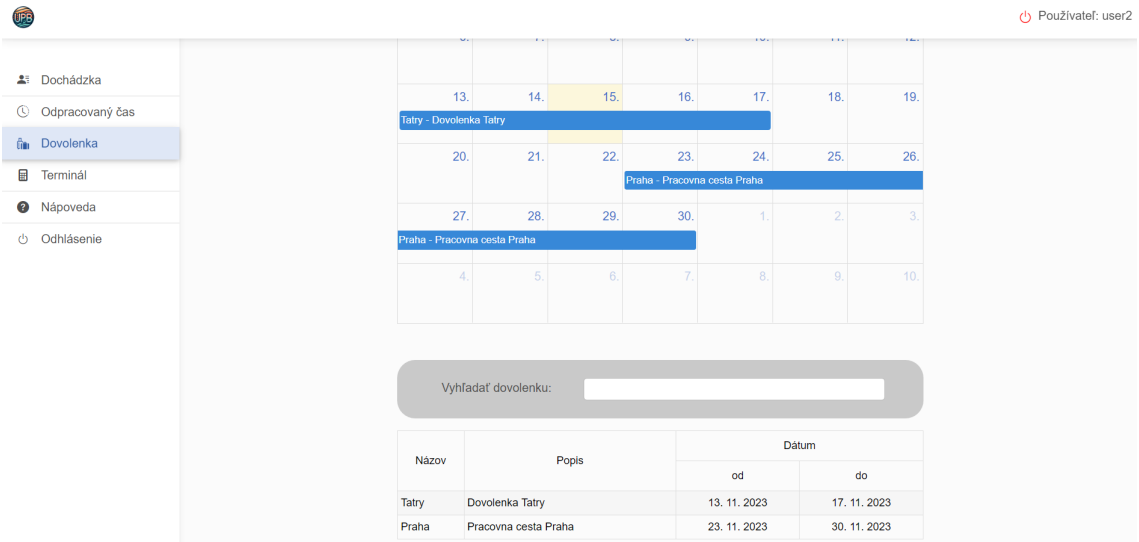


Obr. 9: Nahratie dovolenky

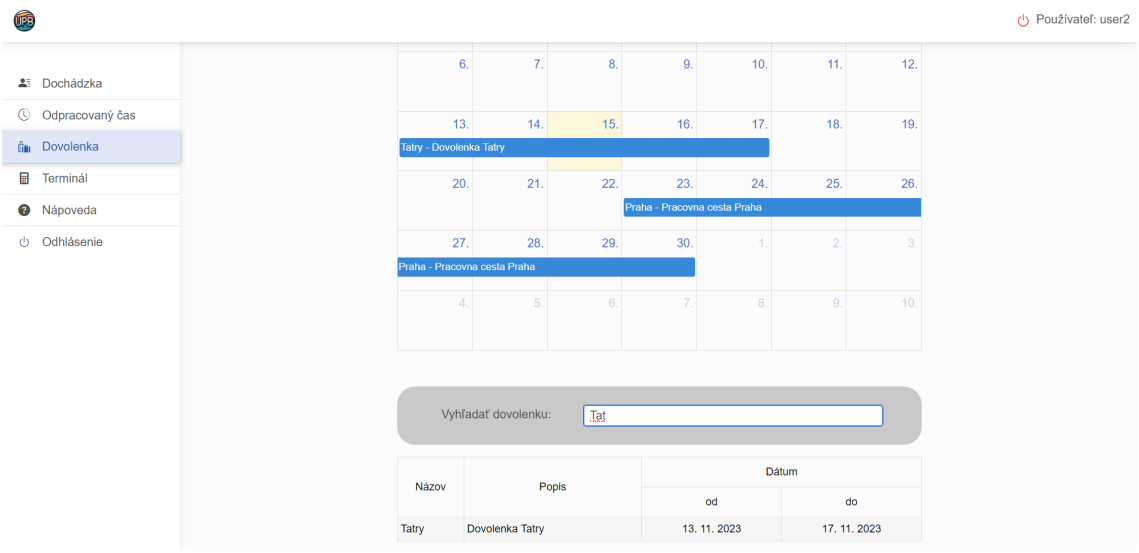


Obr. 10: Kalendár dovolenky

V záložke *Dovolenka*, sa nachádza pole na vyhľadávanie dovolenky, ako môžeme vidieť na obrázku 11. Toto pole slúži na vyhľadanie dovolenky podľa názvu, dátumu a aj popisu dovolenky. Pri zadaní textu do vyhľadavacieho poľa, sa nám zobrazia dovolenky, ktoré obsahujú text zadaný do poľa, to môžeme vidieť na obrázku 12.

