Slovenská technická univerzita v Bratislave
Fakulta informatiky a informačných technológií

FIIT-XXXX-XXXXX

Richard Kello

Operačný systém ako web CMS (WCM) - Manažment používateľov a používateľských skupín v operačnom systéme cez webové rozhranie

Bakalárska práca

Pedagogický vedúci: Ing. Katarína Jelemenská, PhD.
Vedúci práce: Ing. Gabriel Szabó

Máj 2023

Slovenská technická univerzita v Bratislave
Fakulta informatiky a informačných technológií

FIIT-XXXX-XXXXX

Richard Kello

Operačný systém ako web CMS (WCM) - Manažment používateľov a používateľských skupín v operačnom systéme cez webové rozhranie

Bakalárska práca

Študijný program: Informatika

Študijný odbor: 9.2.5 Informatika

Miesto vypracovania: Ústav informatiky a softvérového inžinierstva, FIIT STU, Bratislava

Pedagogický vedúci: Ing. Katarína Jelemenská, PhD.

Vedúci práce: Ing. Gabriel Szabó

Máj 2023

Obsah

Kapitola 1

Analýza

1.1 WCMS

Používateľ môže spravovať digitálne informácie na webovej lokalite pomocou systému správy obsahu webu (WCMS), čo je typ systému správy obsahu (CMS), vývojom a správou materiálu bez predchádzajúcej znalosti webového programovania alebo markup jazykov.[9]

1.1.1 Fungovanie WCMS

Používatelia môžu spravovať, kontrolovať, meniť a rekonštruovať obsah na webovej lokalite pomocou WCMS. Používatelia môžu zostaviť materiál pomocou flexibilného jazyka ako XML alebo .NET a uložiť ho do databázy. Používatelia môžu použiť webový prehliadač na prístup k WCMS a potom použiť rozhranie založené na prehliadači na úpravu obsahu a prispôsobenie rozloženia.[9]

Dve základné časti WCMS:

1. **Aplikácia pre správu obsahu (CMA)** - je používateľské rozhranie, ktoré

umožňuje používateľom navrhovať, upravovať, meniť a odstraňovať materiál z webovej lokality bez zásahu oddelenia IT. Medzi používateľov, ktorí môžu používať toto rozhranie, patria napríklad marketéri a tvorcovia obsahu.

2. **Aplikácia pre doručovanie obsahu (CDA)** - ponúka služby typu backend, ktoré transformujú materiál, ktorý používatelia vytvárajú v CMA, na webovú stránku, ktorú si návštevníci môžu prezerať.

1.1.2 Základné nevýhody WCMS

1. **Požiadavky na úložný priestor** - Bežné webové stránky často obsahujú kombináciu textu, grafiky a fotografií. S rastúcim množstvom grafiky alebo obrázkov však rastie aj množstvo pamäte potrebnej na uloženie každej stránky. Výsledkom je, že ak sa nepoužije kompresia, na uchovanie celej stránky je potrebné veľa úložného priestoru. V skutočnosti z článku[18] nielen obmedzuje počet webových stránok, ktoré môžu byť prepojené so stránkou, ale tiež výrazne znižuje efektivitu triedenia a získavania údajov spojených s touto stránkou.

2. **Nízka flexibilita týkajúca sa inovácií webových stránok** - Webová stránka musí byť vždy „up“ pre firemných používateľov, ktorí chcú mať stálu online prítomnosť. Keď je však potrebné pridať nové stránky alebo zmeniť alebo odstrániť zastarané stránky, webové stránky vytvorené a udržiavané pomocou konvenčných metód zvyčajne vyžadujú uvedenie celej stránky do režimu offline.[18]

3. **Bezpečnostné riziká** - Hackeri majú stále prístup k WCMS, ak ho správca často neopravuje kvôli bezpečnostným problémom. Správcovia musia sledovať a spravovať rôzne pohyblivé časti WCMS, vrátane MySQL, softvéru webového servera a akýchkoľvek doplnkov alebo doplnkov, aby sa znížili bez-

pečnostné hrozby.[9]

