Posudek oponenta bakalářské práce

Student: Solich Filip
Téma: Pokyny pro bezpečné programování- React (id 24646)
Oponent: Firc Anton, Ing., UITS FIT VUT

1. Náročnost zadání **průměrně obtížné zadání**

2. Splnění požadavků zadání **zadání splněno s drobnými výhradami**
Zadanie bolo splnené v minimálnom rozsahu. Bod 5 zadania udáva navrhnúť a implementovať reálne príklady exploitov, v práci je však popísaná implementácia len jedného exploitu.

3. Rozsah technické zprávy **splňuje pouze minimální požadavky**
Práca obsahuje 40 vysázených strán textu, tento rozsah mierne prevyšuje minimum 40 normostrán.

4. Prezentační úroveň předložené práce **55 b. (E)**
Kapitola 2 popisujúca použité technológie je dosť stručná a len povrchne popisuje fakty vytiahnuté z dokumentácií jednotlivých technológií. Referencie na použitú literatúru sú slabé, väčšinou odkazujú len na domovskú stránku doplnkovej technológie, pre tieto odkazy je vhodnejšie použiť odkaz v pätičke.

Kapitola 3 systematicky diskutuje vybrané zraniteľnosti webových aplikácií a na príkladoch sa snaží demonštrovať ako je tieto zraniteľnosti možné využiť pre útok. Takisto je k uvedeným zraniteľnostiam pridaný popis toho, ako je možné im predchádzať. Nelogicky vyzerá obsah sekcie 3.1 ktorá sa venuje bezpečnostným problémom jazyka JavaScript, no jedna z pod sekcií popisuje prístupy k súborovému systému a nakoniec konštatuje, že to nie je problém. Nechápem teda logické napojenie na obsah kapitoly. Z kapitoly nie je jasné, prečo boli vybrané práve uvedené zraniteľnosti. Zavádzajúci je aj názov kapitoly, ktorá pojednáva o zraniteľnostiach, nie pokynoch pre bezpečné programovanie.

Kapitoly venujúce sa existujúcim riešeniam a návrhu sú zbytočne stručné a vzhľadom na rozsah odovzdanej práce by bolo vhodné ich rozšíriť.

Kapitola popisujúca testovanie iba konštatuje, že študent nástroj testoval a vtedy fungoval.

Z celej práce nie je jasné, z akého dôvodu je implementovaná vybraná zraniteľnosť v knižnici React.

Názov práce a takisto zadanie uvádza, že sa jedná o pokyny pre bezpečné programovanie v knižnici React. Nikde v práci však tieto pokyny nie sú explicitne uvedené. Kapitola venujúca sa týmto pokynom popisuje zraniteľnosti u ktorých sa odvoláva na možné riešenia. Očakával by som, že jedným z výstupov práce budú jasne formulované a výrazné pokyny ako postupovať v súlade s aktuálnymi bezpečnostnými odporúčaniami. Táto informácia je však skrytá v uvedenom texte, čo platí aj pre výukový nástroj.

5. Formální úprava technické zprávy **70 b. (C)**
Často sa v práci nachádzajú citácie alebo odkazy na iné sekcie bez medzery pred. Obrázky nie sú odkazované z testu práce. Obrázok 6.2 je v angličtine a bez prekladu. Technická správa obsahuje niekoľko preklepov ako diakritika a chýbajúce bodky alebo čiarky ako napríklad nadpis sekcie 8.2.1. Práca miestami pôsobí neupravene a na niektorých stranách je veľké množstvo prázdneho miesta (napríklad strany 17-19).

6. Práce s literaturou **55 b. (E)**

Použitá literatúra je primárne tvorená online článkami a webovými stránkami. Odborného charakteru sú len 2 pramene z 30. Obecne je z práce náročné určiť ktoré informácie sú prevzaté a ktoré sú výsledkom práce študenta. Citácie v práci primárne odkazujú na web. stránky technológií alebo aplikácií a nevedú k relevantným zdrojom odkiaľ sú uvedené informácie čerpané. Napríklad kapitola 3 obsahuje len šesť citácií a to tiež len v jednej pod sekcii zo šiestich. Zarážajúci je aj odkaz do pätičky na konci vety na strane 14 odkazujúci na vysvetlenie pojmu "man in the middle" na wikipediu.

7. Realizační výstup **75 b. (C)**

Hlavným výstupom práce je výukový nástroj pre programátorov v kniž React predstavujúci päť zraniteľností. Nástroj je verejne dostupný ako webová aplikácia a obsahuje prihlasovanie cez služby GitHub a GitLab. Odovzdané súbory obsahujú textovú dokumentáciu pre spustenie všetkých odovzdaných aplikácií.

8. Využitelnost výsledků

Práca sumarizuje doterajšie znalosti v oblasti zraniteľností webových aplikácií napísaných v knižnici React a implementuje výukove nástroje pre zoznámenie sa s pokynmi pre bezpečné programovanie. V momentálnom stave poskytne aplikácia nové informácie začínajúcim programátorom. Pre plnohodnotné využite však bude potreba aplikáciu rozšíriť, tak aby pokrývala väčšie spektrum zraniteľností, hlavne takých ktoré sú priamo zamerané na knižnicu React.

9. Otázky k obhajobě

1. Čo presne znamená pojem použiteľné zabezpečenie (usable security)?
2. Na základe akého kritéria boli vybrané zraniteľnosti popisované v práci (kapitola 3)?
3. Akým spôsobom bola hodnotená použiteľnosť implementovaného výukového nástroja?
4. Ako je možné výukový nástroj rozšíriť o funkčné spustiteľné príklady zraniteľností, tak aby ukážkové útoky neohrozovali samotný nástroj?

10. Souhrnné hodnocení **60 b. uspokojivě (D)**

Študent sumarizoval poznatky o zraniteľnostiach webových aplikácií so zameraním na knižnicu React. Odovzdaná technická správa pôsobí, že bola dokončená na poslednú chvíľu a potrebovala by sa viac venovať častiam popisujúcim návrh, testovanie a existujúce riešenia, formálnej úprave a prezentácii výsledkov. Samotný názov práce odkazuje na pokyny pre bezpečné programovanie, tieto pokyny však z práce nie sú zrejmé a je potreba ich hľadať v poskytnutých informáciách. Implementovaný výukový nástroj funguje, no pre ozajstnú využiteľnosť v praxi ho bude potreba ešte rozšíriť. Vo výsledku hodnotím túto prácu stupňom D (60 bodov).

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

V Brně dne: 30. května 2022

Firc Anton, Ing.
oponent