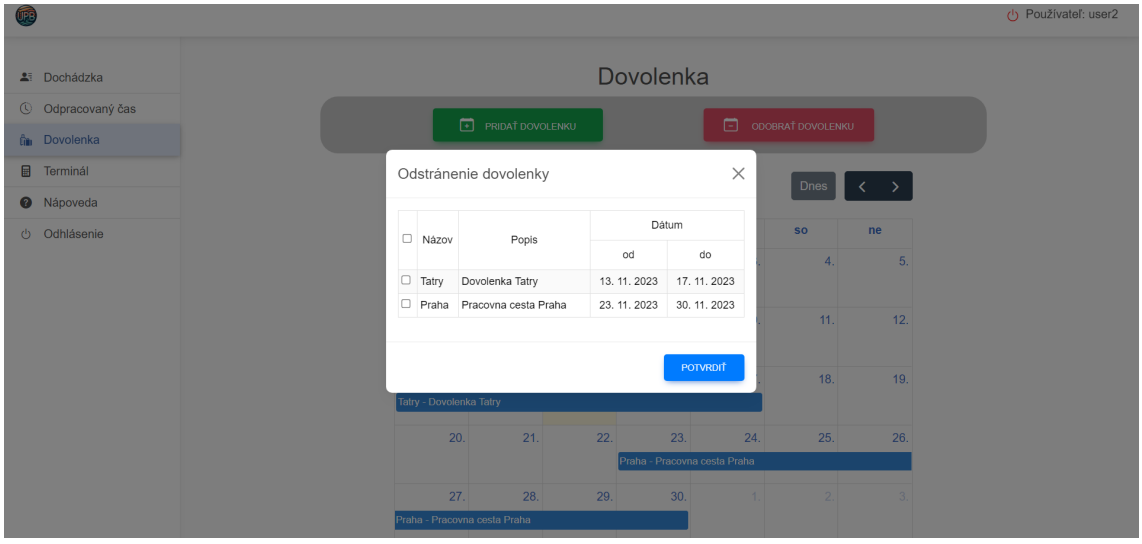


Obr. 11: Vyhľadávanie dovolenky



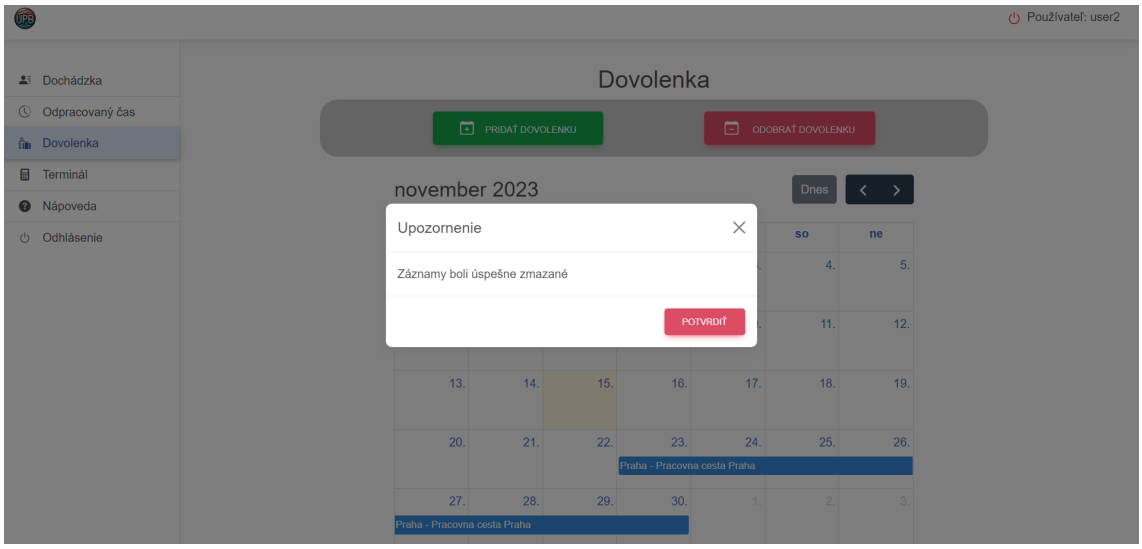
Obr. 12: Vyhľadávanie dovolenky

Rovnako v záložke dovolenka sa nachádza aj tlačidlo na odstránenie dovolenky. Po stlačení tlačidla sa nám zobrazí okno so všetkými dovolenkami daného používateľa, čo môžeme vidieť na obrázku 13.

