UNIVERZITET CRNE GORE
PRIRODNO-MATEMATIČKI FAKULTET
DOKTORSKE STUDIJE

Crna Gora
UNIVERZITET CRNE GORE
PRIRODNO-MATEMATIČKI FAKULTET
Broj 137
Podgorica, 6 MAR 2020 20__ god.

VIJEĆU PRIRODNO-MATEMATIČKOG FAKULTETA

Predmet: Ocjena podobnosti doktorske teze i kandidata

U skladu sa članom 35, stav 2, Pravila doktorskih studija, Komisija za ocjenu podobnosti doktorske teze i kandidata koju je imenovao Senat Univerziteta Crne Gore na sjednici održanoj 24. 12. 2019. godine, u sastavu

1. **Dr Milo Tomašević**, redovni profesor Elektrotehničkog fakulteta Univerziteta u Beogradu, mentor
2. **Dr Savo Tomović**, vanredni profesor Prirodno-matematičkog fakulteta Univerziteta Crne Gore
3. **Dr Srđan Kadić**, docent Prirodno-matematičkog fakulteta Univerziteta Crne Gore

podnijela je Vijeću Prirodno-matematičkog fakulteta **Izvještaj sa javne odbrane polaznih istraživanja doktorske disertacije** i **Ocjenu podobnosti teme doktorske disertacije** (**Obrazac D1**) kandidata **mr Krenara Kepuške.**

Komisija za doktorske studije PMF-a je na sjednici održanoj 06. 03. 2020. godine, zaključila da dostavljeni Izvještaj sadrži sve elemente propisane Pravilima doktorskih studija i Vodičem za doktorske studije i prosljeđuje ga na razmatranje Vijeću Prirodno-matematičkog fakulteta.

Podgorica, 06. 03. 2020. god.

ZA KOMISIJU ZA DOKTORSKE STUDIJE

Doc. dr Goran Popivoda

Crna Gora
UNIVERZITET CRNE GORE
PRIRODNO-MATEMATIČKI FAKULTET
Broj 68
Podgorica 03 MAR 2020 20__ god.

OCJENA PODOBNOSTI DOKTORSKE TEZE I KANDIDATA

OPŠTI PODACI O DOKTORANDU	
Titula, ime i prezime	M.Sc. Eng. Kepuska Krenar
Fakultet	Prirodno-matematički fakultet
Studijski program	Računarske nauke
Broj indeksa	1/2016
Podaci o magistarskom radu	2012-2014 University of Tirana Faculty of Natural Science Departament of Mathematics and Informatics Master of Science M.Sc. Eng. Engineering in Mathematics and Informatics
NASLOV PREDLOŽENE TEME	
Na službenom jeziku	Pristup penetracionog testiranja u web aplikacijama kao proaktivna i odbrambena tehnologija
Na engleskom jeziku	Penetration test approach in web applications as a proactive and defensive technology
Datum prihvatanja teme i kandidata na sjednici Vijeća organizacione jedinice	9. 12. 2019. god.
Naučna oblast doktorske disertacije	Računarske nauke
Za navedenu oblast matični su sljedeći fakulteti	
Prirodno-matematički fakultet, Elektrotehnički fakultet	

A. IZVJEŠTAJ SA JAVNE ODBRANE POLAZNIH ISTRAŽIVANJA DOKTORSKE DISERTACIJE

Javna odbrana polaznih istraživanja doktorske disertacije kandiata Krenara Kepuške održana je na Prirodno-matematičkom fakultetu u Podgorici 24.1.2020. u prisustvu kandidata i doljepotpisanih članova komisije. Počela je u 12:00, a završena je u 13:15.

Kandidat je prvo održao prezentaciju u trajanju od dvadesetak minuta u kojoj je predstavio pregled oblasti sigurnosti računarskih sistema, formulisao problem koji će rješavati, motivaciju i hipoteze istraživanja, ciljeve i pristup istraživanju, metodologiju i plan istraživanja, kao i očekivane rezultate. Zatim su članovi komisije postavili pitanja data u prilogu ovog izvještaja na koja je kandidat odgovorio na zadovoljavajući način.

