

Návrh klient-server fakturačního systému s podporou exportu účetních dat pomocí standardního přenosového formátu a možností použití na mobilních zařízeních

Design of Client-Server Billing System with Support of Accounting
Data Export Using a Standard Exchange Format and with the
Possibility of Use on Mobile Devices

Bc. Jakub Nacík



Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2013/2014

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení: **Bc. Jakub Nacík**
Osobní číslo: **A12472**
Studijní program: **N3902 Inženýrská informatika**
Studijní obor: **Informační technologie**
Forma studia: **kombinovaná**

Téma práce: **Návrh klient-server fakturačního systému s podporou exportu účetních dat pomocí standardního přenosového formátu a možností použití na mobilních zařízeních**

Zásady pro vypracování:

1. Prostudujte vhodné technologie pro návrh klient-server aplikací, dále standardní přenosové formáty účetních dat v IT a možnosti adaptace GUI pro mobilní zařízení.
2. Vypracujte požadavky na fakturační systém a porovnejte je s již existujícími klient-server fakturačními systémy.
3. Navrhněte databázi a aplikační logiku systému, splňující výše uvedené požadavky.
4. Implementujte systém dle návrhu pomocí některého z objektových vývojových frameworků, věnujte pozornost zabezpečení systému.
5. Vytvořte ukázkovou instalaci.

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. VRÁNA, Jakub. 1001 tipů a triků pro PHP. Vyd. 1. Brno: Computer Press, 2010, 456 s. ISBN 978-80-251-2940-1.
2. PROKOPOVÁ, Zdenka. Databázové systémy MySQL+PHP. FAI UTB Zlín, 2006, s. 126, ISBN 80-7318-486-9.
3. SCHNEIDER, Robert D. MySQL: oficiální průvodce tvorbou, správou a laděním databází. Praha: Grada Publishing, 2006. ISBN 80-247-1516-3.
4. BORONCZYK, Tim. PHP 6, MySQL, Apache: vytváříme webové aplikace. Vyd. 1. Brno: Computer Press, 2009, xiv s., 280 s. Databáze. ISBN 978-80-251-2767-4.
5. MARCOTTE, Ethan a Iforeword by Jeremy KEITHI. Responsive web design. A Book Apart, 2011. ISBN 09-844-4257-X.
6. KOSEK, Jiří. PHP a XML. 1. vyd. Praha: Grada, 2009. ISBN 978-80-247-1116-4.

Vedoucí diplomové práce:

Ing. Radek Vala

Ústav informatiky a umělé inteligence

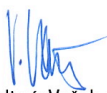
Datum zadání diplomové práce:

21. února 2014

Termín odevzdání diplomové práce:

20. května 2014

Ve Zlíně dne 21. února 2014



prof. Ing. Vladimír Vašek, CSc.
děkan



doc. Mgr. Roman Jašek, Ph.D.
ředitel ústavu

ABSTRAKT

Hlavným cieľom mojej diplomovej práce bolo vytvoriť webovú aplikáciu, ktorá bude fungovať ako nástroj pre generovanie elektronických faktúr s možnosťou vytvorené účtovné dáta následne exportovať. Export dát je do formátov PDF pre tlač, TXT pre účtovný softvér MRP a UBL ako štandardného prenosového formátu. GUI webovej aplikácie je vytvorené s plnou podporou mobilných zariadení a rôznych rozlíšení displeja. Aplikácia je vytvorená v jazyku PHP s využitím objektového frameworku Nette a prepojením na MySQL databázu.

Kľúčové slová: fakturácia, webová aplikácia, responzívny webdizajn, PHP, Nette, MySQL

ABSTRACT

The main goal of my diploma thesis was to create web application, which will be used for generating electronic invoices with ability to export created invoice data. Data export supports PDF format for printing, TXT format for accounting software MRP and UBL as standard data transfer format. GUI of this application is created with full support for mobile devices and different screen resolutions. Application is created in PHP language with object oriented framework Nette and is connected to MySQL database.

Keywords: invoicing, web application, responsive webdesign, PHP, Nette, MySQL

Na tomto mieste by som chcel poďakovať Ing. Radkovi Valovi za jeho čas, pripomienky a cenné rady, ktoré mi odovzdal pri vedení tejto práce.

Motto: "Stay hungry. Stay foolish."

~ Steve Jobs

Prohlašuji, že

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

Prohlašuji,

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

Ve Zlíně

.....
podpis diplomanta

OBSAH

| | |
|--|-----------|
| OBSAH..... | 7 |
| ÚVOD | 9 |
| I. TEORETICKÁ ČASŤ..... | 10 |
| 1 POŽIADAVKY NA FAKTURAČNÝ SYSTÉM..... | 11 |
| 2 EXISTUJÚCE KLIENT-SERVER FAKTURAČNÉ SYSTÉMY..... | 13 |
| 2.1 SUPERFAKTÚRA.SK | 13 |
| 2.2 iKROS.SK | 14 |
| 2.3 FAKTÚRY-ONLINE.COM | 15 |
| 3 ŠTANDARDNÉ PRENOSOVÉ FORMÁTY ÚČTOVNÝCH DÁT | 17 |
| 3.1 EDI..... | 17 |
| 3.1.1 ASC X12 | 18 |
| 3.1.2 UBL | 19 |
| 3.1.3 EDIFACT | 20 |
| 4 TECHNOLOGIE PRE TVORBU KLIENT-SERVER APLIKÁCIÍ..... | 21 |
| 4.1 HTML..... | 21 |
| 4.2 CSS | 21 |
| 4.3 PHP | 22 |
| 4.4 MYSQL..... | 22 |
| 4.5 PHP FRAMEWORK NETTE | 22 |
| 4.6 FRONT-END FRAMEWORK BOOTSTRAP | 23 |
| 5 ADAPTÁCIA GUI PRE MOBILNÉ ZARIADENIA | 25 |
| 6 BEZPEČNOSŤ WEBOVÝCH APLIKÁCIÍ | 28 |
| 6.1 SQL INJECTION | 28 |
| 6.2 CROSS-SITE-SCRIPTING | 28 |
| 6.3 CROSS-SITE REQUEST FORGERY (CSRF) | 29 |
| 6.4 INSECURE CRYPTOGRAPHIC STORAGE | 30 |
| 6.5 BRUTE-FORCE ATTACK | 30 |
| II. PRAKTICKÁ ČASŤ..... | 32 |
| 7 ŠTRUKTÚRA SYSTÉMU | 33 |

| | | |
|-----------|--|-----------|
| 7.1 | DASHBOARD | 33 |
| 7.2 | SPRÁVA FAKTÚR..... | 34 |
| 7.2.1 | <i>Automatické generovanie faktúr</i> | 35 |
| 7.2.2 | <i>Export dát</i> | 36 |
| 7.2.3 | <i>Export do PDF</i> | 37 |
| 7.3 | SPRÁVA PROJEKTOV | 38 |
| 7.4 | SPRÁVA ZÁKAZNÍKOV..... | 38 |
| 7.5 | NASTAVENIA | 38 |
| 8 | DATABÁZOVÁ ŠTRUKTÚRA | 40 |
| 9 | OPTIMALIZÁCIA GUI PRE MOBILNÉ ZARIADENIA..... | 42 |
| 10 | ZABEZPEČENIE APLIKÁCIE..... | 44 |
| 10.1 | OCHRANA PRED SQL INJECTION..... | 44 |
| 10.2 | OCHRANA PRED CROSS-SITE SCRIPTING (XSS)..... | 45 |
| 10.3 | OCHRANA PRED BRUTE-FORCE ATTACK..... | 45 |
| 10.4 | SSL CERTIFIKÁT | 45 |
| 10.5 | PENETRAČNÝ TEST | 46 |
| 11 | UKÁŽKOVÁ INŠTALÁCIA | 47 |
| | ZÁVER..... | 48 |
| | ZÁVER V ANGLIČTINE | 49 |
| | ZOZNAM POUŽITEJ LITERATÚRY | 50 |
| | ZOZNAM POUŽITÝCH SYMBOLOV A SKRATIEK | 52 |
| | ZOZNAM OBRÁZKOV | 53 |
| | ZOZNAM TABULIEK..... | 54 |
| | ZOZNAM PRÍLOH | 55 |

ÚVOD

Potreba evidencie rôznorodých dát je zrejماً v naprieč celým dnešným fungovaním spoločnosti. V oblasti informačných technológií túto potrebu veľmi dobre napĺňajú rôzne databázové systémy, ktoré sú vytvorené s cieľom uľahčiť, urýchliť a zefektívniť evidenciu dát v našom každodennom živote. K vedeniu firiem a podnikaniu neoddeliteľne patrí aj vedenie účtovnej agendy každej firmy, bez rozdielu jej veľkosti, ročného obratu či zamerania. Aj v tejto oblasti sa ukazuje využívanie rôznych účtovných softvérov a databázových systémov ako veľmi efektívne.

Táto práca pojednáva o tvorbe elektronického fakturačného systému, fungujúceho ako klient-server aplikácia, ktorý sa nesnaží byť komplexným ekonomickým softvérom, no jeho cieľom je zefektívniť každodennú evidenciu fakturácie pre malé a stredné podniky, zároveň byť cenovo dostupným a zrozumiteľným pre bežného užívateľa. Oproti bežným účtovným softvérom je tento systém možné plnohodnotne používať aj na mobilných zariadeniach a vďaka možnosti exportu účtovných dát je možné ho jednoducho prepojiť s inými ekonomickými aplikáciami.

V teoretickej časti je práca zameraná na všeobecnú problematiku evidencie fakturačných dát. V druhej kapitole práca obsahuje porovnanie vyvíjaného systému s už existujúcimi klient-server fakturačnými systémami. Tretia kapitola sa venuje problematike štandardných prenosových formátov účtovných dát. Záverečná časť teoretickej časti práce sa venuje samotnej tvorbe webových aplikácií, rozobrané sú dostupné technológie a frameworky, taktiež problematika optimalizácie užívateľského rozhrania pre mobilné zariadenia a v neposlednom rade bezpečnosť webových aplikácií.

Praktická časť sa venuje samotnej tvorbe fakturačného systému. V siedmej kapitole je popis jednotlivých sekcií a funkcionalít fakturačného systému. Nasleduje popis použitej databázovej štruktúry aplikácie a jednotlivých jej tabuliek. Ďalej je v praktickej časti rozobraná optimalizácia aplikácie pre mobilné zariadenia. V závere sa táto časť práce venuje problematike zabezpečenia pred rôznymi typmi zraniteľností.

I. TEORETICKÁ ČASŤ

1 POŽIADAVKY NA FAKTURAČNÝ SYSTÉM

Elektronický fakturačný systém je nástroj, ktorého hlavným cieľom je uľahčiť správu a evidenciu agendy faktúr každej väčšej či menšej firmy. Vytváranie, evidenciacia, sledovanie a archivácia účtovných dát je neoddeliteľnou súčasťou fungovania každej firmy. S rastúcou veľkosťou firmy sú nároky na účtovný systém stále rozsiahlejšie, keďže práca s účtovnými dátami začína byť časovo náročná.

Pre firmy existuje niekoľko možností, ako môžu spravovať svoju účtovnú agendu. Výber konkrétneho riešenia závisí na preferenciách a požiadavkách danej firmy. Prvoradé je rozlíšiť, či firma hľadá komplexný účtovný softvér, ktorý poskytuje kompletne vedenie účtovnej agendy vrátane všetkých daňových a mzdových povinností alebo hľadá nástroj, ktorý bude fungovať ako evidenciacia fakturácie a teda evidenciacia príjmov financií do firmy. V prípade voľby komplexného ekonomického systému je dôležité, aby bol vo firme zamestnaný ekonomicky vzdelaný pracovník, ktorý bude s účtovnou agendou pracovať. Toto riešenie je tak vhodné najmä pre väčšie firmy, ktoré majú vlastné ekonomické oddelenie.

V prípade menších firiem alebo živnostníkov je predpoklad, že sa o vedenie účtovnej agendy stará externá firma a interne sa spravuje len fakturácia za svoje služby alebo tovar, pričom všetky ostatné účtovné náležitosti sa outsourcujú. Nákup ekonomického softvéru len pre účely fakturácie by bol neekonomický. V takom prípade množstvo týchto subjektov siahne po rôznych provizórnych riešeniach, napríklad tvorba faktúr v programe MS Excel. Takéto riešenie je však veľmi obmedzujúce a v prípade väčšieho počtu faktúr aj časovo náročné, keďže absentuje akákoľvek automatizácia rutinných procesov pri tvorbe faktúr. Ďalším nedostatkom tohto riešenia je nutnosť manuálne sledovať splatnosti faktúr a ich úhrady, čo si opäť vyžaduje čas. Následne chýba možnosť prenášať takto vystavené faktúry do účtovného softvéru externej firmy a vznikajú teda ďalšie časové nároky na nahrávanie faktúr pre účely vedenia účtovníctva, čo sa nepriamo odzrkadlí na nákladoch na účtovnú firmu.