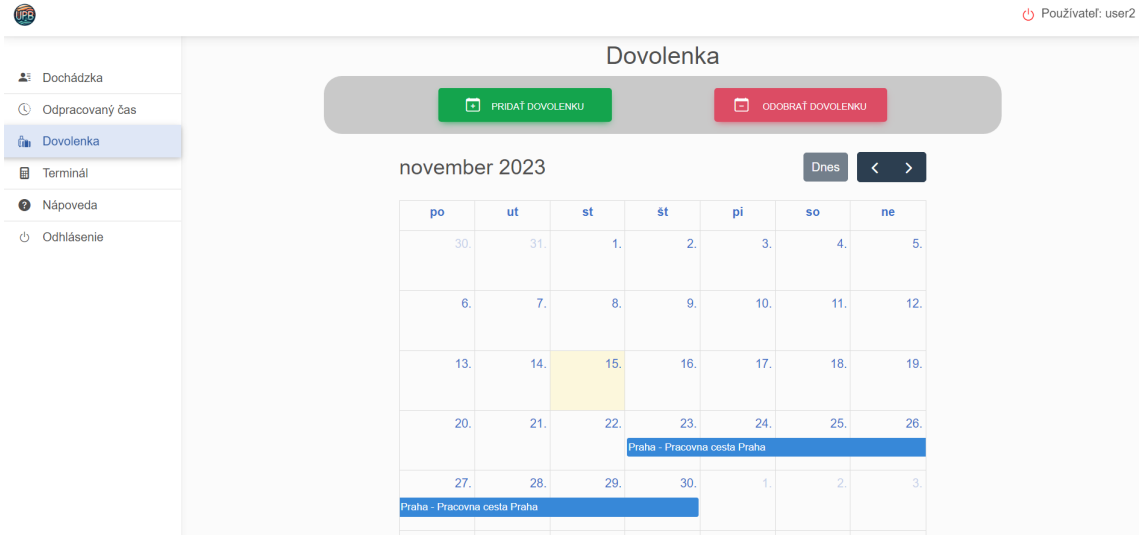


Obr. 13: Odstránenie dovolenky

Používateľ si zvolí, ktoré dovolenky chce odstrániť a potvrdí tlačidlom potvrdiť. Po úspešnom odstránení sa mu zobrazí okno, ktoré ho informuje o odstránení dovolenky, ako môžeme vidieť na obrázku 14. Zároveň sa dovolenka odstráni aj z kalendára, čo vidíme na obrázku 15.



