FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Posudek oponenta závěrečné práce

Student:	David Pokorný
Oponent práce:	Ing. Josef Kokeš
Název práce:	Zabezpečení webové aplikace
Obor:	Bezpečnost a informační technologie

Datum vytvoření: 19. 5. 2019

Hodnotící kritérium:	*Způsob hodnocení – následující škálou 1 až 4:*
1. Splnění zadání	***1=zadání splněno,*** *2=zadání splněno s menšími výhradami,* *3=zadání splněno s většími výhradami,* *4=zadání nesplněno*

Popis kritéria:
Posuďte, zda předložená ZP dostatečně a v souladu se zadáním obsahově vymezuje cíle, správně je formuluje a v dostatečné kvalitě naplňuje. V komentáři uveďte body zadání, které nebyly splněny, posuďte závažnost, dopady a případně i příčiny jednotlivých nedostatků. Pokud zadání svou náročností vybočuje ze standardů pro daný typ práce nebo student případně vypracoval ZP nad rámec zadání, popište, jak se to projevilo na požadované kvalitě splnění zadání a jakým způsobem toto ovlivnilo výsledné hodnocení.

Komentář:
Zadání požaduje provedení analýzy webové aplikace s ohledem na několik vnímaných zranitelností (nepoužívání HTTPS, neexistence testovací verze, nevyřešená problematika oprávnění uživatelů, potenciál pro škodlivé vstupy od uživatele) a následnou úpravu programu tak, aby tyto zranitelnosti byly odstraněny. Toto bylo splněno.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
2. Písemná část práce	*70 (C)*

Popis kritéria:
Zhodnoťte přiměřenost rozsahu předložené ZP vzhledem k obsahu, tj. zda všechny části ZP jsou informačně bohaté a ZP neobsahuje zbytečné části. Dále posuďte, zda předložená ZP je po věcné stránce v pořádku, případně vyskytují-li se v práci věcné chyby nebo nepřesnosti. Zhodnoťte dále logickou strukturu ZP, návaznosti jednotlivých kapitol a pochopitelnost textu pro čtenáře. Posuďte správnost používání formálních zápisů obsažených v práci. Posuďte typografickou a jazykovou stránku ZP, viz Směrnice děkana č. 26/2017, článek 3. Posuďte, zda student využil a správně citoval relevantní zdroje. Ověřte, zda jsou všechny převzaté prvky řádně odlišeny od vlastních výsledků, zda nedošlo k porušení citační etiky a zda jsou bibliografické citace úplné a v souladu s citačními zvyklostmi a normami. Zhodnoťte, zda převzatý software a jiná autorská díla, byly v ZP použity v souladu s licenčními podmínkami.

Komentář:
Písemná část práce postupně zachycuje problematiku základů zabezpečení webových aplikací, ošetření vstupů od uživatele a speciálně problematiku zabezpečení webů postavených na platformě WordPress, a následně přechází k popisu implementačních úprav autora. Z hlediska obsahu jsem vcelku spokojen, i když struktura místy mírně pokulhává (např. zálohování by mělo být řešeno už v kapitole o webových aplikacích obecně, ne až u WordPressu) a některé části nejsou dobře srozumitelné (zejm. celá kapitola 3.3). Studentovo porozumění problematice certifikátů zjevně není úplné, zaměňuje typ ověření (DV, EV) a typ certifikační autority.

Horší je to s technickou stránkou práce: Abstrakt je velmi krátký a sotva někoho zaujme k přečtení právě této práce. Jazyk práce je v řadě míst skoro až hovorový. Gramatických chyb je poměrně hodně, hlavně v čárkách a ve správných tvarech slov (pády odpovídající slovesu, "svojí" vs. "svoji" apod.). Neustále se mění osoba, použita je jak první osoba v obou číslech, tak třetí osoba a dokonce i osoba druhá. Podivně byla upravena šablona práce, takže v obsahu nacházíme odkazy na sekce, které by tam být neměly, bibliografie je až na úplném konci za (číslovanými!) kapitolami "Seznam použitých zkratek" a "Obsah přiloženého CD".