Pre tento typ firiem je ideálnym riešením systém, ktorý nie je komplexným účtovným systémom, ale stará sa len o evidenciaciu fakturácie, dokáže samostatne sledovať vyššie popísané veličiny a je finančne nenáročný. Na tvorbu takéhoto systému sa ponúka ako vhodné riešenie vytvoriť ho ako webovú aplikáciu, ktorá dokáže splniť všetky očakávané požiadavky a zároveň prináša aj ďalšie výhody v porovnaní s bežným účtovným softvérom

a to sú hlavne jeho nezávislosť na operačnom systéme, dostupnosť kedykoľvek a z akéhokoľvek zariadenia a možnosť prispôbiť takúto aplikáciu na mobilné zariadenia, ktoré sa v súčasnosti tešia veľkej popularite.

Z uvedeného vyplýva, že fakturačný systém by mal spĺňať nasledovné požiadavky:

- Evidencia odberateľov a ich fakturačných údajov
- Tvorba bežných faktúr za tovary alebo služby
- Automatická tvorba periodicky sa opakujúcich faktúr
- Sledovanie dátumov splatnosti faktúr
- Archivácia faktúr
- Základné štatistiky
- Export fakturačných dát pre možnosť prenosu do iných informačných systémov
- Dostupnosť na mobilných zariadeniach
- Nízka obstarávacía cena a cena prevádzky

2 EXISTUJÚCE KLIENT-SERVER FAKTURAČNÉ SYSTÉMY

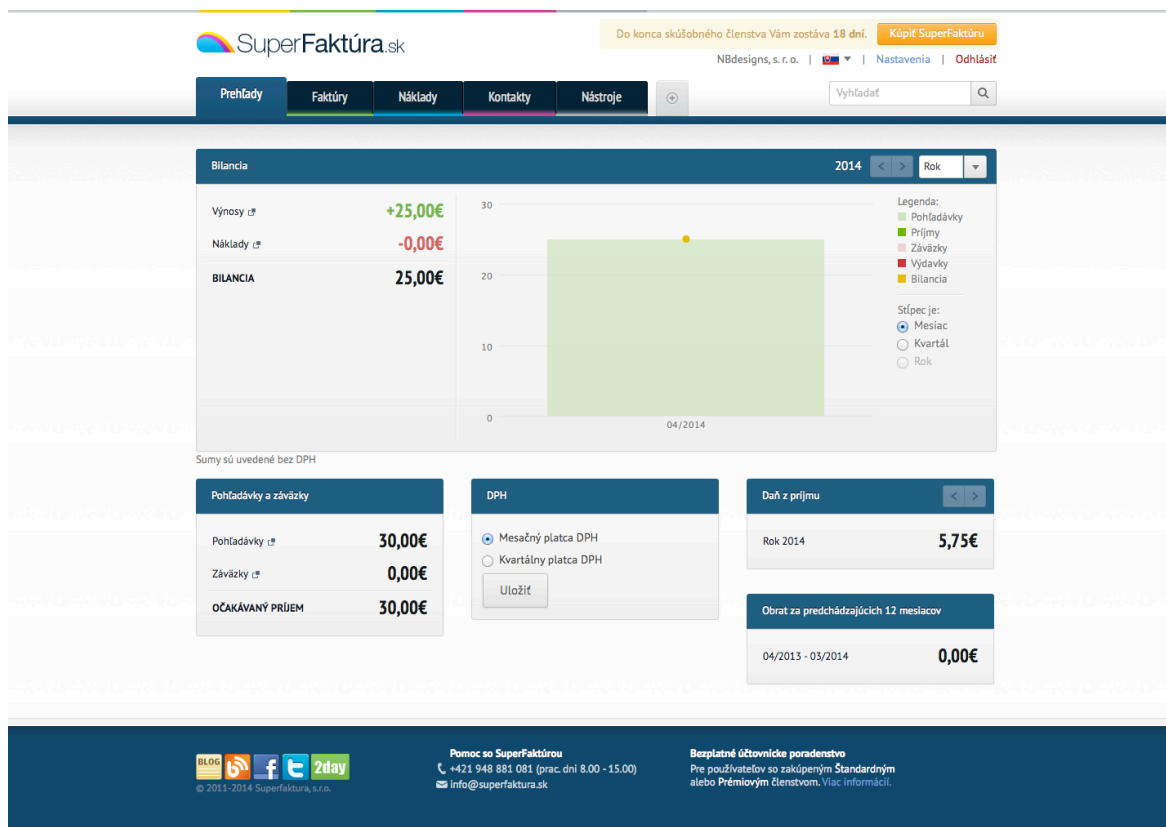
Potreba riešiť správu účtovnej agendy hlavne pre malé a stredné podniky a stále rastúca popularita internetu a webových aplikácií spôsobili, že na trhu figuruje niekoľko spoločností, ktoré ponúkajú riešenia účtovných a fakturačných systémov postavené na báze využívania webovej aplikácie ako služby pre správu účtovných dát.

2.1 SuperFaktúra.sk

Medzi najznámejšie služby na slovenskom trhu patrí SuperFaktúra.sk od spoločnosti SuperFaktura.sk, s.r.o. Služba vznikla v roku 2009 ako jednoduchá webová aplikácie pre generovanie PDF faktúr. Služba sa začala medzi živnostníkmi a malými podnikateľmi veľmi rýchlo tešiť veľkej popularite a jej vývoj napredoval. Aplikácia postupne rozširovala svoje funkcionality a dnes je možné ju považovať za komplexný on-line účtovný systém.

SuperFaktúra.sk poskytuje široké spektrum funkcionalít pre vedenie účtovnej agendy. Obsahuje možnosť vytvárať jednorázové aj automaticky sa opakujúce faktúry, vytvárať cenové ponuky, dodacie listy. Ďalej je tu evidencia došlých faktúr, takže služba ponúka aj systém pre sledovanie firemných nákladov. Ďalšou funkcionalitou je evidencia kontaktov odberateľov aj dodávateľov, s ktorými firma spolupracuje. Tieto údaje sú používané pri vytváraní faktúr, nie je teda potrebné zadávať fakturačné údaje pre každú faktúru, stačí len vybrať firmu zo zoznamu kontaktov. Medzi ďalšie funkcionality patrí možnosť predvyplnenia daňového priznania, evidencia skladu a evidencia bankových výpisov. Veľkou výhodou SuperFaktúry je tiež možnosť exportu dát pre rozne účtovné softvéry. SuperFaktúra tiež ponúka svoje API, vďaka čomu je možné ju jednoducho prepojiť napríklad s internetovým obchodom, či inou webovou aplikáciou. Webová aplikácia SuperFaktúry neponúka verziu prispôbenú pre mobilné zariadenia.

Služba SuperFaktúra.sk je spoplatnená na mesačnej báze, ponúka na výber z troch úrovní predplatného, ktoré sa líšia v množstve dostupných funkcionalít. Základný balík stojí 4,10€ mesačne, najvyšší balík zahŕňajúci všetky dostupné funkcionality je spoplatnený sumou 12,40€ mesačne. SuperFaktúru možno považovať za veľmi vyspelý, on-line účtovný systém, ktorý okrem vytvárania a evidencie faktúr ponúka široké spektrum ďalších funkcionalít, čím sa z neho stáva takmer plnohodnotný účtovný softvér.



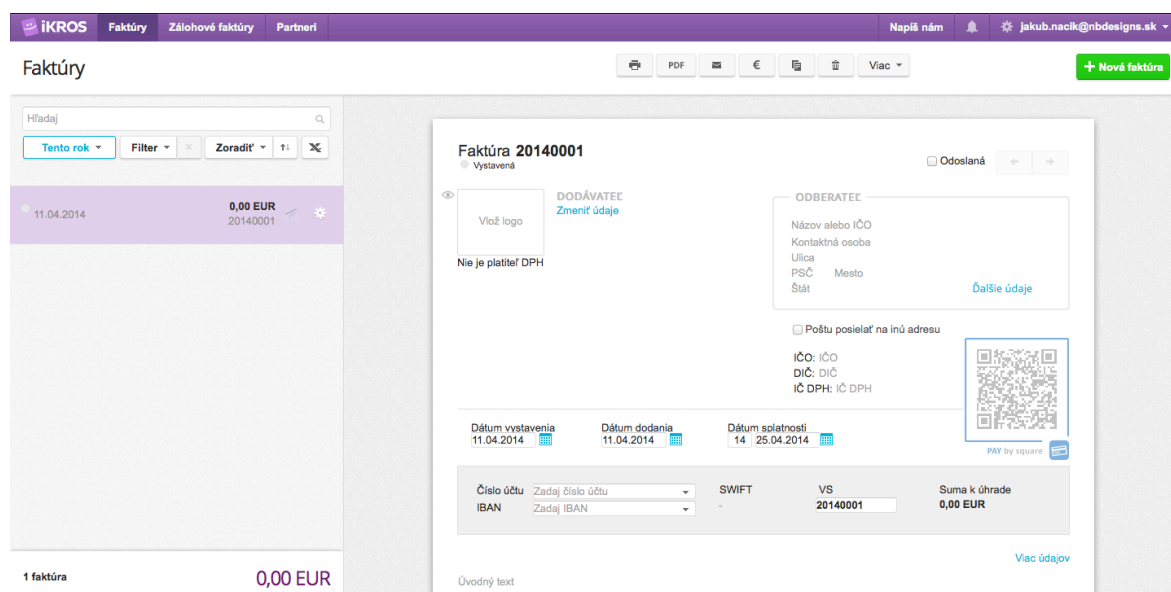
Obrázok 1. Náhľad GUI SuperFaktúra.sk

2.2 iKros.sk

Webová aplikácia iKros.sk je produkt spoločnosti KROS, a.s., ktorá sa zaoberá tvorbou ekonomických a účtovných softvérov. Popri svojej hlavnej činnosti ponúkajú klientom aj službu iKros.sk, ktorá je on-line fakturačným systémom. iKros.sk môžeme považovať za jednoduchý systém, zameraný primárne na samotnú tvorbu a evidenciu faktúr, bez pokročilých možností ostatnej účtovnej evidencie. Tvorba faktúry je vyriešená formulárom zobrazeným priamo na stránke faktúry, takže užívateľ vyplňa jednotlivé dáta presne na tom mieste, kde budú zobrazené vo výstupnom PDF. iKros ponúka možnosť faktúry tlačiť, filtrovať a kopírovať. V systéme však absentuje možnosť automatickej tvorby opakujúcich sa faktúr, chýba tiež možnosť exportu dát pre účely prenosu do iných systémov a iKros neponúka ani verziu pre mobilné zariadenia.

Fakturačný systém iKros.sk je bezplatným čo je jeho výhoda, no svojou obmedzenou funkcionalitou je vhodný len pre veľmi nenáročných užívateľov, ktorí

hľadajú nástroj na vystavovanie faktúr, bez možnosti použiť systém na pokročilejšiu evidenciu účtovných dát.



Obrázok 2. Náhľad GUI iKros.sk

2.3 Faktúry-online.com

Webová aplikácia Faktúry-online.com je produktom vývojára Mgr. Jozefa Vacvala. Táto aplikácia je podobne ako iKros.sk zameraná primárne na samotný proces vytvorenia faktúry a jej následného uloženia vo formáte PDF.

Okrem vytvárania faktúr ponúka aj možnosť vytvárať rôzne ďalšie účtovné tlačivá ako napríklad príjmové pokladničné doklady. Služba ponúka taktiež evidenciu odberateľov, základné štatistiky, posielanie faktúr e-mailom. Je tu aj možnosť exportu dát do formátu MS Excel, no chýba možnosť exportu pre jednotlivé účtovné softvéry alebo do štandardného prenosového formátu. GUI webovej aplikácie je prispôbené pre mobilné zariadenia. Webová aplikácia disponuje podobne ako SuperFaktúra.sk aj API rozhraním, ktoré umožňuje ju jednoducho prepojiť s inými aplikáciami, ktoré potrebujú využívať služby elektronickej fakturácie.

