КОМИСИЈИ ЗА СТУДИЈЕ II СТЕПЕНА ЕЛЕКТРОТЕХНИЧКОГ ФАКУЛТЕТА У БЕОГРАДУ

Комисија за студије II степена, Електротехничког факултета у Београду, на својој седници одржаној 06.06.2023. године именовало нас је у Комисију за преглед и оцену мастер рада дипл. инж. Милоша Гвозденовића под насловом „Примери криптографских рањивости веб апликација и метода њихове превенције". Након прегледа материјала Комисија подноси следећи

И З В Е Ш Т А Ј

1. Биографски подаци кандидата

Милош Гвозденовић је рођен 07.08.1997. године у Крагујевцу. Прву крагујевачку гимназију је завршио са одличним успехом. Електротехнички факултет у Београду уписао је 2016. године. Дипломирао је на модулу за Рачунарску технику и информатику 2021. године са просечном оценом 7,84. Дипломски рад на тему „Анализа ARWU методологије и њене корелације са THE и Vebometriks методологијама" одбранио је у априлу 2021. године са оценом 10. Дипломске академске – мастер студије на Електротехничком факултету у Београду, на модулу за Рачунарску технику и информатику, уписао је у октобру 2021. године. Положио је све испите са просечном оценом 9,20.

2. Извештај о студијском истраживачком раду

Кандидат Милош Гвозденовић је као припрему за израду мастер рада урадио истраживање релевантне литературе из области којој припада тема рада. У оквиру израде рада анализирани су пропусти са OWASP (енг. *Open Web Application Security Project*) листе десет најчешћих пропуста из 2021. године, а посебно су истражени криптографски пропусти. Након тога анализиране су постојеће апликације које се користе за демонстрацију криптографских пропуста и за детаљнију анализу је одабрана *WebGoat* апликација, као репрезентативна.

3. Опис мастер рада

Мастер рад обухвата 82 стране (од чега прилог обухвата 9 страна), са укупно 98 слика и 35 референци. Рад садржи увод, 3 поглавља и закључак (укупно 5 поглавља), списак коришћене литературе, списак скраћеница, списак слика и прилог.

Прво поглавље представља увод у коме је изложен предмет рада, важност проблема којим се рад бави, циљ рада, као и преглед осталих поглавља у раду.

У другом поглављу су изложене специфичности проблема који је тема рада, као и детаљна анализа већ постојећих решења.

У трећем поглављу су представљени детаљи апликације која је настала као резултат рада. Ово поглавље садржи архитектуру апликације, технологије које су коришћене у имплементацији, изворни код, као и упутства за инсталацију, покретање и коришћење апликације.

У четвртом поглављу су објашњене рањивости које постоје у апликацији. Представљено је како се оне јављају на примерима изворног кода, како их је могуће злоупотребити, као и како их је могуће поправити.

Пето поглавље је закључак у оквиру кога је направљен осврт на сам предмет рада, важност проблема, као и на кључне резултате рада.

4. Анализа рада са кључним резултатима

Мастер рад дипл. инж. Милоша Гвозденовића се бави проблематиком криптографских рањивости веб апликација и метода њихове превенције. У оквиру рада анализирани су постојећи системи и на основу резултата анализе предложено је и имплементирано ново решење. Криптографски пропусти које рањива апликација демонстрира су: слабост на *length extension* напад, хеш колизије MD5 алгоритма, слабост *login* функционалности на *Brute Force* нападе, слабост на преотимање сесије због недовољне насумичности идентификатора сесије и рањивост на *SSL Stripping* напад.

Основни доприноси рада су: 1) анализа криптографских рањивости веб апликација и метода њихове превенције; 2) анализа постојећих система за демонстрацију криптографских рањивости; 3) имплементација сопствене рањиве апликације за демонстрацију криптографских рањивости.

5. Закључак и предлог

Кандидат Милош Гвозденовић је у свом мастер раду успешно спровео анализу криптографских рањивости веб апликација. На основу спроведене анализе кандидат је успешно имплементирао рањиву веб апликацију за потребе демонстрације криптографских пропуста.

Кандидат је исказао самосталност и систематичност у своме раду.

На основу свега изложеног, Комисија предлаже Комисији за студије II степена Електротехничког факултета у Београду да рад дипл. инж. Милоша Гвозденовића под насловом „Примери криптографских рањивости веб апликација и метода њихове превенције” прихвати као мастер рад и кандидату одобри јавну усмену одбрану.

Београд, 31.08.2023. године

Чланови комисије:

др Жарко Станисављевић, ванредни професор

др Павле Вулетић, ванредни професор