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
3. Nepísemná část, přílohy	*80 (B)*

Popis kritéria:
Dle charakteru práce se případně vyjádřete k nepísemné části ZP. Například: SW dílo – kvalita vytvořeného programu a vhodnost a přiměřenost technologií, které byly využité od vývoje až po nasazení. HW – funkční vzorek – použité technologie a nástroje, Výzkumná a experimentální práce
– opakovatelnost experimentů

Komentář:
Nepísemnou část práce tvoří jednak změny provedené nad původní aplikací (nejsou přiloženy), a dále samostatné kódy: skript pro vytváření uživatelských rolí a plugin pro vytváření a správu formulářů. Z pohledu zadání jde o odpovídající obsah, i když rozsah není velký.

Plugin by si zasloužil větší opatrnost vůči hrozbám. Neobsahuje vyslovené chyby, ale mnohdy předpokládá věci, které nejsou zaručeny a měly by být explicitně otestovány - např. parametr $file v Form::__construct nesmí obsahovat jiné než alfanumerické znaky a podtržítko; ověření podmínky "required" na vstupy pracuje s hodnotou null, ale už ne s prázdným řetězcem; výchozí filtr pro vstupy je žádný, měl by být htmlspecialchars (s možností ho potlačit u vstupů, kde chceme zachovat speciální znaky).

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
4. Hodnocení výsledků, jejich využitelnost	*80 (B)*

Popis kritéria:
Dle charakteru práce zhodnoťte možnosti nasazení výsledků práce v praxi nebo uveďte, zda výsledky ZP rozšiřují již publikované známé výsledky nebo přinášející zcela nové poznatky.

Komentář:
Výsledkem práce je zejména lepší zabezpečení webu moveandfight.com. To se podle všeho podařilo. Obecně použitelným výsledkem může být plugin FormPlugin, zvlášť pokud bude dotažen k větší uživatelské přívětivosti (zejm. generování HTML kódu, včetně validačních podmínek na straně klienta, na základě definice formuláře). Nejde však o oblast, kterou už by dříve neřešil někdo jiný, často na podstatně sofistikovanější úrovni. Přínosem pro začínající tvůrce webů postavených na systému WordPress jsou kapitoly 4.2 a 4.3.

Hodnotící kritérium:	*Způsob hodnocení – nehodnotí se*
5. Otázky k obhajobě	

Popis kritéria:
Uveďte případné dotazy, které by měl student zodpovědět při obhajobě ZP před komisí (body oddělte odrážkami).

Otázky:
1) Co máte na mysli tvrzením, že "Self-signed certifikát je certifikát, který doméně poskytne asymetrickou šifru" (str. 11)? Co znamená to "poskytne"? Je to specifikum self-signed certifikátu, nebo to platí i pro certifikáty ostatní?
2) Píšete, že na moveandfight.com nedovolujete nepřihlášeným uživatelům přistupovat na přihlašovací stránku (str. 36). Jak se tedy vůbec někdo dokáže přihlásit?
3) Váš plugin je veřejně dostupný. Máte nějakou zpětnou reakci od uživatelů?

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
6. Celkové hodnocení	*75 (C)*

Popis kritéria:
Shrňte stránky ZP, které nejvíce ovlivnily Vaše celkové hodnocení. Celkové hodnocení nemusí být aritmetickým průměrem či jinou hodnotou vypočtenou z hodnocení v předchozích jednotlivých kritériích. Obecně platí, že bezvadně splněné zadání je hodnoceno klasifikačním stupněm A.

Text hodnocení:
Posuzovaná práce je aplikační, soustředí se na zabezpečení připravovaného webu, který zatím byl pouze implementován, ne zabezpečen. Věřím, že práce tento účel plní, protože přiměla studenta systematicky se danou oblastí zabývat a realizovat ji tak, aby uspokojila několik byznysově nezainteresovaných osob (komise, vedoucí, oponent). Slabinou je horší textová stránka práce a nejistá použitelnost pro další aplikace. Z těchto důvodů se přikláním k hodnocení C-dobře, s výhledem na B, pokud vytýkané nedostatky nebyly po studentovi vedoucím požadovány.

Podpis oponenta práce: