КОМИСИЈИ ЗА СТУДИЈЕ II СТЕПЕНА
ЕЛЕКТРОТЕХНИЧКОГ ФАКУЛТЕТА У БЕОГРАДУ

Комисија за студије II степена, Електротехничког факултета у Београду, на својој седници одржаној 01.04.2026 године именовала нас је у Комисију за преглед и оцену мастер рада дипл. инж. Игор Карић под насловом „Унапређење робусности вишекласне детекције напада на веб апликације". Након прегледа материјала Комисија подноси следећи

И З В Е Ш Т А Ј

1. Биографски подаци кандидата

Игор Карић је рођен 29.04.1999. године у Лазаревцу. Завршио је основну школу „Дуле Караклајић" у Лазаревцу и Електротехничку школу „Никола Тесла" у Београду. Електротехнички факултет уписао је 2018. године. Дипломирао је на одсеку за Софтверско инжењерство 2022. године са просечном оценом 8,00. Дипломски рад одбранио је у септембру 2022. године. Дипломске академске – мастер студије на Електротехничком факултету у Београду, на Модулу за Софтверско инжењерство уписао је у октобру 2022. године. Положио је све испите са просечном оценом 10,00. Професионално искуство стицао је у компанијама Prodyna, Maxeler Technologies, Heliant и Easy Aerial, као и током научноистраживачког рада на унивезитету Temple у Филаделфији у Сједињеним Америчким Државама у области машинског учења и примене алгоритама на дроновима. Тренутно је запослен на позицији Quantitative Data Analyst у компанији AMINA Bank, као и у звању сарадника у настави на Рачунарском факултету Универзитета Унион у Београду.

2. Извештај о студијском истраживачком раду

Кандидат Игор Карић је као припрему за израду мастер рада проучио релевантну литературу из области машинског учења, безбедности веб апликација, обмањујућег машинског учења и интерпретабилности модела. У оквиру студијског истраживачког рада анализирани су различити типови напада на веб апликације — Cross-Site Scripting (XSS), SQL Injection (SQLi) и Cross-Site Request Forgery (CSRF) — њихов историјат, начин извођења и постојеће технике одбране. Посебно су проучени постојећи приступи детекцији напада на веб апликације засновани на машинском учењу, са акцентом на ансамблске алгоритме (Random Forest, XGBoost, LightGBM) и инжењеринг одлика специфичних за сваки тип напада. У оквиру припреме истражени су и обмањујући напади на моделе машинског учења и њихова примена у black-box поставци, са посебним фокусом на алгоритме HopSkipJump и ZooAttack из Adversarial Robustness Toolbox (ART) библиотеке. Анализирана је и могућност генерисања семантички валидних обмањујућих примера применом великих језичких модела (Large Language Models, LLM) као новог вектора напада. Поред тога, проучена је SHAP (SHapley Additive exPlanations) анализа као метод за интерпретацију одлука ансамблских модела машинског учења.

3. Опис мастер рада

Мастер рад обухвата 60 страна без насловне стране, са укупно 20 слика, 16 табела и 38 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. У другом поглављу су представљени најважнији концепти три врсте напада на веб апликације које су предмет истраживања у овом раду: XSS, SQLi и CSRF.

У трећем поглављу дат је преглед метода детекције ових напада, са акцентом на машинско учење. Описани су традиционални приступи детекцији, ансамбл алгоритми машинског учења, као и обмањујући напади на моделе машинског учења. Посебна пажња посвећена је алгоритмима HopSkipJump и ZooAttack, обмањујућем тренингу као одбрамбеном механизму, генерисању обмањујућих примера применом великих језичких модела, и SHAP методи интерпретације одлика модела.

У четвртом поглављу описана је методологија рада. Описано је формирање скупа података комбиновањем три различита извора, процес инжењеринга 30 одлика груписаних у три категорије (URL, Body, Request), тренирање четири класификатора, и трокомпонентна обмањујућа евалуација кроз ART библиотеку, јавно доступне базе и LLM-генерисане примере.

У петом поглављу приказани су резултати свих експеримената и дата је детаљна анализа. Анализирани су

резултати cross-validation и тест евалуације четири модела, ablation студија по групама одлика, SHAP анализа за интерпретацију одлука XGBoost и LightGBM модела, резултати HopSkipJump и ZooAttack напада, перформансе обмањујуће-робусног модела, евалуација на SecLists и PayloadsAllTheThings колекцијама, као и резултати LLM-генерисаних адверзаријалних напада у white-box и black-box режиму. У шестом поглављу су дати закључак рада и могући правци даљег истраживања, укључујући комбиновани обмањујући тренинг, анализу хедер информација, реално-временску детекцију и проширење на нове типове напада.

4. Анализа са кључним резултатима

Мастер рад дипл. инж. Игора Карића бави се развојем и евалуацијом вишекласног класификатора заснованог на машинском учењу за детекцију Cross-Site Scripting, SQL Injection и Cross-Site Request Forgery напада на веб апликације, са детаљном анализом његове обмањујуће робусности. У раду је успешно формиран хетероген скуп података комбиновањем три различита извора, тренирана су четири класификатора од којих је XGBoost изабран као финални модел, и спроведена је трокомпонентна обмањујућа евалуација кроз Adversarial Robustness Toolbox (ART) библиотеку, јавно доступне колекције и обмањујуће примере генерисане великим језичким моделима (Large Language Models, LLM).
Основни доприноси рада су: 1) формирање хетерогеног скупа података од 10.511 узорака у четири класе (Normal, XSS, SQLi, CSRF) комбиновањем CSIC 2010 HTTP скупа, OpenBugBounty XSS пријава и реалних CSRF payload-а из PortSwigger Web Security Academy лабораторија; 2) инжењеринг 30 одлика специфичних за вишекласни проблем, груписаних у URL, Body и Request категорије, на основу синтезе постојећих радова и оригиналних доприноса; 3) тренирање и поређење четири класификатора уз ablation студију и SHAP анализу интерпретације одлика модела; 4) систематична трокомпонентна обмањујућа евалуација кроз HopSkipJump и ZooAttack нападе, евалуацију на SecLists и PayloadsAllTheThings колекцијама од преко 13.000 payload-а, и LLM-генерисане обмањујуће примере; 5) имплементација и евалуација обмањујућег тренинга као одбрамбеног механизма, са демонстрацијом његове ефикасности на математички генерисаним нападима, али и идентификацијом његових ограничења при семантички валидним обмањујућим нападима генерисаним LLM-овима; 6) поправка проналажена грешка у ART библиотеци која узрокује бесконачну петљу при имплементацији HopSkipJump напада на моделе са чврстом границом одлучивања.

5. Закључак и предлог

Кандидат Игор Карић је у свом мастер раду успешно развио и евалуирао вишекласни класификатор за детекцију XSS, SQL Injection и CSRF напада на веб апликације, са детаљном анализом његове обмањујуће робусности. Кандидат је исказао самосталност и систематичност у раду, као и способност да релевантне резултате експериментално прикаже и протумачи.
На основу горе наведеног, Комисија предлаже Комисији за студије II степена Електротехничког факултета у Београду да рад дипл. инж. Игора Карића под насловом „Унапређење робусности вишекласне детекције напада на веб апликације" прихвати као мастер рад и кандидату одобри јавну усмену одбрану.

Београд, 28.05.2026. године

Чланови комисије:

др Павле Вулетић Редовни професор
сагласан, 28.05.2026.

Теодора Радаљац Асистент
сагласан, 28.05.2026.