Webové stránky s administrací pro Baby Club Katka

Bc. Pavel Dubčák

Diplomová práce
2019

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2018/2019

ZADÁNÍ DIPLOMOVÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Pavel Dubčák**
Osobní číslo:	**A17279**
Studijní program:	**N3902 Inženýrská informatika**
Studijní obor:	**Informační technologie**
Forma studia:	**kombinovaná**
Téma práce:	**Webové stránky s administrací pro Baby Club Katka**
Téma anglicky:	**Admin pages for Baby Club Katka**

Zásady pro vypracování:

1. **Proveďte literární rešerši nástrojů pro tvorbu webových projektů.**
2. **Vyhledejte již realizovaná řešení webových portálů typu "Baby Club".**
3. **Zvolte vhodné řešení pro realizaci z pohledu dostatečného výkonu, uživatelsky přívětivého prostředí, administrace, bezpečnosti a požadavků GDPR.**
4. **Do navrženého řešení implementujte vhodné moduly umožňující využití QR kódů dle požadavků zadání.**
5. **Realizujte a vyhodnoťte zvolené řešení.**

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **BROWN, Tiffany B., Kerry BUTTERS a Sandeep PANDA. HTML5 Okamžitě. Brno: Computer Press, 2014, 256 s. ISBN 978-80-251-4296-7.**
2. **LAZARIS, Louis. CSS Okamžitě. Brno: Computer Press, 2014, 168 s. ISBN 978-80-251-4176-2.**
3. **SKLAR, David. PHP 7 – Praktický průvodce nejrozšířenějším skriptovacím jazykem pro web. Brno: Zoner Press, 2018, 368 s. ISBN 978-80-7413-363-3.**
4. **Bootstrap Documentation [online]. Twitter, 2011 [cit. 2018-10-03]. Dostupné z: www.getbootstrap.com**
5. **SELECKÝ, Matúš. Penetrační testy a exploitace. Brno: Computer Press, 2012. ISBN 978-80-251-3752-9.**
6. **STUTTARD, Dafydd a Marcus PINTO. The web application hacker's handbook: finding and exploiting security flaws. 2nd ed. Chichester: John Wiley [distributor], c2011. ISBN 9781118026472.**

Vedoucí diplomové práce: **Ing. Bc. Pavel Vařacha, Ph.D.**
Ústav informatiky a umělé inteligence

Datum zadání diplomové práce: **3. prosince 2018**

Termín odevzdání diplomové práce: **15. května 2019**

Ve Zlíně dne 7. prosince 2018

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

doc. Mgr. Milan Adámek, Ph.D.
děkan

prof. Mgr. Roman Jašek, Ph.D.
garant oboru

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové 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 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 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 práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování diplomové 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 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, dne 15.5.2019 Pavel Dubčák, v. r.

ABSTRAKT

Cílem této diplomové práce je seznámit se s dostupnými nástroji pro tvorbu webových projektů, jejich výhodami a nevýhodami a vyhledat již dostupná řešení webových portálů typu „Baby Club“. Na základě toho vybrat vhodné řešení k realizaci nového projektu a implementovat moduly pro generování faktur s QR kódy pro platby za přihlášky do kurzů. V teoretické části je vybráno několik redakčních systémů a online nástrojů pro tvorbu webových projektů, které jsou srovnány z hlediska uživatelského prostředí, rozšiřitelnosti, bezpečnosti a dalších kritérií. Je zde také představeno několik webů typu Baby Club a následně zmíněna kapitola o bezpečnosti webových stránek a možné útoky na ně. Praktická část práce je zaměřena na nově vytvořenou aplikaci. Popsány jsou použité technologie a následně implementované moduly. Poslední kapitola se zabývá tím, jak byla aplikace řešena, její funkcionalitou, zabezpečením a vyhodnocením tohoto řešení.

Klíčová slova: webový portál, baby club, QR kód, faktury.

ABSTRACT

The aim of this master’s thesis is get to know with existing tools for creating websites, theirs advantages and disadvantages, look for solved solutions of website projects of type „Baby Club“. Based on this choose appropriate solution for realization of a new project and implement modules for generating invoices with QR codes for paying applications to swimming courses. In the theoretical part are selected several content management systems and online tools for creating web projects, which are compared in terms of user environment, extensibility, security and other criteria. There are also a number of Baby Club sites and a chapter on website security and possible attacks on them. The practical part is focused on the newly created application. There are described used technologies and subsequently implemented modules. The last chapter deals with how the application was solved, its functionality, security and evaluation of this solution.

Keywords: website, baby club, QR code, invoices.

Na tomto místě bych rád poděkoval své vedoucí paní RNDr. Lence Kozákové, Ph.D. a následně panu Ing. Bc. Pavlu Vařachovi, Ph.D., který vedení této práce převzal, za cenné rady ať už při řešení nebo psaní této diplomové práce. Poděkování patří také panu prof. Mgr. Romanu Jaškovi, Ph.D. za pomoc při řešení problémů, které tuto práci provázely.

Dále bych chtěl poděkovat své rodině za podporu a trpělivost, svému kamarádovi Honzovi za rady při vývoji webového portálu a za čtení a připomínky při psaní této práce.

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

OBSAH

ÚVOD **8**
I TEORETICKÁ ČÁST **10**
1 REDAKČNÍ SYSTÉMY **11**
1.1 WordPress 13
1.2 Drupal 14
1.3 Joomla! 16
1.4 ExpressionEngine 18
1.5 TextPattern 19
1.6 Typo3 20
1.7 Grav 21
1.8 Prestashop 22
1.9 Magento 23
2 ONLINE NÁSTROJE PRO TVORBU A SPRÁVU WEBOVÝCH STRÁNEK **24**
2.1 Webnode.cz 25
2.2 eStránky.cz 25
2.3 Zombeek.cz 26
2.4 Wix.com 27
2.5 Weebly.com 28
3 PORTÁLY TYPU „BABY CLUB“ **29**
3.1 babyclubuh.cz 29
3.2 babyclub.cz 30
3.3 babyclubkosatka.cz 30
3.4 babyclub-hrosik.cz 31
3.5 aquababyclub.cz 32
3.6 babyclub-nessie.cz 32
4 BEZPEČNOST A HROZBY WEBOVÝCH APLIKACÍ **34**
4.1 SQL Injection 34
4.2 Cross-site Scripting (XSS) 35
4.3 Cross-site Request Forgery (CSRF) 36
4.4 Broken Authentication 37
4.5 XML External Entities (XXE) 38
4.6 Security misconfiguration 38
4.7 Nezabezpečený přímý odkaz na objekt 39
4.8 Sensitive data exposure 39
4.9 Insecure deserialization 40
II PRAKTICKÁ ČÁST **41**
5 ZVOLENÉ TECHNOLOGIE **42**

5.1 HTML A CSS 42
5.2 BOOTSTRAP 4 42
5.3 PHP 7 42
5.4 REDAKČNÍ SYSTÉM – WORDPRESS 43
6 POUŽITÉ PLUGINY 44
6.1 CONTACT FORM 7 44
6.2 SEND PDF FOR CONTACT FORM 7 44
6.3 WP MAIL SMTP 45
6.4 WP LIMIT LOGIN ATTEMPTS 45
6.5 REALLY SIMPLE SSL 45
6.6 API QR SERVER 45
7 REALIZACE NAVRHNUTÉHO ŘEŠENÍ 46
7.1 FUNKCIONALITA FORMULÁŘE PŘIHLÁŠKY 47
7.2 ZABEZPEČENÍ 51
7.3 ZHODNOCENÍ VÝVOJE 53
ZÁVĚR 54
SEZNAM POUŽITÉ LITERATURY 56
SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK 62
SEZNAM OBRÁZKŮ 64
SEZNAM PŘÍLOH 66

ÚVOD

Dnešní doba s sebou přináší obrovské možnosti využití moderních technologií, a to platí i o propagaci organizací a společností. Pokud nemá daná organizace své webové stránky, jako by neexistovala. Dnes je tato propagační činnost povýšena na úroveň propagace na sociálních sítích, avšak dobré webové stránky přináší řadu výhod. Například přehlednost, pokud jsou dobře navrhnuty, dále informace dostupné na jednom místě, a tak není potřeba hledat všude možně.

Tato diplomová práce obsahuje v teoretické části celkem čtyři kapitoly, ve kterých splňuje první dva body uvedené v oficiálním zadání.

V první kapitole nazvané „Redakční systémy“ se zabývá představením redakčních systémů a jejich srovnáním z pohledu přívětivosti uživatelského rozhraní, rozšiřitelnosti a bezpečnosti. Představuje zde pár více či méně známých CMS systémů. Ve druhé kapitole navazuje představení online nástrojů pro tvorbu webových stránek, které jsou většinou zdarma.

Třetí kapitola se zaměřuje na průzkum webových portálů typu Baby Club a hodnotí jejich vzhled, přehlednost, dostupnost informací a uživatelskou pohodlnost při jejich prohlížení a používání.

V další a zároveň poslední kapitole teoretické části této práce jsou zmíněny a přiblíženy bezpečnostní hrozby a útoky na weby, které mohou nastat a jsou nejčastější. Na úvod kapitola zlehka představuje http protokol a dále již představuje jednotlivé útoky.

Následuje praktická část této práce obsahující tři kapitoly, ve kterých se snaží splnit zbylé body z oficiálního zadání.

Kapitola číslo pojmenovaná „Zvolené technologie“ pět popisuje vybrané technologie pro vývoj webové stránky v rámci této práce a zdůvodňuje proč byly vybrány zrovna tyto nástroje.

V šesté kapitole se čtenář práce může dozvědět něco o použitých pluginech při tvorbě webu a k čemu jednotlivé moduly slouží. Je zde také zmíněno, jak byly tyto pluginy vybírány a co všechno bylo zvažováno.

Poslední část práce představuje vytvořený webový portál pro Baby Club Katka. Porovnává starý web s novým, představuje novou funkcionalitu, kde je uveden i její kód. Dále popisuje i zabezpečení celého portálu jak z pohledu administrace, tak v uživatelské části

a zhodnocuje celý vývoj webového portálu, navrhuje jeho cenu a zmiňuje se o hostingu a případném rozšíření.

V závěru je pak vyhodnocení vytvořeného řešení v rámci této diplomové práce.

I. TEORETICKÁ ČÁST

1 REDAKČNÍ SYSTÉMY

Tyto systémy jsou někdy také nazývány jako publikační. Často se pro ně používá zkratka CMS (z angličtiny Content Management System), což znamená systém pro správu obsahu. Je to vlastně druh software, chápán jako webová aplikace, který zajišťuje správu webového obsahu. [1]

Existují dva druhy redakčních systémů. Toto rozdělení je především podle typu licence, pod kterou jsou šířeny, a to na open source (volně dostupné, upravovatelné a použivatelné) a premium (komerční, placené). [5]

Open source systémy jsou vyvíjeny komunitami programátorů, kteří poskytují svůj produkt volně k šíření a možností dalšího vývoje. Jejich hlavní výhodou je jejich použití zcela zdarma. Avšak pro minimalizaci bezpečnostních rizik je potřeba je neustále aktualizovat. Tato rizika jsou způsobena právě dostupností zdrojových kódů komukoli. Jejich počty využívání jsou obrovské, proto jsou tyto volně dostupné redakční systémy pod neustálým tlakem na zdokonalení bezpečnosti a funkčnosti. Šance na odhalení nějaké bezpečnostní trhliny je tak daleko vyšší než u systémů, které běží na pozadí pár desítek, stovek stránek.

Komerční systémy mají tak velkou nevýhodu v tom, že firma, která tento CMS systém vyvinula jej nechce dát z ruky a díky tomu jsou uživatelé často odkázáni na tuto firmu. Pokud by chtěli s firmou přestat spolupracovat, přichází tak i o webové stránky, protože takovýto web nebude možné nikam přesunout a jeho podpora také zanikne. [6]

Nainstalovaný redakční systém na webovém serveru umožňuje svému uživateli bez znalosti programování či pouze se základní znalostí značkovacího jazyka HTML, přidávat, upravovat a mazat obsah webové stránky. Jedinou věcí, kterou obsluha publikačního systému musí umět je psaní textu a klikání na ikonky pro formátování již napsaného textu. S výjimkou psaní textu může uživatel nahrávat a vkládat i obrázky do webové stránky. [2]

Redakční systémy se dnes vyskytují jako běžná součást většiny nově vytvořených webů. Naprosté minimum webových stránek je tvořeno úplně od začátku. Vkládaná data se uchovávají v databázi, nejčastěji MySQL a pomocí vloženého administračního rozhraní s nimi lze velmi jednoduše pracovat. Existence různých druhů šablon, které si uživatel může zvolit a doinstalovat do publikačního systému umožňuje jednoduchou tvorbu webu. Šablona samotná slouží jen jako grafická prezentace dat poskytnutých z databáze návštěvníkovi webových stránek. [4]

Dále je zde možnost do každého publikačního systému doinstalovat pluginy, nebo také nazývány jako moduly, které slouží k nejrůznějším účelům. Mohou to být například moduly pro tvorbu kontaktních formulářů, přidání kalendáře, změna jazyka administračního rozhraní a mnoho dalších užitečných věcí, které časem uživatel může potřebovat.

V administrační části je možné vytvářet uživatele s různými rolemi, řídit přístup k dokumentům, zpravidla se správou přístupových práv a uživatelů, spravovat diskuse s komentáři, obrázky, videa, soubory, nebo galerie. Je zde možnost nastavení publikování článků v dané datum, zobrazení statistik přístupů na webové stránky. Nechybí ani možnost do webu integrovat funkce jako například kalendář, nebo propojení se sociálními sítěmi. [5]

Výhodami těchto systémů je snadná tvorba a modifikovatelnost obsahu téměř bez jakýchkoliv znalostí kódování. Celá obsluha webu probíhá v podstatě pomocí klikání. Dalšími výhodami je snadné nahrávání obrázků a videí pomocí intuitivního editoru pro vytváření a úpravu obsahu webové stránky, modulárnost celého systému, kdy je možnost, některé nevyužívané části rozšiřující funkčnost redakčního systému vypnout. A v neposlední řadě je výhodou dostupnost výše zmíněných pluginů, které pomáhají usnadnit a někdy i urychlit tvorbu některých částí webu. [3]

Pro úspěšný start s publikačním systémem, aby jej mohl uživatel začít používat, je zapotřebí nainstalovat ho na webový server a připojit k vytvořené databázi. Dále nastavit údaje pro přihlášení do administrace a poté pár věcí souvisejících se samotnou webovou stránkou. [7]

CMS systémy jsou v drtivé většině napsány ve skriptovacím jazyce PHP, proto pokud chce webový vývojář vytvořit svoji vlastní šablonu, je třeba tento jazyk pochopit a znát základní příkazy, na kterých daný redakční systém staví. V kombinaci se značkovacím jazykem HTML a kaskádovými styly CSS lze vytvořit mnoho hezkých webových prezentací. O zbytek se již postará publikační systém, pomocí kterého už jen zbývá samotný web naplnit obsahem a dále tento obsah udržovat aktuální. Pokud je obsah webových stránek neaktuální, například zastaralé ceny zboží, kontaktní údaje, nebudí to dobrý dojem a také přichází firma rychle o své zákazníky a stává se proděléčnou. [4]

V následujících podkapitolách je představeno a srovnáno několik nejznámějších a nejpoužívanějších redakčních systémů. Jsou zde zmíněny jejich výhody, nevýhody a možnosti využití.

1.1 WordPress

Jedním z trojice nejoblíbenějších, nejznámějších a také nejpoužívanějších redakčních systémů kladoucí důraz na výkon, přístupnost, bezpečnost a jednoduchost použití. Jeho vývojáři věří, že dobrý software by měl fungovat jen s minimálním nastavováním. To je důvod k tomu, že jeho uživatel se může rovnou zaměřit na svůj vytvářený produkt, poslání či službu. Současně je zde velká nabídka různých funkcí pro růst a vývoj. [5] Tento CMS systém je vyvíjen jako open-source projekt a je tedy dostupný zcela zdarma ke stažení pro kohokoliv. Jeho celý zdrojový kód je popsán v dokumentaci, což dává možnost každému programátorovi zapojit se do rozvoje a upravovat jeho části ke svému obrazu. WordPress používají desetitisíce lidí a podílí se tak na jeho vývoji. Toto ho staví před komerční produkty, které vytváří jen malé týmy, a nikoliv široká veřejnost. [8]

Ke vzniku WordPressu vedla vývojáře touha po elegantním, dobře strukturovaném publikačním systému postaveném na PHP a MySQL s licencí pod GPL. Je to poměrně mladý redakční systém, jehož kořeny sahají někde do roku 2001. Od ostatních CMS systémů se odlišuje svou vyspělostí, stabilitou a zaměřením na uživatele a webové standardy. [9]

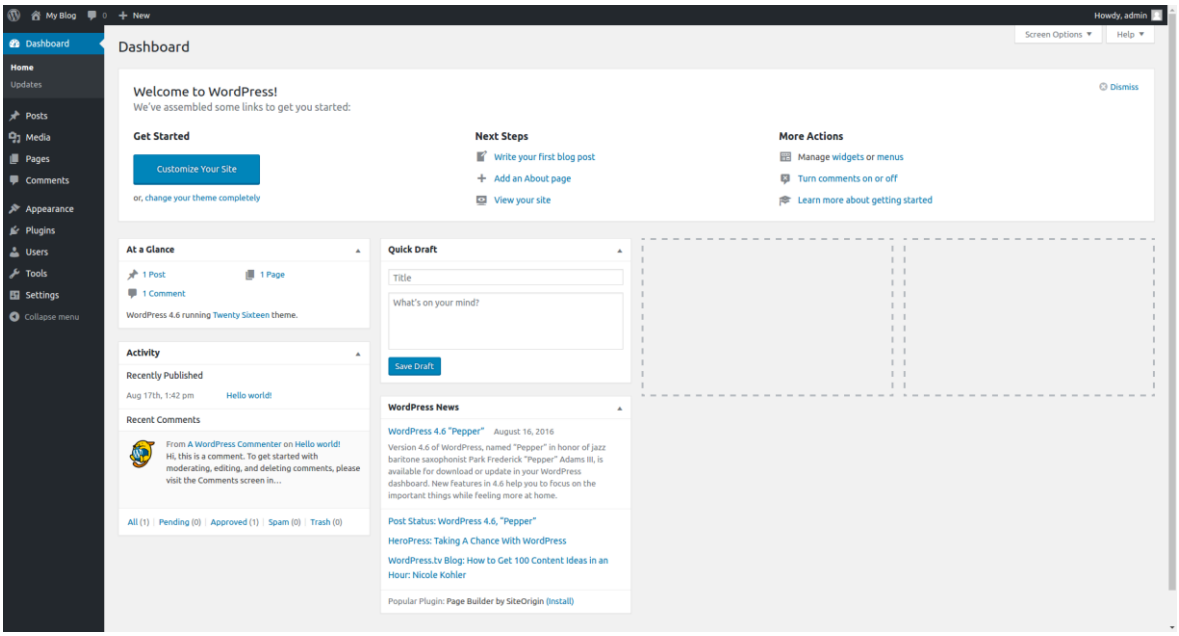
Obr. 1. WordPress – Logo. [12]

Od roku 2005, kdy byla vydána verze 1.5, která byla stažena více než 900 000 uživateli, to odstartovalo spuštění hostingové služby wordpress.com, kde si může uživatel vytvořit vlastní web či blog bez nutnosti jakékoli instalace a nastavování. Stačí k tomu se jen jednoduše na tento webový portál zaregistrovat a využít tak pohodlného prostřední WordPressu.

Je zde možnost předinstalovaní mnoha funkcí v podobě pluginů a šablon, jejíchž instalace je velmi snadná. K dispozici je kolem 55 000 pluginů různých druhů, většina z nich je dostupná zcela zdarma. Co se šablon týče, je dostupných kolem tisíce grafických návrhů jak zdarma, tak placených. Má široké možnosti úpravy menu, aby obsahovalo stránky, kategorie atp. Další výhodou, jak již bylo zmíněno výše, je velká komunita stojící za tímto produktem. Má jednu z největších internetových komunit (v angličtině), avšak technická

podpora je dostupná i v českém jazyce. Pro tento redakční systém je dostupné obrovské množství návodů, videí a dokumentace. Pro správu formulářů je možné pomocí pluginů jednoduše do formuláře přidávat pole. To dovoluje k příspěvkům přidávat například popisky, štítky, nebo kategorie. [10]

Tento redakční systém má také své nevýhody. Příkladem může být, že úpravy formuláře si žádají orientaci v jazyce PHP. Při úpravě grafického vzhledu je vyžadována nutná znalost HTML a CSS. Dále je nevýhodou to, že čím více pluginů si uživatel doinstaluje, tím více dojde k poklesu výkonu celého CMS. Problémem může být výběr správného pluginu. Ačkoliv je dostupných několik tisíc pluginů, tvoří ve skutečnosti své klony. Volba toho správného tak zabere někdy spoustu času.



Obr. 2. WordPress – Administrační část. [13]

WordPress je velmi dobrý redakční systém pro blogy nebo jednoduché webové aplikace. Jeho přínosem je jednoduché ovládání z pohledu uživatelského prostředí a je tak vhodný zvláště pro začínající uživatele. [11]

1.2 Drupal

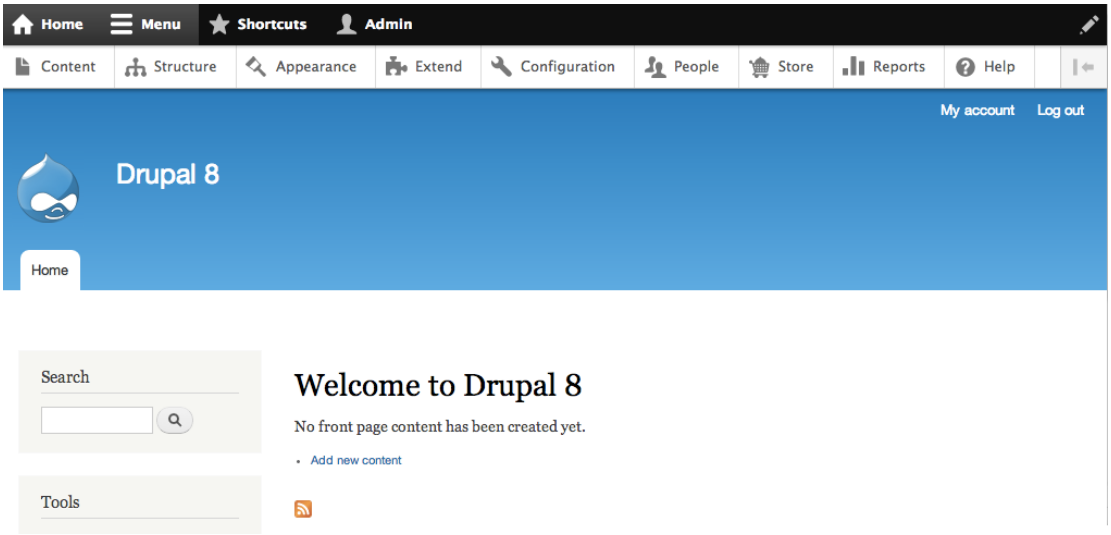
Dalším z trojice nejznámějších redakčních systémů je Drupal. Řadí se mezi jeden z nejkomplexnějších CMS systémů, které na trhu existují. Spíše ho lze označit za programátorskou platformu kvůli jeho velmi specifickému prostředí než jako jednoduchý nástroj pro správu obsahu. Stejně jako WordPress je vyvíjen jako open-source projekt, který volí

programátoři dříve používající jednoduché nástroje, které jim již nevyhovují, nebo nedostačují pro jejich potřeby.

Tento redakční systém využívá celá řada významných společností jako například MIT, Sony Music, New York Observer a další. Obsahuje velké množství funkcionalit pro tvorbu jak interních, tak externích webů a na úpravu jejich obsahu. [10]

Obr. 3. Drupal – logo. [14]

Drupal má k dispozici dokumentaci vytvářenou velkou komunitou za ním stojící, která se neustále vylepšuje a udržuje v aktuálnosti. Dokumentace obsahuje vše potřebné o instalaci, tvorbě modulů a webů, návrhů šablon atd. Pro tento redakční systém existuje více než 40 000 modulů a pluginů pro usnadnění rozšíření jeho funkčnosti. To umožňuje se spíše zaměřit na design a obsah než na samotné programování mnoha složitých funkcí.



Obr. 4. Drupal – administrace. [15]

Výhodou CMS systému Drupal je, že je přístupný téměř pro všechny základní funkcionality jako jsou registrace uživatelů a správa profilů, kanály RSS, správa menu, nástroj pro tvorbu vzhledu webových stránek a systém pro jejich správu. Tyto základní funkce umožňují vytvoření jednoduchého blogu uživatele, stránek, nebo i fóra a sociálního webu a dalších. Díky šablonám a základní možnosti úpravy jednotlivých prvků webové stránky, není nutné vše začínat od nuly. Nadefinované konfigurace funkcí webu dávají možnost

sestavení jednoduchých i složitějších webů. [11] Drupal je především známý tím, že umožňuje správu a tvorbu různorodého obsahu jako je video, správa uživatelů, dotazníky, blogy, texty, statistiky a jiné. Také pluginy jsou jednou z výhod.

Značnou nevýhodou může být pro uživatele to, že tento redakční systém nemá příliš uživatelsky přívětivé prostředí a pro jeho instalaci nebo úpravy jsou nutné pokročilé znalosti. Pokud chce uživatel upravovat obsah stránek, neobejde se bez pokročilejších znalostí HTML, CSS a PHP. Při návyku uživatele na jiná prostředí může zabrat značný čas přechod na tento systém. Výkonnostně Drupal zaostává za WordPressem. [14] Nevýhodou může být také nedostatek kvalitních bezplatných a komerčních šablon, jejichž vytváření je poměrně složité. Při velké návštěvnosti webu generuje velké zatížení serveru. To může vést k odpojení webových stránek správcem serveru, na kterém tento web běží. Částečným řešením je instalace pluginu pro generování webu do vyrovnávací paměti serveru. [15]

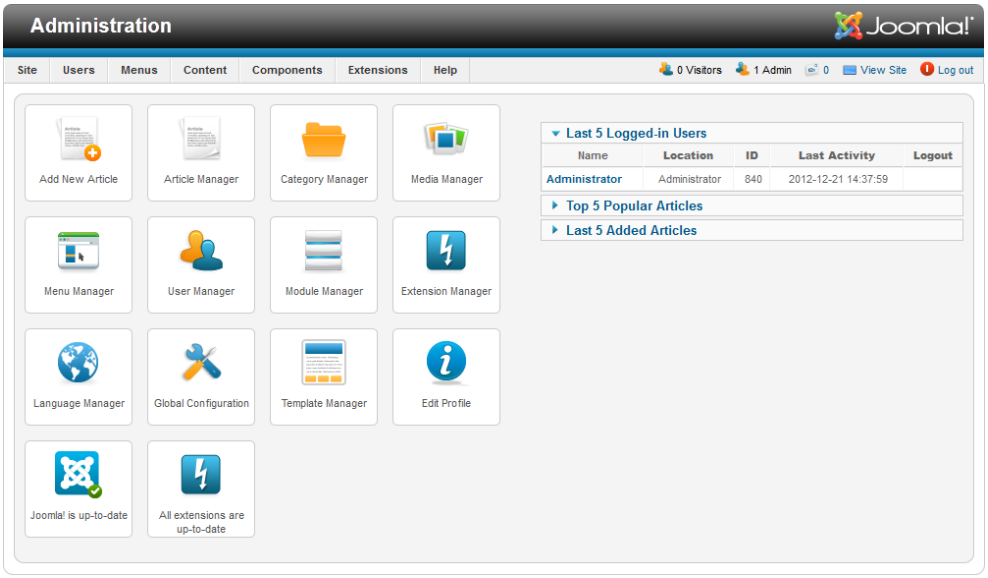
1.3 Joomla!

Posledním z trojice nejznámějších redakčních systému je Joomla!. Vyskytuje se někde mezi jednoduchým přístupem jako tomu je u WordPressu a složitým Drupalem. Na tomto softwaru běží webové stránky významných společností jako MTV, Harvardské univerzity a dalších. Citibank používá tento CMS systém jako back-endovou síť, je to vlastně síť, která není veřejně dostupná. Jinak má velmi pestré využití téměř na vše, kromě webových stránek se dá využít i jako komplexní firemní adresář, systém pro řízení majetku, nebo jako rezervační systém. [10]

Obr. 5. Joomla! – logo. [16]

Jednalo se o nejpoužívanější open-source CMS na trhu, než přišel WordPress. Kvůli svojí nenáročné instalaci a konfiguraci představoval ideální řešení pro tvorbu webových stránek bez nutnosti speciálních technických dovedností. S vydáním třetí verze získal velký náskok před jeho konkurencí, co se bezpečnosti týče. Nabízí tak zajímavé možnosti z hlediska přizpůsobitelnosti práv a profilů uživatelů. Je zde také možnost správy tzv. multi-sites, což díky tomuto lze používat tento redakční systém v kombinaci se složitějšími platformami zahrnujících i privátní prostory, jakými mohou být extranet nebo intranet.

Výhodou CMS Joomla! je docela jednoduchá instalace, kdy již po několika minutách po stažení začne běžet na hostingovém serveru, avšak není až tak jednoduchý jako WordPress, ale s přehledem poráží Drupal. [11] Také jako v předchozích je zde možnost instalace pluginů, kde jich je k dispozici několik tisíc. Avšak WordPress má k dispozici pluginů daleko více. Programátorské nástroje a tutoriály jsou dostupné ve velkém množství i jeho diskusní fórum je velmi rozsáhlé jak v angličtině, tak v češtině. Software je dále vybaven navigačním systémem, který je velmi komplexní a může tak obsluhovat několik hierarchií, což umožňuje spravovat web dokonce i s několika stovkami podstránek. Dále odkazy, které jsou generovány tímto CMS systémem jsou velmi přátelské a mají vliv na optimalizaci pro vyhledavače. Také aktualizace jsou velmi snadno proveditelné. [18] Velké množství funkcí poskytuje také ovládací panel, která na začátku může vypadat pro uživatele děsivě, ale s postupem času se může většinu z nich naučit ovládat a také začít využívat všech možností tohoto softwaru.



Obr. 6. Joomla! – administrace. [17]

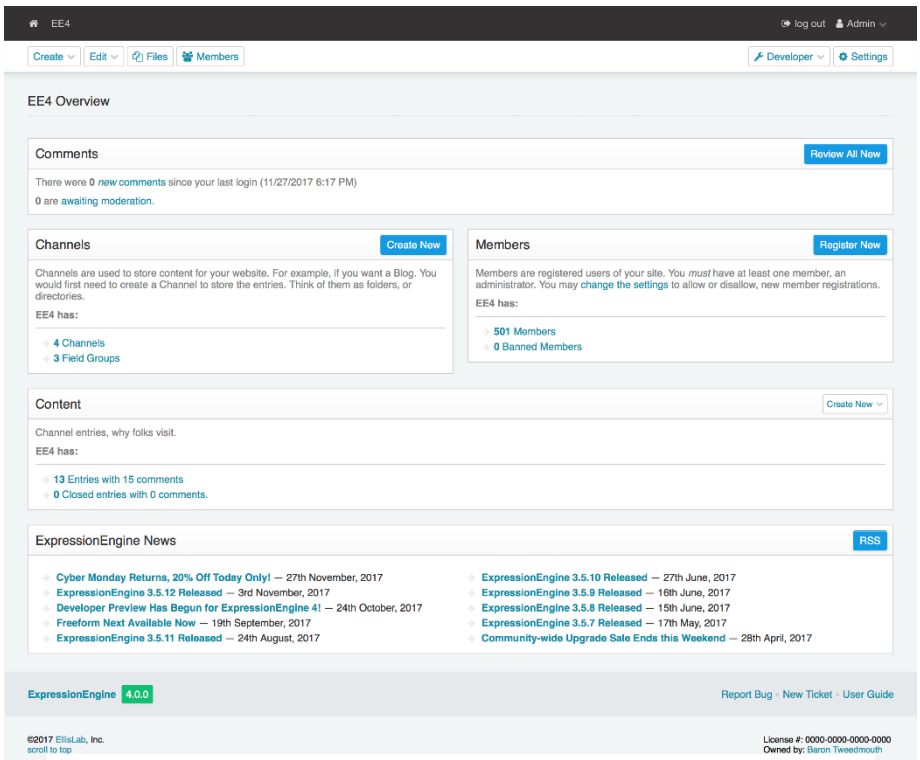
Rozhraní tohoto redakčního systému se může zařadit mezi jeho nevýhody. Není tak přehledné jako u jiných CMS, ale stále je velmi použitelné. Další může být zmíněno nedostatek kvalitních šablon a jejich složité přizpůsobování. Software vyžaduje dosti výkonný server, protože ubírá hodně zdrojů. Čím rozsáhlejší a pokročilejší webová stránka bude, tím pomalejší bude její načítání. Stejně tak to bude v případě velké návštěvnosti při použití ořezané verze. Dále zde existují pluginy a šablony, které jsou pouze placené což je velkou nevýhodou. Může se taky stát, že bude problém s kompatibilitou a některá funkcionalita nebude dostupná bez nutnosti zásahu do PHP kódu. První dojem, zejména začátečníka

může být odrazující kvůli velkému množství dostupných funkcí, proto je lepší pro jednoduchý web zvolit jiný redakční systém. [19]

1.4 ExpressionEngine

Tento redakční systém byl svého času spojen s vývojem jednoho z PHP frameworků nazvaný CodeIgniter. Až do podzimu 2018 byl poskytován jako placený. To trvalo celých 15 let. Nyní je již dostupný zcela zdarma, avšak kompenzaci příjmů si firma směřuje poskytováním placených prémiových služeb. Firma EllisLab, která tento CMS vyvíjí a je bývalým tvůrcem frameworku CodeIgniter by ráda dostala svůj software mezi trojici nejpoužívanějších redakčních systémů, čili WordPress, Drupal a Joomla!, které zároveň pokrývají cca 75 % celého trhu. [11]

Velkou výhodou ExpressionEngine je jeho komerční podpora. Dále se hlavně zaměřuje na celkovou bezpečnost, což ukazuje fakt, že nikdy nedošlo k závažnému bezpečnostnímu narušení. Také možnost přizpůsobení designu webů není nijak omezena. [20, 21]



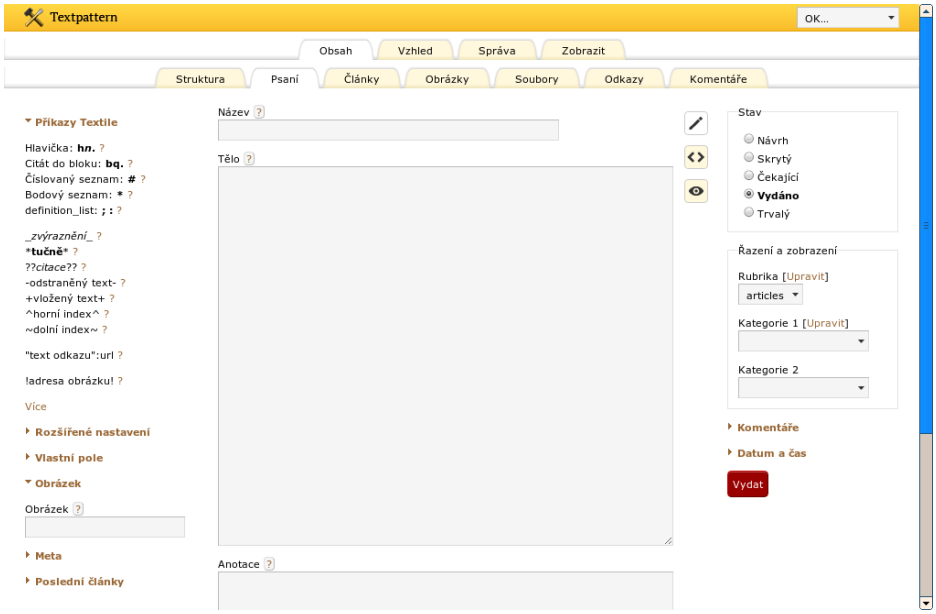
Obr. 7. ExpressionEngine – administrace. [20]

Jako za jeho nevýhodu lze považovat zbytečnou pokročilost pro jednoduché a menší webové stránky. Další věc je, že pro něj není dostupné tolik doplňků a pluginů jako pro jiné redakční systémy. Obsahuje celkem asi 22 doplňujících modulů a něco málo přes 100 oficiálních pluginů. Jsou to především pluginy a doplňky, které patří k těm nejpravděpodobněji

použitelným, tzn. diskusní fórum, e-mailová konference, wiki, správce členů, statistiky, elektronický obchod a další. [22]

1.5 TextPattern

Jedná se o velmi flexibilní redakční systém, ale bohužel není tolik známý a je docela přehlížený. Přičemž se jedná o velmi lehký, snadno použitelný a přizpůsobitelný systém. Pro snadno vyhledatelný a rychle převoditelný obsah webu na XHTML používá svůj značkovací jazyk nazvaný Textile. Celý CMS je velmi přímočarý – napsat článek a publikovat. Od svého začátku je vytvořen především pro bloggery. Kompletně celý web se upravuje ve čtyřech záložkách, a to Psaní, Články, Obrázky a Soubory. Pokud ale chce uživatel pomocí TextPatternu vytvořit firemní prezentaci, neobejde se bez značného zásahu do kódu a alespoň základních znalostí programování. [11]



Obr. 8. TextPattern – administrační část. [23]

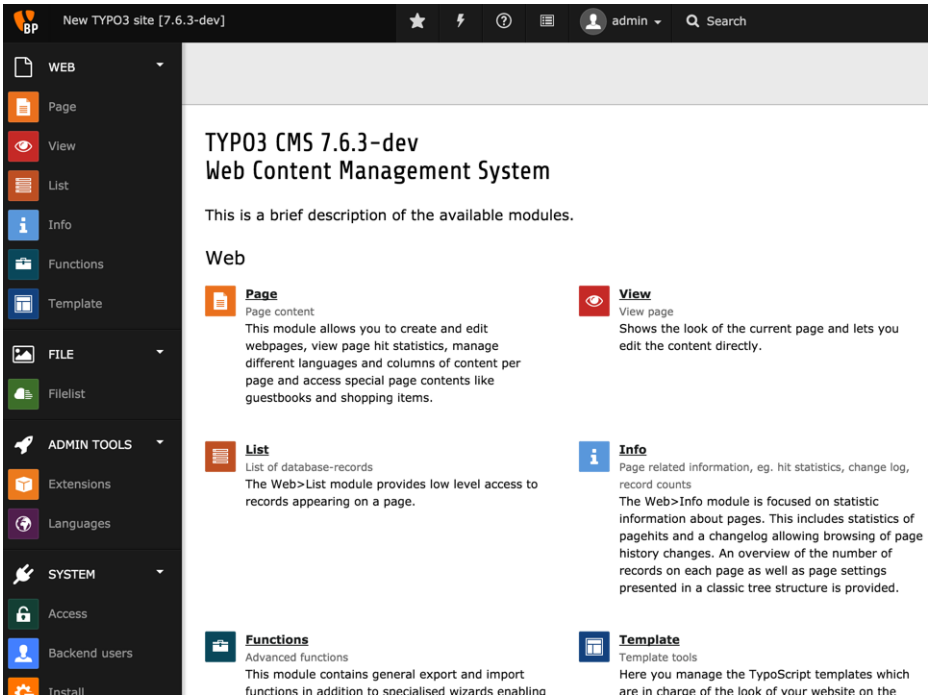
Výhodou je možnost již v základní instalaci velmi výrazně upravit funkcionalitu webové stránky, kde jsou velmi snadné zásahy do struktury a dat a také jednoduchost a čistota kódu. Tento CMS je málo známý, což znamená z pohledu bezpečnosti, že není velkým cílem pro spamovací roboty. Dobře se hodí pro weby všech velikostí a jeho dokumentace je velmi dobrá včetně úplného online manuálu. [22]

Ovšem slabou stránkou je malá komunita za ním stojící. Dále je pro něj dostupné malé množství pluginů a relativně málo kvalitních šablon stránek. Nevýhodou může být také zápis textů v jazyku Textile, namísto ve WYSIWYG editoru. Jeho základní šablona je

nepoužitelná. Je zde značně komplikovaná tvorba statických stránek firemního webu – vyžaduje si zásah do kódu šablon. [23] Instalace pluginů a šablon je velmi složitá pro běžného uživatele. Také aktualizace na novější verzi není jednoduché provést a nejsou ani moc časté. TextPattern má velmi uživatelsky nepříjemnou administraci obrázků a jejich vkládání do článků. [24]

1.6 Typo3

Tento CMS se řadí mezi nejkomplexnější a nejrozsáhlejší systémy postavený na kombinaci PHP a MySQL jako většina. Je šířen na licenci open-source a je možné na něm stavět jak weby firemní, tak osobní blogy nebo e-shopy. Především se hodí ale pro rozsáhlejší projekty. [10] Důkladně odděluje vzhled, správu obsahu a obsah samotný, jehož správa je velmi snadná a intuitivní. Využívají ho společnosti jako Lufthansa, Mercedes, nebo Philips. Obsahuje téměř 1800 rozšíření a modulů a běží na něm více jak 500 000 webových prezentací. Úprava obsahu webové stránky založené na tomto redakčním systému nevyžaduje znalost programování. Počítá se zde s několika úrovněmi práv editorů a administrátorů webu a je možnost využití procesu schvalování obsahu. Ovládání editoru textu je velmi podobné softwaru Microsoft Word. [25, 26]



Obr. 9. Typo3 – administrace. [25]

Velkou výhodou je, že Typo3 má rozsáhlou základnu vývojářů a jsou poskytovány pravidelné aktualizace. Administrace je vícejazyčná a je poskytováno schvalování obsahu

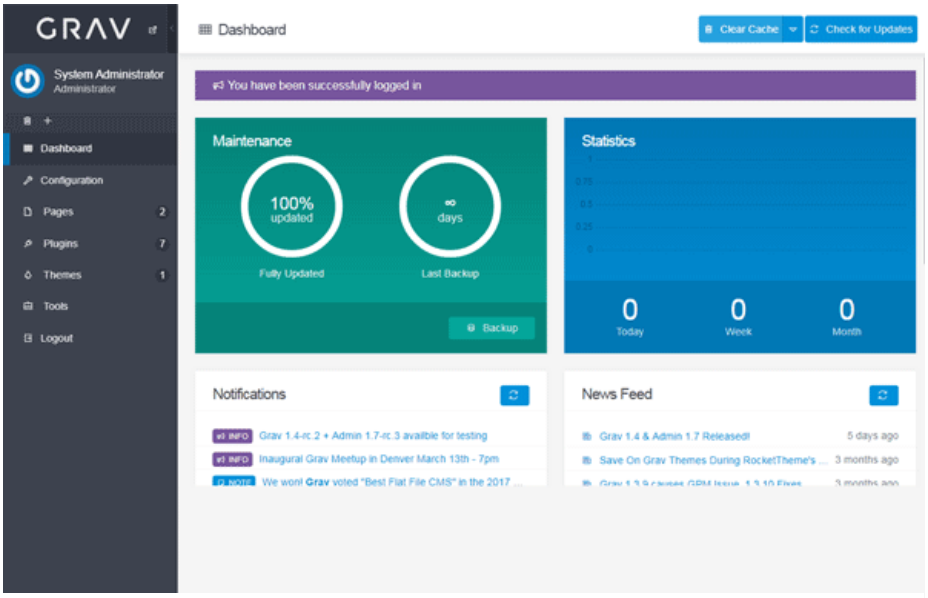
administrátorem. CMS je připraven pro mobilní stránky a pro propojení se sociálními sítěmi. Je zde také možnost spravování více webů v jedné instalaci tohoto systému. Jednotlivé úrovně historie umožňují vrácení více verzí obsahu, nebo celých stránek. [27] Pro některé uživatele může být také jako výhoda integrace Google Analytics a vlastních analytických nástrojů.

Jako nevýhoda může být, že pokud uživatel chce využít všechny poskytované možnosti opravdu dokonale, vede k tomu náročná a dlouhá cesta. Ne všechna řešení jsou opravdu kvalitní. Typo3 je vhodný především pro komplexní řešení. [28]

1.7 Grav

Velmi zajímavým a poměrně novým redakčním systémem, takzvaně na redukční dietě, je Grav. Pro svůj běh totiž vyžaduje pouze webový server a PHP 5.5.9 a vyšší, nic víc. Samotný obsah lze vytvářet pomocí Markdown syntaxe značkovacího jazyka. Instalace je velmi jednoduchá. Stačí nahrát instalační balíček s CMS systémem na webový server a je hotovo. To přináší snadnou zálohu celého webu. Ze stránek projektu je k dispozici okolo 90 šablon pro vzhled a 240 rozšíření. [29]

Výhodou je jeho snadné zálohování a přenositelnost. Samotný balíček má zhruba 35 MB, což z něj v podstatě dělá nejúspornější systém, co se velikosti týče. Dokumentace je také velmi hezky a přehledně zpracována.



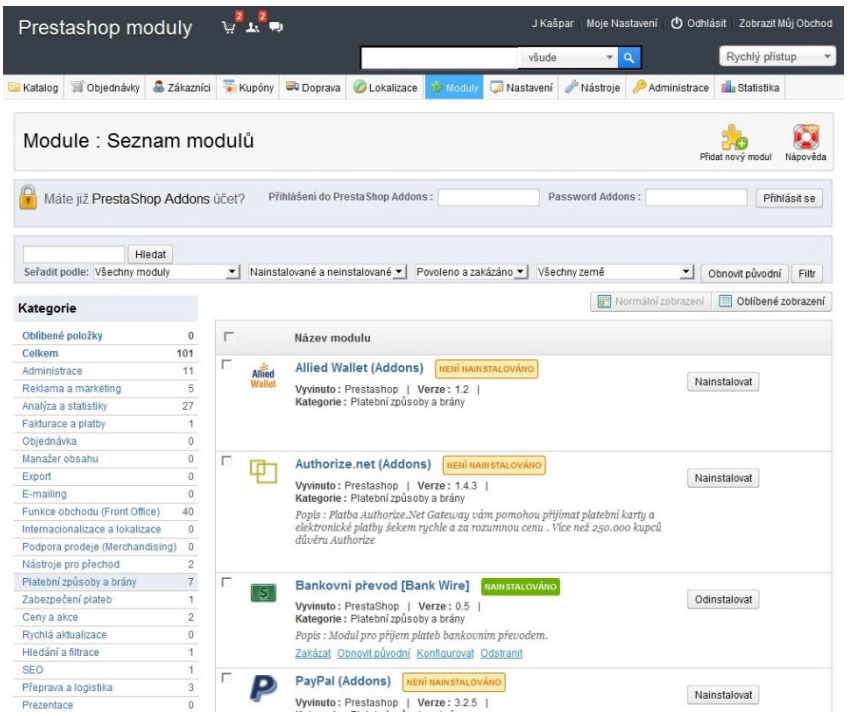
Obr. 10. Grav – administrace. [31]

Tento software je spíše vhodný pro správu velmi malého webu, kterou ještě více zjednodušuje. Komplexní web by se v něm tvořil velmi těžko. [30]

1.8 Prestashop

Bezesporu jedním z nejoblíbenějších řešení současného trhu pro tvorbu elektronických obchodů je redakční systém Prestashop. Jeho instalace je snadná a poskytuje velkou škálu pluginů. To z něj dělá pomocníka, který šetří uživateli e-shopu nemalé peníze a také čas. [19]

Nejedna vedoucí značka trhu dala přednost právě tomuto softwaru. Je stavěn i na velký nápor návštěv obchodu či katalogu zboží. Následkem je jeho velká stabilita při velkém zatížení. Je tedy jasnou volbou pro ty, kteří se chystají spustit svůj e-shop.

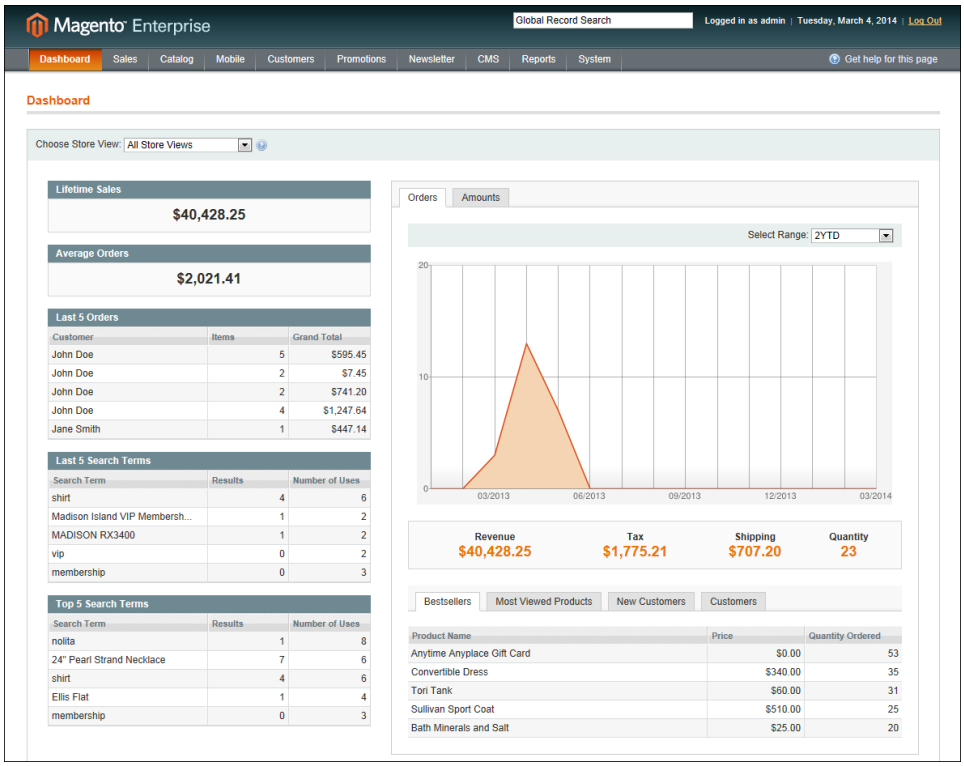


Obr. 11. Prestashop – administrace. [32]

Co se zabezpečení týče je Prestashop bezpečný a poskytuje ochranu jak zákazníků, tak samotného e-shopu. Tento redakční systém je univerzálním a jedním z nejlepších řešení pro vytvoření vlastního elektronického obchodu nebo katalogu. [32, 33].

1.9 Magento

Jedná se o e-shopový etalon mezinárodního významu. Rozmanitost konfigurace a robustnost tohoto CMS systému ho nabízí k jeho nasazení v rozsáhlých a komplexních projektech, především e-komerčních. [19] Díky tomuto je oblíben především v rámci profesionální komunity. Je to tak rozsáhlý software, že pouhé seznámení se s jeho administračním rozhraním zabere docela dost času. [34]



Obr. 12. Magento – administrace. [35]

Jeho výhodou je velká rychlost nasazení do produkčního používání a nízké náklady na pořízení. Podporuje také více jazykových verzí a optimalizací pro vyhledavače (SEO). Je zde možnost uživatelského přizpůsobení a nabízí bohaté reference na realizované projekty. [35, 36].