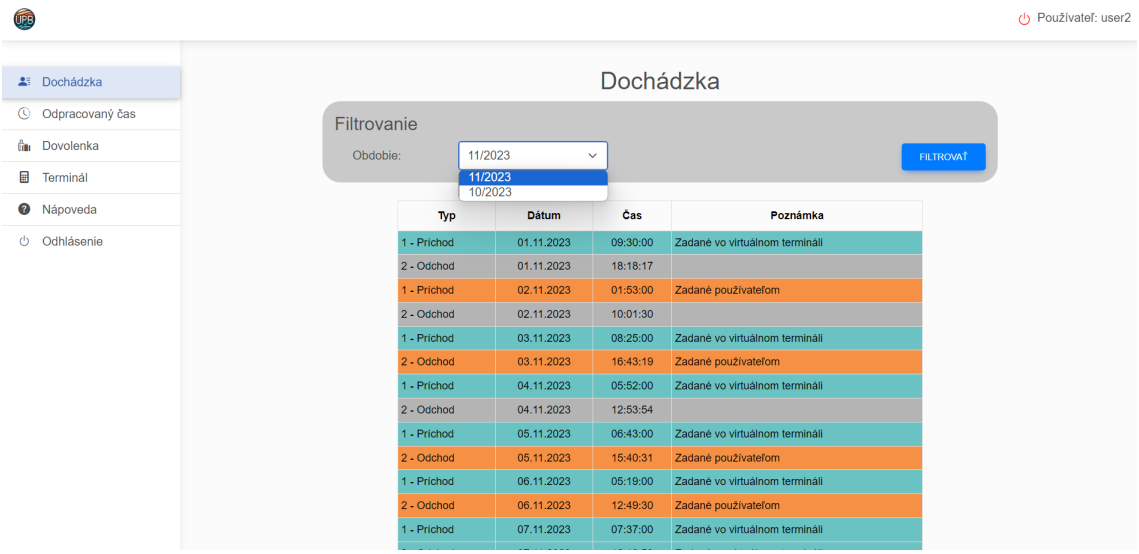
Obr. 14: Odstránenie dovolenky



Obr. 15: Odstránenie dovolenky - kalendár

2.3 Dochádzka

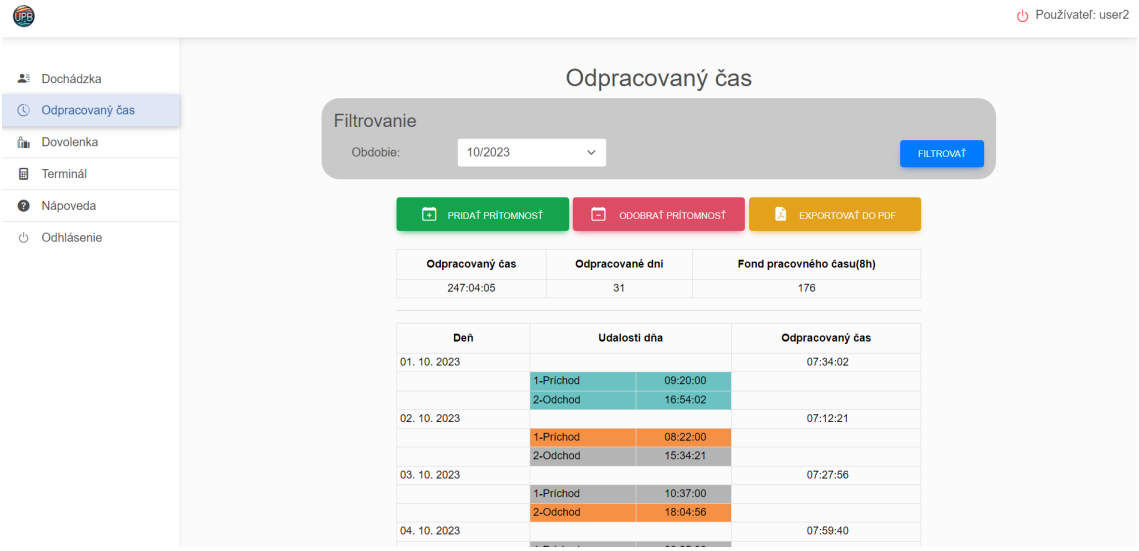
Po prejdení na záložku *Dochádzka* sa nám zobrazí tabuľka príchodov a odchodov za daný mesiac. To môžeme vidieť aj na obrázku 16. Zároveň sa na záložke *Dochádzka* nachádza aj pole na filtrovanie, kde si môže používateľ vybrať, mesiac, ktorý chce zobraziť. Toto filtrovanie funguje aj na záložke *Odpracovaný čas* v kapitole 2.4. Keď si používateľ zvolí 10/2023 tak sa mu tento mesiac prenesie aj do záložky *Odpracovaný čas*.



