Posudek oponenta diplomové práce

Student: Mazura František, Bc.
Téma: Framework pro bezpečný vývoj webových aplikací (id 20239)
Oponent: Ovšonka Daniel, Ing., UITS FIT VUT

1. Náročnost zadání **průměrně obtížné zadání**

Jedná se o průměrně obtížné zadaní implementačního charakteru. Student musel nastudovat detaily o nejběžnějších webových zranitelnostech a navrhnut framework v jazyku PHP který implementuje obecné OWASP doporučení.

2. Splnění požadavků zadání **zadání splněno**

3. Rozsah technické zprávy **je v obvyklém rozmezí**

4. Prezentační úroveň předložené práce **85 b. (B)**

Technická zpráva je dobře strukturovaná a jednotlivé kapitoly na sebe logicky navazují. Teoretická část práce je zpracovaná nadprůměrně. Student podrobně věnoval popisu nejběžnějších zranitelností a možných protiopatření, přičemž popis je přehledně strukturovaný. Jako nedostatek vidím nedostatečný popis struktury vlastního frameworku a chybějící popis jeho instalace a konfigurace.

5. Formální úprava technické zprávy **90 b. (A)**

Práce je typograficky na nadprůměrné úrovni a neobsahuje žádné zásadní chyby. V textu se vyskytuje minimum překlepů a gramatických chyb.

6. Práce s literaturou **70 b. (C)**

Student citoval převážně online dokumentace, vědeckých publikací je minimum, co je vzhledem na kompilační typ práce přípustné. Převzaté části jsou snadno odlišitelné od vlastního přínosu autora. Drobným nedostatkem je zařazení do seznamu literatury aj zdroje odkazující na nástroje a články které s prací souvisí pouze okrajově ([3], [4], [22]).

7. Realizační výstup **65 b. (D)**

Framework je dobře strukturovaný a využívá MVC model, ale samotná realizace za textovou častou mírně zaostává. Přiložené zdrojové kódy neobsahují žádnou dokumentaci, kód je komentovaný jen minimálně přičemž autor mícha anglické a české komentáře. Na první pohled není vůbec zřejmé, jak framework nainstalovat. Framework v odevzdané podobě nefunguje a spuštění vyžaduje více manuálních zásahů (např. externí knihovna "jsor/doctrine-postgis" úplně chybí ve výčtu závislostí obsluhovaných nástrojem "composer", přičemž v kódu je použita). Přiložený konfigurační soubor .htaccess obsahuje část přebranou z jiného frameworku bez uvedení reference. V kódu se vyskytují hard-kódovaná hesla mimo konfiguračních souborů, co významně zhoršuje jednoduchost instalace. Demo aplikace uvedená v Kapitole 5 se na CD v popisované podobě nenachází.

8. Využitelnost výsledků

Jedná se o práci kompilačního charakteru, která implementuje známe praktiky obrany proti nejběžnějším útokům vůči webovým aplikacím. Po drobných úpravách by bylo možné použít framework v praxi.

9. Otázky k obhajobě

- Přináší Vámi navrhované regenerovaní uživatelské relace při každém dotazu nějakou přidanou hodnotu oproti odporučení OWASP-u regenerovat ID jen při změně úrovně privilegií (login, log-out, změna role)?
- Myslíte si, že by zavedení HSTS zvýšilo úroveň zabezpečení Vaší aplikace?

10. Souhrnné hodnocení **75 b. dobře (C)**

Technická zpráva je na lehce nadprůměrné úrovni, je srozumitelná a má dobrou logickou strukturu. Na druhé straně má odevzdaná implementační část několik nedostatků, které práci mírné degradují. Celkově s přihlédnutím na průměrnou obtížnost a uvedené fakty navrhuji hodnocení **C - dobře**.

Prohlášení: Uděluji VUT v Brně souhlas ke zveřejnění tohoto posudku v listinné i elektronické formě.

V Brně dne: 8. června 2017

.....
podpis