2 ONLINE NÁSTROJE PRO TVORBU A SPRÁVU WEBOVÝCH STRÁNEK

Další možností pro uživatele, kteří si chtějí vytvořit webovou prezentaci, ať už osobní stránky, nebo stránky organizace, jsou online WYSIWYG (z angličtiny „What You See Is What You Get“) editory určené pro tvorbu a správu webových stránek. Jsou to webové stránky, pomocí kterých může vytvářet vlastní web i úplných začátečník.

Jedná se o velmi jednoduchý a rychlý způsob, jak si web vytvořit bez řešení technických záležitostí. Uživateli je poskytnuto hotové řešení, díky kterému je schopný si sám webovou stránku vytvořit. Stačí se na takovýto portál zaregistrovat, vymyslet si svůj název domény a pak si jen vybrat vzhled, nastavit pár dalších věcí podle osobních preferencí a během chvilky je možné plnit web samotným obsahem. Vše jde takzvaně naklikat, kdy i běžný uživatel je schopen tuto aktivitu zvládnout, přičemž nemusí mít žádnou znalost programování. Tudíž obsluha takového editoru je udělána velmi intuitivně a cíleně pro tyto osoby.

Ačkoli se vše může zdát snadné a působit dojmem, že tento způsob přináší samé výhody, není tomu zdaleka tak. Komplikace to přináší zejména webovým vývojářům, kdy se při vytváření stránek za pomoci takového editoru přenáší do kódu velké množství často i zbytečných a nepotřebných informací. To z něj pak dělá nepřehledný a zmatečný kód, ve kterém se těžko orientuje a často je pro programátora jednodušší nakódovat web úplně od začátku než se snažit vyznat v generovaném kódu WYSIWYG editoru a provádět v něm nějaké úpravy. Malou nevýhodou pro osobu využívající těchto služeb může být v některých případech placení za používání těchto služeb.

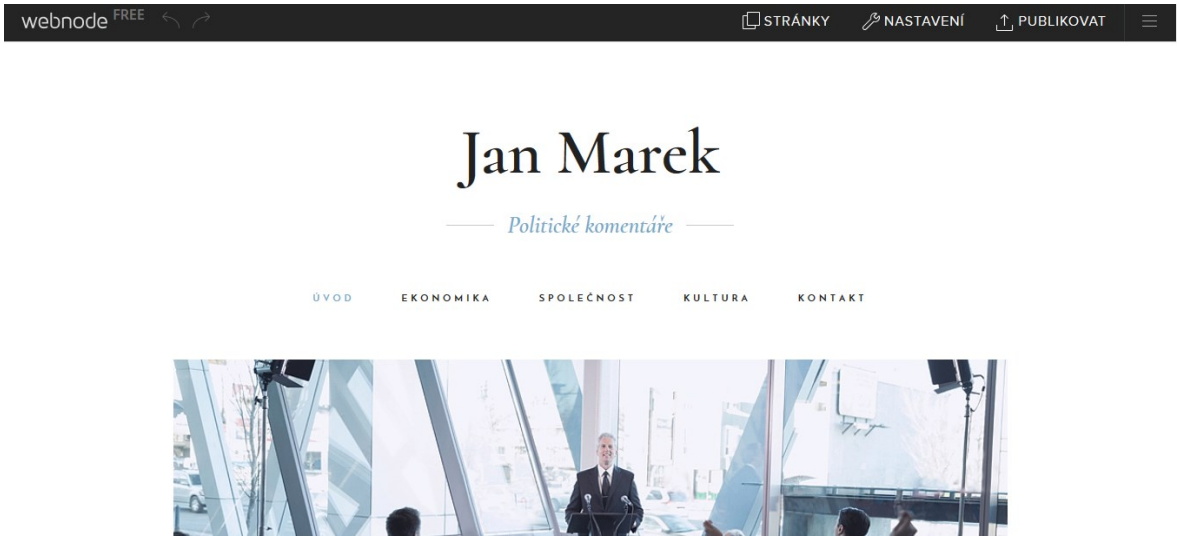
Takových nástrojů pro tvorbu webových stránek je samozřejmě obrovské množství a může být problém některý z nich vybrat. Nejprve by si vlastně měl uživatel uvědomit, co od takového webu očekává a co je pro něj důležité, pak se musí rozhodovat podle parametrů služeb, které jednotlivé nástroje poskytují jako může být například měsíční poplatek, velikost prostoru pro web, množství dostupných šablon, možnost e-mailu s doménou webu, kontaktní formulář, ovládání drag & drop, jazyk prostředí atd. Také je důležité si zjistit, do jaké míry umožňuje daná služba upravit web podle sebe. U většiny je možné si bezplatně nástroj vyzkoušet a na základě toho se následně rozhodnout.

V následujících podkapitolách uvedu pár nejznámějších editorů, které jsou nejen v češtině a také se řadí mezi často využívané.

2.1 Webnode.cz

Patří mezi jeden z nástrojů svého druhu, který má českou lokalizaci. Existuje již velmi dlouho a hlavním cílem bylo vytvořit nástroj pro snadnou a kvalitní tvorbu ať už osobního, firemního webu či e-shopu, který bude publikovatelný během několika hodin. [37]

Při vytvoření účtu je možné na něj mít navázáno více než jeden web a jejich počet není omezen. Je zde dostupných 75 šablon vzhledu a možnost upravit celou řadu věcí. K dispozici je jak verze placená, tak zdarma, která však má řadu omezení. Za příplatek je taky možné navýšit místo pro web z původně dostupných 2 GB. Propagace webu je jednou z důležitých věcí, proto je zde nabídka několika funkcí pro tuto činnost. Nejdůležitějšími jsou SEO a napojení na Google Analytics a Google Search Console. Tento nástroj disponuje také uživatelskou podporou, kdy dostane uživatel odpověď většinou do druhého dne od odeslání dotazu. Celý web je snadno upravovatelný pomocí drag & drop technologie. Bohužel nástroj postrádá zabezpečení pomocí SSL. [38]

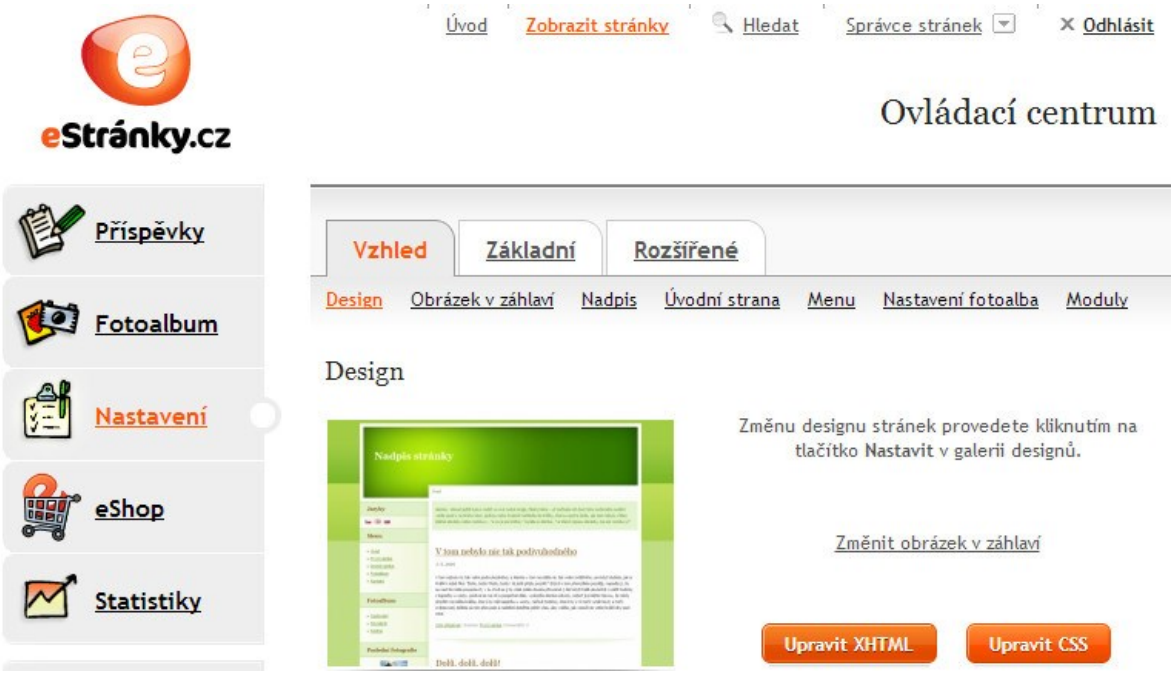


Obr. 13: Webnode – administrace webu. [38]

2.2 eStránky.cz

Jsou dalším nástrojem pro rychlé vytvoření webových stránek jak osobních, firemních tak i elektronických obchodů. Pokud se osoba rozhodne pro tuto možnost, může si vybrat ze tří variant, a to zdarma, kde je dostupných 15 šablon, pro nekomerční verzi to je 35 šablon a komerční, která poskytuje výběr ze 39 šablon. Zajímavou možností je poskytnutí služby, která umožňuje různé jazykové verze webu.

Dále je možnost sledovat návštěvnost stránek pomocí různých statistik, blokování stránek pomocí zámku jen pro VIP uživatele, vytvoření domény druhého řádu, nebo vlastní reklamy. Samozřejmostí je také poskytnutí technické podpory jak e-mailem, tak telefonicky. Bohužel pro web je vyhrazeno pouze 1 GB místa. [39]



Obr. 14. eStránky – administrace. [39]

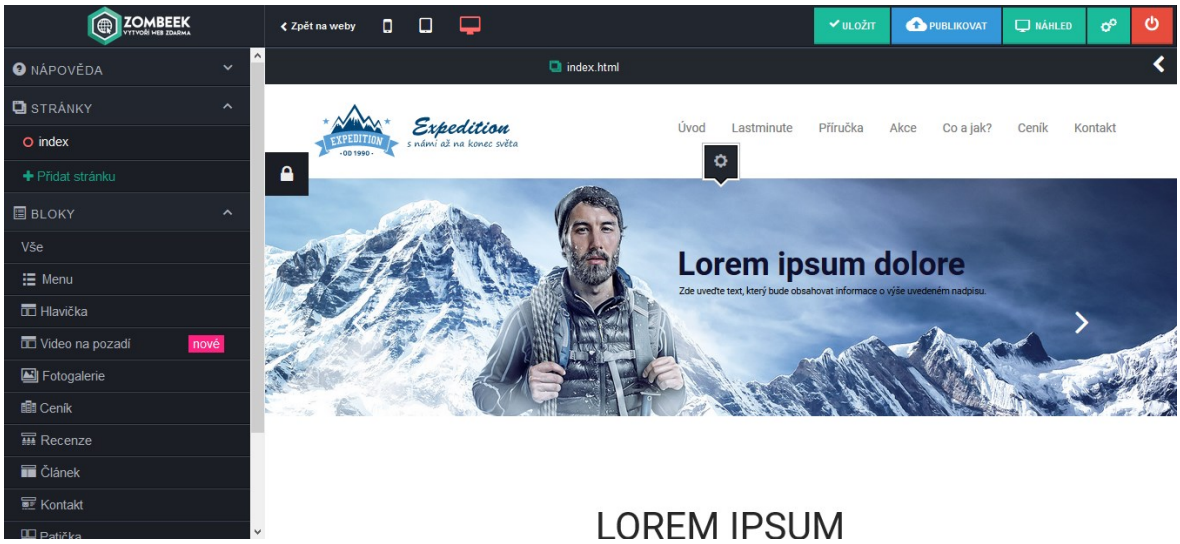
2.3 Zombeek.cz

Tento portál slibuje svým uživatelům rychlé, jednoduché a bezpečné zřízení webových stránek za pouhých deset minut. Přičemž web má být moderní, technicky dokonalý a responzivní. [40]

Poskytovány jsou dvě varianty, a to zdarma a bez starostí. Pokud je zvolena možnost bez starostí, pak může být připojena vlastní doména, e-mailové schránky a další služby. [41]

Je zde k dispozici zatím 10 šablon a další by měly postupně přibývat. Poskytuje i zabezpečení pomocí SSL certifikátu. Fotky lze upravovat s využitím vestavěného editoru. Web se vytváří už z hotových elementů, které může uživatel vkládat podle jeho gusta. Nechybí ani technická podpora, kterou je možné kontaktovat e-mailem nebo telefonicky a odpovídá maximálně do jednoho dne. Nástroj je kompletně v češtině, takže zde není žádná jazyková bariéra.

Autoři tohoto nástroje současně tvoří blog, který výrazně uživateli pomáhá při tvorbě samotných webových stránek. [42]

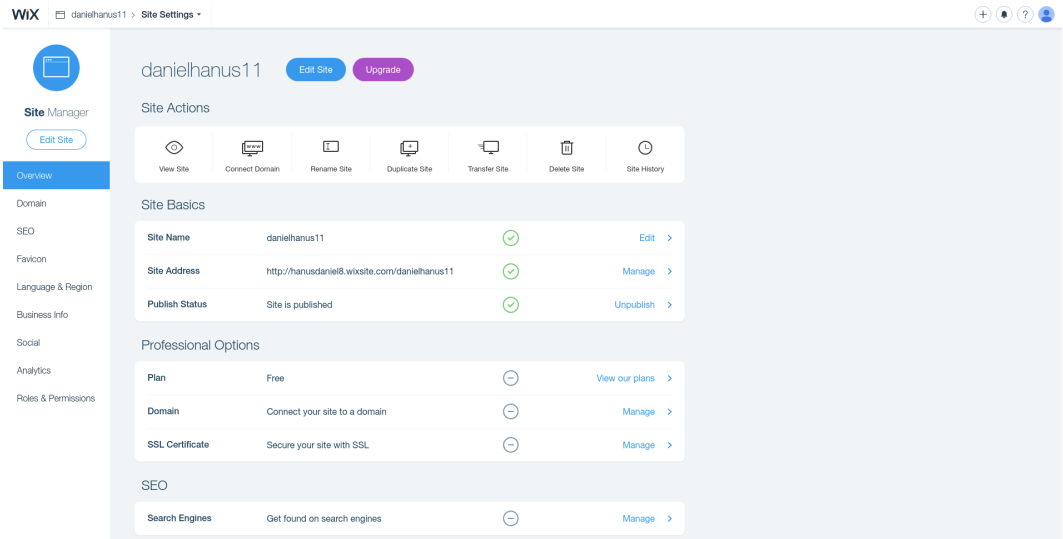


Obr. 15. Zombeek.cz – administrace.

2.4 Wix.com

Je nástroj od zahraničních tvůrců. Ať už se jedná o vytvoření jen jednoduchého blogu, nebo prezentace či e-shopu, je vhodný téměř pro vše. Poskytována je rozsáhlá databáze responzivních šablon (cca 400), která značně ulehčuje tvorbu webu. [43]

Jedná se o nejkomplexnější nástroj pro tvorbu webových stránek, na který je možné na trhu narazit. Uživateli je nabízena celá řada užitečných funkcí pro propagaci webu a k dostání se do popředí výsledků vyhledávání nebo třeba i do feedů. Velkou předností je jednoduchost tohoto nástroje. Uživatelská přívětivost je na vysoké úrovni.