B. OCJENA PODOBNOSTI TEME DOKTORSKE DISERTACIJE

B1. Obrazloženje teme

Oblast zaštite u računarskim sistemima je veoma aktuelna sa praktičnog i poslovnog stanovišta pa zato izaziva i veliku pažnju u akademskoj zajednici. Kako je povezivanje sistema na mrežu sve prisutnije, tako su i ovi sistemi sve više izloženi napadima. Neka istraživanja navode da se svakih 40 sekundi u svijetu desi neki napad preko mreže i da su svake godine osetljive informacije oko 150 miliona ljudi izložene napadima. Narušavanje sigurnosti računarskih sistema danas izaziva velike gubitke pa su zato pokušaji da se ona podigne na što veći nivo vrlo relevantni.

Jedna od metoda koja služi povećanju sigurnosti sistema u smislu njihove dostupnosti, integriteta i poverljivosti je i penetraciono testiranje. On se može sprovoditi na više nivoa, a jedan od najinteresantnijih i najvažnijih je penetraciono testiranje veb aplikacija s obzirom na njihovu zastupljenost. Ono se zasniva na simuliramim napadima koji se sve više sprovode u računarskim sistemima sa ciljem da se podigne zaštita informacionih sistema i servisa tako da se pronađu i otklone eventualne slabosti prije nego što oni budu izloženi stvarnim napadima iz okruženja.

B2. Cilj i hipoteze

Glavni ciljevi istraživanja su:

- Predložiti model napada efektivnog i proaktivnog penetracionog testiranja za nalaženje ranjivosti veb aplikacija,
- Projektovati odbrambene tehnike u vidu preventivnih kontrola koje se sprovode prije penetracionog testiranja i predložiti model protivmjera za bolju sigurnost veb aplikacija od napada referenciranih u OWASP modelu,
- Predložiti metode validacije ulaza u prevenciji poznatnih napada.

Glavne hipoteze istraživanja su:

- Korišćenje pristupa penetracionog tesiranja kao odbrambne metodologije povećava sigurnost sistema,
- Primjena penetracionog testiranja i preventivnih kontrola kao kontinualnog proaktivnog okvira smanjuje vjerovatnoću da napadač pronađe i iskoristi ranjivost zaštite sistema,
- Preventivne kontrole u vidu validacije ulaza smanjuju ranjivost veb aplikacia na napade tipa injekcije.

B3. Metode i plan istraživanja

Predviđena metodologija će biti zasnovana na sledećim fazama:

- Sakupljanje informacija o sigurnosnim propustima ciljnih veb aplikacija kroz inspekciju izvornog koda,
- Statička i dinamička analiza i testiranje tipičnih napada u klijentskim aplikacijama,
- Simuliranje napada u laboratorijskim uslovima,
- Kreiranje i primjena preventivnih kontrola i odbrambenih tehnika,
- Evaluacija predloženih mehanizama u realnim uslovima

B4. Naučni doprinos

Predviđeni naučni doprinos ove disertacije je predlog specifične metodologije penetracionog testiranja web aplikacija i proaktivnog radnog okvira u kojem se penetraciono testiranje namijenjeno otkrivanju slabosti i ranjivosti vebv aplikacija na razne napade kombinuje u prethodnoj fazi kombinuje sa preventivnim kontrolama sa ciljem da se rizici smanje, kao i protivmjerama u narednoj fayi da se ti rizici smanje ili uklone.

B5. Finansijska i organizaciona izvodljivost istraživanja

Kandidat radi kao predavač na univerzitetu što mu omogućava da se bavi istraživanjem. Pored toga, kandidat je aplicirao za stipendiju za višemjesečni boravak na jednom američkom univezitetu u istraživačnoj grupi koja se bavi računarskom zaštitom. Dobijanje ove stipendije bi mnogo pomoglo da se zamišljena istraživanja efikasno sprovedu.

Mišljenje i prijedlog komisije

Komisija smatra da je predložena tema veoma aktuelna i adekvatna za doktorsku disertaciju, da je oblast jako kompetitivna, da je predlog veoma ambiciozan i široko postavljen, tako da bi se trebalo ograničiti na pojedine segmente testiranja kako bi se dobio konkretan pomak u odnosu na postojeća rješenja.

