

КОМИСИЈИ ЗА СТУДИЈЕ II СТЕПЕНА ЕЛЕКТРОТЕХНИЧКОГ ФАКУЛТЕТА У БЕОГРАДУ

Комисија за студије II степена, Електротехничког факултета у Београду, на својој седници одржаној 09.06.2026 године именовала нас је у Комисију за преглед и оцену мастер рада дипл. инж. Милош Стојковић под насловом „Анализа и демонстрација рањивости код примене JWT за аутентикацију у монолитним и API Gateway архитектурама". Након прегледа материјала Комисија подноси следећи

ИЗВЕШТАЈ

1. Биографски подаци кандидата

Милош Стојковић је рођен 07.03.2001. године у Чачку. Завршио је Основну школу „Бранислав Петровић” у Слатини код Чачка као носилац Вукове дипломе и ђак генерације. Уписао је Техничку школу у Чачку, коју је такође завршио као носилац Вукове дипломе. Електротехнички факултет уписао је 2020. године. Дипломирао је на одсеку за Рачунарску технику и информатику 2024. године са просечном оценом 8,66. Дипломски рад одбранио је у септембру 2024. године са оценом 10. Дипломске академске – мастер студије на Електротехничком факултету у Београду, на Модулу за софтверско инжењерство уписао је у октобру 2024. године. Положио је све испите са просечном оценом 9,6.

2. Извештај о студијском истраживачком раду

Кандидат Милош Стојковић је као припрему за израду мастер рада урадио истраживање релевантне литературе која се односи на област којој припада тема мастер рада. Конкретно, анализирани су постојећи безбедносни пропусти и заштитни механизми везани за примену JWT (JSON Web Token) стандарда за аутентикацију у веб апликацијама, како у монолитним, тако и у савременим архитектурама заснованим на API Gateway обрасцу. Истраживањем области утврђено је да значајне рањивости обухватају неадекватно управљање тајним кључевима, погрешну валидацију алгоритама потписивања, недостатак механизма опозива токена, те неодговарајућу ауторизацију на нивоу појединачних објеката и функција система. Анализом релевантне литературе и признатих индустријских класификација, попут OWASP API Security Тор 10 листе, одабран је скуп од десет карактеристичних рањивости који представља репрезентативан узорак за практичну демонстрацију у оквиру рада.

3. Опис мастер рада

Мастер рад обухвата 55 страна, са укупно 64 слике, 1 табелом и 34 референце. Рад обухвата садржај, увод, четири поглавља и закључак (укупно шест поглавља) и спискове коришћене литературе, скраћеница, слика и табела.

Прво поглавље представља увод у коме су описани предмет, циљ и очекивани допринос рада, као и организација рада по поглављима.

У другом поглављу дате су теоријске основе неопходне за разумевање остатка рада. Представљена је структура JWT токена, алгоритми потписивања, као и улога JWT-а у процесима аутентикације и ауторизације.

У трећем поглављу приказана је имплементација и демонстрација пет карактеристичних JWT рањивости у монолитној веб апликацији: слабог тајног кључа, `alg=none` рањивости, забуне алгоритама, недостатка опозива токена, и Broken Object Level Authorization рањивости.

Четврто поглавље бави се дизајном и имплементацијом система заснованог на API Gateway архитектури, реализованог помоћу YARP библиотеке у оквиру .NET 8 окружења. Приказана је архитектура система, ток JWT токена кроз систем, те су демонстриране рањивости релевантне за дистрибуиране архитектуре: директан приступ сервису заобилажењем Gateway-а, недостатак валидације audience атрибута токена, погрешна конфигурација граница поверења, злоупотреба токена за освежавање, и недостатак валидације обима овлашћења на нивоу Gateway-а.

У оквиру петог поглавља дата је упоредна анализа резултата добијених у обе архитектуре, са освртом на безбедносне изазове специфичне за прелазак са централизованог на дистрибуирани модел аутентикације и ауторизације. Анализирани су заједнички обрасци рањивости, утицај архитектуре на безбедносни ризик, као и примери рањивости идентификованих у стварним системима.

Шесто поглавље представља закључак у оквиру ког су сумирани најважнији резултати и доприноси рада,

ограничења спроведеног истраживања, и предложени правци даљег истраживања.

4. Анализа са кључним резултатима

Мастер рад дипл. инж. Милоша Стојковића се бави проблематиком безбедности JWT механизма аутентикације, са посебним освртом на разлике у безбедносним изазовима између монолитних и дистрибуираних архитектура заснованих на API Gateway обрасцу. Овакав приступ аутентикацији налази широку примену у савременим веб системима, укључујући системе засноване на микросервисној архитектури, у којима расподела одговорности за аутентикацију и ауторизацију између више компоненти доноси додатне безбедносне изазове. У оквиру рада имплементирана су два намерно рањива система: монолитна апликација заснована на Java Spring Boot технологији, и систем заснован на API Gateway архитектури реализован у .NET 8 окружењу коришћењем YARP библиотеке, уз PostgreSQL базу података и Docker/Docker Compose за контејнеризацију и оркестрацију сервиса. Основни резултати рада су: 1) практична демонстрација десет карактеристичних JWT рањивости кроз намерно рањиве и одговарајуће безбедне имплементације; 2) формална класификација свих демонстрираних рањивости према OWASP API Security Top 10 листи; 3) упоредна анализа безбедносних изазова монолитне и дистрибуиране архитектуре, са практичним препорукама за примену модела дубинске одбране приликом валидације токена.

5. Закључак и предлог

Кандидат Милош Стојковић је у свом мастер раду успешно решио проблем практичне демонстрације и анализе карактеристичних безбедносних рањивости JWT механизма аутентикације, кроз реализацију два функционална система који омогућавају поређење безбедносних изазова монолитних и дистрибуираних архитектура. Предложене митигације и препоруке могу значајно да допринесу безбеднијој имплементацији механизма аутентикације и ауторизације у савременим веб системима.

Кандидат је исказао самосталност и систематичност у своме поступку, као и способност повезивања теоријски познатих безбедносних концепата са конкретном, реалистично дизајнираном имплементацијом. На основу изложеног, Комисија предлаже Комисији за студије II степена Електротехничког факултета у Београду да рад дипл. инж. Милоша Стојковића под насловом „Анализа и демонстрација рањивости код примене JWT за аутентикацију у монолитним и API Gateway архитектурама” прихвати као мастер рад и кандидату одобри јавну усмену одбрану.

Београд, 04.09.2026. године

Чланови комисије:

др Жарко Станисављевић Ванредни
професор
сагласан, 02.09.2026.

Данко Миладиновић Асистент
сагласан, 04.09.2026.