4. **Potreba špecializovaného tímu údržby webových stránok** - Technický tím správy databáz je často povinný spracovať údaje tak, aby dodržiavali potrebný formát, a pridať tieto údaje do databázy webovej stránky, aby mohol spravovať dátový obsah webovej stránky. Podľa zdroja[18] to výrazne zvyšuje náklady na údržbu webovej stránky a znižuje flexibilitu procesu aktualizácie, ako aj predlžuje čas potrebný na aktualizáciu webovej stránky, čím sa zvyšuje riziko, že údaje sú pri zverejnení na webových stránkach neaktuálne.

1.1.3 Základné Výhody WCMS

1. **Jednoduché na používanie** - WCMS sú zvyčajne jednoduché na používanie. Z toho dôvodu predstavujú veľkú výhodu pre ľudí, ktorí nie sú zručný v programovaní alebo s ním nemajú žiadne skúsenosti.

2. **Nízka cena** - Prevádzkové náklady na WCMS sú zvyčajne nízke v porovnaní s tým, čo ponúka používateľom alebo firmám. V niektorých prípadoch sa môže jednať aj o bezplatné predplatné.

3. **Nenáročné na spravovanie** - Väčšina WCMS je nenáročná na prevádzku z pohľadu administrátorov. Poskytujú celú radu nástrojov a možností, ako si napríklad upraviť pracovné toky či spravovať používateľov.

1.1.4 Bezpečnosť WCMS

Každý informačný systém, ktorý je pripojený na internet, musí byť bezpečný, inak môžu používatelia a operátori utrpieť vážne následky, ako napríklad odcudzenie informácií o ich kreditnej karte alebo zákazníkovi. Open source WCMS sú pre útočníkov príťažlivým cieľom pre ich široké využitie. Používatelia so zlými úmyslami

môžu spustiť útoky proti mnohým, ak nie všetkým, aplikáciám vytvoreným pomocou určitého WCMS, ak sa dozvedia o jeho zraniteľnosti.[13] WCMS sú zvyčajne podľa MDPI[12] cieľmi útokov ako: Manipulácia dát napríklad za pomoci SQL injekcie. Phishing dát ako bankové účty alebo iné používateľské dáta za pomoci aj XSS útoku. Spúšťanie kódu pomocou aj jednoduchých grafických súborov. Spam, kedy bežný webový "crawler"prechádza lokalitu a hľadá validné emailové adresy pre použitie u tohoto typu útoku. Napodobovanie WCM portálu, kedy útočníci použijú upravené formuláre na stránkach poskytovaných daným WCMS a čakajú, kým sa obete autorizujú, aby získanie ich prihlasovacích údajov. Poskytnuté informácie od MDPI[12] sa zhodovali aj s OWASP top 10, čo je list naj využívanejších cyber útokov.[14]

Podľa analýzy údajov na obrázku 1.1[1], 49.8% týchto útokov na webové prehliadače sú útoky XSS, ktoré teda tvoria skoro polovicu napadnutí. Pri XSS útoku používateľ objaví spôsob, ako zadať časť škodlivého kódu na webovú stránku [13]. Inak povedané, útok XSS vloží do renomovanej webovej stránky zákernú sériu pokynov, ktoré sa vykonávajú vo webovom prehliadači návštevníka (bez vedomia návštevníka), čím útočníkovi poskytne prístup k citlivým údajom používateľa vrátane tokenov relácie a uložených súborov cookie, v prehliadači [20].