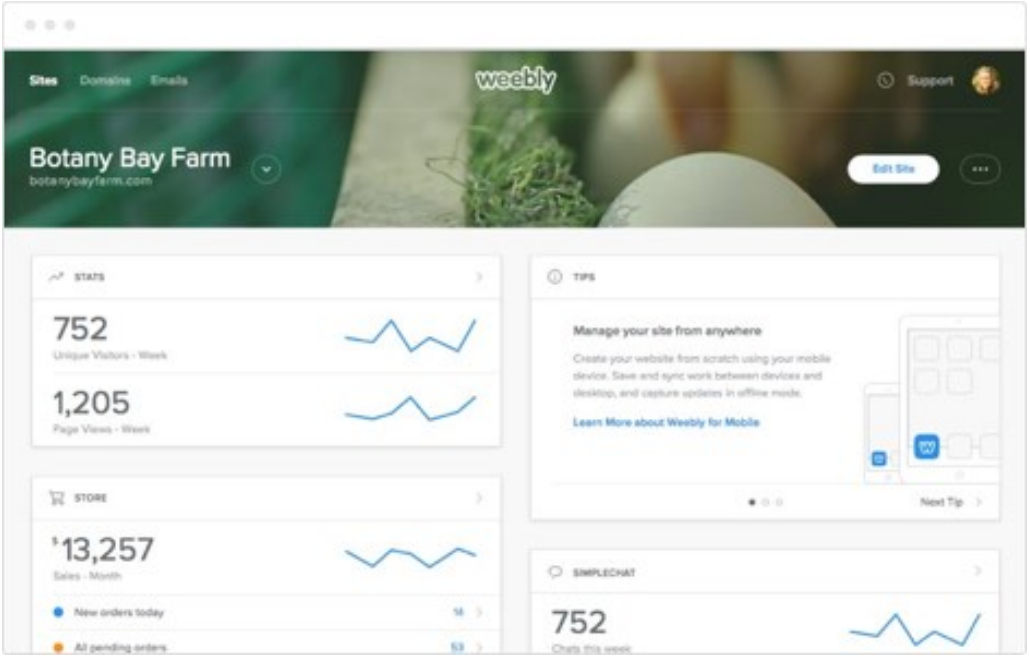
Obr. 16. Wix.com – administrace. [43]

Menší nevýhodou může být cena za služby, která je lehce vyšší. Ačkoli je nástroj zahraniční, je poskytnuta i česká lokalizace, která občas nemusí být srozumitelná. [44]

2.5 Weebly.com

Dalším ze zahraničních nástrojů je weebly.com. Jako předchozí uvedené nástroje, tak i tento je intuitivní a jednoduše použitelný s poskytnutím responzivních šablon. Zároveň je zde možnost spravovat až deset webových stránek. Výhodou jsou přehledně zpracované statistiky návštěvnosti. Nechybí ani mít svůj e-mail založený na doméně webu. [45]

Tento nástroj není však vhodný pro tvorbu elektronického obchodu. Také disponuje špatnou integrací sociálních médií a pro web je k dispozici jen pouhých 500 MB ve variantě zdarma. Při zaplacení možnosti „Pro“, nebo „Business“ je prostor pro web neomezený. Nevýhodou může být, že celé prostředí je v angličtině a neposkytuje českou lokalizaci. [46]



Obr. 17. Weebly.com – administrace. [45]

3 PORTÁLY TYPU „BABY CLUB“

Každá organizace či firma se v dnešní době snaží nějakým způsobem zviditelnit a dostat se tak to povědomí veřejnosti. Nejinak je tomu i u různých sdružení typu Baby Club. Většinou se jedná o uspořádání vykazující činnost mateřské školy, setkávání maminek s dětmi, cvičení, hlídání dětí a v neposlední řadě také plavání kojenců a dětí s rodiči.

Následující podkapitoly představují některé spolky tohoto druhu, které se zaměřují na výuku plavání kojenců a dětí s rodiči. Popisují spíše vzhled a přehlednost jejich webových stránek.

3.1 babyclubuh.cz

Jako první byla vybrána webová prezentace organizace Baby Club Uherské Hradiště. Stránky působí na první pohled jednoduchým vzhledem s horizontálním menu, ve kterém je možno nalézt ceník, básničky, dotazy, dárkový poukaz, fotogalerii. Hned při zobrazení stránky se objeví aktuality a v pravé části pak kontakt s přihláškou, videogalerií a partnerskými weby. Avšak to důležité, jako kategorie o nás, instruktorky, rozpis kurzů, provozní řád a další, najde uživatel až ve spodní části na úvodní straně, což je nevýhoda, protože si toho nemusí uživatel ani všimnout. Z tohoto pohledu se stává web trochu nepřehledným.

Web samotný běží na redakčním systému Vismo od firmy Webhouse. Jedná se o komerční systém této společnosti, což je i pro organizaci jistá nevýhoda. Pokud firma přestane tento software podporovat a vyvíjet, ohrozí to i chod webu Baby Clubu, jak již bylo zmíněno v předchozí kapitole. Mínusem je i to, že web není responzivní. [47]

Obr. 18. Baby Club Uherské Hradiště.

3.2 babyclub.cz

Jedná se o sdružení sídlící v Opavě. Při příchodu na web se návštěvníkovi zobrazí úvodní stránka, kde má na výběr mezi Baby Clubem Kačka, nebo Jeslemi Kačka. Po vstupu na stránku Baby Clubu vidí uživatel přehledně uspořádaný obsah s důležitými informacemi nahoře v horizontálním menu a nalevo se nachází služby seřazeny do vertikálního přehledu. Celkově webové stránky působní jednoduchým, ale poněkud zastaralým vzhledem, což až takový problém není, ale jejich nepřipravenost pro mobilní zařízení už problémem je. Přehlednost a poskytnutí důležitých informací pro návštěvníka je jejich malým plusem. [48]

Obr. 19. Baby Club Kačka.

3.3 babyclubkosatka.cz

Další webová prezentace patří organizaci Baby Club Kosatka věnující se výuce plavání kojenců v Mladé Boleslavi. Po zadání adresy do prohlížeče se návštěvníkovi objeví stránka s hlavním menu v podobě bublin ve vodě, což působí velmi nápaditě a designově. Když je některá z kategorií rozkliknuta, naskytne se pohled na přehlednou stránku laděnou do tmavě modré s bílým písmem s danými informacemi.

Celkový dojem z této prezentace spolku je velmi netradiční, avšak je přehledně zpracována a uvedeno je vše, co zájemce potřebuje vědět.

Web zpracovala firma WebRex, která pro tvorbu používá CMS systém. Bohužel na svých stránkách neuvádí jeho jméno.

Vytknout lze těmto stránkám to, že nejsou responzivní, tudíž pro návštěvníka, který používá mobilní telefon je prohlížení webu nepříjemné. [49]

Obr. 20. Baby Club Kosatka Mladá Boleslav.

3.4 babyclub-hrosik.cz

Baby Club Hrošík poskytuje své služby ve městě Beroun. Kromě dětského plavání poskytuje klub aquaerobik a plavání dětí mateřské školy. Jeho webové stránky působí dosti roztahaně a chaoticky. Barvy jsou nevýrazné a vybledlé, což je po delším prohlížení webu nepříjemné pro oči. Hlavní menu je docela nenápadně zastrčeno pod velkým úvodním obrázkem.

Web byl vložen do šablony od w3layouts.com. Ačkoli to může působit, že jsou zde samá negativa, není tomu tak. Na rozdíl od předchozích stránek se jedná o zcela responzivní web, který je na mobilních zařízeních snadno čitelný, a to je její výhodou. [50]

Obr. 21. Baby Club Hrošík.

3.5 aquababyclub.cz

Tato organizace, která působí v Praze a Kolíně s názvem Aqua Baby Club, nabízí kurzy plavání kojenců a batolat rozřazených do skupin dle věkových kategorií. Webové stránky budí jednoduchý dojem, kdy vpravo nahoře jsou tři položky – bazény, kontakt a přihlášení. Nalevo pak je možné nalézt nabídku, kde návštěvník najde všechny potřebné informace. Na pravé straně je v úzkém pásu zobrazena nástěnka z facebookové stránky tohoto sdružení.

Celý web běží na redakčním systému Drupal a využívá typickou šablonu pro tento systém. Stránky jsou pro návštěvníka přehledné a uživatelsky velmi přívětivé, avšak opět nejsou optimalizovány pro mobilní zařízení. [51]

Obr. 22. Aqua Baby Club Praha, Kolín.

3.6 babyclub-nessie.cz

Pražský Baby Club nazvaný Nessie poskytuje plavání pro kojence a batolata. Jeho webové stránky působí dětským a jednoduchým vzhledem. Nachází se zde dvě horizontální menu, kdy jedno obsahuje pouze odkazy a druhé je obrázkové s odkazy schovanými u různých druhů mořských živočichů. Pod oběma menu se nachází úvodní strana s informacemi ohledně přihlášek do kurzů a pár videi z průběhu kurzů plavání, v pravém sloupci pak aktuality.

Při čtení na mobilním zařízení se sice schovají obě nabídky, ale článkům zůstává původní velikost, tudíž se nemůžeme bavit o responzivním webu. neboť je obsah obtížně čitelný. [52]

Obr. 23. Baby Club Nessie.

4 BEZPEČNOST A HROZBY WEBOVÝCH APLIKACÍ

Každá webová aplikace může být napadena na mnoha úrovních, což znamená od operačního systému běžícího na serveru až po samotný webový prohlížeč uživatele. Předtím, než budou uvedeny některé příklady nejčastějších útoků na webové aplikace, jsou zmíněny základní poznatky o protokolu HTTP.

Protokol HTTP je *bezestavový* a jeho základem je URL, což je identifikace dokumentu, který je poskytnut uživateli. I přesto, že je HTTP bezstavový protokol, může být předán stav aplikace několika způsoby. Prvním způsobem je, že si webová aplikace uloží údaje přímo do URL a ty přenáší ze stránky na stránku (např. index.php?JSESSIONID=abc). Druhým způsobem je využití cookie webového prohlížeče. Jedná se o textovou informaci, která je přijata v HTTP hlavičce požadavku ze serveru. Cookie je vázána na doménu, ze které byla přijata. Během komunikace se serverem z dané domény se posílá cookie s každým HTTP požadavkem zpátky na server.

Protokol HTTP obsahuje několik metod pro komunikaci. První z metod je *GET*, která se používá pro zjištění nebo přečtení informace ze serveru. Požadavky poslané touto metodou nemodifikují stav na serveru, proto mohou internetové vyhledavače generovat požadavky s využitím této metody. Druhou z metod je *POST*, která se využívá ke změně stavu na serveru a v případě, že potřebujeme na server nahrát větší množství dat (např. soubor). [57]

4.1 SQL Injection

Tento typ útoku na webovou aplikaci zneužívá nesprávného vstupu od uživatele při skládání dotazů a jejich parametrů do jiného systému. Znamená to vlastně špatnou obsluhu parametrů při samotném vytváření SQL dotazu.

Příkladem může být následující dotaz:

```
String query = "select * from tabulka where field = '"+vstupni_text+"'";
```

Avšak pokud uživatel místo vstupni_text napíše “‘ or 1=1 or field= ‘“, může tímto způsobem přečíst všechna data uložená v databázi, protože spojením vznikne dotaz:

```
select * from tabulka where field = '' or 1=1 or field = ''
```

Uživatel může také za pomocí subselectů či joinů přečíst data i z jiných tabulek.

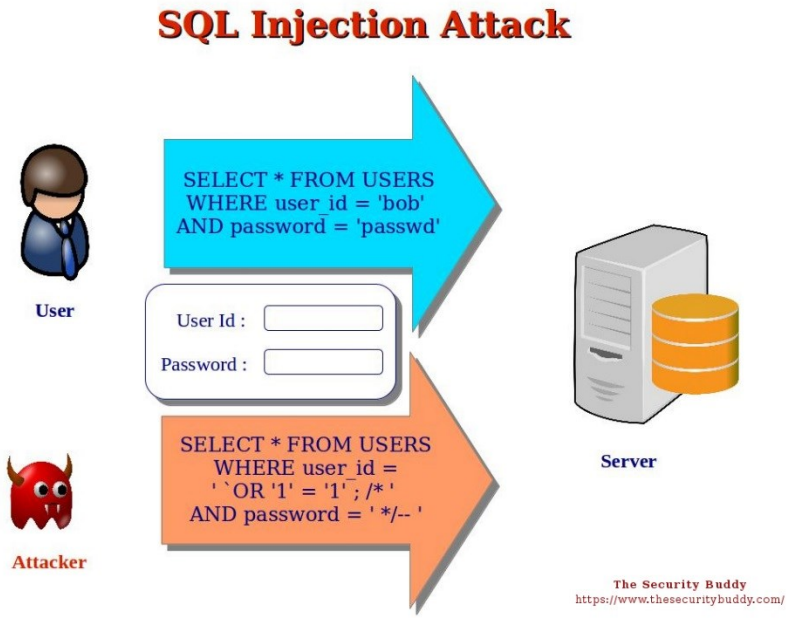
Problém takovéhoto rozsahu má naštěstí snadné řešení, což znamená nesestavovat dotaz SQL pomocí skládání jednotlivých řetězců. Správně sestavený dotaz by vypadal například takto:

```
String query = "select * from tabulka where field = :p_field";

Query q = session.createQuery(query);

q.setString("p_field", param);
```

Při dodržování tohoto přístupu můžeme snadno identifikovat případné problémy již pouhým pohledem na kód. Následující obrázek ukazuje útok SQL injection graficky. [57] [64]



Obr. 24. SQL Injection. [58]

4.2 Cross-site Scripting (XSS)

Útok nazvaný Cross-site Scripting, neboli zkráceně XSS spočívá ve schopnosti útočníka vložit nedůvěryhodné údaje nebo skripty do webové stránky. Tyto vložené údaje/skripty se uživateli spustí ve webovém prohlížeči a mohou mu ukrást důležitá data, poškodit webové stránky atd.

Typy XSS jsou 3:

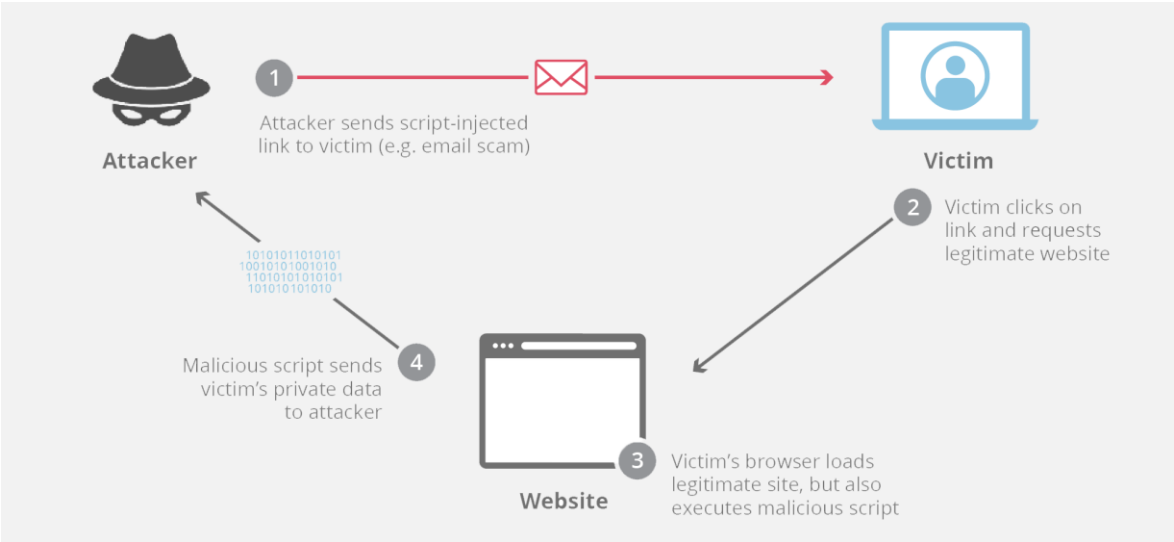
- *Reflected* – jako příklad může být stránka s vyhledávacím polem: Uživatel zadá JavaScriptový kód a jakmile je stiknuto tlačítko pro vyhledávání, skript je zpracuje a na obrazovce se zobrazí vyskakovací okno. Nyní může být skript změněn podle potřeby a krást data, nebo poškozovat webové stránky.

- *Stored* – příkladem může být web s komentáři a uživatelův komentář je uložen a zobrazen. Uživatel může vložit nakažený skript do pole pro psaní komentáře a tento skript bude spouštěn pokaždé, když se stránka načte.
- *DOM-based*

Obrana proti tomuto útoku je povolení CSP (Content-Security-Policy, Zásady ochrany obsahu), kódování výstupu a vynechání nedůvěryhodných znaků.

[55] [64]

Obrázek uvedený níže znázorňuje útok XSS.



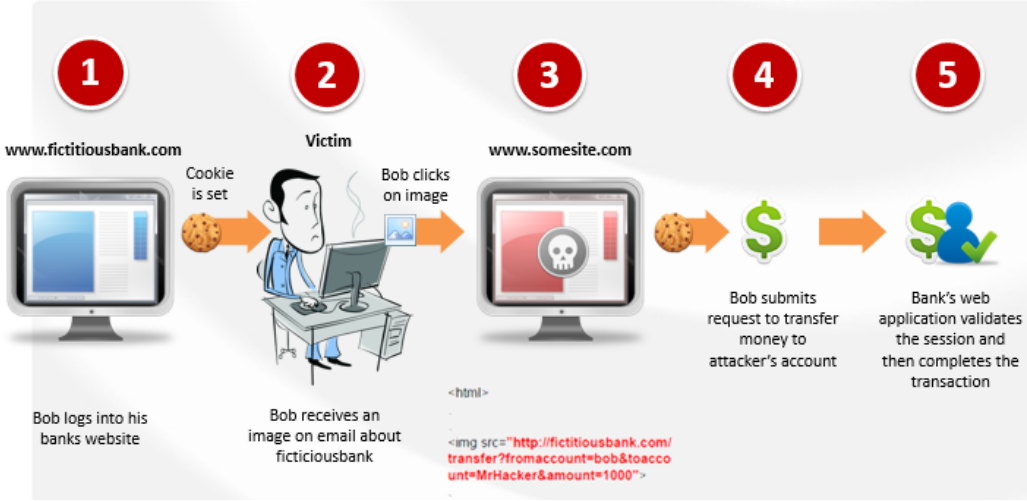
Obr. 25. Cross-site Scripting útok. [59]

4.3 Cross-site Request Forgery (CSRF)

Dalším příkladem útoku, který může nastat je takovýto:

<img src="http://www.vasebanka.cz/submitTranser/?account=**1/1234**&amount=**1000000**&confirm=1">

Cílem obrázku je URL, ve skutečnosti je to ale formulář, který je odeslaný pomocí metody GET. Kdyby systém na adrese www.vasebaka.cz nepožadoval další údaje pro potvrzení této operace (account – číslo účtu, amount – částka, confirm=1 – potvrzení), mohlo by nastat opravdové odeslání peněz. Předpokladem je uživatelovo přihlášení a jeho platná cookie ve webovém prohlížeči.



