УНИВЕРЗИТЕТ У БЕОГРАДУ - ЕЛЕКТРОТЕХНИЧКИ ФАКУЛТЕТ
Булевар краља Александра 73, 11000 Београд, Србија
Тел. 011/324-8464, Факс: 011/324-8681

КОМИСИЈИ ЗА СТУДИЈЕ II СТЕПЕНА ЕЛЕКТРОТЕХНИЧКОГ ФАКУЛТЕТА У БЕОГРАДУ

Комисија за студије II степена, Електротехничког факултета у Београду, на својој седници одржаној 04.07.2017. године именовала нас је у Комисију за преглед и оцену мастер рада дипл. инж. Наде Јанковић под насловом „Анализа алата за детекцију SQLi сигурносних пропуста у апликацијама“. Након прегледа материјала Комисија подноси следећи

И З В Е Ш Т А Ј

1. Биографски подаци кандидата

Нада Јанковић је рођена 27.12.1993. године у Београду. Гимназију у Београду је завршила са одличним успехом. Електротехнички факултет у Београду уписала је 2012. године, а дипломирала је на одсеку за Софтверско инжењерство у септембру 2016. године са просечном оценом на испитима 9,29 и на дипломском 10. Мастер студије на Електротехничком факултету у Београду, на Модулу за софтверско инжењерство, уписала је у октобру 2016. године. Положила је све испите са просечном оценом 10,00.

2. Опис мастер рада

Мастер рад обухвата 68 страна, са укупно 33 слике, 12 табела и 24 референце. Рад садржи увод, 4 поглавља и закључак (укупно 6 поглавља), списак коришћене литературе, списак слика, списак табела, списак скраћеница и прилог.

Прво поглавље представља увод у коме су описани предмет и циљ рада. Представљен је појам сигурносних пропуста у програмском коду, као и процеса детекције истих. Затим је поменут коришћени бенчмарк за аутоматизацију анализе алата за сигурну ревизију кода, OWASP (*The Open Web Application Security Project*). Наведен је разлог употребе овог бенчмарка и значај који он има за анализу алата за детекцију сигурносних претњи, са посебним акцентом на SQLi (*SQL injection*) сигурносне пропусте у апликацијама. На крају су наведени циљеви рада и дат је кратак преглед осталих поглавља рада.

У другом поглављу образложени су намена и детаљи захтева везаних за OWASP бенчмарк, као и сигурносне претње које он покрива. Посебно је објашњена SQLi сигурносна претња. Приказана је структура бенчмарк апликације са становишта имплементације и дато је објашњење процеса инсталације и покретања бенчмарка.

У трећем поглављу су детаљно представљени анализирани алати за статичку анализу кода. Објашњени су и алати који су иницијално већ били укључени у бенчмарк, као и алати који су додати у бенчмарк у оквиру овог рада. Дати су описи алата који укључују њихов процес интеграције у оквиру бенчмарка, сигурносне претње које детектују и процес вршења анализе.

У четвртом поглављу урађена је анализа тестова бенчмарка који се односе на SQLi сигурносну претњу. На основу спроведене анализе уочене су ситуације које нису покривене постојећим тестовима, па су направљени додатни тестови. Описане су ситуације које покривају додатни тестови, а затим је објашњен поступак имплементације и интеграције са бенчмарком.

У оквиру петог поглавља је направљен преглед резултата алата, који је добијен анализом тестова поменутих у поглављу четири. Резултати се односе на успешност покривености алата за тестове који се налазе у оквиру кода бенчмарка. Направљено је и графичко поређење успешности алата.

У шестом поглављу (закључак) дат је критички осврт на све што је урађено у раду. Наведени су и предлози за могућа даља унапређења везана за коришћене технологије.

3. Анализа рада са кључним резултатима

Мастер рад дипл. инж. Наде Јанковић се бави проблематиком проналажења ефикасног алата за детекцију SQLi (*SQL injection*) сигурносних пропуста у апликацијама. Сигурносне претње представљају велики изазов приликом пројектовања апликација, јер се у већини случајева оне или занемарују или се примењују алати који не могу да детектују све претње из дате категорије. Из тог разлога је важна анализа OWASP бенчмарка која је спроведена у овом раду, јер омогућава детаљно проучавање предности и недостатака различитих алата, као и њихово међусобно поређење.

Главни допринос рада представља детаљна анализа OWASP бенчмарка и одабраних алата за статичку анализу кода, којима се врши детекција SQLi сигурносних пропуста, као и интеграција пронађених алата у бенчмарк. Спроведена анализа биће применљива приликом развоја нових апликација за детекцију сигурносних пропуста. Поред тога, у раду је извршена и анализа самих тестова из бенчмарка који се односе на SQLi сигурносни пропуст и на основу спроведене анализе осмишљени су нови тестови који повећавају број анализираних ситуација.

4. Закључак и предлог

Кандидаткиња Нада Јанковић је у свом мастер раду успешно представила проблем анализе алата за статичку анализу кода за детекцију SQLi сигурносних пропуста у програмском коду. У оквиру рада кандидаткиња је успешно имплементирала OWASP бенчмарк, систем за поређење поменутих алата, и извршила интеграцију нових алата у бенчмарк, као и додала нове тестове у бенчмарк. На овај начин показано је да је бенчмарк довољно флексибилан да се може употребити за детаљнију анализу постојећих и нових алата који ће у будућности бити развијени.

На основу горе наведеног Комисија предлаже Комисији за студије II степена Електротехничког факултета у Београду да рад „Анализа алата за детекцију SQLi сигурносних пропуста у апликацијама“ дипл. инж. Наде Јанковић прихвати као мастер рад и кандидаткињи одобри јавну усмену одбрану.

Београд, 30.08.2017. године

Чланови комисије:

Др Зоран Јовановић, редовни професор

Др Жарко Станисављевић, доцент