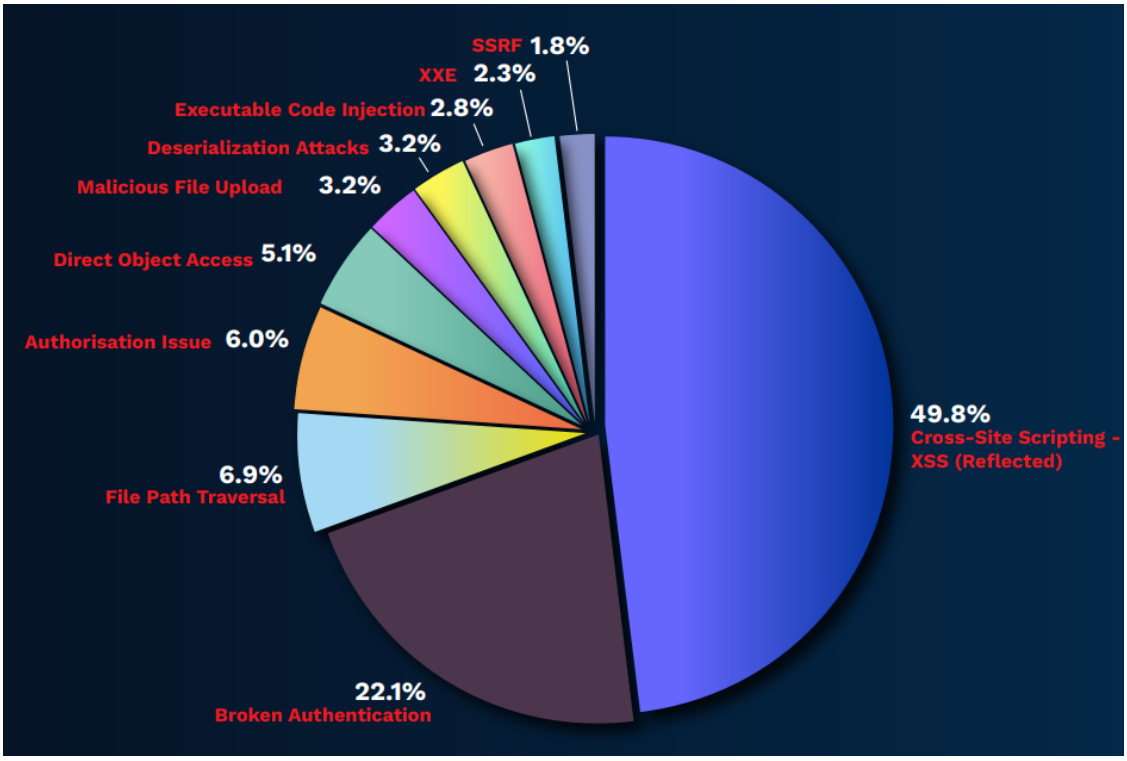
Niektoré varianty útoku XSS:

1. **Reflected XSS útok** - Tento útok používa iné komunikačné prostriedky, aby sa dostal k svojim cieľom, ako sú falošné odkazy v e-mailoch alebo iných webových stránkach, ktoré hlásia útok do webového prehliadača používateľa. Keďže skript pochádza z „dôveryhodného servera“, webový prehliadač ho môže spustiť. Netrvalé alebo XSS útoky typu I sú iným názvom pre tento druh útoku.[8]

2. **Stored XSS útok** - Keď obeť odošle dotaz, škodlivý skript sa uloží niekde na

webový server (napríklad do databázy, správy vo fóre, denníkov, komentárov atď.). Trvalé alebo XSS typu II sú ďalšie názvy pre tento typ útoku.[8]

3. **DOM-Based (Document Object Model) útok** - Na rozdiel od predchádzajúcich typov, kde skript servera spracováva údaje používateľa a vkladá ich späť na webovú stránku, tento druh injekcie vykonáva používateľ.[7]



Obr. 1.1: Distribúcia rôznych techník útoku na prehliadač. Obrázok prevzatý z [1].

Ďalším útokom s vysokým zastúpením bol podľa [1] práve útok porušenia autentifikácie. Jedná sa o útok súvisiacimi s autentifikáciou a potvrdením identity používateľa. Z analýzy údajov na obrázku 1.1[1], celkový počet týchto útokov tvoril až 22.1% celkových útokov.