Obr. 26. Cross-site Request Forgery (CSRF) [60]

Obrana proti tomuto útoku je možná například pomocí CAPTCHA nebo SMS, poté nelze operace z prohlížeče nijak podvrhnout. [55]

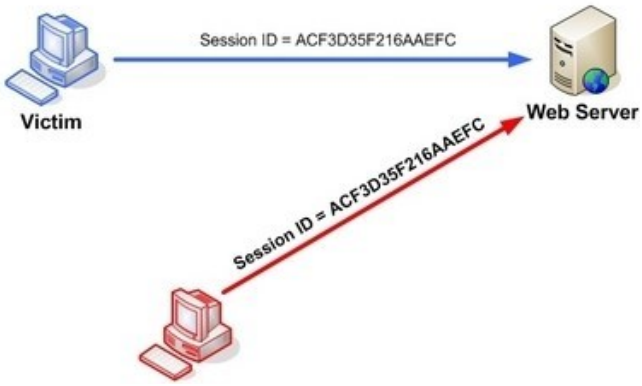
4.4 Broken Authentication

Prolomené ověřování neboli Broken Authentication znamená, že pokud aplikace nesprávně spravuje informace související se session tak, že je narušena totožnost uživatele. Tyto informace mohou být ve formě souborů cookie, hesel, tajných klíčů atd.

Cílem je se buď dostat do relace jako někdo jiný, nebo použít session, která byla ukončena uživatelem, anebo ukrást informace související s touto session.

Obrana proti této krádeži session může být:

- Použití multifaktorového ověření.
- Izolace session.
- Vypršení session.
- Používání zabezpečených souborů cookie. [55]



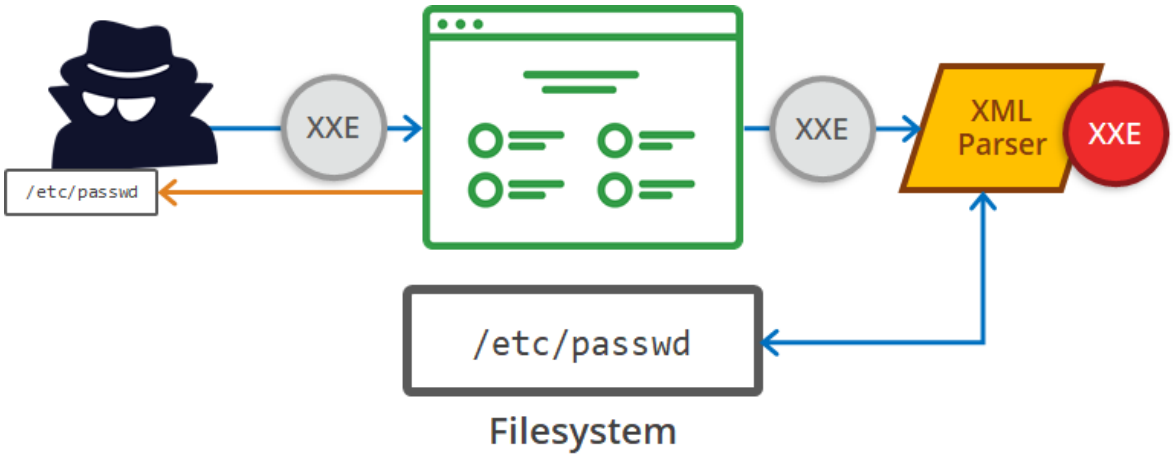
Obr. 27. Broken Authentication. [61]

4.5 XML External Entities (XXE)

Webová aplikace je náchylná k XXE útokům, pokud je útočníkovi dovoleno nahrát nakažený XML kód, který dále zneužívá zranitelný kód. To může být použito pro krádež dat a provádění dalších škodlivých úloh.

Jako protiopatření mohou být udělána:

- Vyhnout se serializaci citlivých dat.
- Provést přístup založeného na whitelistu na straně serveru, aby se zabránilo nahrávání škodlivého XML kódu.
- Používání WAF pro detekci a blokování XXE.
- Code review, neboli kontrola kódu druhou osobou. [55]

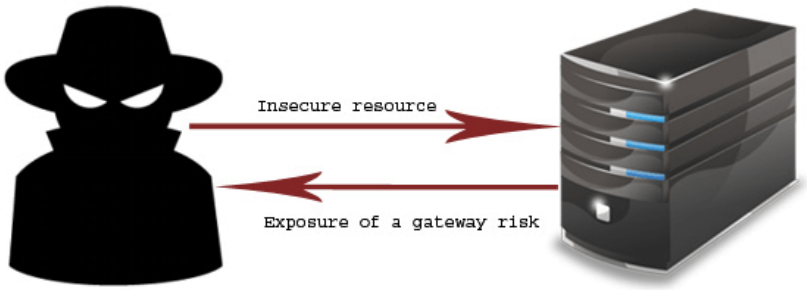


Obr. 28. XML External Entities (XXE). [62]

4.6 Security misconfiguration

Vývojáři a IT pracovníci zajišťují funkčnost, ale nikoli bezpečnost. Konfigurace jsou prováděny na aplikačním serveru, databázovém serveru, proxy, aplikacích a dalších zařízeních a musí být v souladu s bezpečnostními požadavky. Většina těchto požadavků se vynechá, pokud nejsou zjištěny odborníky, nebo hackery.

Příklady těchto chybných konfigurací jsou například slabá hesla, výchozí hesla, výchozí skripty uložené na serverech, výchozí adresáře, výchozí chybové hlášky atd.



Obr. 29. Security misconfiguration. [55]

4.7 Nezabezpečený přímý odkaz na objekt

Jako parametry v URL adrese webové stránky jsou často předávány jména souborů, nebo primární klíče z databáze. Pro útočníka je to možnost, jak aplikaci zneužít a pomocí změny jména, nebo klíče se do aplikace dostat bez potřebné autorizace.

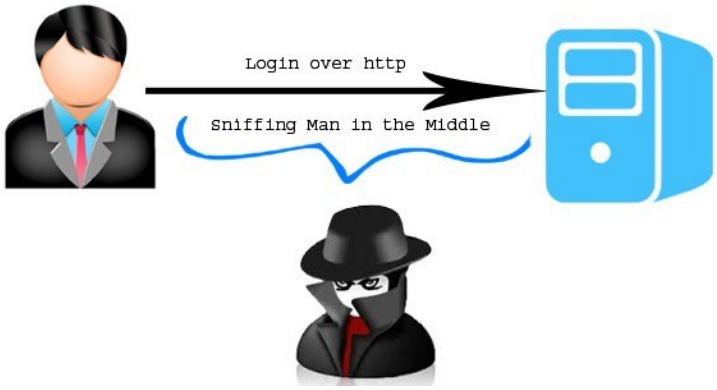
Obrana před touto zranitelností webové aplikace může být použití nepřímé reference, validace přímého odkazu, nebo kontrolu přístupu a nespoléhat na předchozí ověření uživatele. [56]

4.8 Sensitive data exposure

Tento útok spočívá v tom, že útočník může zachytit nebo modifikovat citlivá data, pokud se s nimi v aplikaci nezachází bezpečně. Příkladem je použití slabých šifrovacích klíčů. Nebo použití slabých TLS (z angličtiny Transport Layer Security). Cílem útoku je identifikace citlivých datových bitů a jejich využití.

Jako ochrana může být:

- Šifrování všech dat při jejich přenosu i nečinnosti.
- Použití zabezpečených protokolů a algoritmů.
- Zablokování cachování odpovědí s citlivými daty, kdy by mohli hackeři získat kopii cache a ukrást z ní informace. [55]



Obr. 30. Sensitive data exposure. [63]

4.9 Insecure deserialization

Některé aplikace ukládají data na straně klienta a používají při tom serializaci objektů. Aplikace, které spoléhají na zachování stavu klienta mohou umožnit manipulaci se serializovanými daty. Toto je pak nový vstup v seznamu a je těžké ji využít.

Příkladem je změna serializovaných objektů v souborech cookie po eskalaci privilégií.

X: x: {z: z:”NAME”: r:”USER”} -->> Původní cookie
X: x: {z: z:”NAME”: r:”ADMIN”} -->> Změněný cookie object

Jako opatření proti tomuto útoku můžeme provést:

- Šifrování serializovaných dat.
- Spouštění deserializace s nejmenšími oprávněními. [55]

II. PRAKTICKÁ ČÁST

5 ZVOLENÉ TECHNOLOGIE

Technologií pro vývoj webových aplikací existuje celá řada. Mnohdy není jednoduché vybrat ty pravé mezi takovým množstvím. Vývojář musí dopředu vědět co se od dané aplikace očekává a co by měla splňovat. Podle toho odhadne její složitost a zvolí ty, které jsou vyhovující pro samotný vývoj konkrétního webu. Následující podkapitoly představují vybrané technologie pro vývoj nové webové stránky Baby Clubu Katka.

5.1 HTML a CSS

Základem každé webové stránky je značkovací jazyk HTML. Skládá z jednotlivých značek tzv. tagů a jejich vlastností nazvaných atributy. Mezi tyto značky se nejčastěji uzavírají části textu, avšak některé tagy nejsou párové, což znamená, že jsou uvedeny jen před blokem textu. Dokument HTML má danou svoji strukturu, kterou je potřeba dodržet. Současná verze tohoto značkovacího jazyka je verze 5, která přináší řadu vylepšení.

Kaskádové styly neboli CSS se starají o vzhled webu a udávají, jak se má každý prvek zobrazit. Dokument obsahuje vždy selektor, což je název id, nebo class HTML tagu a následuje blok deklarací oddělenými středníky. CSS obsahuje mnoho různých selektorů, které se mohou kombinovat.

5.2 Bootstrap 4

Tento open source toolkit slouží pro vývoj responzivních webových a mobilních projektů a je nejpopulárnější front-end knihovnou. Obsahuje velkou sadu předdefinovaných prvků, které je možné ihned využít uvnitř HTML tagů a případně si je přizpůsobit ve svém vlastní CSS a přepsat tak původní styl prvku. Bootstrap má přehledně zpracovanou dokumentaci všech prvků a pomocí něj je možno velmi rychle nastylovat webovou stránku. Tento velmi užitečný nástroj vyvinul Twitter a v současnosti je ve verzi 4.

5.3 PHP 7

Serverovým skriptovacím jazykem, který se stará o logiku webové aplikace a dělá z ní interaktivní a dynamickou je PHP. Příkazy toho jazyka jsou prováděny na serveru a vráceny zpět do webového prohlížeče (klienta). PHP může být použit pro generování dynamického obsahu stránky, k práci s databází, cookies, sessions, k řízení přístupu uživatelů, nebo šifrování dat a dalších činností. Nově vydaná verze 7 poskytuje mnoho vylepšení

jako například celkové zrychlení, vylepšení obsluhy chyb, podporuje přísnější typovou deklaraci pro argumenty funkcí, přináší nové operátory a mnoho dalšího.

5.4 Redakční systém – WordPress

Jak již bylo zmíněno v předchozích kapitolách, v dnešní době se webové stránky tvoří tak, že se vezme již existující řešení (nejčastěji některý z redakčních systémů) sloužící jako administrace a dodělá se šablona a potřebná funkcionalita, která se na toto řešení naváže. Tento moderní způsob byl zvolen i zde při vývoji nových webových stránek.

Jako administrační rozhraní byl zvolen redakční systém WordPress. Důvodů je hned několik, a to že v první řadě má velmi *uživatelsky intuitivní a přívětivé rozhraní*, které zvládne obsluhovat jakýkoli uživatel, tedy i ten, který se o webové stránky vůbec nezajímá. To je také hlavním důvodem, proč je WordPress nejpopulárnější platformou. Jako jeden z menšiny CMS systémů má *pravidelné aktualizace* týkající se především bezpečnosti a jiných vylepšení – v poslední době například byl přidán nový editor příspěvků. Dalšími důvody jsou *cena* – kdy stáhnutí, instalace a provoz je zdarma, *podpora* – pokud má uživatel problém, stačí se zeptat v diskuzi, *rozšiřitelnost* – velké množství pluginů je možnost jednoduše rozšířit web o novou funkcionalitu a je zde možnost nepřeberného množství možnosti úprav a práce přímo s kódem.

6 POUŽITÉ PLUGINY

V přechozích kapitolách byla zmíněna rozšiřitelnost redakčních systémů. Pokud se uživatel rozhodne doinstalovat nějaký plugin, není vůbec jednoduché vybrat ten pravý a vyhovující daným potřebám. Doplňků s hledanou funkcionalitou existuje velké množství, které se liší většinou jen minimálně. Pro web byly vybrány takové moduly, které jsou často aktualizované, udržované a v neposlední řadě byla zvažována také oblíbenost uživatelů a počet instalací. K dosažení potřebné funkcionality byly zde použity pluginy, které jsou popsány v následujících podkapitolách.

6.1 Contact Form 7

Tento plugin slouží pro vytváření formulářů jak kontaktních, tak i pro jiné účely. Umožňuje přizpůsobení samotného formuláře, tak i obsahu zprávy za pomoci jednoduchých formátovacích značek.

Je zde také implementována podpora, která je řízena Ajaxem, ochrana za pomocí CAPTCHA či Aksimet spam filtraci.

Přes pět milionů uživatelů si stáhlo tento doplněk a aktivně jej používá. Přeložen je do 56 světových jazyků, takže si uživatel může nastavit svůj mateřský jazyk.

6.2 Send PDF for Contact Form 7

Podmínkou pro jeho použití je instalace předchozího pluginu, protože za pomocí tohoto doplňku lze získávat data z Contact Form 7 s využitím pojmenovaných značek, kterými byly vytvořeny prvky formuláře. Ty se zde dají volat a podle potřeby vkládat do vestavěného editoru a následně exportovat do souboru PDF.

Možnost je i exportu do souboru CSV. Soubory je možno ukládat do databáze, nebo ihned po odeslání e-mailem vymazat a šetřit tak místo.

Plugin poskytuje mnoho nastavení jako například hlavičku a patičku, kde může být vložen i obrázek.

Pro soubor PDF poskytuje ochranu buďto náhodně vygenerovaným heslem, nebo může uživatel zadat svoje unikátní heslo. Nastavit lze také jméno souboru, formát data a času a zda se má vygenerovaný soubor zobrazit v tom samém, nebo v novém okně.

6.3 WP Mail SMTP

Aby mohl být z WordPressu odeslán e-mail, je nutné doinstalovat tento plugin, který se o tuto činnost stará. Tyto zprávy jsou posílány přes protokol SMTP, což je standardní protokol. Vybrat si lze ze čtyř možností SMTP, a to Mailgun, SendGrid, Gmail anebo ostatní. Nechybí ani volba pro autentizaci a výběr SSL nebo TLS šifrování a zadání portu.

6.4 WP Limit Login Attempts

Plugin sloužící pro omezení počtu pokusů přihlášení do administračního rozhraní. Pokud je počet pokusů o přihlášení přesažen, plugin automaticky zablokuje danou IP adresu. Chrání také web proti útokům hrubou silou, kdy je snaha o uhodnutí uživatelského jména a hesla znovu a znovu a pokusu o přihlášení. Integrována je CAPTCHA, kdy je po uživateli požadováno opsání kódu z obrázku. Splňuje také požadavek GDPR, kde jsou IP adresy zahashovány algoritmem MD5.

6.5 Really Simple SSL

Po aktivování tohoto doplňku je automaticky zjištěno nastavení webu a každý nezabezpečený požadavek přesměrován na zabezpečený. Pro jeho aktivaci je potřeba platný SSL certifikát, který by se získal až po nasazení na hosting. V novém webu je jen nainstalovaný, ale ne aktivovaný.

Plugin skenuje celý web a ukazuje, co je potřeba opravit v případě, že se neukáže zelený zámek. Je zde také kontrola vypršení platnosti certifikátu, kdy je uživateli odeslán e-mail, že jeho certifikát brzy vyprší.