Faktúry-online je možné využívať bezplatne v prípade, že počet firemných dokladov nepresiahne za posledných 12 mesiacov počet 60. Po presiahnutí tohto počtu je potrebné prejsť na platenú verziu aplikácie, ktorej cena je na úrovni 30€ ročne.

Faktúry online

DOKUMENTY - ZOZNAMY - INFO - KONTAKT Odhlásiť sa

Účtovníctvo Štatistika EmailLog JakubTN (Mój profil)

Faktúry

Zoznam faktúr

Voľba novej faktúry

Dodávateľ: všetcí
 Hľadať:

Odberateľ: všetcí
 Uhradené: ---

Rok: ---
 Zobraziť sumy s DPH
 Vynechať zálohové

Radkov: 25

| | Číslo f. | Dodávateľ | Odberateľ | Suma | Dátum vystavenia | Dátum splatnosti | Možnosti |
|--------------------------|----------|-------------------|--------------|----------|------------------|------------------|----------|
| <input type="checkbox"/> | 2014004 | NBdesigns, s.r.o. | Test, s.r.o. | 300 EUR | 19.04.2014 | 04.05.2014 | |
| <input type="checkbox"/> | 2014003 | NBdesigns, s.r.o. | Test, s.r.o. | 2500 EUR | 19.04.2014 | 04.05.2014 | |
| <input type="checkbox"/> | 2014002 | NBdesigns, s.r.o. | Test, s.r.o. | 600 EUR | 19.04.2014 | 04.05.2014 | |
| <input type="checkbox"/> | 2014001 | NBdesigns, s.r.o. | Test, s.r.o. | 1250 EUR | 19.04.2014 | 04.05.2014 | |

Účtovníctvo | Faktúry online API | Cenník | Otázky a odpovede | Podmienky používania | Kontakt

Sledujte novinky na Facebooku

© 2014 Faktúry online, všetky práva vyhradené

Obrázok 3. Náhľad GUI Faktúry-online.com

3 ŠTANDARDNÉ PRENOSOVÉ FORMÁTY ÚČTOVNÝCH DÁT

Nevyhnutnou súčasťou fakturačného systému musí byť možnosť prepojiť ho s inými ekonomickými a účtovnými softvérmi a umožniť tak vzájomný prenos účtovných dát. Možnosť ako exportovať dáta z fakturačného systému je niekoľko. Každý ekonomický softvér disponuje možnosťou importovať dáta v určitom formáte, prispôsobenom pre daný softvér. Medzi najpoužívané formáty pri prenosoch dát patria TXT, CSV alebo XML.

Aby sa predišlo nutnosti prispôbovať štruktúru exportného súboru individuálne pre každý ekonomický softvér, existuje niekoľko štandardných prenosových formátov, ktoré definujú spoločné pravidlá pre štruktúru súborov pre jednotlivé typy účtovných dát ako sú faktúry, objednávky, karty zákazníka a iné. Vývojári ekonomických softvérov majú možnosť implementovať import alebo export s podporou niektorého zo štandardných prenosových formátov a zvýšiť tak šancu na prenositeľnosť dát medzi svojím softvérom a softvérmi tretích strán.

3.1 EDI

EDI alebo tiež Electronic data interchange je elektronický komunikačný systém, ktorý definuje štandardy pre elektronickú výmenu dát, vďaka ktorým je možné vymieňať elektronické dokumenty ako sú objednávky, faktúry, dodacie listy a mnohé ďalšie naprieč rôznymi krajinami a obchodnými spoločnosťami. [5]

V roku 1996 Národný Inštitút pre Štandardy a Technológie v USA definoval elektronickú výmenu dát ako komunikáciu medzi dvomi počítačmi formou striktné formátovaných správ, ktoré reprezentujú jednotlivé dokumenty v rámci obchodného styku, pričom dáta môžu byť prenášané buď pomocou telekomunikačnej techniky alebo na elektronickom úložnom médiu. [5]

Elektronická výmena dát by nemala slúžiť len ako úspora času a financií, ale taktiež ako nástroj pre uľahčenie, zefektívnenie a zníženie chybovosti v komunikácii medzi obchodnými partnermi. V praxi však dochádza ku komplikáciám pri implementovaní štandardných formátov v rôznych obchodných odvetviach a platformách, nakoľko žiadny zo súčasných EDI štandardov neumožňuje urobiť určité individuálne prispôbenie pre potreby danej spoločnosti.

3.1.1 ASC X12

Jedným zo štandardov EDI je ASC X12, ktorý bol vyvinutý v American National Standards Institute v roku 1979 ako štandard pre národnú aj medzinárodnú elektronickú výmenu dát. V súčasnosti ASC X12 obsahuje viac ako 315 štandardov pre rôzne druhy dokumentov a stále pribúdajú ďalšie. ASC X12 zastrešuje výbor s názvom Accredited Standards Committee, ktorého členov tvoria zástupcovia spoločností z rôznych obchodných oblastí v rámci celého sveta. Členovia výboru ASC X12 sa stretávajú 3 krát ročne. [6]

Formát ASC X12 je založený na princípe kódov, oddelovačov a riadkov. Pre každý údaj na danom type dokumentu je pridelený jeden 2 – 3 miestny kód, ktorý môže obsahovať číslice aj písmená. Každý dokument je označený kódom ST na prvom riadku, ktorý označuje Transaction Set ID. Za týmto riadkom nasledujú všetky ďalšie údaje prislúchajúce danému dokumentu. Na jednom riadku môže byť uvedených aj viacero kódov, ktoré dopĺňajú označenie konkrétnej položky na danom riadku. Tieto kódy a ďalšie hodnoty su oddelené znakom *.

Príklad štruktúry prenosového súboru faktúry v ASC X12:

```
ST*810*0001
BIG*20140103*1081427260

CUR*SE*EUR
N1*SE*NÁZOV DODÁVATEĽA*1*12345678
N3*ULICA

N4*MESTO*SK*91101
N1*BT*NÁZOV ODBERATEĽA
N3*ULICA

N4*MESTO*SK*91101
IT1*1

PID*F***NÁZOV POLOŽKY

SAC*C*D340***15.00

TDS*15.00

PID*F***ĎAKUJEME ZA VÁŠ NÁKUP
```

3.1.2 UBL

Universal Business Language je ďalším zo štandardov EDI, ktorý definuje štruktúru elektronických obchodných dokumentov. UBL bolo vyvinuté organizáciou OASIS a jeho prvá verzia 1.0 bola dostupná v roku 2004. V súčasnosti je aktuálna dostupná verzia 2.1 uvoľnená v roku 2013. [7]

Formát UBL používa pre svoje prenosové súbory bežné štandardy XML a obsahuje schémy pre 31 typov obchodných dokumentov. Vďaka použitiu XML je štruktúra UBL súborov prehľadná a zrozumiteľná aj v ľudskej forme. Jednotlivé údaje z dokumentov sú uzavreté každý vo svojom vlastnom XML elemente. Celá jedna faktúra je potom označená elementom Invoice.

Príklad štruktúry prenosového súboru v štandarde UBL:

```
<Invoice>
  <cbc:UBLVersionID>2.1</cbc:UBLVersionID>
  <cbc:ID>14001</cbc:ID>
  <cbc:TaxPointDate>20014-01-03</cbc:TaxPointDate>
  <cac:AccountingSupplierParty>
    ...
  </cac:AccountingSupplierParty>
  <cac:AccountingCustomerParty>
    ...
  </cac:AccountingCustomerParty>
  <cac:InvoiceLine>
    <cac:Item>
      ...
    </cac:Item>
  </cac:InvoiceLine>
</Invoice>
```

3.1.3 EDIFACT

Prenosový štandard EDIFACT bol vyvinutý pod hlavičkou Organizácie Spojených Národov ako prenosový formát pre elektronickú výmenu dát v oblasti administratívy, obchodu a dopravy. Štandard vznikol v roku 1987 a jeho syntax bola schválená ako norma ISO 9735. [8]

Svojou štruktúrou EDIFACT vychádza z ASC X12, no zatiaľ čo ASC X12 je používaný hlavne v USA, EDIFACT sa vďaka OSN rozšíril do celého sveta. EDIFACT taktiež používa pre jednotlivé údaje kódové označenia a oddelovače spolu s riadkami. EDIFACT má hierarchickú štruktúru, kde najvyššia úroveň označuje o aký typ výmeny dát sa jedná a nižšie úrovne obsahujú jednotlivé prenášané správy, ktoré sa skladajú zo segmentov, pričom je možné označiť, ktorý segment je povinný a ktorý voliteľný.

Ukážka štruktúry prenosového súboru v EDIFACT:

```
UNB+UNOB:1+102096559TEST:16:ZZUK+PARTNERID:01:ZZUK+071101
1++INVOIC++1++1
UNH+509010117+INVOIC:D:97A:UN
BGM+380:::TAX INVOICE+0013550417+9
DTM+3:20070926:102
DTM+4:20061123:102
RFF+ON:2080943S
RFF+VN:3474552
RFF+UC:22233221
RFF+AGE:33445312
NAD+II+0000343810::91++Názov Firmy.:Ulica+Mesto++D24+IE
NAD+BY+0000138978::91++PARTNER LIMITED+MAIN
DRIVE:WYMBUSH+MILTON KEYNES++MK8 8DF+GB
NAD+IV+0000343810::91++PARTNER LIMITED:C/O CAP IM
COORDINATION CENTER:CENTRAL ACCOUNTS PAYABLE+MAIN
DRIVE:WYMBUSH-MILTON KEYNES+BUCKINGHAMSHIRE++MK8 8DF+GB
RFF+VA:GB440355280
TAX+7+VAT+++:::10072.14+S
NAD+PL+0000343810::91++PARTNER LIMITED:C/O CAP IM
COORDINATION CENTER:CENTRAL ACCOUNTS PAYABLE+MAIN
```

4 TECHNOLOGIE PRE TVORBU KLIENT-SERVER APLIKÁCIÍ

Tvorba pokročilých klient-server aplikácií vyžaduje prepojenie niekoľkých druhov technológií na jednom mieste. Dnešné webové aplikácie sa nezaobídu bez technológií, vďaka ktorým je možné docieľiť vykreslenie užívateľského rozhrania optimalizovaného pre mobilné zariadenia, či vytváranie pokročilých funkcií na pozadí aplikácie. Na jednom mieste sa tak stretáva niekoľko vývojových jazykov a množstvo podporných knižníc.

4.1 HTML

HTML (HyperText Markup Language) je hlavným značkovacím jazykom webových stránok. Jazyk HTML tvoria značky - elementy, ktoré sa zapisujú v tvare ostrých zátvoriek - napríklad `<html>`, v rámci ktorých je definovaný obsah webovej stránky. HTML tvoria prevažne párové značky – napríklad `<div> </div>`, poznáme ale aj nepárové značky - napríklad ``. [9]

Zdrojové súbory webových stránok napísané v HTML sa ukladajú s príponou `.html`. Úlohou webového prehliadača je HTML súbor prečítať a uvedené značky interpretovať do vizuálnej podoby webovej stránky.

HTML značky umožňujú vkladať do webových stránok textový či obrázkový materiál alebo vytvárať formuláre, ktoré môžu návštevníci stránky vyplňať priamo v prehliadači.

4.2 CSS

CSS (Cascading Style Sheets) je primárne navrhnuté na formátovanie dokumentu napísaného v HTML. Medzi najpoužívanejšie funkcie CSS patrí nastavovanie fontov, farieb, okrajov či pozadí. Pomocou CSS je možné taktiež špecifikovať pozície jednotlivým HTML elementom, čo umožňuje veľmi podrobne pracovať so štruktúrou webovej stránky. CSS taktiež umožňuje nastavovať HTML dokumentu rôzne vlastnosti podľa toho, v akej podobe je HTML dokument prezentovaný. Môžeme teda upraviť jeho vzhľad ak ide dokument do tlače alebo je zobrazovaný na monitore s malým rozlíšením. [9]

4.3 PHP

PHP (Hypertext Preprocessor) je univerzálny skriptovací jazyk, ktorý sa na rozdiel od HTML a CSS prekladá na strane webového servera a návštevníkovi stránky zobrazí už len výsledok v podobe bežného HTML výstupu. Ku koncovému užívateľovi sa teda vždy dostáva len konkrétny HTML výsledok, nie je možné vidieť syntax PHP skriptov cez webový prehliadač.

PHP bolo navrhnuté pre vývoj dynamických webových aplikácií. Je jedným z prvých skriptovacích jazykov, ktoré je možné priamo vkladať do zdrojových kódov HTML dokumentov a vzkonávať tak najrôznejšie dynamické akcie (napríklad odosielanie vyplneného formuláru) priamo v konkrétnom dokumente, bez nutnosti volania externého súboru, ktorý by vykonal požadovanú operáciu. [1]

4.4 MySQL

MySQL je vo svete najpoužívanejší relačný databázový systém, postavený na báze Structured Query Language, ktorý je štandardizovaným a veľmi rozšíreným jazykom pre prístup k databázam.

MySQL databázy si našli svoje stabilné miesto hlavne pri tvorbe webových aplikácií, keďže umožňujú veľmi rýchlo a prehľadne ukladať aj veľké množstvá dát a následne s nimi pracovať. Dáta sú ukladané do tabuliek, pričom jeden záznam tvorí jeden riadok tabuľky. Medzi tabuľkami v MySQL databáze môžeme definovať rôzne vzťahy - relácie, na základne takzvaných kľúčov. [1]

4.5 PHP framework Nette

Framework je knižnica, ktorá slúži vývojárovi pre uľahčenie práce, odbúrava nutnosť písať opakovane ten istý kód a stará sa o niektoré rutinné činnosti v rámci aplikácie bez nutnosti zásahu programátora, takže výsledkom by mal byť rýchlejší a prehľadnejší vývoj aplikácie. Súčasťou frameworku môžu byť aj rôzne vývojové nástroje pre ladenie aplikácie, hľadanie a odstraňovanie chýb vznikutých pri vývoji.

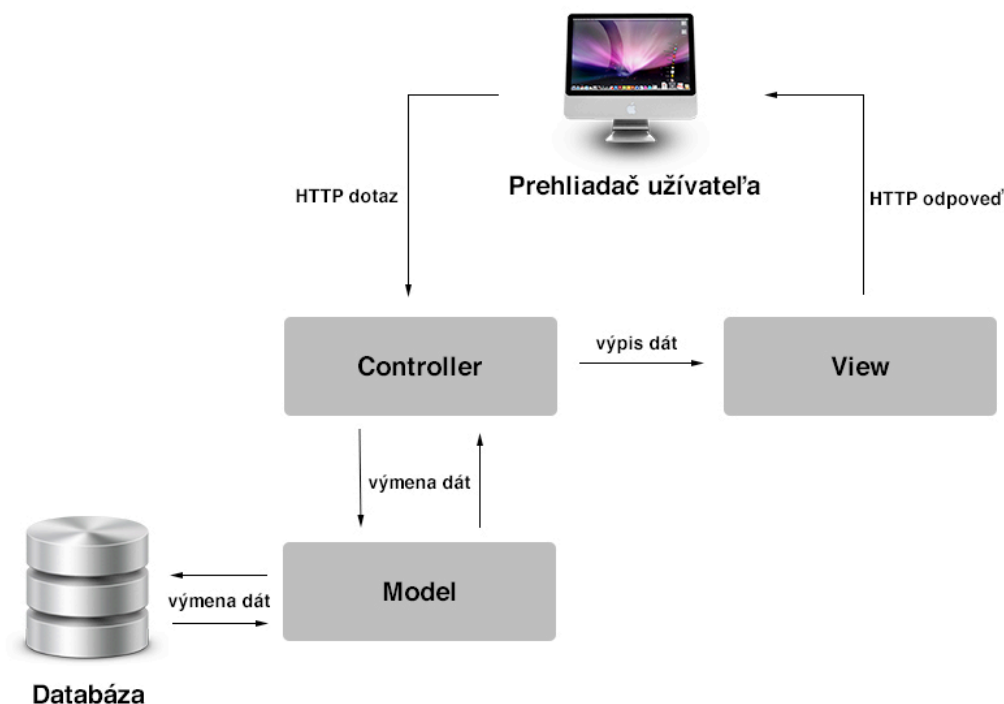
Medzi takéto frameworky patrí aj PHP framework Nette v aktuálnej verzii 2.1. šírený pod voľnou licenciou BSD. [10]

Nette framework plne využíva objektové PHP a MVC alebo Model-View-Controller architektúru aplikácie, kedy je aplikácia na pozadí rozdelená na 3 logické celky, z ktorých každý plní inú funkciu.

Model – tvorí funkčnú a dátovú časť webovej aplikácie, slúži najmä na prácu s dátami, ktoré sú uložené napríklad v MySQL databáze.

View – tvorí výstup aplikácie vo webovom prehliadači vo forme vygenerovaného HTML kódu.

Controller – nazývaný aj *Presenter* riadi priamy chod aplikácie, spracováva jednotlivé HTTP požiadavky, komunikuje s modelom aj s view.



Obrázok 4. Schéma MVC architektúry.

4.6 Front-end framework Bootstrap

Ako bolo spomenuté v úvode tejto kapitoly, webové aplikácie spájajú na jednom mieste niekoľko rôznych technológií. Oproti frameworku Nette, ktorý tvorí základ pre funkčnosť systému na pozadí a je prekladaný na strane webového servera, tvorí front-end

framework Bootstrap základ pre grafický výstup z webovej aplikácie v podobe HTML, CSS a JavaScriptu v prehliadači užívateľa webovej aplikácie.

Bootstrap obsahuje široký súbor predpripravených HTML elementov, nastavení typografie či JavaScriptových komponent, ktoré umožňujú jednoducho a rýchlo vytvárať grafické užívateľské rozhranie webovej aplikácie, ktoré je výborne optimalizované pre široké spektrum prehliadačov či už z hľadiska správnosti zobrazovania jednotlivých HTML elementov, ale aj z hľadiska optimalizácie rýchlosti vykresľovania stránky v prehliadači.

Bootstrap je navyše vytvorený technológiou mobile-first, je plne responzívny a prispôsobený pre tvorbu GUI optimalizovaného na mobilné zariadenia (viac v kapitole 5).

Aktuálne je Bootstrap dostupný vo verzii 3.1.1, šírený pod licenciou MIT. [11]

5 ADAPTÁCIA GUI PRE MOBILNÉ ZARIADENIA

Podľa portálu statcounter.com tvorili mobilné zariadenia v marci 2014 takmer 30% návštevnosti internetových stránok. Trend smartphonov a tabletov je v súčasnosti stále na vzostupe a množstvo používateľov týchto zariadení rastie. Ich cenová dostupnosť a ľahká prenosnosť vďaka kompaktným rozmerom z nich tvoria každodennú súčasť života mnohých ľudí, ktorých tieto zariadenia sprevádzajú doslova všade.

Kombinácia týchto skutočností vyústila v trend adaptácie užívateľských rozhraní webových aplikácií pre mobilné zariadenia, známy aj pod pojmom *responzívny web*. Jedná sa o postup, kedy je užívateľské rozhranie vytvorené v niekoľkých verziách, prispôbených pre rôzne šírky displejov zariadení, na ktorých sa webová aplikácia zobrazuje. Najčastejšie sa v responzívnom webe odlišujú 4 verzie rozhrania – pre mobilné zariadenia, pre tablety, pre bežné monitory a pre nadštandardne veľké monitory. Cieľom tejto technológie tvorby webových užívateľských rozhraní je docieľiť pre užívateľa maximálny komfort pri ovládaní aplikácie vzhľadom na zobrazovacie možnosti na zariadení, cez ktoré k aplikácii pristupuje.



Obrázok 5. Ukážka princípu responzívneho GUI [15].

Nosným prvkom adaptácie užívateľského rozhrania je CSS a konkrétne jeho funkcionálna *media query*, ktorú CSS prinieslo vo verzii CSS3. [3] Media query umožňuje špecifikovať rôzne vlastnosti jednej triedy v kaskádovom štýle na základe šírky displeja, na

ktorom sa aplikácia s načítaným kaskádovým štýlom práve nachádza. V CSS súbore tak stačí špecifikovať každej triede všetky základné atribúty a následne pomocou media query upraviť odlišnosti pre jednotlivé rozlíšenia obrazoviek.

Ukážka použitia media query v CSS:

Základná definícia CSS triedy, spoločná pre všetky rozlíšenia:

```
.text {  
    font-size: 16px;  
    color: #000000;  
}
```

A následná úprava pre s rozlíšením 1200 pixelov a viac:

```
@media (min-width: 1200px) {  
    .text {  
        font-size: 18px;  
    }  
}
```

V praxi však pre dosiahnutie plne responzívneho a hlavne užívateľsky prívetivého rozhrania použitie samotných media queries nestačí. Ich nevýhodou je slabšia podpora v starších verziách prehliadačov, hlavne Internet Explorer. Túto podporu je možné v prehliadači navodiť použitím rôznych podporných skriptov v JavaScripte, vďaka ktorým je možné využiť media query aj v starších prehliadačoch. Ďalej sa JavaScript používa aj pre dosiahnutie lepšej užívateľskej prívetivosti rozhrania, pri rôznych dynamicky sa zobrazujúcich prvkoch aplikácie.

Pri tvorbe responzívneho užívateľského rozhrania existuje niekoľko pracovných postupov, ako môže vývojár pristupovať k tejto problematike. Medzi najrozšírenejšie metódy patrí takzvaná *mobile first* metóda, kedy je celý proces užívateľského rozhrania webovej aplikácie vedený od displejov s nízkym rozlíšením – mobilné zariadenia, po displeje s nadštandardným rozlíšením – veľké HD monitory. Či už tvorba grafického návrhu alebo samotného CSS kódu začína od mobilnej verzie. V CSS súbore sú teda všetky triedy v sekcii bez media query definované pre mobilné zariadenia a následným

pridávaním príslušných media query sekcií do CSS súboru sa špecifikujú nastavenia tried pre rozne typy rozlíšení smerom od najmenších po najväčšie.

Okrem prispôsobovania štýlu HTML elementov vzhľadom na šírku displeja, umožňujú media queries detekovať napríklad displeje s vysokým zobrazovacím DPI, známe pod skratkou HiRes. V takomto prípade sa v rámci media query uvádzajú nastavenia hlavne pre elementy, ktoré využívajú nejaké obrázky, kde sa definuje použitie verzie obrázka s dvojnásobným rozlíšením.

Ukážka CSS kódu pre HiRes displeje:

```
@media (-webkit-min-device-pixel-ratio: 2), (min-resolution:
192dpi) {
    .icon {
        background-image: url(../images/ico_@2x.png);
        background-size: 14px 14px;
    }
}
```

6 BEZPEČNOST WEBOVÝCH APLIKÁCIÍ

Správy o rôznych úspešných či neúspešných webových útokoch sa k nám dostávajú čoraz častejšie. Najviac rezonujú úspešné útoky na svetoznáme internetové giganty. Jedným z posledných úspešných útokov bol na spoločnosť Adobe, kedy došlo k úniku užívateľských dát pre milióny užívateľských účtov. Známe sú tiež útoky rôznych hackerských skupín na webové stránky vládnych organizácií alebo politických strán.

V tejto kapitole sú popísané najbežnejšie útoky na webové aplikácie.

6.1 SQL Injection

Jeden z najčastejších útokov na webové aplikácie, ktorý je akýmsi nosným typom útokov na webové aplikácie. Napriek tomu, že obrana proti tomuto útoku je v skutku veľmi jednoduchá, stretávame sa s ním pomerne pravidelne. Tento útok veľmi nebezpečný, nakoľko útočník je schopný behom niekoľkých sekúnd získať plnú kontrolu nad databázou webovej aplikácie.

Útok spočíva v zneužití neošetrených formulárových vstupov vo webovej aplikácii. Útočník vloží do formulárového vstupu, ktorý priamo pracuje s databázou webovej aplikácie, určitý reťazec, ktorým sa snaží upraviť SQL dotaz na databázu, s ktorým pracuje webová aplikácia a získať tak kontrolu nad samotnou databázou. Útočník je takto schopný dostať sa nielen k samotným dátam, ale aj s nimi pracovať, meniť ich alebo dokonca celú databázu zmazať. [12]

Účinná obrana pred SQL Injection spočíva v takzvanom escapovaní hodnôt, ktoré sú do aplikácie posielané cez formulárové vstupy. Escapovanie znamená, že reťazec, ktorý je odoslaný cez formulár webovej aplikácie prejde funkciou, ktorá ošetrí všetky nebezpečné znaky, ktoré môže reťazec obsahovať a ktoré by mohli svojou prítomnosťou v reťazci pozmeniť dotaz do databázy.

6.2 Cross-Site-Scripting

Tento typ útoku býva vývojármi webových aplikácií často veľmi podceňovaný, pritom ide o veľmi nebezpečný typ útoku, ktorý je síce často prezentovaný ako nástroj na rozbitie layoutu webovej aplikácie, pritom však dokáže napríklad ukradnúť z prehliadača návštevníka, ktorý napadnutú webovú aplikáciu zobrazí, citlivé dáta o prihlásení a odoslať

ich k útočníkovi, takže je útočník schopný pristúpiť k danej webovej aplikácii ako prihlásený užívateľ, ktorému boli dáta z prehliadača odcudzené.

Princíp akým sa útok vykonáva je takmer totožný s SQL Injection, kedy útočník taktiež využíva neošetrené formulárové vstupy webovej aplikácie, cez ktoré odošle škodlivý kód napísaný napríklad v JavaScripte. Tento kód sa uloží do databázy a v mieste, kde sa konkrétne dáta z databázy vypisujú na obrazovku užívateľovi dôjde k interpretovaniu tohto kódu prehliadačom. [13]

XSS útok využíva okrem neošetrených formulárových vstupov aj neošetrené výstupy v HTML šablónach, ktoré tak umožňujú, aby sa dáta z databázy bez akéhokoľvek obmedzenia zobrazili v HTML šablóne a teda v prípade, ak tieto dáta obsahujú napríklad škodlivý JavaScript, tento sa aj vykonal v prehliadači návštevníka, ktorému sa tieto dáta vypisujú do prehliadača.

Účinná obrana pred XSS útokom spočíva jednak vo validácii a escapovaní formulárových vstupov a dát, ktoré sa ukladajú do databázy, ale hlavne v escapovaní vypisovaných dát v HTML šablónach.

6.3 Cross-Site Request Forgery (CSRF)

Tento typ útoku je založený na podvrhovaní požiadavkov medzi rôznymi stránkami. K tomuto útoku je využívaný samotný užívateľ webovej aplikácie častokrát tak, že o tom vôbec nevie. Stačí, že normálne pracuje s webovou aplikáciou a nevedomky tak na pozadí vykonáva škodlivé požiadavky, ktoré môžu mať za následok manipuláciu s dátami, ich zmazanie alebo odosielanie na neautorizované miesta. Pri tomto útoku dochádza k zneužitiu HTTP požiadavkov GET alebo POST. [13]

Častým prípadom zneužitia je napríklad vloženie škodlivej URL adresy do HTML tagu a takýto tag vložiť napríklad niekam na vysoko navštevovaný portál či diskusné fórum.

Pred CSRF je najúčinnnejšou obranou vkladanie kontrolného tokenu ako hodnotu skrytého poľa vo formulároch. Tento token je náhodne vygenerovaný reťazec, uložený v session a vložený do formulára. Po odoslaní formuláru sa vykoná kontrola, či token odoslaný zo skrytého poľa formuláru súhlasí s tým, ktorý je uložený v session. Podľa toho je možné identifikovať, či je odosielaný formulár skutočne odoslaný z našej webovej aplikácie alebo je podstrčený z tretej strany.

6.4 Insecure cryptographic storage

Tento typ bezpečnostného rizika je opäť pomerne rozšírený a aj napriek veľkému množstvu informácií a varovaní či už v odbornej literatúre alebo na odborných portáloch sa s ním stretávame stále veľmi často. Jedná sa o problematiku ukladania citlivých dát v databáze webovej aplikácie. Medzi takéto dáta patria napríklad heslá k užívateľským účtom. Riziko vzniká, keď programátor webovej aplikácie neošetrí ukladanie týchto dát v dostatočne šifrovanej podobe, prípadne keď ich ukladá čisto v textovej podobe.

V prípade nežiadaneho úniku dát z databázy má tak útočník, ktorý ich získal kompletný prístup k všetkým používateľským kontám. Toto riziko má však ďaleko rozsiahlejšie dopady. Veľkým problémom je zvyk laických užívateľov internetu, používať jedno rovnaké heslo pre všetky svoje internetové účty a dokonca aj pre e-mailovú schránku. Takto môže aj zjavne nepatrný únik citlivých dát spôsobiť komplikácie v oveľa širšom spektre, než sa na prvý pohľad môže zdať.

Účinnou a opäť pomerne jednoduchou obranou je ukladať citlivé dáta vo forme hashu použitím dostatočne silnej hashovacej funkcie akými su napríklad šifra SHA-512 alebo šifra Blowfish. V PHP máme k dispozícii funkciu *crypt()*, ktorá dokáže pracovať s viacerými šifrovacími algoritmami podľa toho, ako sú dostupné na danom operačnom systéme.

6.5 Brute-force attack

V preklade známy ako útok hrubou silou, spočíva v snahe o prelomenie prihlasovacích údajov do webovej aplikácie formou skúšania veľkého množstva kombinácií veľmi rýchlo za sebou. Týmto typom útoku je pomerne jednoduché odhaliť slabé používateľské heslá do webovej aplikácie a získať tak prístup do užívateľských účtov.

Pred týmto útokom je možné nepriamo sa brániť už v momente vytvárania nového užívateľského konta, kedy užívateľa vedieme k tomu, aby si vytvoril dostatočne dlhé a bezpečené heslo.

Priama obrana spočíva napríklad v obmedzení počtu neúspešných pokusov o prihlásenie sa, kedy po určitom počte dôjde k zablokovaniu používateľského konta, kedy je

například uživateli zaslaný overovací kód formou e-mailu a tento je potřeba zadat spolu s přihlasovacími údaji.

Využívá se také captcha, která se zobrazí když počet neúspěšných přihášení překročí stanovenou hranici a zabrání tak robotickému skúšaníu přihlasovacích údajov.

Medzi jednoduchšie formy obrany patrí například "uspanie" aplikácie na niekoľko sekúnd v prípade neúspešného pokusu o prihlásenie. V PHP je možné využiť funkciu *sleep()*. To má za následok výrazné spomalenie celého procesu skúšania kombinácií přihlasovacích údajov a zníženie pravdepodobnosti jeho úspešnosti.

II. PRAKTICKÁ ČASŤ

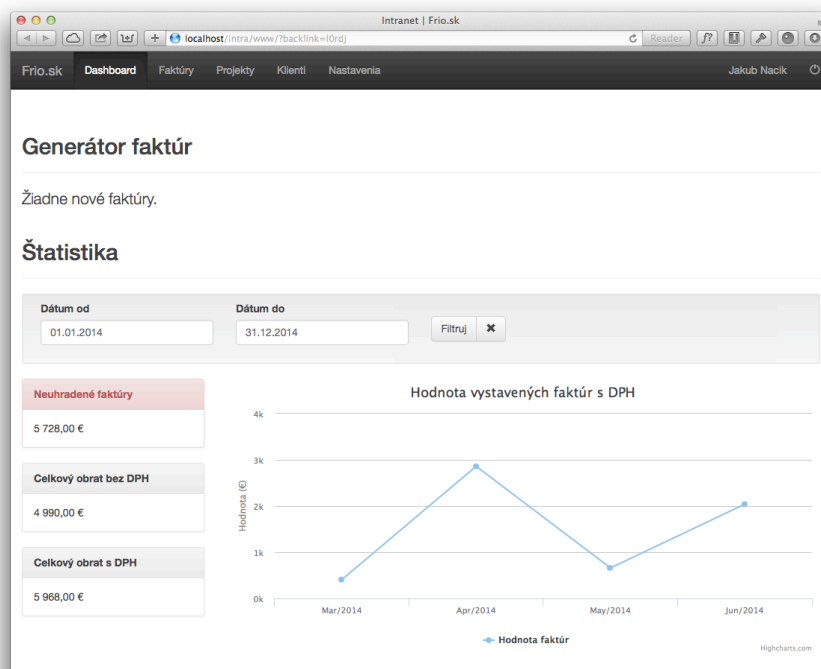
7 ŠTRUKTÚRA SYSTÉMU

Fakturačný systém bol navrhutý s dôrazom kladeným na dobrú užívateľskú prívetivosť, prehľadnosť rozhrania a jednoduchosť ovládania. Celý systém je členený na niekoľko logických celkov, z ktorých každý slúži na správu a prácu s údajmi z daného celku. Ovládanie systému je riešené pomocou hlavnej navigačnej lišty, ktorá ma pevnú pozíciu na hornom okraji obrazovky a je tak dostupná vždy aj v prípade, že užívateľ sa nachádza v spodnej časti podstránky s dlhým obsahom. V niektorých sekciách sa nachádza statický bočný panel, ktorý je taktiež užívateľovi dostupný vždy, bez ohľadu na polohu v rámci podstránky. Ďalej si popíšeme jednotlivé sekcie systému.

7.1 Dashboard

Po prihlásení do systému sa užívateľ dostáva na východziu obrazovku, ktorej hlavnou úlohou je ihneď po prihlásení informovať užívateľa o aktuálnom stave systému a jednotlivých fakturačných dát v ňom.

Dashboard obsahuje prehľad automaticky vygenerovaných faktúr, ktoré pred odoslaním zákazníkovi musia prejsť schválením povereného pracovníka. Pre užívateľa sú tu zobrazené aj základné štatistické údaje, ktoré poskytnú jasnú informáciu o aktuálnom vývoji cashflow firmy. Graf zobrazuje trend hodnoty vystavených faktúr za jednotlivé mesiace, je tu zobrazená aj celková suma všetkých faktúr spolu s celkovou sumou neuhradených faktúr, ktorá vypovedá o predpokladaných príjmoch firmy, ktoré by mali byť dostupné v krátkom čase.



Obrázok 6. Dashboard fakturačného systému.

7.2 Správa faktúr

Nosnou časťou fakturačného systému je určite sekcia pre správu faktúr. V tejto sekcii má užívateľ možnosť vykonávať všetky potrebné úkony s faktúrami a ich evidenciou. Už v základnom zobrazení zoznamu faktúr dostáva prehľadné informácie o aktuálnom stave faktúr, farebne sú vyznačené faktúry po lehote splatnosti. Navyše je tu možnosť faktúry filtrovať podľa dátumu vystavenia, podľa zákazníka pre ktorého sú určené, alebo podľa stavu úhrady.

V zozname faktúr sú pri každej faktúre umiestnené na pravej strane ovládacie prvky, pomocou ktorých má užívateľ možnosť vykonávať základné akcie s fakturami ako sú úprava, stiahnutie PDF súboru, zaznamenanie úhrady, zobrazenie detailu faktúry či úplné odstránenie faktúry zo systému.

| Číslo | Klient | Dátum vystavenia | Dátum splatnosti | Suma s DPH | Uhradená |
|----------|------------------------|------------------|----------------------|------------|----------|
| 20130006 | Partner Group, s.r.o. | 06.06.2014 | 19.06.2014 | 2 040,00 € | ✓ |
| 20130005 | PREMIUM OFFICE, s.r.o. | 05.05.2014 | 19.05.2014 | 660,00 € | ✓ |
| 20130003 | Test, s.r.o. | 27.04.2014 | 11.05.2014 (+5 dni) | 1 540,00 € | ✗ |
| 20130002 | PREMIUM OFFICE, s.r.o. | 07.04.2014 | 21.04.2014 | 240,00 € | ✓ |
| 20130001 | Partner Group, s.r.o. | 06.04.2014 | 20.04.2014 (-15 dni) | 1 080,00 € | ✗ |
| 20130004 | PREMIUM OFFICE, s.r.o. | 07.03.2014 | 13.05.2014 (+7 dni) | 408,00 € | ✗ |

Obrázok 7. Zoznam faktúr.

7.2.1 Automatické generovanie faktúr

V praxi sa firmy pravidelne stretávajú so situáciami, kedy je potrebné poslať faktúry v rovnakej sume zákazníkom v pravidelných časových intervaloch. Bežne sa jedná hlavne o rôzne poplatky za správu a údržbu systémov, ale aj iné služby, ktorých platby sú dohodnuté na báze mesačného paušálu.

Z tohto dôvodu disponuje fakturačný systém možnosťou vybrané faktúry generovať automaticky v pravidelnom časovom intervale. Takúto faktúru teda stačí vystaviť iba raz, nastaviť jej interval opakovania a faktúra sa v tomto čase vygeneruje automaticky a zobrazí na Dashboarde systému, kde počká na potvrdenie pracovníkom. Ten ju môže potvrdiť jedným kliknutím a zároveň odoslať zákazníkovi na e-mail, bez nutnosti opätovne zadávať do faktúry všetky údaje. Firme tak odpadá nutnosť viesť evidenciu zákazníkov, s ktorými sú dohodnuté pravidelné paušálne platby, pravidelne ju sledovať a manuálne vytvárať faktúry.

