Review of Master's Thesis

Student: Dušek Daniel, Bc.
Title: Web Application Penetration Testing Automation (id 21678)
Reviewer: Polčák Libor, Ing., Ph.D., UIFS FIT VUT

1. **Assignment complexity** — **more demanding assignment**
   Zadání vyžaduje nejen komplexní pochopení problematiky bezpečnosti webových aplikaci, ale i jejich uplatnění v praxi v kontextu vytvoření nástroje pro penetrační testování.
2. **Completeness of assignment requirements** — **assignment fulfilled**
   Zadání bylo splněno svědomitě a jak teoretický rozbor, tak implementace nástroje ReconJay, jsou zpracovány velice pečlivě.
3. **Length of technical report** — **exceeds requirements**
   Většina textu je zajímavá a obsahově bohatá. Sekce 4.7 by se více hodila do příloh. V této sekci se také objevují nadbytečná slova, proč je podstatné, že testující Bob je muž a jeho zákaznice žena?
4. **Presentation level of technical report** — **85 p. (B)**
   Práce je napsaná srozumitelně a pochopitelně. Trochu v ní však chybí spojující linka a např. kapitola 2 působí dojmem, že není dobře propojená a reflektovaná ve zbytku textu.
   Mám několik drobných připomínek:

   - Sekce 4.7 se nezabývá návrhem ani implementací ReconJay.
   - V sekci 3.3 by bylo vhodnější také citovat české zákony, protože 4 z 5-ti testovaných domén jsou české.
   - Na straně 41 se práce zabývá entropii a autor píše, že je v intervalu [1; 8], ale minimum je 0 pro jistý jev. Např. pokud funkci z výpisu 4.4 zavoláme `shannon_entropy("a"*20, "abcd")`, vrací 0.
   - Není jasné, co znamená číslo 54 mimo větu na str. 55.
   - Z práce není jasné, že počty artefaktů zmíněné na str. 55, byly opravdu přesně ověřeny. Postup mně byl objasněn na osobní schůzce.
5. **Formal aspects of technical report** — **95 p. (A)**
   Technická zpráva je psaná velice pěknou angličtinou bez chyb a překlepů. Mám jen následující výhrady: zkratka URL je psaná malými písmeny a na str. 63 přetéká text okraje stránky.
6. **Literature usage** — **85 p. (B)**
   Student čerpá z velkého množství literatury. Všechny důležité prameny jsou citované. Postrádám však citace v kapitole 4, není jasné, které myšlenky jsou autorovi a kde čerpal z existujících přístupů a metod.
7. **Implementation results** — **95 p. (A)**
   Zdrojové kódy jsou přehledné, komentované a správně členěné do modulů.
8. **Utilizability of results**
   Výsledky práce jsou rozhodně použitelné v praxi, jak dokládá testování aplikace na několika existujících webových aplikacích. Postrádám však to, že ReconJay nevyužívá existující nástroje (popsané v sekci 2.5) a že s nimi ani nebyl porovnán. Namísto toho byl porovnán s Acunetixem, který nepopisuje sekce 2.5.
9. **Questions for defence**
   - Na CD se nachází adresář ReconJay/payloads obsahující databáze řetězců. Jde o dílo autora, nebo jsou řetězce převzaté?
   - Jak moc jsou navržené a implementované algoritmy vlastním dílem a jak moc jsou čerpány odjinud?
   - Jaká je budoucnost nástroje?
10. **Total assessment** — **95 p. excellent (A)**
    Pan Dušek odevzdal velice kvalitní a čtivou práci. Obrovský kus odvedené práce částečně kazí nejasná návaznost vlastní práce na existující nástroje. Také nejsou jasně vyznačeny myšlenky samotného autora ovlivňující návrh a implementaci od myšlenek přejatých. I přes tyto nedostatky si myslím, že jde o výbornou práci.

In Brno 29. May 2019

Polčák Libor, Ing., Ph.D.
reviewer