6.6 API QR Server

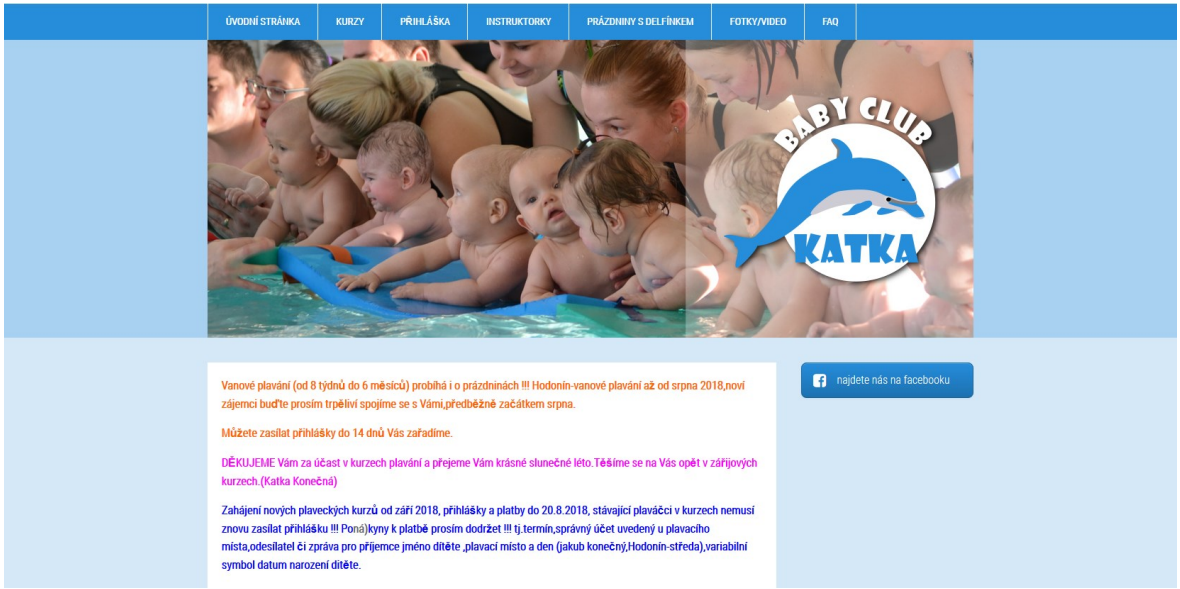
Toto webové rozhraní slouží pro generování a čtení QR kódů. V nové webové aplikaci je využito pro generování těchto kódů, kde se potřebné parametry předají v adrese a server vrátí obrázek ve formě QR kódu.

Možno je generovat jak klasické černobílé kódy, tak barevné. Barvu si může uživatel zvolit podle svých preferencí a potřeby.

Poskytnuta je také přehledná dokumentace, kde jsou uvedeny všechny parametry a způsoby jejich zápisu a jak je předat v samotné URL adrese pro vygenerování QR kódu.

7 REALIZACE NAVRHNUTÉHO ŘEŠENÍ

Důvodem pro vytvoření nových webových stránek pro Baby Club byla převážně jejich nepřehlednost a zastaralost. V době, kdy se tato práce začínala řešit, vypadaly stránky jako na obrázku č. 31. Jejich horizontální menu působí sice na první pohled docela přehledně, avšak některé položky jsou rozevírací a pro uživatele je problém nalézt potřebné informace na takovémto webu. Čili úkolem bylo zpřehlednit a utřídit toto množství informací.

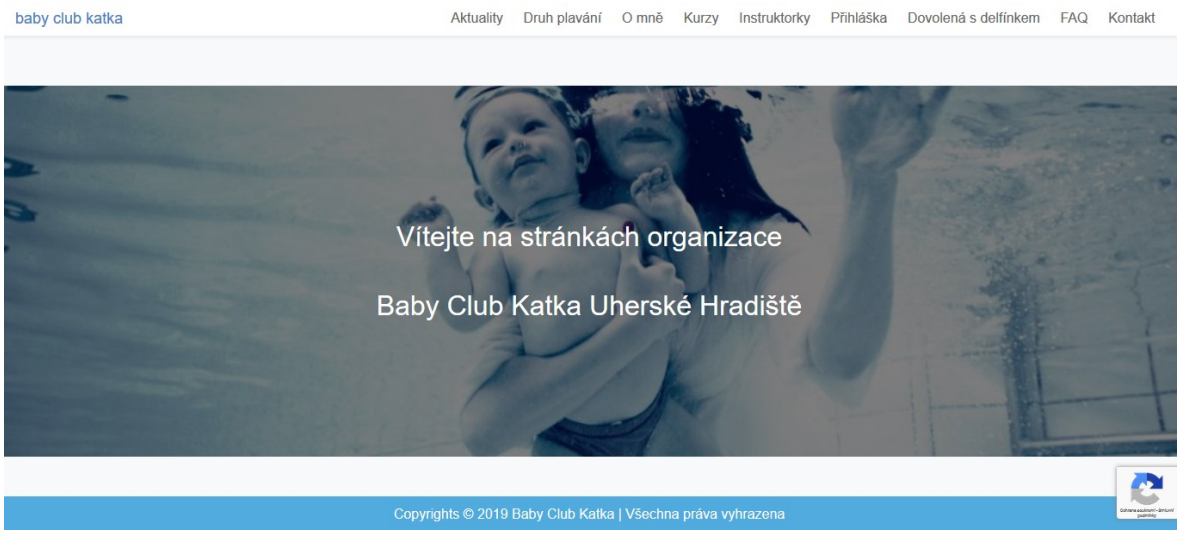


Obr. 31. Staré webové stránky Baby Clubu Katka.

Dalším požadavkem nebo spíše funkcionalitou nového webu byl formulář pro přihlášení se do kurzu a vygenerování faktury s QR kódem, která se následně odešle na e-mail vedoucí Baby Clubu a také na zadaný e-mail přihlášeného rodiče dítěte.

Nové řešení webové stránky přináší opět horizontální menu umístěné v horní části a skládá se z devíti rubrik. V některých se nachází další dokumenty a příspěvky jako například návštěvní řád, podmínky plavání, informace ohledně GDPR, o místech konání kurzů a dalších potřebných údajů k nim. Prostřední část vždy vyplňuje obsah zvolený uživatelem z menu. V dolní části se pak nachází patička webu s ochranou proti kopírování.

Návrh nového webu po příchodu na úvodní stránku je možné vidět na obrázku č. 32. Uživatel si na první pohled může všimnout modernějšího a čistějšího vzhledu. Webový portál je také plně přizpůsoben pro prohlížení na mobilních zařízeních, čímž se také liší od staré verze webové stránky.



Obr. 32. Nový web Baby Clubu.

7.1 Funkcionalita formuláře přihlášky

Pokud se uživatel přepne do rubriky *Přihláška*, uvidí obrazovku, která se skládá ze dvou částí. Vpravo se nachází tři důležité dokumenty, které by si měl přečíst předtím, než vyplní a odešle samotnou přihlášku. Jsou to dokumenty *GDPR*, *Návštěvní řád* a *Podmínky plavání*. Po kliknutí na tlačítko *Více* se zobrazí celý příspěvek s daným dokumentem. Nalevo se pak nachází tlačítko *Přihláška*, odkud se dostane na zmíněný formulář. Ten byl vytvořen následujícím kódem pomocí pluginu Contact Form 7.

```
<label> Jméno dítěte (vyžadováno)
   [text* child-name] </label>
<label> Jméno rodiče (vyžadováno)
   [text* parent-name] </label>
<label> Datum narození (vyžadováno)
   [date* date-407] </label>
<label> Ulice a č. p. (vyžadováno)
   [text* street-name] </label>
<label> Město (vyžadováno)
   [text* city-name] </label>
<label> PSČ (vyžadováno)
   [number number-351] </label>
<label> Telefon (vyžadováno)
   [tel tel-300] </label>
<label> E-mail (vyžadováno)
```

```
    [email* your-email] </label>
<label> Poznámky
    [textarea textarea-270] </label
Typ Kurzu
    [radio radio-537 default:1
      "rehabilitační vany v Uh. Hradišti.....1000,- Kč"
      "rehabilitační vany v Hodoníně.....1000,- Kč"
      "bazén v aquaparku Uh. Hradiště (ÚT dopoledne) .....1600,- Kč"
      "bazén v aquaparku Uh. Hradiště (ST dopoledne) .....1600,- Kč"
      "bazén v aquaparku Uh. Hradiště (NE dopoledne) .....1600,- Kč"
      "plavecký bazén v Hodoníně (PO odpoledne) .....1850,- Kč"
      "plavecký bazén v Hodoníně (ÚT odpoledne) .....1850,- Kč"
      "plavecký bazén v Hodoníně (ST dopoledne) .....1850,- Kč"
      "plavecký bazén v Hodoníně (SO dopoledne) .....1850,- Kč"
      "plavecký bazén v Břeclavi (PÁ odpoledne) .....1850,- Kč"
      "plavecký bazén v Břeclavi (NE dopoledne) .....1850,- Kč"
      "plavecký bazén v Hustopečích (ČT odpoledne) .....1500,- Kč"]
Souhlas s podmínkami
[checkbox* checkbox-521 "Odesláním formuláře souhlasím s návštěvním řádem, podmínkami plavání a zpracováním osobních údajů."]
[submit "Odeslat"]
```

Když uživatel vyplní a odešle přihlášku kliknutím na tlačítko *Odeslat* vygeneruje se na pozadí PDF soubor s fakturou a QR kódem, který může posloužit po přečtení mobilní aplikací banky pro vyplnění některých polí pro zaplacení plaveckého kurzu. Uživateli i vedoucí klubu přijde e-mail o přihlášení se do kurzu, kde v příloze je možné nalézt již zmíněný PDF soubor s fakturou. Soubor je generován následujícím kódem. Poslední řádek je vložení samotného QR kódu, který se vygeneruje pomocí API QR Serveru a je přímo nakódován pro přečtení mobilní aplikací banky.

```
<h2>Číslo faktury: <b>[reference]</b></h2>
<hr>
<h4><b>Dodavatel:</b></h4>
Baby Club Katka
U Kina 207
687 24 Uherský Ostroh
```

```
Tel.: +420 604 25 76 85
E-mail: babyclub.katka@seznam.cz
Číslo účtu: 2401266052/2010
<hr>
<h4><b>Odběratel:</b></h4>
[parent-name]
[street-name]
[number-351] [city-name]
Tel.: [tel-300]
E-mail: [your-email]
<hr>
[radio-537]
<hr>
<h4><b>Kód pro platbu:</b></h4>
<img src="https://api.qrserver.com/v1/create-qr-code/?size=150x150&data=SPD*1.0*ACC:CZ4220100000002401266052*CC:CZK*MSG: [reference]">
```

K zobrazení zadaných informací uživatelem do formuláře slouží speciální značky, kterých je možné si všimnout ve výše zmíněném kódu.

Vygenerovaná faktura je zobrazena na obrázku č. 33 na následující straně.

Číslo faktury: 5cd1bf6309671

Dodavatel:

Baby Club Katka

U Kina 207
687 24 Uherský Ostroh
Tel.: +420 604 25 76 85
E-mail: babyclub.katka@seznam.cz

Číslo účtu: 2401266052/2010

Odběratel:

Ludmila Maříková

Lucemburská 286
12345 Plzeň
Tel.: 456987231
E-mail: Dupla@seznam.cz

---

plavecký bazén v Hodoníně (ÚT odpoledne).....1850,- Kč

Kód pro platbu:

Obr. 33. Vygenerovaný PDF soubor faktury s QR kódem.

7.2 Zabezpečení

Útoky na webové aplikace nejsou žádnou novinkou. Činnost, kdy se útočník snaží narušit provoz webu, ukrást citlivá data, nebo jiným způsobem webovou stránku poškodit, je velmi častá. Vývojáři webů se snaží je zabezpečit, jak to jen jde. Ani tento web není výjimkou a má svá zabezpečení.

Prvním zabezpečením je modul, který byl již zmíněn v kapitole použitých pluginů WP Limit Login Attempts. Ten se snaží administrační rozhraní chránit proti útokům hrubou silou, kdy útočník hádá uživatelské jméno a heslo a snaží se tak přihlásit. Plugin chrání proti tomuto útoku požadovaným vyplněním kódu CAPTCHA a poté, pokud se po pár přihlášeních nezdaří úspěšně zadat přihlašovací údaje, zablokuje IP adresu a znemožní tak dalším pokusům.

Dalším způsobem je zabezpečení za pomoci souboru *.htaccess*, v němž se dá nastavit mnoho věcí a zamezit tak přístup k různým částem webové stránky. Je zde zakázáno zobrazení souboru *wp-config.php*, procházení adresářové struktury, ochrana samotného souboru *.htaccess*, zákaz skenování autorů, kteří se mohou přihlásit do administrace, a také je zakázán přístup externím aplikacím k WordPressu. Níže je kód hlavního souboru *.htaccess*.

```
# BEGIN WordPress

<IfModule mod_rewrite.c>
RewriteEngine On
RewriteBase /baby-club-katka-wordpress/
RewriteRule ^index\.php$ - [L]
RewriteCond %{REQUEST_FILENAME} !-f
RewriteCond %{REQUEST_FILENAME} !-d
RewriteRule . /baby-club-katka-wordpress/index.php [L]
</IfModule>

# zabezpečení wp-config.php
<Files wp-config.php>
order allow,deny
deny from all
</Files>
```

```
# zákaz procházení adresářů
Options All – Indexes

# ochrana samotného .htaccess
<files .htaccess="">
order allow,deny
deny from all
</files>

# ochrana všech .htaccess
<Files ~ "^.*\.([Hh][Tt][Aa])">
order allow,deny
deny from all
satisfy all
</Files>

# BEGIN block author scans – zákaz skenování autorů -> proti útoku hrubou silou
RewriteEngine On
RewriteBase /
RewriteCond %{QUERY_STRING} (author=\d+) [NC]
RewriteRule .* - [F]
# END block author scans

# Block WordPress xmlrpc.php requests – zákaz přístup pro externí aplikace k WP
<Files xmlrpc.php>
order deny,allow
deny from all
</Files>

# END WordPress
```

7.3 Zhodnocení vývoje

Při vývoji nových webových stránek s administračním rozhraním, o které se stará redakční systém WordPress, byl kladen důraz na jednoduchost při jejich editaci, přehlednost uvedených informací a na zabezpečení proti napadení. Oproti staré verzi

Nově vytvořený webový portál by mohl být nahrán na hostingový server wedos.cz s měsíčním tarifem necelých 40,- Kč, kde by probíhal zkušební provoz. Podle následných ohlasů uživatelů webových stránek by byly následně implementovány vylepšení a další funkce, které by jim usnadnily orientaci na webu a jeho používání.

Sběr požadavků na funkcionalitu webu trval 2 hodiny. Výběr vhodných technologií a nástrojů a následné seznámení se s nimi zabralo cca 8 hodin. Na samotném vývoji bylo stráveno okolo 175,- člověkohodin. Nasazení webových stránek na hostingový server by zabralo cca 1,5 hodiny. Celkový počet hodin je tedy 186,5 a celková cena je vyčíslena na 24 245,- Kč.

Pravidelná údržba by probíhala jednou za půl roku a v rámci ní by byla provedena aktualizace CMS systému, což by trvalo cca 1 hodinu. Dále dodělání funkcionality podle náročnosti okolo 4 hodin. To je vyčísleno na cca 1 490,- Kč.

Ovládání administračního rozhraní je intuitivní a uživatelsky přívětivé a web je navrhnut tak, že si vedoucí Baby Clubu může jeho obsah editovat sama. V případě chybějící funkcionality by bylo možno ji dodělat za poplatek dle její náročnosti.

ZÁVĚR

Úkolem této diplomové práce bylo provést literární rešerši nástrojů pro tvorbu webových projektů, seznámit se a vyhledat již realizovaná řešení webů typu „Baby Club“. Na základě toho zvolit vhodné řešení z pohledu dostatečného výkonu, uživatelsky přívětivého prostředí, administrace, bezpečnosti a požadavků GDPR. Do tohoto řešení poté implementovat vhodné moduly pro využití QR kódů dle požadavků vedoucí Baby Clubu.

V rámci výše zmíněných úkolů byl vytvořen nový webový portál, založený na redakčním systému WordPress, který si vedoucí klubu může editovat podle svého uvážení a libosti. Tento web se velmi liší od svého předchůdce, protože přináší přehledně utříděné informace pro zájemce o služby výše zmíněné organizace. Dále zde byla implementována nová funkcionalita pro přihlašování zájemců do kurzů, kdy se po vyplnění a odeslání přihlášky vygeneruje faktura v PDF souboru se zadanými informacemi a QR kódem, který je možno využít pro předvyplnění některých polí platby v mobilní aplikaci banky. Následně jsou zaslány e-maily jak vedoucí klubu, tak zájemci o kurz i s touto fakturou.

Web je také zabezpečen jak v části administračního rozhraní proti útokům hrubou silou a je zde omezeno opakované přihlášení, tak v uživatelské části, kde je znemožněno zobrazování a procházení složek webu a různé další operace zmíněné v předchozích kapitolách.

Tato práce se v teoretické části zabývala srovnáváním nástrojů pro tvorbu webových stránek. Uvedla některé více či méně známé redakční systémy, které jsou moderním způsobem tvorby webů a také několik online editorů za pomocí kterých lze také vytvořit svůj blog či webovou prezentaci jednoduchým způsobem. Dále byly uvedeny portály podobného typu a zhodnoceno jejich provedení z hlediska vzhledu, přehlednosti dostupných informací a používání běžným uživatelem. Zmíněny byly i vybrané nejčastější útoky na webové aplikace.

V praktické části byly představeny a zdůvodněny technologie a nástroje, které byly použity při vytváření nového webového portálu. Následně byly představeny implementované pluginy, které byly popsány z pohledu funkčnosti a odůvodněny proč byly použity a podle jakých kritérií se vybíraly. Poslední kapitola se zabývala samotným popisem nově vytvořeného webu, srovnáním se starým webem a dále popisovala novou funkcionalitu včetně kódů a bylo zde také popsáno zabezpečení samotného portálu. Dále byl zhodnocen celý vývoj webového portálu.

