ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

POSUDEK OPONENTA ZÁVĚREČNÉ PRÁCE

I. IDENTIFIKAČNÍ ÚDAJE

Název práce:	**Časté zranitelnosti webových aplikací**
Jméno autora:	**Tomáš Klouček**
Typ práce:	bakalářská
Fakulta/ústav:	Fakulta elektrotechnická (FEL)
Katedra/ústav:	Katedra počítačové grafiky a interakce
Oponent práce:	Ing. Matěj Klíma, Ph.D.
Pracoviště oponenta práce:	Katedra počítačů

II. HODNOCENÍ JEDNOTLIVÝCH KRITÉRIÍ

Zadání — **průměrně náročné**

Zadání hodnotím jako standardně náročné. V analytické části práce má autor za úkol rozebrat a seznámit čtenáře se známými zranitelnostmi webových aplikací a na ukázkách vysvětlit, jak fungují. V praktické části následně autor vytvoří webovou aplikaci, která bude obsahovat zmíněné zranitelnosti a testovací program, který ověří přítomnost daných zranitelností. Nakonec autor demonstruje, jak lze před těmito zranitelnostmi webové aplikace chránit.

Splnění zadání — **splněno s menšími výhradami**

V zadání se pro Broken Access Control požaduje zpracovat DoS, nebo Privilege escalation. Zpracování DoS jsem v práci nenašel a IDOR se může sice privilege escalation podobat, ale není to to samé. V ostatních bodech autor zadání splnil.

Zvolený postup řešení — **správný**

Postup řešení považuji za správný.

Odborná úroveň — **D - uspokojivě**

U jednotlivých kapitol mi chybí vždy v úvodu dané části text shrnující probíranou problematiku. Například hned u kapitoly 2 student začíná zabezpečovacími frameworky, aniž by uvedl, proč se zmiňuje zrovna o tom. Slovník pojmů bych dal na začátek práce, aby měl čtenář povědomí o tom, jaké pojmy tam najde (mimo to, slovník pojmů je v obsahu uveden dvakrát).
V textu často není vysvětleno, z jakého důvodu si student do aplikace vybral zrovna ty zranitelnosti, které si vybral, ze seznamu častých zranitelností (OWASP CWE). A dle jakého klíče vybral část z nich, kterou zmiňuje (například pro Broken Access Control je definováno v seznamu CWE 34 zranitelností, ze kterých autor v práci zmiňuje 3).
V části 2.2.5 jsou zmíněny zranitelnosti, které patří do části 2.2.4.
V části 2.2.1 mi chybí podrobnější vysvětlení zmíněné „politiky stejného původu“.
Zatímco kód v ukázce 2.1 je podrobně vysvětlen, pro 2.2 vysvětlení chybí a pro další časté příklady útoků už autor ukázky neuvádí vůbec. Část 4.1.4 spadá z velké části spíše do implementace než do návrhu. Pojem „Laravel“ je použit několik stránek předtím, než autor vysvětlí, co to je.
V práci mi chybí větší rozvedení Python skriptu. Vysvětlení, proč autor zvolil právě tento jazyk a tento přístup a lépe zpracovaná uživatelská příručka (například chybí informace, že port aplikace je napevno nastaven na 81).
Dobře zpracovaná část popisující funkcionality jednotlivých PHP frameworků pomáhajících zlepšit zabezpečení webových aplikací. Stejně tak jsou dobře popsané požadavky na systém. V návrhu mi chybí použití standardizovaných diagramů, které by pomohly demonstrovat architekturu aplikace.

Formální a jazyková úroveň, rozsah práce — **C - dobře**

Rozsahem práce vyhovuje pravidlům. Text práce je bez zjevných syntaktických chyb, výjimkou je v kapitole 5 „Níže ukazuji jaké barvy pou69v8 pro zv7razn2n9 syntaxe jaký jazyk“. Stylisticky má práce občas nedostatky (např: „Použijeme-li při vývoji webové aplikace použijeme framework, předpokládáme, že framework již nějak bezpečnost řeší“). Jinak je práce čtivá a srozumitelná, byť občas psaná příliš neformálně.
Formální úroveň práce je dobrá, použité tabulky a obrázky jsou popsané, ovšem není na ně v textu explicitně odkazováno jejich číslem, jak je tomu u vědeckých prací zvykem. Úvod i závěr práce by si zasloužily lepší zpracování, působí neformálně a čtenáře příliš nepřesvědčí o kvalitě práce.

Výběr zdrojů, korektnost citací	**C - dobře**
Práce obsahuje 21 zdrojů, složených z vědeckých článků a relevantních online zdrojů. Citační styl je jednotný a obsahuje potřebné prvky. V části 2.1.3 mi však chybí zdroj OWASP Top Ten seznamu. V sekci 2.3.1 chybí zdroj textu o frameworku Laravel, stejně jako v 2.3.3 pro Code Igniter. V kapitole 2 také není zdroj pro tvrzení, že nejčastěji používané zabezpečovací frameworky jsou CIA a NIST framework.	

III. CELKOVÉ HODNOCENÍ, OTÁZKY K OBHAJOBĚ, NÁVRH KLASIFIKACE

V této práci, zabývající se důležitým tématem zranitelností webových aplikací, autor seznamuje čtenáře s častými zranitelnostmi a představuje svou webovou aplikaci, která dané zranitelnosti obsahuje a skript, který testuje jejich přítomnost.

Autor zadání naplnil, ovšem v práci chybí lepší dokumentace webové aplikace a „útočného“ skriptu. Také text práce má určité nedostatky, které podrobněji popisuji v jednotlivých částech tohoto posudku.

Předloženou závěrečnou práci hodnotím klasifikačním stupněm **C - dobře.**

Datum: 5.6.2024 Podpis: