

КОМИСИЈИ ЗА СТУДИЈЕ II СТЕПЕНА ЕЛЕКТРОТЕХНИЧКОГ ФАКУЛТЕТА У БЕОГРАДУ

Комисија за студије II степена, Електротехничког факултета у Београду, на својој седници одржаној 09.07.2024 године именовала нас је у Комисију за преглед и оцену мастер рада дипл. инж. Маја Нишевић под насловом „Имплементација заштитног зида веб апликација за превенцију SQL инјекционих напада коришћењем алгоритама машинског учења“. Након прегледа материјала Комисија подноси следећи

ИЗВЕШТАЈ

1. Биографски подаци кандидата

Маја Нишевић је рођена 11.5.1999. године у Београду. Завршила је Основну школу „Соња Маринковић“ у Земуну и Девету гимназију у Београду као вуковац. Електротехнички факултет у Београду уписала је 2018. године. Дипломирала је на студијском програму Електротехника и рачунарство, на модулу Рачунарска техника и информатика, са просеком 7,98. Дипломски рад одбранила је у априлу 2023. године са оценом 10. Дипломске академске – мастер студије на Електротехничком факултету у Београду, на Модулу за софтверско инжењерство уписала је у октобру 2023. године. Положила је све испите са просечном оценом 8,40. Запослена је у струци на позицији софтверски инжењер, у компанији Symphony Digital.

2. Извештај о студијском истраживачком раду

Кандидаткиња Маја Нишевић је као припрему за израду мастер рада урадила истраживање релевантне литературе која се односи на различите векторе SQL инјекционих напада као и њихову реализацију у веб апликацијама. У складу са тим истраживањем, имплементиран је заштитни зид веб апликације који за детекцију напада користе за ту сврху трениране моделе. Уз то је дато поређење успешности различитих метода детекције.

3. Опис мастер рада

Мастер рад обухвата 40 страна, са укупно 16 слика, 4 табеле и 10 референци. Рад садржи увод, 4 поглавља и закључак (укупно 6 поглавља), списак коришћене литературе, списак скраћеница, списак слика и списак табела.

Прво поглавље представља увод у коме су описани предмет, мотивација и циљ рада. Уведен је појам SQL инјекционог напада и описана је његова заступљеност. У другом поглављу је дат кратак историјат релационих база података и језика SQL, као и опис SQL инјекционог напада, као и подела ових напада. У трећем поглављу је дат опис веб апликације на којој је симулиран рад заштитног зида, њених рањивости на различите врсте овог напада, као и лоше инжењерске праксе које су заступљене и које апликацију чине рањивом. Приказани су начини на које се ове рањивости могу експлоатисати SQL инјекционим нападом. Апликација је имплементирана у радном оквиру Flask програмског језика Python.

У четвртм поглављу је описан развој самог заштитног зида. Дат је опис алгоритама машинског учења који су коришћени за његову реализацију, XGBoost и Random Forest, уз објашњење процеса обучавања модела и избор њихових најбољих хиперпараметара. Такође је дат опис трећег метода детекције који користи регуларне изразе који препознају познате шаблоне карактеристичне за инјекциони напад. На крају поглавља објашњено је како је функционалност заштитног зида интегрисана у рањиву апликацију. У петом поглављу су приказани резултати овог рада, односно компарација различитих метода детекције и анализа резултата. Успешност ових различитих метода детекције мерена је на основу резултата аутоматизованих тестова, који симулирају интеракцију са апликацијом позивом њених метода са малициозним или бенигним садржајем. Дата је компаративна анализа резултата на основу релевантних метрика.

Шесто поглавље је закључак у оквиру ког је дат осврт на резултате анализе. Такође је изнето неколико различитих идеја за унапређење рада заштитног зида, као и примери његових могућих примена у развоју веб апликација,

4. Анализа са кључним резултатима

Мастер рад дипл. Инж. Маје Нишевић се бави детекцијом SQL инјекционих напада веб апликација. Успешно је имплементиран заштитни зид који може да детектује и спречи реализацију ових напада. Реализовани су XGBoost и Random Forest модели који класификују корисничке уносе и тиме детектују SQL инјекционе нападе, који заједно са скупом правила чине заштитни зид, а дато је и поређење рада ових функционалности.

Основни доприноси рада су: 1) тренирање XGBoost и Random Forest модела за детекцију напада; 2) имплементација детектора инјекције на основу карактеристичних шаблона; 3) анализа перформанси заштитног зида у зависности од методе детекције по релевантним метрикама.

5. Закључак и предлог

Кандидаткиња Маја Нишевић је у свом мастер раду успешно имплементирала функционалност заштитног зида веб апликација који детектује SQL инјекционе нападе. Приказала је обучавање алгоритама машинског учења коришћених у ту сврху, а онда приказала анализу успешности заштитног зида. Кандидаткиња је исказала самосталност и систематичност у своме поступку као и иновативне елементе у решавању проблематике овог рада.

На основу горе наведеног, Комисија предлаже Комисији за студије II степена Електротехничког факултета у Београду да рад дипл. инж. Маје Нишевић под насловом „Имплементација заштитног зида веб апликација за превенцију SQL инјекционих напада коришћењем алгоритама машинског учења“ прихвати као мастер рад и кандидату одобри јавну усмену одбрану.

Београд, 01.10.2025. године

Чланови комисије:

др Павле Вулетић Ванредни професор
сагласан, 30.09.2025.

др Жарко Станисављевић Ванредни
професор
сагласан, 01.10.2025.

Михајло Огризовић Асистент
сагласан, 30.09.2025.