КОМИСИЈИ ЗА СТУДИЈЕ II СТЕПЕНА
ЕЛЕКТРОТЕХНИЧКОГ ФАКУЛТЕТА У БЕОГРАДУ

Комисија за студије II степена, Електротехничког факултета у Београду, на својој седници одржаној 07.10.2025 године именовала нас је у Комисију за преглед и оцену мастер рада дипл. инж. Душан Цвјетичанин под насловом „Евалуација LLM приступа за детекцију SQL Injection рањивости у Java коду". Након прегледа материјала Комисија подноси следећи

И З В Е Ш Т А Ј

1. Биографски подаци кандидата

Душан Цвјетичанин је рођен 30.11.1997. године у Пожаревцу. Гимназију општег смера у Великом Градишту завршава 2016. године са одличним успехом. Електротехнички факултет Универзитета у Београду уписује 2017. на студијском програму Софтверско инжењерство и успешно завршава 2021. године. Дипломски рад под називом "Апликација за визуелизацију ChaCha20 криптографског алгоритма" одбранио је у септембру 2021. године са оценом 10. Мастер академске студије на Електротехничком факултету у Београду, на модулу за Софтверско инжењерство уписао је у октобру 2023. године. Тренутно је запослен у компанији NetSeT Global Solutions d.o.o. где ради на позицији софтверског инжењера

2. Извештај о студијском истраживачком раду

Кандидат Душан Цвјетичанин је као припрему за израду мастер рада спровео истраживање релевантне литературе и постојећих техничких решења у области детекције SQL Injection рањивости. Рад обухвата анализу примене великих језичких модела (LLM) у области безбедности програмског кода, као и испитивање могућности њиховог извршавања путем Hugging Face Inference API интерфејса. Поред тога, анализирани су и традиционални приступи статичке анализе кода, са освртом на алате као што је SonarQube, који користе правила и шаблоне за откривање безбедносних пропуста. За потребе експеримената коришћен је OWASP Benchmark dataset, који представља стандардизован скуп примера за евалуацију безбедносних алата. У раду су коришћени и упоређени модели Qwen2.5-Coder, DeepSeek-R1, Gemma-2-2B-IT, Llama-3.2-1B/3B-Instruct, Mistral-7B и GPT-OSS-20B.

3. Опис мастер рада

Мастер рад обухвата 46 страна са укупно 5 слика, 9 табела, 18 листинга и 46 референци. Рад садржи увод, 3 поглавља и закључак (укупно 5 поглавља) и списак коришћене литературе, списак скраћеница, списак слика, списак табела, списак листинга.
Прво поглавље представља увод, у коме су описани предмет, циљ и мотивација истраживања. Истакнут је значај безбедности софтвера у савременим веб апликацијама, уз посебан нагласак на SQL Injection као једну од најраспрострањенијих рањивости.
У другом поглављу дата је теоријска позадина која обухвата преглед SQL Injection технике, постојећих метода њеног откривања и превенције, опис рада алата статичке анализе, као и увод у концепт великих језичких модела, њихову архитектуру, фазе обуке и примену у анализи безбедности кода.
Треће поглавље представља методологију истраживања, где је описан скуп података OWASP Benchmark, изабрани модели (Qwen2.5-Coder, DeepSeek-R1, Gemma-2-2B-IT, Llama-3.2-1B, Llama-3.2-3B-Instruct, Mistral-7B и GPT-OSS-20B), као и процес комуникације са моделима преко Hugging Face Inference API интерфејса. У овом поглављу дефинисан је и дизајн prompt-а, структура упита и метрике евалуације.
Четврто поглавље обухвата експериментални део рада. Приказани су резултати добијени за сваки модел појединачно, као и њихово поређење са резултатима статичког анализатора SonarQube. Анализирани су конкретни примери кода из OWASP Benchmark-а, уз илустрацију начина на који модели доносе одлуке и у којим ситуацијама греше. Посебно је размотрен утицај различитих формулација prompt-а на тачност и конзистентност резултата.

Пето поглавље садржи закључак, у коме су резимирани најважнији резултати истраживања, дате препоруке за даљи рад и могућности унапређења. Истакнут је значај LLM приступа као допуне традиционалним методама анализе безбедности кода и предложени су правци будућег истраживања, укључујући примену специјализованих модела и интеграцију LLM-а у алате за статичку анализу.

4. Анализа са кључним резултатима

Мастер рад дипл. инж. Душана Цвјетичанина бави се проблематиком детекције SQL Injection рањивости у програмском коду применом великих језичких модела (LLM). Рад се ослања на идеју да се модели тренирани на великим корпусима изворног кода и техничке документације могу користити као системи за анализу безбедности софтвера. У истраживању су упоређени резултати више LLM модела (Qwen2.5-Coder, DeepSeek-R1, Gemma-2-2B-IT, Llama-3.2-1B, Llama-3.2-3B-Instruct, Mistral-7B и GPT-OSS-20B), са резултатима традиционалног статичког анализатора SonarQube.
Основни резултати рада су:
1. систематско поређење више LLM-ова у задацима откривања SQL Injection рањивости у Java коду
2. анализа утицаја различитих prompt формулација на тачност резултата
3. анализа предности и ограничења LLM приступа
4. поређење са алатима за статичку анализу
5. постављање оквира за даља истраживања у области примене LLM технологија у безбедности софтвера

5. Закључак и предлог

Кандидат Душан Цвјетичанин је у свом мастер раду успешно истражио примену великих језичких модела (LLM) у детекцији SQL Injection рањивости у програмском коду. Рад представља свеобухватну анализу могућности великих језичких модела у препознавању безбедносних пропуста, чиме се истражује нови правац у примени ових модела у области софтверске безбедности.
Кандидат је исказао самосталност и систематичност у своме поступку као и иновативне елементе у решавању проблематике овог рада.
На основу изложеног, Комисија предлаже Комисији за студије II степена Електротехничког факултета у Београду да рад дипл. инж. Душана Цвјетичанина прихвати као мастер рад и кандидату одобри јавну усмену одбрану.

Београд, 13.10.2025. године

Чланови комисије:

др Маја Вукасовић Доцент
сагласан, 13.10.2025.

Адриан Милаковић Асистент
сагласан, 13.10.2025.