Z informácií z dostupných článkov[9, 1, 20, 12] môžeme dedukovať že pred typmi útokov na Obr. 1.1, sa vieme chrániť napríklad nasledovne:

1. Vytváranie rutinnej zálohy WCMS (súbory a databázy).
2. Vedenie služieb v skúsenej hostingovej spoločnosti, aby sme sa vyhli útokom ako SQL injekcia.
3. Používanie najnovšej verzie WCMS a doplnkov.
4. Používanie špecializovaných bezpečnostných doplnkov ako JHackGuard.
5. Obmedziť prístup k súborom a priečinkom k administrácii.
6. Odstránenie inštalačných skriptov ako napríklad install.php
7. Vytvorenie bezpečných používateľských rolí a povinná zmena predvoleného hesla.
8. Povolenie captcha pre anonymných používateľov, aby sa zabránilo spamu.
9. E-mailové adresy by mali byť skryté, aby sa zabránilo nežiaducemu spamu.
10. Úprava nastavení globálnych parametrov webových stránok.
11. Pokiaľ je to možné, počas procedúry inštalácie je vhodná zmena predvolenej predpony databázy.
12. Nezobrazovať súkromné údaje WCMS v klientskom rozhraní.

1.1.5 Existujúce riešenia

Medzi existujúce riešenia, ktoré sú dostupné na internete patria napríklad:

1. HubSpot
2. WooCommerce
3. WordPress
4. Joomla

5. Wix
6. Drupal
7. BigCommerce
8. Ghost
9. Magento
10. Textpattern
11. TYPO3

1.1.6 WordPress

Najznámejším WCM systémom v dobe písania tejto práce je WordPress. Zdroj WordPress[5] uvádza, že až 42% web content management systémov používa práve túto platformu. Výhody pri používaní wordpress zahŕňajú: Blockový editor, ktorý zabezpečuje jednoduchosť pri implementácii web portálov. Používatelia, teda nemusia mať žiadne znalosti v oblasti programovania. Medzi výhody rovnako patria aj stovky pluginov a tém[5], ktoré sú platené alebo aj zdarma. Obrovskou výhodou WordPress je fakt, že to je opensource platforma. Používatelia, teda môžu vyhľadať rôzne komunitné skupiny v prípade, že narazia na nejaký problém a nemusia sa spoliehať na support team produktu. Aj napriek množstvu výhod, ktoré WordPress poskytuje, nie je to bez nevýhod. Bezpečnosť na webovom portáli si používatelia musia zabezpečovať sami. Je to spôsobené tým, že WordPress je práve opensource platforma. Z rovnakého dôvodu si vlastník WCMS bude musieť hradiť aj vedenie doménového mena alebo, aj robenia záloh.

User Management - Je jedným z pluginov pre správu používateľov voľne dostupných v portáli WrodPress. Dáva možnosť spravovať používateľov a ich údaje z

jedného dashboardu. Import, export a aktualizácia používateľských údajov pomocou rolí a filtrov. Okrem toho ponúka správu používateľov pre WordPress, ktorá umožňuje správcom webových stránok importovať alebo exportovať informácie o používateľoch cez CSV súbor.[17]

1.1.7 HubSpot

HubSpot je ďalším známym web content management systémom. Rovnako, ako WordPress ani pri používaní tohoto web content management systému používatelia nepotrebujú žiadne programátorské znalosti vďaka ich drag-and-drop editoru.[11]. Pre developerov ponúka HubSpot príkazový riadok, ktorý z vlastných skúseností s podobnou featurou značne uľahčuje a urýchľuje prácu. Nakoľko sa jedná o platený produkt, obsahuje aj vbudované bezpečnostné features ako: Content delivery network (CDN), teda doručovanie obsahu, ktorý obsahuje citlivé údaje, chráni heslom. Zašifruje určité súbory na doručovanie obsahu a podobne. No rovnako produkt poskytuje aj web application firewall (WAF), a tak isto, aj dedikovaný bezpečnostný tím, ktorý zabezpečuje stránky pred DDoS útokmi, hakermi a inými bezpečnostnými porušeniami.[11]

Manažment používateľov pre HubSpot je zabudovaný a nie je potreba inštalácie žiadnych ďalších pluginov.[16] Pridávanie je riešené priamo cez nastavenia používateľov a teamov. HubSpot poskytuje rôzne templaty[16] pre nastavenie používateľských práv ako: Super admin, bežný používateľ, vedúci služby a podobne. Tieto práva sú aplikovateľné aj pre používateľské teamy, čo značne uľahčuje prácu nakoľko stačí raz nastaviť práva pre team a ďalej už len pridávať ľudí do daného tímu.

1.2 Linux

Naša implementácia WCMS bude zahŕnať Linux. Jedná sa o open-source operačný systém navrhnutý pánom Linus Torvalds. Pre C, C++, Pascal, Modula-2 a 3, Oberon, Smalltalk a Fortran poskytuje špičkové kompilátory.[4] Existujú rôzne verzie editorov ako vi a Emacs. Virtuálna pamäť, multitasking, viacnásobné prihlásenia, zabezpečenie heslom a ochrana súborov sú plne podporované. Veľké siete teraz umožňujú vzdialené prihlásenie, vzdialené shelly a e-mail vďaka pokrokom v sieťovaní Linuxu.[4] Pre Linux bol vytvorený variant Network File System (NFS). To umožňuje zdieľanie súborového systému medzi niekoľkými počítačmi, takže spotrebúva menej miesta na pevnom disku a vyžaduje menej práce so správou systému.[15] Používatelia Linuxu majú teraz prístup k systému na spracovanie textu TeX/LaTeX, ako aj kresliacim programom (ghostview a xdvi) a nástrojom na náhľad (xfig a idraw).[4] Neplatia sa žiadne licenčné poplatky a všetky tieto funkcie sú bezplatné čo predstavuje obrovskú výhodu pre developmente napríklad WCM systému.

1.2.1 Bezpečnosť operačného systému Linux

Táto časť vysvetľuje, ako chrániť systém Linux pred vnútornými aj vonkajšími útokmi. Tieto techniky môžu zahŕňať používanie úložísk na zabezpečenie systému, používanie anti-vírusu na kontrolu, či stiahnutý softvér nie je napadnutý vírusmi, opatrnosť pri spúšťaní softvéru Windows na systémoch Linux, aktualizáciu softvéru, konfiguráciu pravidiel brány firewall, správu hesiel a používanie rôznych prístupových povolení pre rôznych používateľov.

1. **Zabezpečenie prostredníctvom úložísk** - Softvér v linuxových distribúciách sa často sťahuje a inštaluje cez úložiská, ktoré obsahujú veľké množstvo balíkov, ktoré môžu používatelia používať a sťahovať. [10] Kali Linux na-

príklad obsahuje nástroje navrhnuté špeciálne na penetračné testovanie. [2] Pretože vývojári týchto linuxových distribúcií schválili repozitáre, ktoré sú povolené s predvolenou dodávkou operačného systému, tento spôsob inštalácie softvéru je všeobecne považovaný za vysoko bezpečný. [19] Repozitáre však nedávajú všetko. Vo všeobecnosti by sa používatelia mali snažiť vyhnúť inštalácii softvéru z internetu alebo z iných zdrojov a namiesto toho sa zamerať na používanie repozitárov, ktoré ponúka linuxová distribúcia, ktorú si vybrali.

2. **Použitie antivírusu: ClamAV** - Pokiaľ používateľ nemá inú možnosť, ako stiahnuť softvér, ktorý sa nachádza mimo repozitára jeho distribúcie, mal by použiť antivírusový program. Dostupný priamo v repozitároch distribúcií alebo na oficiálnej stránke, ClamAV je jednou z možností.[19] Vo svojej podstate je podobný známemu antivírusovému programu Windows Defender. Oba obsahujú možnosť plánovania kontroly systému, v prípade, že používateľ obľubuje písanie skriptov vie ClamAV ignorovať dané repozitáre.[6] Obsahuje konzolovú verziu, ale aj verziu s GUI pre používateľov menej zdatných s konzolou. Databáza hrozieb pre ClamAV je neustále aktualizovaná a práve aj z tohoto dôvodu považujeme program za valídnu možnosť pre Linux distribúcie.

3. **Aktualizácia softvéru** - Stiahnuté aplikácie aj systémové balíky je potrebné aktualizovať, aby bol systém Linux bezpečný. Pre aktualizáciu celého softvéru, ktorý bol získaný z úložísk, ako je prehliadač alebo jadro, je potrebné navštíviť buď webovú lokalitu, z ktorej bol softvér stiahnutý, a nainštalovať najnovšie verzie, alebo použiť terminál na vykonanie pre distribúciu špecifického sledu príkazov. Záverom možno povedať, že tragédiám, ako je strata údajov, sa dá predísť udržiavaním aktuálnych systémov Linuxu.

4. **Firewall** - Firewally môžu byť nainštalované na ochranu pred útokmi zo zariadení pripojených k rovnakej sieti. Firewall je súbor pravidiel, ktoré určujú, ktoré porty sú prístupné počítačom zvonku a ktoré správy môže lokálny počítač prenášať na iné počítače. [3] Napríklad SSH je sieťový protokol, ktorý umožňuje bezpečné spojenie medzi počítačmi cez sieť. Uskutočňovanie určitých spojení by však nemalo byť povolené, ak sú ostatní používatelia siete neznámi alebo ak ide o verejnú sieť umiestnenú vo verejnej oblasti. Pracovná stanica s príliš veľkým počtom otvorených portov je tiež zraniteľná voči útokom DDoS, čo môže spôsobiť nefunkčnosť systému, kým nebude reštartovaný.[19] Pravidlá môžu byť nastavené na zastavenie takýchto útokov pomocou softvéru iptables, ktorý je prítomný vo väčšine linuxových repozitárov. Napríklad brána firewall určená výhradne pre domácu sieť môže byť menej prísna, aby umožňovala pripojenia ako SSH. Pre verejné siete je možné vytvoriť nový súbor smerníc, ktoré povolia iba HTTP a HTTPS, aby boli aktívne, ale zakázali ostatným používateľom v tej istej sieti používať a útočiť na porty SSH a FTP. Keď sú tieto dve sady pravidiel vytvorené, možno ich zameniť pomocou príkazu „iptables-restore < rules“, kde pravidlá sú názov súboru pravidiel brány firewall, ktorý sa nachádza v aktuálnom pracovnom adresári.[19]

5. **Správa hesiel** - Používatelia sú často požiadaní, aby si zaregistrovali používateľské konto pri inštalácii distribúcie Linuxu na počítač, ktorý generuje adresár pre všetky údaje tohto používateľa v rámci súborového systému. Aby sa predišlo neúmyselnému alebo úmyselnému zničeniu dôležitých systémových súborov používateľa, tieto súbory musia byť uložené oddelene od súborov používateľa root. Okrem toho musia byť pre každého používateľa v systéme vytvorené samostatné účty, ak existuje niekoľko používateľov. Jednotlivé používateľské súbory môžu byť oddelené od seba vďaka tejto izolácii,

ktorá tiež zabraňuje neoprávneným používateľom v prístupe k údajom. Používateľské heslá a heslá root sa musia navzájom líšiť. Dobrou praktikou je používať silné heslá, ktoré ideálne používateľ nepoužíva nikde inde.