Na to, aby mohla nejaká akcia vo webovej aplikácii prebehnúť, je potrebné vykonať príslušný skript. To nám umožňuje funkcia časovaného spúšťania skriptov s názvom CRON, ktorú obsahujú všetky unixové operačné systémy. Príkazy, ktoré má

CRON vykonať sa zapisujú do špeciálneho súboru zvaného *crontab*, ktorý ma predpísanú štruktúru a zvyčajne je umiestnený v systémovej zložke */etc*.

Ukážka crontab súboru pre fakturačný systém:

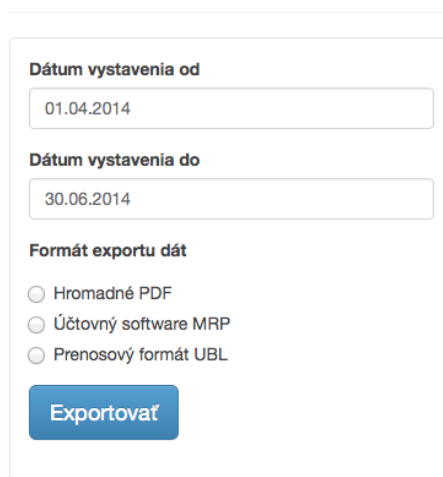
```
0 0 * * * php www/index.php app:generateinvoice
```

Uvedný zápis hovorí, že každý deň v týždni v čase 00:00 sa vykoná skript *index.php* s parametrom *app:generateinvoice*, ktorý v rámci aplikácie vykoná generovanie faktúr.

7.2.2 Export dát

Nevyhnutnou súčasťou fakturačného systému musí byť možnosť jednoducho exportovať účtovné dáta, ktoré systém obsahuje a prenášať ich tak do iných ekonomických softvérov a aplikácií.

Export dát



The screenshot shows a web form titled "Export dát". It contains two date input fields: "Dátum vystavenia od" (01.04.2014) and "Dátum vystavenia do" (30.06.2014). Below these is a section "Formát exportu dát" with three radio button options: "Hromadné PDF", "Účtovný software MRP", and "Prenosový formát UBL". A blue "Exportovať" button is at the bottom.

Obrázok 8. Rozhranie pre export dát.

Vo fakturačnom systéme som zvolil tri rôzne formáty pre export dát. Ako tlačový formát som zvolil PDF, takže užívateľ má možnosť vyfiltrovať si faktúry podľa dátumu vystavenia a exportovať ich do jedného viac stranového PDF dokumentu, ktorý je možné jednoducho vytlačiť. Ďalej som zvolil formát UBL ako jeden zo štandardných prenosových formátov, ktoré su popísané v kapitole 3 tejto práce. Poslednou možnosťou je export vo formáte TXT s upravenou štruktúrou pre účtovný softvér MRP, ktorý používa účtovná firma, s ktorou spolupracuje spoločnosť NBdesigns, s.r.o., pre ktorú bol fakturačný systém vyvíjaný.

7.2.3 Export do PDF

Pre export faktúr do formátu PDF využíva webová aplikácia open-source knižnicu PhantomJS. Knižnica PhantomJS je postavená na engine WebKit, ktorý používajú niektoré populárne webové prehliadače ako napríklad Google Chrome alebo Safari. PhantomJS je vo svojej podstate programovateľný webový prehliadač pre unixový terminál, ktorý nezobrazuje obsah webových stránok, iba ho spracuje na pozadí a vráti výstup. S PHP aplikáciou komunikuje PhantomJS pomocou jednoduchého PHP API.



Faktúra č. 20130006

| Dodávateľ | | Odberateľ | | | | |
|---|--------------------------|---|--------------------------|-------|----------|--------|
| NBdesigns, s.r.o. Palackeho 85/5 911 01, Trenčín Slovenska republika IČO: 44 699 166 DIČ: 2022789868 IČ DPH: SK2022789868 | | Partner Group, s.r.o. Nixbord 7 123 45, Levice Slovenska republika IČO: 12 345 678 DIČ: neuvedené IČ DPH: SK 2022 123 456 | | | | |
| Dátum vystavenia: | Dátum splatnosti: | Dátum dodania: | Daňová povinnosť: | | | |
| 06.06.2014 | 19.06.2014 | 05.06.2014 | 05.06.2014 | | | |
| Fakturujeme Vám | | | | | | |
| Názov položky | MJ | Počet MJ | Cena MJ | %DPH | DPH MJ | Celkom |
| nejaka položka | - | 1 | 1 700,00 € | 20,00 | 340,00 € | 2040 € |

Suma bez DPH: 1 700,00 €
Základ dane pre 20% DPH: 1 700,00 €
Základ dane pre 0% DPH: 0,00 €
DPH celkom: 340,00 €

Celkom k úhrade:
2 040,00 €

Dátum splatnosti: 19.06.2014

Variabilný symbol: 20130006
Konštantný symbol: 0308
Bankové spojenie: ČSOB, a.s.
Číslo účtu: 4007591761/7500
IBAN: SK4007591761/7500
SWIFT/BIC: CEKOSX

Obrázok 9. Ukážka faktúry v PDF exportovanom zo systému.

7.3 Správa projektov

Sekcia správy projektov v rámci fakturačného systému slúži pre evidenciu dohodnutých a rozpracovaných zákaziek s možnosťou poznačiť k zákazke predpokladaný rozpočet, zákazníka s ktorým je realizovaná a popis.

Hlavným cieľom tejto sekcie je ustrážiť zákazky, ktorých realizácia trvá dlhšie obdobie alebo je prípadne rozdelená na viacero etáp. Na tomto mieste je možné vidieť termíny jednotlivých projektov ako aj ich rozpočty, čo opäť pomáha firme strážiť svoj cashflow.

7.4 Správa zákazníkov

Dôležitou súčasťou fakturačného systému je správa zákazníkov. Fakturačný systém je svojím spôsobom aj CRM systém, preto by mal umožňovať jednoducho zobrazit' detail zákazníka a prehľad údajov týkajúcich sa tohto zákazníka, jeho faktúry, kontaktné osoby a ostatné súvisiace údaje.

K zákazníkovi patria aj kompletne fakturačné údaje, ktoré sa následne používajú pri vytváraní novej faktúry, kde nie je nutné zadávať tieto údaje pre každú faktúru zvlášť, ale ich načítanie prebehne automaticky.

7.5 Nastavenia

Sekcia nastavenia poskytuje pre firmu možnosť kedykoľvek upraviť základné nastavenia a údaje vo fakturačnom systéme, ktoré sa následne využívajú hlavne pri vytváraní faktúr, kde sú použité v samotných faktúrach. Medzi nastaveniami sú okrem kontaktných a fakturačných údajov aj nastavenia aktuálnej hodnoty DPH, nastavenia pre číselnú radu vytváraných faktúr alebo predvolený text e-mailu, ktorý je možné poslať priamo zo systému zákazníkovi s priloženou PDF faktúrou.

Pridruženou časťou nastavení systému je správa užívateľov, ktorá umožňuje vytvárať používateľské kontá s rônou úrovňou oprávnení pre pracovníkov firmy, ktorí budú môcť obsluhovať fakturačný systém.

Nastavenia

Fakturačné údaje Kontaktné údaje Bankové spojenie **Fakturácia** E-mail

Predčísle faktúr

Začiatok číselnej rady
Splatnosť faktúr (dni)
DPH (%)

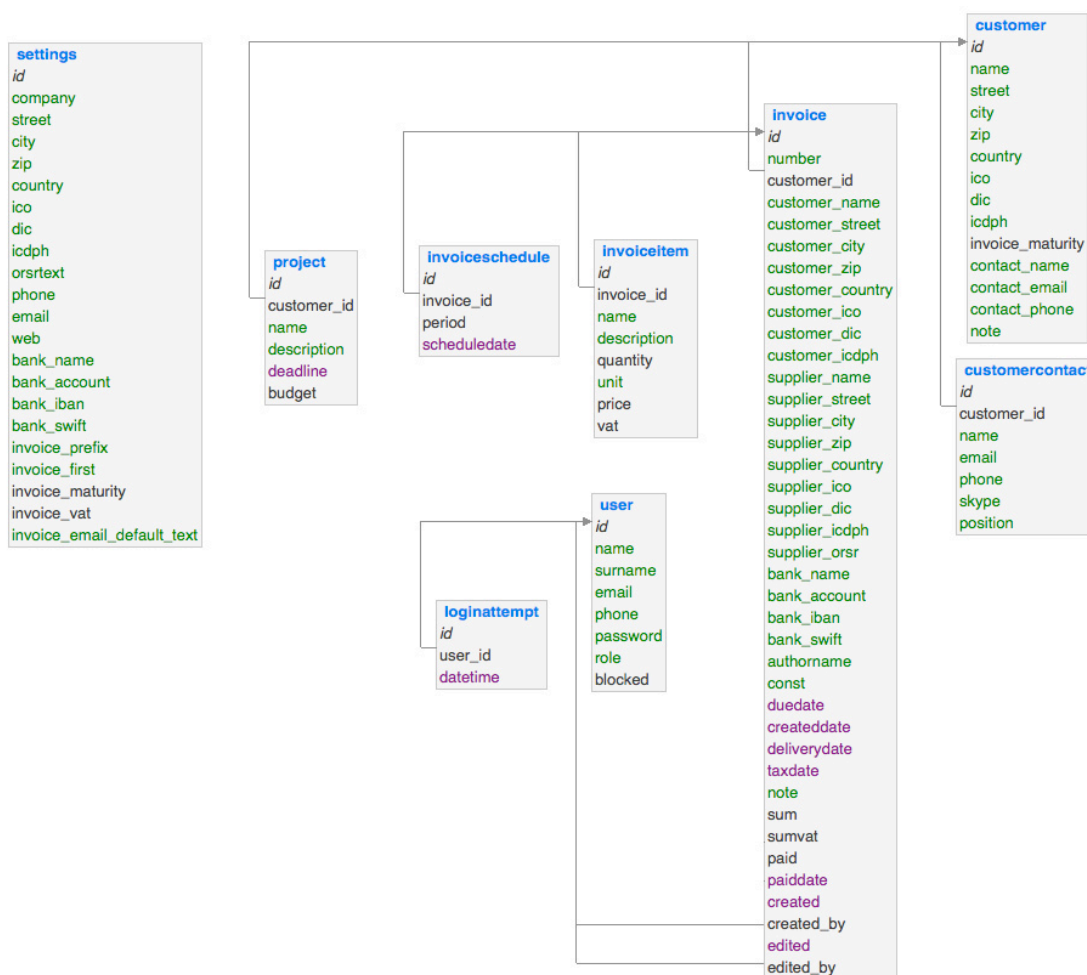
Uložiť nastavenia

Obrázok 10. Formulár s nastaveniami systému.

8 DATABÁZOVÁ ŠTRUKTÚRA

Neoddeliteľou súčasťou v procese tvorby webovej aplikácie je návrh databázovej štruktúry. Pri návrhu je potrebné dbať na správnu logiku usporiadania tabuliek, relácií medzi jednotlivými tabuľkami ako aj na správny výber dátových typov v jednotlivých stĺpcoch tabuliek. Dôležitosť správneho návrhu databázovej štruktúry sa s narastajúcim množstvom dát prejavuje oveľa zreteľnejšie, nakoľko v takom prípade môže chybné navrhnutá databázová štruktúra veľmi nepriaznivo ovplyvniť výkonnosť webovej aplikácie.

Fakturačný systém používa pre ukladanie dát databázu MySQL vo verzii 5.6. Hlavnou výhodou tejto databázy je jej veľké rozšírenie v oblasti webových aplikácií a to hlavne z dôvodu bezplatnej dostupnosti. Databáza fakturačného systému obsahuje 9 tabuliek a využíva databázový engine InnoDB, vďaka ktorému je možné medzi tabuľkami vytvárať relácie pomocou kľúčov - foreign keys.



Obrázok 11. Schéma databázovej štruktúry.

Databáza fakturačného systému vychádza z dvoch základných tabuliek *customer* a *invoice*. V týchto tabuľkách sa ukladajú základné dáta potrebné pre faktúry. V tabuľke *customer* sú to hlavne fakturačné údaje zákazníka - odberateľa, ktoré sú použité pri vytváraní faktúry. Tabuľka *invoice* naopak obsahuje dáta, potrebné pre vytvorenie hlavičky faktúry ako napríklad dátum vystavenia faktúry, dátum splatnosti a iné. Zároveň sa však v tabuľke *invoice* ukladajú pre každú faktúru fakturačné údaje ako odberateľa tak aj dodávateľa a to z dôvodu spätnej archivácie dát, nakoľko počas existencie fakturačného systému môže dôjsť k zmene údajov či už na strane odberateľa alebo dodávateľa, no údaje na archivovanej faktúre musia zostať rovnaké aké boli platné v čase jej vytvorenia.