Obr. 16: Dochádzka

2.4 Odpracovaný čas

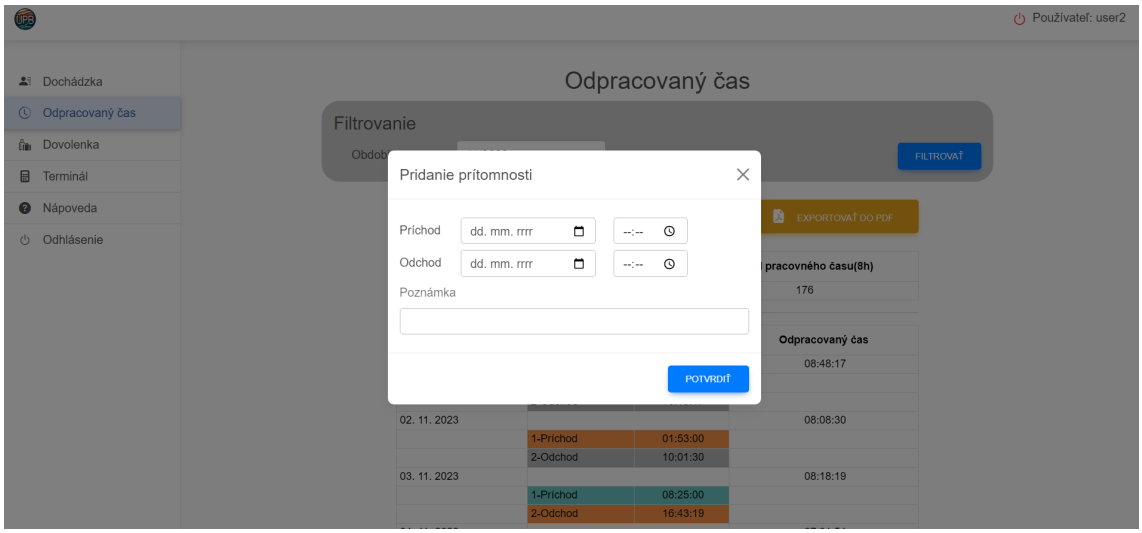
Po prejdení na záložku *Odpracovaný čas* sa nám zobrazí tabuľka s príchodmi a odchodmi. Zároveň sa zobrazí tabuľka s odpracovaným časom, odpracovanými dňami a počtom hodín za daný mesiac. Na záložke sa nachádzajú aj tlačidlá na pridanie dochádzky, odobratie dochádzky a tlačidlo na exportovanie dochádzky do PDF. Na obrázku 17. vidíme danú záložku s dochádzkou a s tlačidlami.