6. **Povolenia na prístup k súborom** - V systéme musia byť nakonfigurované rôzne povolenia, aby sa ostatným používateľom zabránilo v prístupe k súborom, ku ktorým by nemali mať prístup. Na dokončenie je možné použiť príkazy ako chmod. Príkaz chgrp je možné použiť aj na vytváranie skupín používateľov, aby bolo možné nastaviť povolenia pre viacerých používateľov naraz. Používatelia nebudú môcť manipulovať alebo spúšťať súbory alebo potenciálne meniť systém spôsobom, akým by nemali, nastavením povolení pre osoby, ktoré môžu čítať, zapisovať a spúšťať súbory.[19]

[9] [18] [13] [12] [14] [20] [1] [8] [7] [5] [17] [11] [16] [4] [15] [10] [2] [19] [6] [3]

Literatúra

[1] *2022 vulnerability statistics report*. 2022. URL: https://www.edgescan.com/2022-vulnerability-statistics-report-lp/#form.

[2] Lee Allen, Tedi Heriyanto a Shakeel Ali. *Kali Linux-Assuring security by penetration testing*. Packt Publishing Ltd, 2014.

[3] David Barrera, Ian Molloy a Heqing Huang. "IDIoT: Securing the Internet of Things like it's 1994". In: (dec. 2017). arXiv: 1712.03623 [cs.CR].

[4] SN Bokhari. "The Linux operating system". In: *Computer* 28.8 (1995), s. 74–79.

[5] *Build a site, Sell your stuff, start a blog amp; more*. URL: https://wordpress.com/?aff=190.

[6] *ClamAV documentation*. URL: https://docs.clamav.net/.

[7] *Common weakness enumeration*. URL: https://cwe.mitre.org/data/definitions/79.html.

[8] *Cross site scripting (XSS)*. URL: https://owasp.org/www-community/attacks/xss/.

[9] Demetra Edwards et al. *What is a web content management system (WCMS)?* 2021. URL: https://www.techtarget.com/searchcontentmanagement/definition/web-content-management-WCM.

[10] J A Galindo, D Benavides a S Segura. "Debian Packages Repositories as Software Product Line Models. Towards Automated Analysis". In: *the 1st International Workshop on Automated Configuration and Tailoring of Applications*. 2010.

[11] HubSpot. *HubSpot website builder and Marketing Free*. URL: https://www.hubspot.com/marketing/am_website-builder-hsmf?irclickid=TWW1z\%3A3vxxyNRuXWgJQMRRfEUkAzBZUpDy-IVo0&irgwc=1\&mpid=11535\&utm_id=am11535\&utm_medium=am\&utm_source=am11535\&utm_campaign=amcid_TWW1z\%3A3vxxyNRuXWgJQMRRfEUkAzBZUpDy-IVo0_irpid_11535\&utm_content=wordpress.

[12] Jose-Manuel Martinez-Caro et al. "A comparative study of web content management systems". In: *Information* 9.2 (2018), s. 27.

[13] Michael Meike, Johannes Sametinger a Andreas Wiesauer. "Security in Open Source Web Content Management Systems". In: *IEEE Security Privacy* 7.4 (2009), s. 44–51. DOI: 10.1109/MSP.2009.104.

[14] *Owasp Top Ten*. URL: https://owasp.org/www-project-top-ten/.

[15] Spencer Shepler et al. *Network file system (NFS) version 4 protocol*. Tech. spr. 2003.

[16] Support. *Add HubSpot users*. 2018. URL: https://knowledge.hubspot.com/settings/add-and-remove-users.

[17] WPExperts a Uzair Ahmed. *User management*. 2022. URL: https://wordpress.org/plugins/user-management/.

[18] Ming-Ju Yang et al. "A User-Friendly Web Content Management System". In: *2008 3rd International Conference on Innovative Computing Information and Control*. IEEE. 2008, s. 367–367.

[19] Matthew R. Yaswinski, Md Minhaz Chowdhury a Mike Jochen. "Linux Security: A Survey". In: *2019 IEEE International Conference on Electro Information Technology (EIT)*. 2019, s. 357–362. DOI: 10.1109/EIT.2019.8834112.

[20] Imran Yusof a Al-Sakib Khan Pathan. "Mitigating Cross-Site Scripting Attacks with a Content Security Policy". In: *Computer* 49.3 (2016), s. 56–63. DOI: 10.1109/MC.2016.76.