K tabuľke *customer* sa cez cudzí kľúč viaže tabuľke *customercontact*, v ktorej sú uložené dáta používané pre vytváranie viacerých kontaktných osôb v rámci jednej firmy v systéme.

Tabuľka *invoice* ma dve podradené tabuľky *invoiceitem* a *invoiceschedule*, z ktorých *invoiceitem* slúži na ukladanie jednotlivých fakturovaných položiek na každej faktúre a v tabuľke *invoiceschedule* sa ukladajú dáta pre automatické generovanie opakujúcich sa faktúr.

Užívatelia, ktorí majú vytvorené svoje účty a môžu tak obsluhovať fakturačný systém sú uložený v tabuľke *user*. K tejto tabuľke sa viaže tabuľka *loginattempt*, kde sa ukladajú neúspešné pokusy o prihlásenie sa do systému pre užívateľa. Tieto dáta slúžia na ochranu pred útokom brute-force, kedy po určitom počte neúspešných pokusov dochádza k zablokovaniu konta, na ktoré je útok vykonaný. Tabuľka *user* je prepojená aj s tabuľkou *invoice*, kde toto prepojenie slúži ako evidencia, ktorý užívateľ faktúru v systéme vytvoril a ktorý užívateľ ju upravoval ako posledný.

Dáta zo sekcie Projekty fakturačného systému sú ukladané v tabuľke *project*, ktorá je previazaná s tabuľkou *customer*. Toto previazanie cudzím kľúčom umožňuje pridelovať projekt konkrétnemu zákazníkovi zo systému.

Databázová tabuľka *settings* ukladá všetky systémové nastavenia, ktoré sa vykonávajú v sekcii Nastavenia, popísanej v kapitole 7.5 tejto práce. Táto tabuľka nie je priamo prepojená na žiadnu inú tabuľku, no údaje v nej sa využívajú naprieč celým systémom.

9 OPTIMALIZÁCIA GUI PRE MOBILNÉ ZARIADENIA

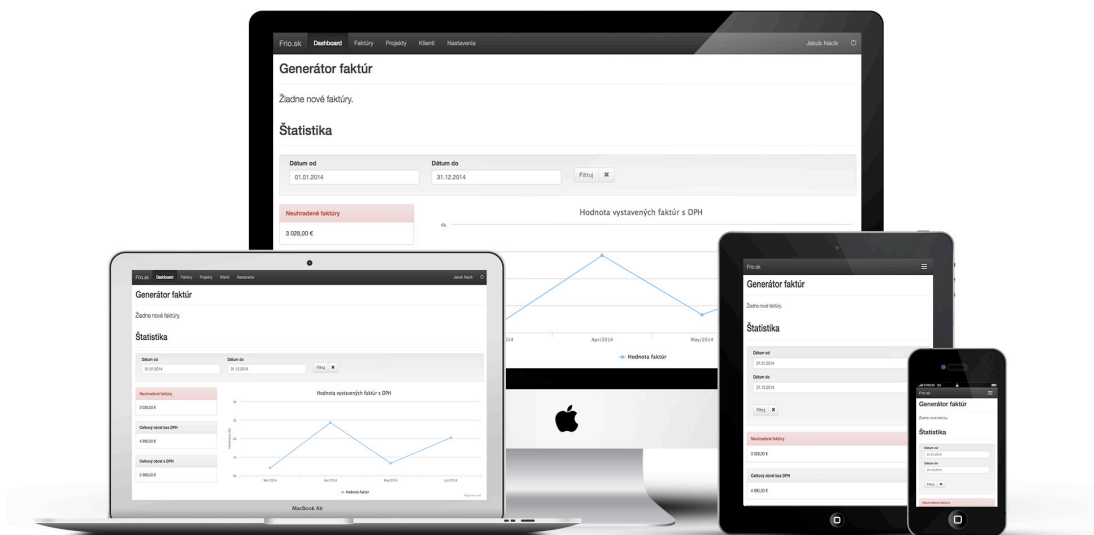
Užívateľské rozhranie fakturačného systému je plne optimalizované pre mobilné zariadenia a displeje s rôznymi rozlíšeniami obrazovky tak, aby na každom type zariadenia poskytlo užívateľovi maximálne pohodlie pri práci so systémom. Práca s fakturačným systémom patrí medzi administratívne činnosti, ktoré mnohí živnostníci alebo malí podnikatelia vykonávajú napríklad pri cestovaní hromadnou dopravou, preto považujem optimalizáciu pre mobilné zariadenia za veľmi prínosnú v tejto oblasti systémov.

HTML šablóny fakturačného systému su vytvorené v štandarde HTML5, kaskádové štýly v štandarde CSS3. Rôzne animácie systémových prvkov, ako sú napríklad potvrdzujúce okná pre mazanie záznamov sú riešené pomocou JavaScriptovej knižnice jQuery.

Všetky elementy, ikony v systéme sú optimalizované pre displeje s vysokým rozlíšením. Ako dobrý základ pre grafické rozhranie a jeho responzivitu sa ukázal front-end webový framework Bootstrap popísaný v kapitole 4 tejto práce. Vďaka využitiu frameworku Bootstrap a jeho výraznej podpore CSS prvkov, je v aplikácií eliminované používanie akýchkoľvek obrázkov, čo sa veľmi pozitívne odzrkadluje na objeme dát, ktorý je potrebné sťahovať s načítaním aplikácie cez prehliadač. Toto je podstatné hlavne pre mobilné zariadenia, kde je užívateľ často pripojený cez pomalé mobilné internetové pripojenia a nízka dátová náročnosť aplikácie mu umožňuje pracovať s ňou rýchlejšie.

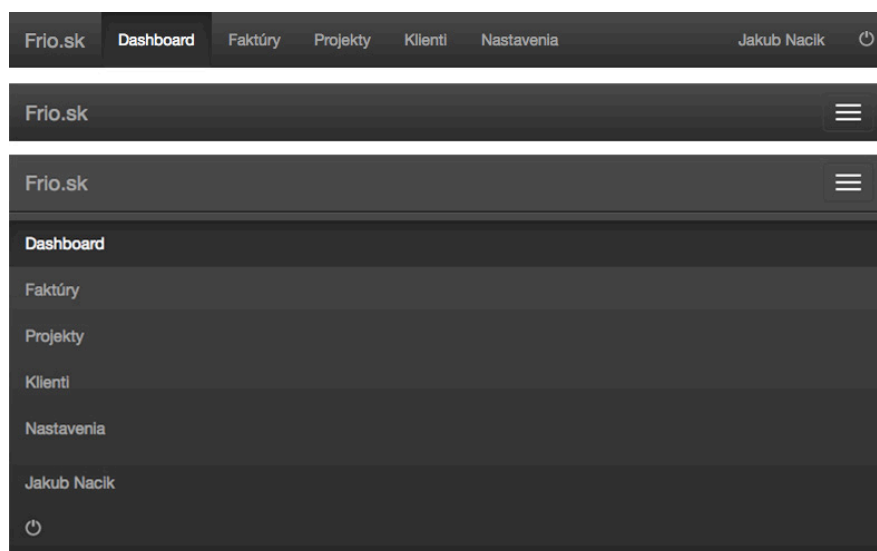
Tabuľka 1. Nastavenia hodnôt CSS media queries.

| Verzia zobrazenia | Minimálne rozlíšenie obrazovky | Maximálne rozlíšenie obrazovky |
|--------------------------|---------------------------------------|---------------------------------------|
| Smartphone | 0 pixelov | 768 pixelov |
| Tablet | 768 pixelov | 992 pixelov |
| Bežný monitor | 992 pixelov | 1200 pixelov |
| Veľký monitor | 1200 pixelov | ∞ pixelov |



Obrázok 12. Ukážka zobrazenia systému na rôznych zariadeniach.

V rámci optimalizácie pre mobilné zariadenia je využitá knižnica jQuery, ktorá sa stará o animované rozbaľovanie hlavného navigačného menu, ktoré je od šírky 768 pixelov a menej zobrazené vo svojej mobilnej verzii, ktorá šetrí miesto na obrazovke no zároveň je možné jedným dotykcom rozbaľiť celú jej ponuku a pohodlne sa navigovať v rámci aplikácie.



Obrázok 13. Rôzne zobrazenia navigačného menu.

10 ZABEZPEČENIE APLIKÁCIE

Webové aplikácie sa s neustálym rozvojom internetu tešia stále väčšej popularite, čo vedie k tomu, že táto oblasť začala byť zaujímavá pre mnoho ľudí z hľadiska bezpečnosti a možnosti prieniku do webových aplikácií a úniku rôznych citlivých dát, ktoré majú aplikácie uložené vo svojich databázach. Objavili sa veľké možnosti zraniteľnosti webových aplikácií a najrôznejšie prípady úniku citlivých dát, čo viedlo k veľkému zvýšeniu záujmu o oblasť bezpečnosti webových aplikácií.

Fakturačný systém nie je výnimkou a obsahuje pomerne citlivé finančné dáta firiem, ktorých únik spôsobený zlým zabezpečením systému je nežiadúci. V tejto kapitole rozoberieme zabezpečenie systému pred hrozbami popísanými v kapitole 6 tejto práce.

Použitie PHP frameworku pri tvorbe aplikácie výraznou mierou zvyšuje úroveň jej zabezpečenia. Framework sa bez zásahu programátora stará o správne nastavenia HTTP hlavičiek, o správne escapovanie hodnôt ako pri posielaní cez formuláre, tak aj pri výpise v HTML šablónach. Framework tiež programátorovi poskytuje vývojarske nástroje, vďaka ktorým je schopný detailne odladiť jednotlivé súčasti aplikácie a odhaliť tak bezpečnostné riziká.

10.1 Ochrana pred SQL injection

Okrem escapovania hodnôt posielaných z formulárov webovej aplikácie je fakturačný systém chránený pred útokom SQL injection aj využívaním spôsobu komunikácie s databázovým serverom nazývaným Prepared Statements. Jedná sa o spôsob, kedy sú dáta posielané v SQL príkaze oddelené od samotného príkazu. Aplikácia najskôr odošle na databázový server dotaz, ktorý má vykonať, databázový server tento dotaz predspracuje a až následne použije dáta poskytnuté webovou aplikáciou. Nemôže sa tak stať, že dáta obsahujúce škodlivé znaky pozmenia SQL dotaz, nakoľko tento je v tom čase už predspracovaný.

O využívanie Prepared Statements sa vo frameworku Nette stará vrstva pre prácu s databázou Nette\Database.

Ukážka použitia Nette\Database vo webovej aplikácii:

```
$this->connection->table('nazov_tabulky')->where('stlpec',  
'hodnota');
```

10.2 Ochrana pred Cross-Site Scripting (XSS)

Ochranu pred XSS útokom opäť výborne zabezpečuje framework Nette a jeho šablónovací systém Latte. Vďaka tomu, sa pre výpis dát získaných napríklad z MySQL databázy v HTML šablónach používajú špeciálne šablónovacie makrá, ktoré automaticky zabezpečujú, že sa hodnoty premenných z PHP vypíšu v šablónach vždy správne escapované. Do úvahy sa berie aj to, či sa daná hodnota vypisuje len v tele stránky alebo je obsiahnutá napríklad ako parameter URL adresy alebo je použitá v rámci JavaScriptu.

Zápis premennej v HTML šablóne

```
{ $premenna }
```

je automaticky prevedený na

```
<?php echo Nette\Templating\Helpers::escapeHtml($premenna, ENT_QUOTES) ?>
```

kde metóda `escapeHtml` z triedy `Nette\Templating\Helpers` slúži na escapovanie premennej v HTML šablóne s využitím PHP funkcie `htmlspecialchars()`.

10.3 Ochrana pred Brute-Force attack

Keďže celá aplikácia je dostupná až po prihlásení užívateľa, je prípadná snaha útočníka o prelomenie prihlasovacieho formuláru metódou Brute-Force pravdepodobnejšia. Z toho dôvodu je nevyhnutná ochrana pred týmto typom útoku.

Fakturačný systém sa snaží eliminovať riziko už pri vzniku nového užívateľského konta, kde je povinná minimálna dĺžka používateľského hesla 10 znakov. Ochrana samotného prihlasovacieho formuláru spočíva v limitovaní maximálneho počtu chybných prihlásení na užívateľa, kde po prekročení 5 chybných pokusov dochádza k zablokovaniu používateľského účtu a je potrebné, aby ho odblokoval administrátor. Okrem toho je v prípade zadania zlého hesla aplikácia na 5 sekúnd uspatá, čo značne eliminuje množstvo skúšaných kombinácií za minútu.

