

КОМИСИЈИ ЗА СТУДИЈЕ II СТЕПЕНА ЕЛЕКТРОТЕХНИЧКОГ ФАКУЛТЕТА У БЕОГРАДУ

Комисија за студије II степена, Електротехничког факултета у Београду, на својој седници одржаној 23.06.2026 године именовала нас је у Комисију за преглед и оцену мастер рада дипл. инж. Тамара Длачић под насловом „Имплементација интеграције великих језичких модела као сервиса у веб апликацију и њихова сигурносна анализа". Након прегледа материјала Комисија подноси следећи

ИЗВЕШТАЈ

1. Биографски подаци кандидата

Тамара Длачић је рођена 01.01.2000. године у Чачку. Завршила је Основну школу „Ратко Митровић” у Чачку као носилац Вукове дипломе и Гимназију у Чачку, такође као носилац Вукове дипломе. Током школовања учествовала је на више научних и спортских такмичења, а основну школу завршила је као спортисткиња генерације. Електротехнички факултет Универзитета у Београду уписала је 2019. године. Дипломирала је на Одсеку за рачунарску технику и информатику 2023. године са просечном оценом 8,73. Дипломски рад, под називом „Развој туристичке мобилне апликације на Андроид платформи” одбранила је у септембру 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 9,60. Шестомесечну стручну праксу одрадила је у Хамбургу, у Немачкој, 2025. године, на позицији софтвер инжењера у сектору за податке и пословну интелигенцију.

2. Извештај о студијском истраживачком раду

Кандидаткиња Тамара Длачић је у оквиру припреме за израду мастер рада истражила релевантну научну и стручну литературу из области интеграције великих језичких модела у веб апликације и сигурносних ризика који при таквој интеграцији настају. Посебна пажња посвећена је начину формирања контекста модела, границама поверења, улазним и излазним тачкама система и ризицима који настају када се излаз модела користи за приказ садржаја, приступ подацима или извршавање операција. Анализиране су све категорије са листе OWASP LLM Top 10 за 2026. годину, као и релевантни научни радови, техничка документација и постојећа решења за заштиту апликација заснованих на великим језичким моделима. Размотрени су заштитни слојеви за контролу улаза и излаза, сигурносни посредници, ограничење доступних алата, минимизација контекста, контрола приступа и механизми који укључују потврду корисника пре извршавања осетљивих радњи. На основу спроведеног истраживања утврђено је да системска подршка и заштитни механизми самог језичког модела не представљају довољну сигурносну границу. Поуздана заштита захтева примену детерминистичких контрола у апликативном слоју, независно од конкретног модела и провајдера који се користе. Овај закључак представља основу за пројектовање и реализацију лабораторијског система описаног у мастер раду.

3. Опис мастер рада

Мастер рад обухвата 138 страна, са укупно 51 сликом, 25 табела и 54 библиографске референце. Рад садржи увод, четири тематска поглавља и закључак, односно укупно шест поглавља, списак коришћене литературе, списак скраћеница, списак слика и списак табела.

Прво поглавље представља увод у којем су описани предмет, циљ и доприноси рада. Образложени су ризици који настају увођењем великих језичких модела у веб апликације и представљен је приступ заснован на поређењу истих функционалности у рањивом и заштићеном режиму.

У другом поглављу дат је теоријски преглед примене великих језичких модела у веб системима.

Описани су улога модела као компоненте апликације, начин састављања контекста, границе поверења, улазне и излазне тачке и могућности повезивања више слабости у сложеније токове напада.

У трећем поглављу описани су спецификација система и развојно окружење. Рад полази од постојеће веб апликације за продају возила, која се користи на предмету Развој безбедног софтвера, која је проширена слојем за рад са великим језичким моделима. Представљени су почетно стање апликације, функционални и нефункционални захтеви и архитектура проширеног решења.

Четврто поглавље садржи детаљан опис реализације система. Представљени су заједнички програмски интерфејс за приступ моделима, имплементације провајдера и компонента за одређивање рањивог или

заштићеног режима рада. Реализовано је осам појединачних лабораторијских сценарија који обухватају директно и индиректно убризгавање упита, откривање личних података и тајни, прекомерну самосталност при употреби алата, откривање системске поруке и скривене конфигурације, као и неправилно руковање излазом приликом формирања електронских порука и CSV датотека.

У петом поглављу приказане су верификација и евалуација реализованог решења. Дефинисани су проверљиви критеријуми успеха напада и заштите, а затим су приказани резултати извршавања појединачних сценарија у рањивом и заштићеном режиму.

Шесто поглавље представља закључак рада.

4. Анализа са кључним резултатима

Мастер рад дипл. инж. електротехнике и рачунарства Тамаре Длачић бави се актуелним проблемом сигурне интеграције великих језичких модела у веб апликације. Посебна вредност рада огледа се у томе што сигурносни ризици нису разматрани само теоријски, већ су реализовани у контролисаном лабораторијском окружењу које омогућава непосредно поређење рањивог и заштићеног начина рада исте функционалности. Основни доприноси рада су: 1) реализација модуларног слоја за рад са великим језичким моделима, са заменљивим локалним, удаљеним и симулираним провајдерима; 2) реализација осам лабораторијских сценарија са јасно раздвојеним рањивим и заштићеним режимом; 3) примена апликативних контрола које обухватају проверу овлашћења, минимизацију контекста, ограничење доступних алата, потврду корисника, санитизацију улаза, контролу и маскирање излаза и безбедно формирање садржаја.

5. Закључак и предлог

Кандидаткиња Тамара Длачић је у свом мастер раду успешно реализовала интеграцију великих језичких модела као сервиса у постојећу веб апликацију и спровела систематичну сигурносну анализу ризика који при таквој интеграцији настају. Реализовано решење омогућава употребу различитих провајдера и модела, извршавање истих сценарија у рањивом и заштићеном режиму, аутоматизовану проверу примењених контрола и поређење добијених резултата.

Кандидаткиња је показала висок степен самосталности, систематичности и стручности у анализи проблема, пројектовању архитектуре, реализацији сигурносних механизма и тумачењу експерименталних резултата. На основу изложеног, Комисија предлаже Комисији за студије II степена Електротехничког факултета у Београду да мастер рад дипл. инж. Тамаре Длачић под насловом „Имплементација интеграције великих језичких модела као сервиса у веб апликацију и њихова сигурносна анализа” прихвати као мастер рад и кандидаткињи одобри јавну усмену одбрану.

Београд, 11.09.2026. године

Чланови комисије:

др Жарко Станисављевић Ванредни
професор
сагласан, 10.09.2026.

Данко Миладиновић Асистент
сагласан, 11.09.2026.