

КОМИСИЈИ ЗА СТУДИЈЕ II СТЕПЕНА ЕЛЕКТРОТЕХНИЧКОГ ФАКУЛТЕТА У БЕОГРАДУ

Комисија за студије II степена, Електротехничког факултета у Београду, на својој седници одржаној 28.12.2021. године именовало нас је у Комисију за преглед и оцену мастер рада дипл. инж. Марије Андрејевић под насловом „Демонстрација одабраних софтверских рањивости и начина њихове елиминације у Андроид апликацијама”. Након прегледа материјала Комисија подноси следећи

ИЗВЕШТАЈ

1. Биографски подаци кандидата

Марија Андрејевић је рођена 05.08.1997. године у Призрену. Завршила је основну школу „Драгојло Дудић” у Београду као вуковац. Уписала је Пету београдску гимназију у Београду, коју је завршила са одличним успехом. Упоредо је завршила и основну и средњу музичку школу „Јосип Славенски” (вокално-инструментални одсек – клавир и теоретски одсек) са одличним успехом, освојеним многобројним наградама и титулом ђака генерације. Електротехнички факултет уписала је 2016. године. Дипломирала је на модулу Рачунарска техника и информатика 2020. године са просечном оценом 8,29. Дипломски рад на тему „Транзиција стандардне веб апликације у прогресивну веб апликацију” одбранила је у септембру 2020. године са оценом 10. Дипломске академске – мастер студије на Електротехничком факултету у Београду, на модулу за Рачунарску технику и информатику, уписала је у октобру 2020. године. Положила је све испите са просечном оценом 9.

2. Извештај о студијском истраживачком раду

Кандидаткиња Марија Андрејевић је као припрему за израду мастер рада „Демонстрација одабраних софтверских рањивости и начина њихове елиминације у Андроид апликацијама” урадила истраживање релевантне литературе која се односи на област којој припада тема мастер рада. Посебно су анализирани постојеће мобилне апликације које имају за циљ проучавање и демонстрацију софтверских рањивости. Примери таквих апликација су: *Android InsecureBankv2*, *DIVA*, *InsecureShop*, *Damn Vulnerable Bank* и сличне. Све наведене апликације су везане за оперативни систем Андроид. Дата је њихова упоредна анализа, а главни фокус је био на демонстрацијама рањивости које се налазе на *OWASP* листи 10 најзаступљенијих рањивости.

3. Опис мастер рада

Мастер рад обухвата 57 страна, са укупно 50 слика, 1 табелом и 36 референци. Рад садржи насловну страну, садржај, увод, 4 поглавља и закључак (укупно 6 поглавља), списак коришћене литературе, списак скраћеница, списак слика, списак табела и прилог.

Прво поглавље представља увод у коме су описани предмет и циљ рада.

У другом поглављу анализиран је проблем, описана је *OWASP* листа 10 најзаступљенијих рањивости, листа која је коришћена као референтна и из које су одабране рањивости приказане у овом раду. У оквиру овог поглавља направљено је и истраживање постојећих решења за изучавање софтверских рањивости у мобилним апликацијама.

У трећем поглављу је описана имплементација система: коришћене технологије, платформе, алати и структура самог система (клијентске стране, серверске стране и базе за чување потребних података).

Четврто поглавље детаљно описује одабране рањивости које су демонстриране и начине њиховог ублажавања. Описане су следеће рањивости: небезбедна комуникација, небезбедна аутентикација и ауторизација, небезбедно складиштење података и обрнути инжењеринг.

У оквиру петог поглавља дат је опис рада система. Ово поглавље представља упутство за упознавање корисника са начином коришћења система. Најпре се објашњава целокупни систем, односно његове основне функционалности, а затим се приказују начини демонстрације претходно описаних одабраних рањивости.

Шесто поглавље је закључак у коме је дискутовано о постојећој реализацији имплементираних апликација, као и о недостацима и могућностима унапређења ради постизања боље заштите у демонстрираним примерима.

4. Анализа рада са кључним резултатима

Мастер рад дипл. инж. Марије Андрејевић се бави имплементацијом рањиве Андроид апликације којом се могу демонстрирати одабране рањивости из *OWASP* листе 10 најзаступљенијих рањивости за мобилне апликације објављеној 2016. године. У оквиру рада направљена је анализа поменутих софтверских рањивости, а затим су одабране рањивости које су демонстриране у апликацији. За имплементацију апликације и демонстрацију рањивости коришћене су технологије: *Python*, *Android* и *PostgreSQL*, затим алати: *ADB*, *BurpSuite*, *Postman* и *APKTool*, као и *Salesforce* платформа.

Основни резултати рада су: 1) анализа рањивости Андроид апликација које су наведене у *OWASP* листи 10 најзаступљенијих рањивости за мобилне апликације објављеној 2016. године и преглед постојећих решења развијених у сврху демонстрације одабраних рањивости; 2) пројектовање и имплементација апликације за демонстрацију одабраних рањивости и елиминације тих рањивости; 3) дефинисање лабораторијских вежби у оквиру којих се демонстрирају одабране рањивости.


5. Закључак и предлог

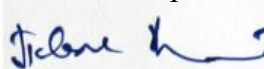
Кандидаткиња Марија Андрејевић је у свом мастер раду успешно спровела анализу постојећих решења развијених у сврху демонстрације одабраних рањивости из *OWASP* листе 10 најзаступљенијих рањивости, као и демонстрирала одабране софтверске рањивости и начине њиховог елиминисања у оквиру имплементираних Андроид апликација.


На основу изложеног, Комисија предлаже Комисији за студије II степена Електротехничког факултета у Београду да рад дипл. инж. Марије Андрејевић под насловом „Демонстрација одабраних софтверских рањивости и начина њихове елиминације у Андроид апликацијама” прихвати као мастер рад и кандидаткињи одобри јавну усмену одбрану.

Београд, 25.02.2022. године

Чланови комисије:


др Жарко Станисављевић, ванредни професор


др Павле Вулетић, ванредни професор


др Захарије Радивојевић, ванредни професор