Prijedlog izmjene naslova

Prijedlog promjene mentora i/ili imenovanje drugog mentora

Predlaže se dodavanje komentora:
Doc. Srđan Kadić, Prirodno-matematički fakultet,
Univerzitet Crne Gore, Crna Gora

Planirana odbrana doktorske disertacije

2021/2022 Drugi semestar

Izdvojeno mišljenje

Ime i prezime

_____

Napomena

ZAKLJUČAK		
Predložena tema po svom sadržaju **odgovara** nivou doktorskih studija.	**DA**	NE
Tema **je** originalan naučno-istraživački rad koji odgovara međunarodnim kriterijumima kvaliteta disertacije.	**DA**	NE
Kandidat **može** na osnovu sopstvenog akademskog kvaliteta i stečenog znanja da uz adekvatno mentorsko vođenje realizuje postavljeni cilj i dokaže hipoteze.	**DA**	NE

Komisija za ocjenu podobnosti teme i kandidata	
Red. prof. Milo Tomašević, Elektrotehnički fakultet, Univerzitet u Beogradu, Srbija	
Vanr. prof. Savo Tomović, Prirodno-matematički fakultet, Univerzitet Crne Gore, Crna Gora	
Doc. Srđan Kadić, Prirodno-matematički fakultet, Univerzitet Crne Gore, Crna Gora	
U Podgorici, 24.1.2020.	

DEKAN

MP

PRILOG

PITANJA KOMISIJE ZA OCJENU PODOBNOSTI DOKTORSKE TEZE I KANDIDATA	
Vanr. prof. Savo Tomović:	1. Kako obezbijediti potrebni skup podataka za potrebe istravanja?
	2. Da li se planira upotreba NLP tehnika?
	3. Da li planirate razvoj tehnika koje će podržati dinamičke „baze znanja“ i inkrementalno učenje?
Doc. Srđan Kadić:	1. Vi ste u vašoj prezentaciji naveli najznačajnije ranjivosti prema OWASP listi, možete li mi dati dublju kategorizaciju navedenih ranjivosti? Da li se vaš pristup u okviru pentest-a odnosi samo na jednu grupu ranjivosti npr Client side ranjivosti ili uopšteno na sve izlistane ranjivosti u okviru OWASP liste? Zar nije produktivnije fokusirati se na specifičnu grupu ranjivosti?
	2. U okviru linux (kali OS) već postoje alati putem kojih se, npr. preko Black Box koncepta, mogu izlistati eventualne ranjivosti testiranog sistema i dobiti adekvatne preporuke za njihovo otklanjanje. U kom segmentu će vaš pristup prevazići postojeće alate? Koji su to glavni nedostaci postojećih alata koje ste vi uočili i koje planirate na nadgradite ili zamijenite boljim komponentama?
	3. Vaš pristup se odnosi na prevenciju penetracije (IPS), da je komponenta koju planirate da razvijate spada u grupu aktivnih ili pasivnih odbrambenih tehnologija? Ukoliko ste planirali aktivnu komponentu, možete li mi dati više infomacija u vezi impolementacije aktivnog modula? Da li se i na koji način vaš pristup pentest-u web aplikacija dovodi u vezu sa kodiranjem odnosno soruce code-om istih?
	4. Kako ste planirali da izvedete testiranje? Na kojim sajtovima? Kako ćete i putem kojih tehnologija obezbediti iste uslove za testiranje za vašu kompnentu i ostale referentne alate koje ste planirali za uporednu analizu rezultata testiranja?
Red. prof. Milo Tomašević:	1. Vi tvrdite da su postojeći metodi penetracionog testiranja neefikasni i da im nedostaju elementi

	proaktivne metodologije. S obzirom da je tvrdnja dosta jaka, kako je obrazlažete? Zašto je potrebno predložiti novi pristup?
	2. S obzirom da je ovaj pristup vrsta etičkog hakovanja, kako naći relevantne aplikacije za testiranje i kako obezbijediti dozvole za penetraciono testiranje za različite aplikacije da bi skup apliacija bio reprezentativan?
	3. S obzirom da arhitekture aplikacija mogu biti različite. od monolitnih do onih baziranih na mikroservisima, da li to utiče na pristup testiranju?
	4. Kakav je odnos predloženih preventivih kontrola i samog penetracionog testiranja? Da li se vrše povremeno i regularno ili samo nakon većih izmjena?
	5. Da li će testiranje podrazumijevati koncept *black box*, *white box* ili *gray box*?
	6. Da li bi se u okviru vašeg pristupa izlaz testiranja mogao predstaviti kao jedan agregatni kvantitativni indikator performanse?
(Titula, ime i prezime člana komisije)	
PITANJA PUBLIKE DATA U PISANOJ FORMI	
(Ime i prezime)	
(Ime i prezime)	
(Ime i prezime)	
ZNAČAJNI KOMENTARI	