10.4 SSL certifikát

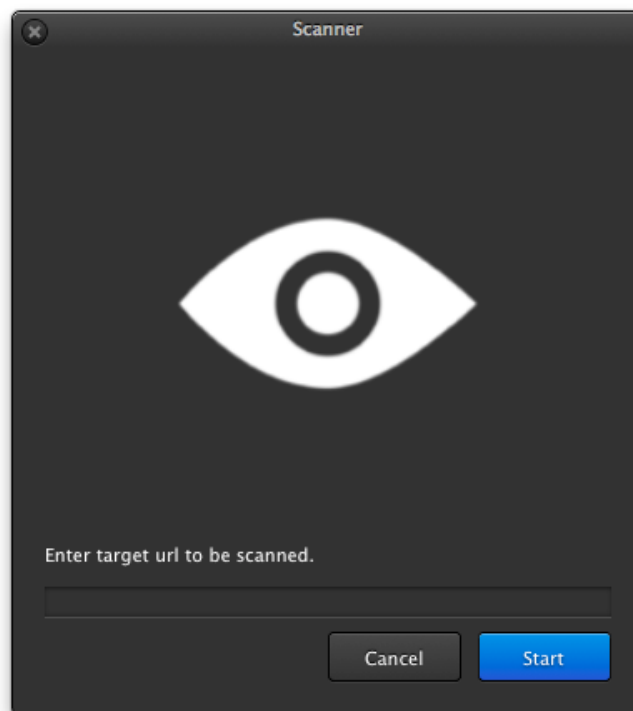
Medzi ďalšie spôsoby zabezpečenia systému patrí nasadenie SSL certifikátu na produkčný server, kde bude systém prevádzkovaný, vďaka čomu dôjde k šifrovaniu

komunikácie medzi serverom a prehliadačom užívateľa a zamedzí sa tak možnému odposluchu prenášaných údajov treťou stranou.

10.5 Penetračný test

Pre overenie zabezpečenia prešla webová aplikácia fakturačného systému automatizovaným penetračným testom, ktorého cieľom bolo odhaliť prípadné zraniteľnosti v zabezpečení. Na automatizovaný penetračný test bola použitá bezplatná aplikácia WebReaver od spoločnosti Websecurify. Do aplikácie stačí zadať URL adresu, na ktorej sa nachádza aplikácia, ktorú chceme otestovať a spustiť automatizovaný test, ktorý skúša na aplikáciu rôzne typy útokov a v prípade že nájde zraniteľnosť, informuje o tom vo výslednom reporte. Okrem bezpečnostných dier upozorňuje aplikácia aj na rôzne rizikové konfigurácie webového servera, ako napríklad výpis chybových hlášok, ktoré by mohli prípadnému útočníkovi poskytnúť nežiadúce informácie o aplikácii.

Automatizovaný penetračný test dopadol úspešne a neodhalil žiadne bezpečnostné diery v aplikácii.



Obrázok 14. Testovací nástroj WebReaver.

11 UKÁŽKOVÁ INŠTALÁCIA

Pre účely tejto práce bola vytvorená plnohodnotná ukážková inštalácia, ktorá obsahuje všetky funkcionality a prevedenie totožné s hlavnou produkčnou verziou. Ukážková inštalácia sa nachádza na adrese <http://demo.frio.sk>. Prihlasovacie údaje pre prístup do aplikácie sú:

E-mail: test@test.sk

Heslo: 1234567890

ZÁVER

Hlavným cieľom tejto práce bolo vytvoriť webovú aplikáciu pre evidenciu fakturačných dát, ktorá bude podporovať prenos účtovných dát pomocou štandardného prenosového formátu a bude plne optimalizovaná pre fungovanie na mobilných zariadeniach.

Problematika fakturácie a evidencie účtovných dát sa týka každodenného života každej firmy bez ohľadu na jej veľkosť. Fakturačný systém sa snaží riešiť problematiku evidencie účtovných dát hlavne pre živnostníkov alebo menšie firmy, ktorí riešia vedenie účtovníctva väčšinou formou outsourcingu u externej firmy a vo vlastnej réžii sa starajú len vystavovanie faktúr za dodané tovary alebo služby svojim odberateľom. V tejto oblasti videlo vedenie firmy NBdesigns, s.r.o., pre ktorú bol fakturačný systém vyvinutý medzeru v ponuke na trhu s ekonomickými softvérmi, preto sa rozhodlo vyvinúť vlastný systém. Ak firma nechce investovať nemalé finančné prostriedky do kúpy licencie niektorého z bežne dostupných komplexných ekonomických softvérov, neexistuje veľa možností, ako spravovať fakturačnú agendu. Na trhu je niekoľko konkurenčných klient-server fakturačných systémov, ktorých výhody a nevýhody sú popísané v kapitole 2 tejto práce.

Hlavnými prínosmi fakturačného systému vyvinutého pri tejto práci je určite jeho plná podpora mobilných zariadení, čo nesplnil ani jeden z konkurenčných systémov. Ďalej je to možnosť jednoduchého prenosu účtovných dát do iných aplikácií, čo je hlavne pri fungovaní s externou účtovnou firmou, kde treba prenášať účtovné dáta veľmi efektívne. Ako prenosové formáty boli použité formát PDF ako tlačový formát, formát XML ako štandardný prenosový formát podľa špecifikácie UBL a formát TXT v štruktúre špecifikovanej ekonomickým softvérom MRP, ktorú využíva externá účtovná firma firmy NBdesigns, s.r.o.

Pri práci bola dostatočná pozornosť venovaná bezpečnosti webových aplikácií a pri tvorbe systému bolo dbané na dodržiavanie dobrých bezpečnostných zásad, aby bola aplikácia chránená pred bežnými typmi útokov ako sú Cross-Site scripting alebo SQL injection. Aplikácia bola podrobená aj automatizovanému penetračnému testu, ktorý mal za cieľ odhaliť prípadné zraniteľnosti v systéme.

Zadanie diplomovej práce bolo splnené v plnom rozsahu a jeho výsledkom je konkurencie schopný fakturačný systém, ktorý môže nájsť uplatnenie v nejednej firme.

ZÁVER V ANGLIČTINE

The main goal of this diploma thesis was to create web application for managing invoicing data, which will support transferring data by standard transfer format and will be fully optimised for working on mobile devices.

The problems of managing invoicing data are connected to everyday life of every company regardless of how it is large. Invoicing system should solve problems with invoicing data management, mainly for small companies, which are mostly outsourcing their accounting management and in-house are managing only creating of invoices for their services or goods for customers.

In this area has management of company NBdesigns, s.r.o., for which was invoicing system developed, seen a space in the market with economics softwares and that's why the company decided to develop own invoicing system. If company does not want to invest significant amount of money to buy licence of some complex economic software, there is no many options how to solve invoice management. In the market are some client-server invoicing system from competitors, which are described in chapter 2 of this thesis.

The main assests of invoicing system which was developed in this thesis is for sure it's full support of mobile devices. This property doesn't have any of competitive applications. Next useful property is easy transfer of invoice data to other applications, what is necessary by outsourcing accounting management. As data transfer formats are used PDF as printing format, XML as standard data transfer format by UBL specification and TXT in structured by MPR economic software specification, because this software is using accounting partner of NBdesigns, s.r.o company.

At work was enough attention paid to security of web applications and by developing of system was looking after good security standards, to protect application against most common attacks such as Cross-Site scripting or SQL injection. Application security was tested by automated penetration test, which should detect possible vulnerabilities.

The assignment of this diploma thesis has been fully met and it's result is competitive invoicing system, which could be used in many companies.

ZOZNAM POUŽITEJ LITERATURY

- [1] VRÁNA, Jakub. 1001 tipů a triků pro PHP. Vyd. 1. Brno: Computer Press, 2010, 456 s. ISBN 978-80-251-2940-1.
- [2] PROKOPOVÁ, Zdenka. Databázové systémy MySQL+PHP. FAI UTB Zlín, 2006, s. 126, ISBN 80-7318-486-9.
- [3] MARCOTTE, Ethan a [foreword by Jeremy KEITH]. Responsive web design. A Book Apart, 2011. ISBN 09-844-4257- X.
- [4] KOSEK, Jiří. PHP a XML. 1. vyd. Praha: Grada, 2009. ISBN 978-80-247-1116-4.
- [5] OPEN TEXT CORPORATION. *EDI Basics* [online]. 2014 [cit. 2014-05-08]. Dostupné z: <http://www.edibasics.com/what-is-edi/>
- [6] ASC X12. *ASC X12* [online]. 2014 [cit. 2014-05-08]. Dostupné z: <http://www.x12.org/x12org/about/index.cfm>
- [7] OASIS. *OASIS Universal Business Language (UBL)* [online]. 2014 [cit. 2014-05-08]. Dostupné z: https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=ubl
- [8] UNECE. *UN/EDIFACT* [online]. 2011 [cit. 2014-05-08]. Dostupné z: <http://www.unece.org/cefact/edifact/welcome.html>
- [9] W3C. *HTML & CSS* [online]. 2013 [cit. 2014-05-08]. Dostupné z: <http://www.w3.org/standards/webdesign/htmlcss>
- [10] NETTE FOUNDATION. *Nette Framework* [online]. 2014 [cit. 2014-05-08]. Dostupné z: <http://nette.org>
- [11] et al *Bootstrap* [online]. 2014 [cit. 2014-05-08]. Dostupné z: <http://getbootstrap.com>
- [12] SQL Injection. *Security-portal.cz* [online]. 2009 [cit. 2014-05-08]. Dostupné z: <http://www.security-portal.cz/clanky/sql-injection-full-paper>
- [13] Escapování - definitivní příručka. *Php-fashion.com* [online]. 2009 [cit. 2014-05-08]. Dostupné z: <http://php-fashion.com/escapovani-definitivni-prirucka>
- [14] Cross-Site Request Forgery. *PHP Triky* [online]. 2006 [cit. 2014-05-08]. Dostupné z: <http://php.vrana.cz/cross-site-request-forgery.php>

- [15] Responsive Web Design Versus Adaptive Web Design. *Designs 4 The Web* [online]. 2014 [cit. 2014-05-08]. Dostupné z: <http://www.designs4theweb.com/responsive-web-design-versus-adaptive-web-design/>

ZOZNAM POUŽITÝCH SYMBOLOV A SKRATIEK

PDF Portable Document Format.

API Application programming interface.

GUI Graphic User Interface - Grafické Uživatelské Rozhranie.

CSV Comma Separated Value.

XML Extensible Markup Language.

EDI Electronic Data Interchange

SQL Structured Query Language

HTTP Hypertext Transfer Protokol

SSL Secure Sockets Layer

ZOZNAM OBRÁZKOV

| | |
|--|----|
| <i>Obrázok 1. Náhľad GUI SuperFaktúra.sk</i> | 14 |
| <i>Obrázok 2. Náhľad GUI iKros.sk.....</i> | 15 |
| <i>Obrázok 3. Náhľad GUI Faktúry-online.com</i> | 16 |
| <i>Obrázok 4. Schéma MVC architektúry.....</i> | 23 |
| <i>Obrázok 5. Ukážka princípu responzívneho GUI.</i> | 25 |
| <i>Obrázok 6. Dashboard fakturačného systému.</i> | 34 |
| <i>Obrázok 7. Zoznam faktúr.</i> | 35 |
| <i>Obrázok 8. Rozhranie pre export dát.</i> | 36 |
| <i>Obrázok 9. Ukážka faktúry v PDF exportovanom zo systému.</i> | 37 |
| <i>Obrázok 10. Formulár s nastaveniami systému.</i> | 39 |
| <i>Obrázok 11. Schéma databázovej štruktúry.</i> | 40 |
| <i>Obrázok 12. Ukážka zobrazenia systému na rôznych zariadeniach.</i> | 43 |
| <i>Obrázok 13. Rôzne zobrazenia navigačného menu.</i> | 43 |
| <i>Obrázok 14. Testovací nástroj WebReaver.</i> | 46 |

ZOZNAM TABULIEK

| | |
|---|----|
| <i>Tabuľka 1. Nastavenia hodnôt CSS media queries.</i> | 42 |
|---|----|

ZOZNAM PRÍLOH

Kompletný zdrojový kód aplikácie a dátázy sú na priloženom CD.