Jako v každé webové aplikaci, i zde se najdou různé chyby a rezervy, které byly opomenuty při vývoji. Autor si je vědom nedostatků a za provozu webové stránky by mohly být tyto chyby odstraněny, nebo implementováno rozšíření zabezpečení celého portálu.

SEZNAM POUŽITÉ LITERATURY

[1] *Stránky k výuce informatiky* [online]. Vlašim: Gymnázium Vlašim, 2019 [cit. 2019-03-22]. Dostupné z: http://www.ivt.mzf.cz/seminar/7-redakcni-systemy/

[2] *Co je redakční systém a k čemu slouží* [online]. 2013 [cit. 2019-03-22]. Dostupné z: http://www.webzpravodaj.cz/236-co-je-redakcni-system-a-k-cemu-slouzi/

[3] *Webové stránky – pořiďte si lepší webové stránky* [online]. 2014 [cit. 2019-03-22]. Dostupné z: https://www.webovestranky.com/webove-stranky-redakcni-systemy/

[4] *Quadronet* [online]. Praha, 2019 [cit. 2019-03-22]. Dostupné z: http://www.quadronet.cz/redakcni-system/

[5] *WPLama – Internetové stránky na WordPressu snadno a česky* [online]. Písek, 2014 [cit. 2019-03-22]. Dostupné z: https://www.wplama.cz/pro-zacatecniky-co-to-vlastne-je-redakcni-system/

[6] *Petr Němeček – Jak se zorientovat v redakčních systémech?* [online]. Plzeň, 2017 [cit. 2019-03-22]. Dostupné z: https://www.nemecekpetr.cz/blog/jak-se-zorientovat-v-redakcnich-systemech

[7] *Critical – Proč byste měli chtít redakční systém?* [online]. Praha, 2016 [cit. 2019-03-22]. Dostupné z: https://www.critical.cz/blog/proc-byste-meli-chtit-redakcni-system

[8] *MCNULTY, Scott. WordPress – Efektivní publikování na webu.* Brno: Zoner Press, 2009. ISBN 978-80-7413-042-7.

[9] *KUDLÁČEK, Luboš. WordPress – Podrobný průvodce tvorbou a správou webu.* Brno: Computer Press, 2010. ISBN 978-80-251-2734-6.

[10] *Jaký CMS zvolit?* [online]. 2019 [cit. 2019-04-05]. Dostupné z: http://jakycmszvolit.cz

[11] *10 nejlepších redakčních systémů (CMS)* [online]. Brno: ZONER software, 2011 [cit. 2019-04-05]. Dostupné z: https://www.interval.cz/clanky/10-nejlepsich-redakcnich-systemu-cms/

[12] *WordPress – logo* [online]. [cit. 2019-04-05]. Dostupné z: https://www.webin.sk/wordpress-logo-hoz-cmyk-1038x360/

[13] *WordPress – administrace* [online]. [cit. 2019-04-05]. Dostupné z: https://www.hostinger.com/tutorials/wordpress/how-to-login-to-wordpress-dashboard

[14] *Drupal – logo* [online]. [cit. 2019-04-05]. Dostupné z: https://www.cludo.com/cms-site-search/drupal-logo/

[15] *Drupal – administrace* [online]. Drupal commerce, 2018 [cit. 2019-04-05]. Dostupné z: https://drupalcommerce.org/blog/10943/how-create-drupal-8-toolbar-icon

[16] *Joomla! - logo* [online]. [cit. 2019-04-06]. Dostupné z: https://docs.joomla.org/Joomla:Brand_Identity_Elements/Official_Logo

[17] *Joomla! - administrace* [online]. [cit. 2019-04-06]. Dostupné z: https://www.webhostinghub.com/help/learn/website/joomla/joomla-login

[18] *RAHMEL, Dan. Joomla – Podrobný průvodce tvorbou a správou webu.* Brno: Computer Press, 2010. ISBN 978-80-251-2714-8.

[19] *OVH – Výběr toho správného redakčního systému pro Vaše stránky* [online]. 2019 [cit. 2019-04-06]. Dostupné z: https://www.ovh.cz/webhosting/website/porovnani-cms/

[20] *ExpressionEngine* [online]. 2019 [cit. 2019-04-07]. Dostupné z: https://expressionengine.com/

[21] *ExpressionEngine je nyní open source a zdarma* [online]. 2018 [cit. 2019-04-07]. Dostupné z: https://www.svetcms.cz/expressionengine-je-nyni-open-source-a-zdarma/

[22] *Nejlepší menší redakční systémy* [online]. 2018 [cit. 2019-04-07]. Dostupné z: https://www.caste.cz/nejlepsi-mensi-redakcni-systemy/

[23] *Textpattern: zapomenutý redakční systém?* [online]. 2013 [cit. 2019-04-07]. Dostupné z: https://www.tomas-dvorak.cz/posts/textpattern-zapomenuty-redakcni-system/

[24] *Textpattern: Výborný redakční systém pro správu obsahu www stránek* [online]. 2008 [cit. 2019-04-07]. Dostupné z: https://www.profimagazin.cz/textpattern/textpattern-vyborny-redakcni-system-pro-spravu-obsahu-www-stranek

[25] *Typo3 – Getting started* [online]. 2019 [cit. 2019-04-07]. Dostupné z: https://docs.typo3.org/typo3cms/GettingStartedTutorial/GeneralPrinciples/BackendAndFrontend/Index.html

[26] *Redakční systém TYPO3* [online]. 2007 [cit. 2019-04-07]. Dostupné z: https://www.linuxexpres.cz/software/redakcni-system-typo3

[27] *TYPO3 CMS – silný redakční systém* [online]. Trmice, 2019 [cit. 2019-04-07]. Dostupné z: https://www.jirimikula.cz/reseni/typo3/

[28] *The TYPO3 Project and Community* [online]. 2019 [cit. 2019-04-07]. Dostupné z: https://typo3.org/

[29] *Grav – A Modern Flat-File CMS* [online]. 2019 [cit. 2019-04-07]. Dostupné z: https://getgrav.org/

[30] *Grav: redakční systém na redukční dietě a bez databáze* [online]. 2018 [cit. 2019-04-07]. Dostupné z: https://www.root.cz/clanky/grav-redakcni-system-na-redukcni-diete-a-bez-databaze/

[31] *Grav* [online]. 2019 [cit. 2019-04-07]. Dostupné z: https://www.ampps.com/apps/cms/GRAV

[32] *Redakční systém Prestashop* [online]. 2013 [cit. 2019-04-08]. Dostupné z: http://ocemsemluvi.cz/redakcni-system-prestashop/

[33] *Vše o CMS Prestashop* [online]. [cit. 2019-04-08]. Dostupné z: https://www.prestacesky.cz/informace/

[34] *Proč využít eshop Magento?* [online]. [cit. 2019-04-08]. Dostupné z: https://www.artio.net/cz/magento-e-obchod/proc-eshop-magento

[35] *Magento* [online]. 2019 [cit. 2019-04-08]. Dostupné z: https://magento.com/

[36] *Exploring all strengths and weaknesses of Magento CMS* [online]. [cit. 2019-04-08]. Dostupné z: https://www.scnsoft.com/blog/magento-cms

[37] *Webnode Recenze* [online]. 2019 [cit. 2019-04-13]. Dostupné z: https://www.5nej.cz/webnode-recenze/

[38] *Webnode* [online]. Brno, 2019 [cit. 2019-04-13]. Dostupné z: https://www.webnode.cz/

[39] *EStránky* [online]. Praha, 2019 [cit. 2019-04-13]. Dostupné z: https://www.estranky.cz/

[40] *ZOMBEEK Recenze* [online]. 2018 [cit. 2019-04-13]. Dostupné z: https://www.5nej.cz/zombeek-recenze/

[41] *Zombeek.cz* [online]. České Budějovice, 2019 [cit. 2019-04-13]. Dostupné z: https://www.zombeek.cz/

[42] *Zombeek: nový český startup, který chce prorazit mezi nástroji nabízejícími bezplatnou tvorbu webových stránek* [online]. Praha, 2016 [cit. 2019-04-13]. Dostupné

z: https://www.czechcrunch.cz/2016/09/zombeek-novy-cesky-startup-ktery-chce-prorazit-mezi-nastroji-nabizejicimi-bezplatnou-tvorbu-stranek/

[43] *Wix.com Recenze* [online]. 2019 [cit. 2019-04-14]. Dostupné z: https://www.5nej.cz/wix-recenze/

[44] *Wix.com* [online]. 2019 [cit. 2019-04-14]. Dostupné z: https://cs.wix.com/

[45] *Weebly.com* [online]. 2019 [cit. 2019-04-14]. Dostupné z: https://www.weebly.com/

[46] *Weebly Review 2019* [online]. 2019 [cit. 2019-04-14]. Dostupné z: https://www.websiteplanet.com/cs/website-builders/weebly/

[47] *Baby Club Uherské Hradiště* [online]. Uherské Hradiště, 2019 [cit. 2019-04-19]. Dostupné z: http://www.babyclubuh.cz/

[48] *Baby Club Kačka* [online]. 2009 [cit. 2019-04-19]. Dostupné z: http://www.babyclub.cz/babyclub/

[49] *Baby Club Kosatka Mladá Boleslav* [online]. Mladá Boleslav, 2009 [cit. 2019-04-19]. Dostupné z: https://www.babyclubkosatka.cz/

[50] *Baby Club Hrošík* [online]. Beroun, 2014 [cit. 2019-04-19]. Dostupné z: http://babyclub-hrosik.cz/

[51] *Aqua Baby Club* [online]. Beroun [cit. 2019-04-19]. Dostupné z: http://www.aqua-babyclub.cz/

[52] *Baby Club Nessie* [online]. Praha, 2014 [cit. 2019-04-19]. Dostupné z: http://babyclub-nessie.cz/

[53] *Bezpečnost a testování webových aplikací* [online]. Brno, 2007 [cit. 2018-11-27]. Dostupné z: https://is.mendelu.cz/lide/clovek.pl?zalozka=13;id=1732;studium=21237;zp=17212;download_prace=1;lang=cz. Diplomová práce. Mendelova zemědělská a lesnická univerzita v Brně, Provozně ekonomická fakulta.

[54] *Acunetix* [online]. 2017 [cit. 2018-11-27]. Dostupné z: https://www.acunetix.com/blog/articles/acunetix-vulnerability-testing-report-2017/

[55] *OWASP – Top 10 Vulnerabilities in web applications (updated for 2018)* [online]. United States: GreyCampus, 2018 [cit. 2018-11-27]. Dostupné z: https://www.greycampus.com/blog/information-security/owasp-top-vulnerabilities-in-web-applications

[56] *Bezpečnost webových aplikací* [online]. Zlín, 2012 [cit. 2018-11-27]. Dostupné z: https://digilib.k.utb.cz/bitstream/handle/10563/22757/zemek_2012_bp.pdf?sequence=1. Bakalářská práce. Univerzita Tomáše Bati, Fakulta aplikované informatiky.

[57] *Bezpečnost na webu – přehled útoků na webové aplikace* [online]. Praha: Devel.cz Labs, 2008 [cit. 2018-11-27]. Dostupné z: https://www.zdrojak.cz/clanky/prehled-utoku-na-webove-aplikace/

[57] *SQL Injection Attack* [online]. India: The Security Buddy, 2017 [cit. 2018-11-28]. Dostupné z: https://www.thesecuritybuddy.com/vulnerabilities/what-is-sql-injection-attack/

[59] *Cross-site Scripting Attack* [online]. United States: Cloudflare, 2018 [cit. 2018-11-28]. Dostupné z: https://www.cloudflare.com/learning/security/threats/cross-site-scripting/

[60] *Cross-site Request Forgery (CSRF)* [online]. Indusface, 2014 [cit. 2018-11-28]. Dostupné z: http://www.indusface.com/blog/wp-content/uploads/2014/07/CSRF_Blog_1.png

[61] *Broken Authentication* [online]. GB Hackers, 2016 [cit. 2018-11-28]. Dostupné z: https://i0.wp.com/gbhackers.com/wp-content/uploads/2016/10/session.jpg?resize=384%2C253&ssl=1

[62] *Acunetix* [online]. 2017 [cit. 2018-11-27]. Dostupné z: https://www.acunetix.com/blog/articles/xml-external-entity-xxe-vulnerabilities/

[63] *Sensitive data exposure* [online]. GB Hackers, 2016 [cit. 2018-11-28]. Dostupné z: https://gbhackers.com/a6-sensitive-data-exposure/

[64] *Jak (si nechat) hacknout webovou aplikaci?* [online]. Praha: ITnetwork.cz, 2018 [cit. 2018-11-28]. Dostupné z: https://www.itnetwork.cz/php/bezpecnost/jak-si-nechat-hacknout-webovou-aplikaci

[65] DUBČÁK, Pavel. *Bezpečnost webových aplikací*. Zlín, 2018. Seminární práce.

[66] *Baby Club Katka* [online]. Uherské Hradiště [cit. 2019-05-08]. Dostupné z: https://www.babyclubkatka.cz/

[67] *Jak zabezpečit WordPress bez pluginů, jen s pomocí .htaccess souboru* [online]. Praha, 2018 [cit. 2019-05-08]. Dostupné z: https://www.active24.cz/jak-na-tvorbu-webu/wordpress/jak-zabezpecit-wordpress-bez-pluginu-jen-s-pomoci-htaccess-souboru

[69] *Zabezpečení WordPressu pomocí .htaccess* [online]. Písek, 2014 [cit. 2019-05-08]. Dostupné z: https://www.wplama.cz/zabezpeceni-wordpressu-pomoci-htaccess/

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

API	Application Programming Interface,
atd.	a tak dále,
atp.	a tak podobně,
CAPTCHA	CAPture CHAracters,
CMS	Content Management System,
CSP	Content-Security-Policy,
CSRF	Cross-Site Request Forgery,
CSS	Cascading Style Sheets,
CSV	Coma-Separated Values,
DOM	Document Object Model,
GDPR	General Data Protection Regulation,
GPL	General Public License,
HTML	HyperText Markup Language,
HTTP	HyperText Transfer Protocol,
IP	Internet Protocol,
IT	Information Technology,
MD5	Message Digest 5,
MIT	Massachusetts Institute of Technology,
MTV	Music Television,
MySQL	My Structured Query Language,
PDF	Portable Document Format,
PHP	HyperText Preprocessor, původně Personal Home Page,
QR	Quick Response,
SEO	Search Engine Optimization,

SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol,
SQL	Structured Query Language,
SSL	Secure Socket Layer,
TLS	Transport Layer Security,
tzn.	to znamená,
tzv.	takzvaně,
URL	Uniform Resource Locator,
VIP	Very Important Person,
WAF	Web Application Firewall,
WP	WordPress.
WYSIWYG	What You See Is What You Get,
XHTML	Extensible HyperText Matkup Language,
XML	Extensible Markup Language,
XSS	Cross-Site Scripting,
XXE	Extensible Markup Language External Entities,

SEZNAM OBRÁZKŮ

Obr. 1. WordPress – Logo. [12] 13
Obr. 2. WordPress – Administrační část. [13] 14
Obr. 3. Drupal – logo. [14]....15
Obr. 4. Drupal – administrace. [15]....15
Obr. 5. Joomla! – logo. [16]....16
Obr. 6. Joomla! – administrace. [17] 17
Obr. 7. ExpressionEngine – administrace. [20] 18
Obr. 8. TextPattern – administrační část. [23]....19
Obr. 9. Typo3 – administrace. [25] 20
Obr. 10. Grav – administrace. [31] 21
Obr. 11. Prestashop – administrace. [32] 22
Obr. 12. Magento – administrace. [35] 23
Obr. 13: Webnode – administrace webu. [38]....25
Obr. 14. eStránky – administrace. [39] 26
Obr. 15. Zombeek.cz – administrace. 27
Obr. 16. Wix.com – administrace. [43]....27
Obr. 17. Weebly.com – administrace. [45]....28
Obr. 18. Baby Club Uherské Hradiště.....29
Obr. 19. Baby Club Kačka.....30
Obr. 20. Baby Club Kosatka Mladá Boleslav.....31
Obr. 21. Baby Club Hrošík. 31
Obr. 22. Aqua Baby Club Praha, Kolín.....32
Obr. 23. Baby Club Nessie.....33
Obr. 24. SQL Injection. [58]....35
Obr. 25. Cross-site Scripting útok. [59]....36
Obr. 26. Cross-site Request Forgery (CSRF) [60] 37
Obr. 27. Broken Authentication. [61] 37
Obr. 28. XML External Entities (XXE). [62] 38
Obr. 29. Security misconfiguration. [55]....39
Obr. 30. Sensitive data exposure. [63]....40
Obr. 31. Staré webové stránky Baby Clubu Katka. 46
Obr. 32. Nový web Baby Clubu. 47

Obr. 33. Vygenerovaný PDF soubor faktury s QR kódem......50

SEZNAM PŘÍLOH

PŘÍLOHA P I: CD SE ZDROJOVÝM KÓDEM A DATABÁZÍ WEBOVÉ APLIKACE