Obr. 17: Záložka odpracovaný čas

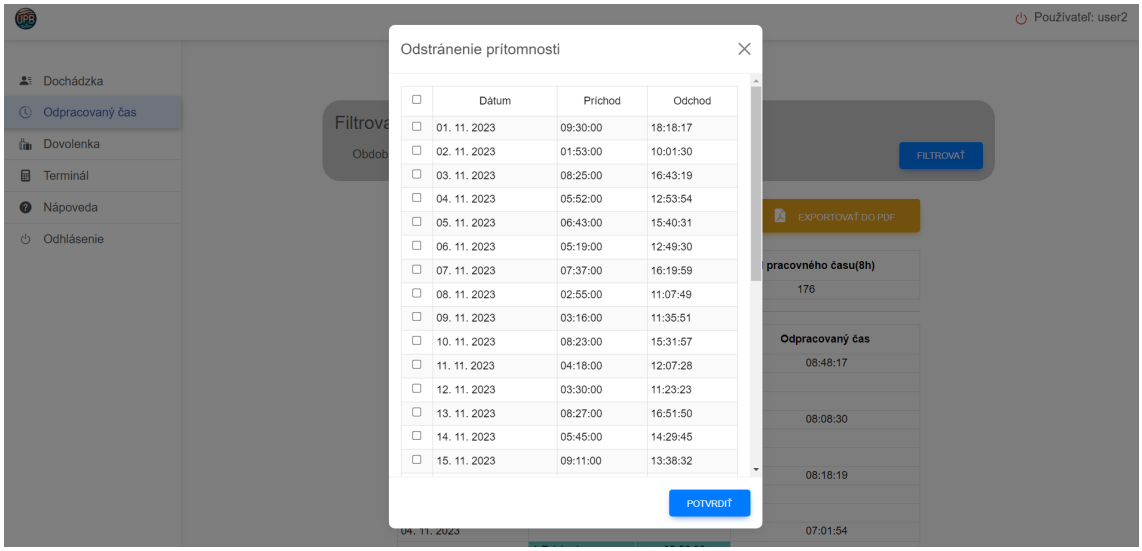
Po stlačení tlačidla *Pridať prítomnosť*, sa nám zobrazí okno na pridanie prítomnosti

kde zadáme príchod odchod a poznámku, čo môžeme vidieť na obrázku 18. Po stlačení tlačidla potvrdiť sa nám dochádzka pridá do tabuľky.



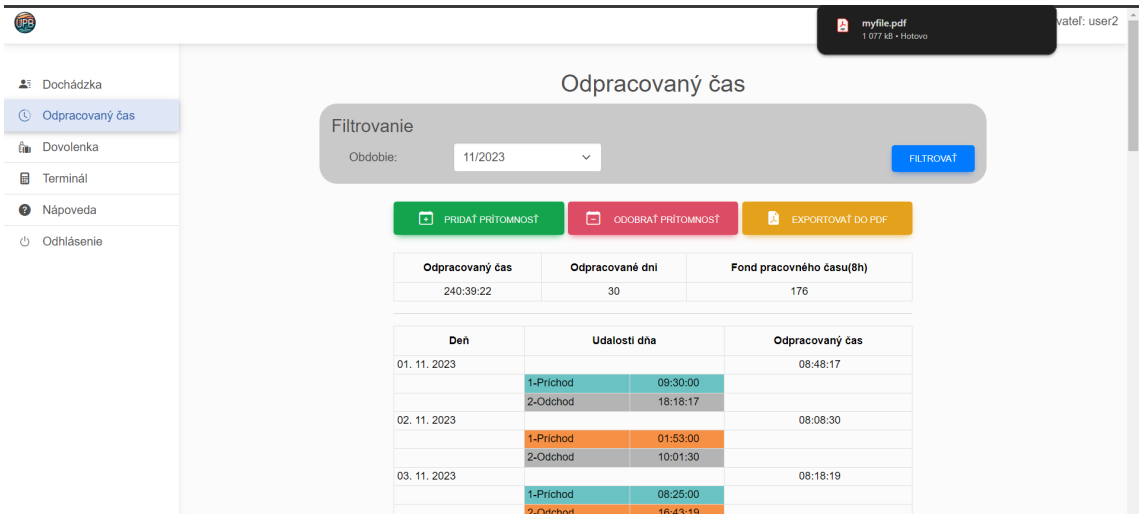
Obr. 18: Pridanie prítomnosti

Po stlačení tlačidla *Odobrať prítomnosť*, sa nám zobrazí tabuľka s dochádzkou, kde si môžeme zaškrtnúť pomocou checkboxu, ktorý záznam chce používateľ odobrať. Po označení daného záznamu a stlačením tlačidla potvrdiť, sa daný záznam odstráni z dochádzky.

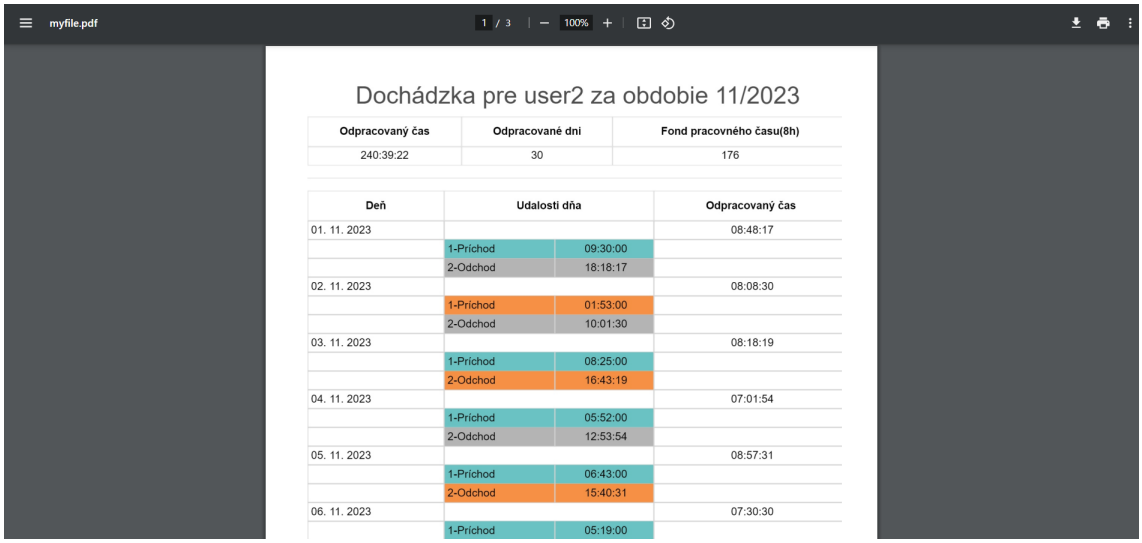


Obr. 19: Odobrať prítomnosť

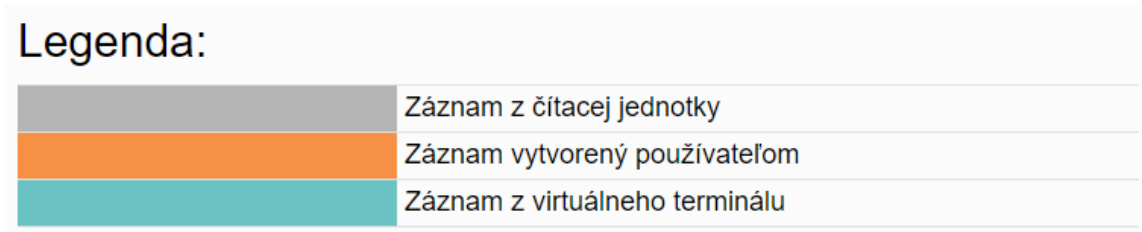
Po stlačení tlačidla *Exportovať do PDF*, sa nám vygeneruje PDF súbor s danou dochádzkou. Na obrázku 20. môžeme vidieť stiahnutie PDF exportu. Po otvorení stiahnutého PDF exportu, môžeme vidieť tabuľku s dochádzkou. To môžeme vidieť aj na obrázku 21.



Obr. 20: Stiahnuté PDF



Obr. 21: Exportované PDF



Obr. 22: Legenda dochádzky

Na obrázku 22. sa nachádza legenda k daným záznamom v tabuľke. Každá farba

záznamu predstavuje akým spôsobom bol záznam vytvorený. Táto legenda je rovnaká aj pre záložku dochádzka aj pre odpracovaný čas.

Zoznam použitej literatúry

1. MONIKA GRIGUTYTĖ. *What is bcrypt and how does it work?* 2023. Dostupné tiež z: `https://nordvpn.com/blog/what-is-bcrypt/`.
2. MAX COUNTRYMAN. *Flask-Bcrypt*. 2011. Dostupné tiež z: `https://flask-bcrypt.readthedocs.io/en/1.0.1/`.