

УНИВЕРЗИТЕТ У БЕОГРАДУ - ЕЛЕКТРОТЕХНИЧКИ ФАКУЛТЕТ

Булевар краља Александра 73, 11000 Београд, Србија

Тел. 011/324-8464, Факс: 011/324-8681

КОМИСИЈИ ЗА СТУДИЈЕ II СТЕПЕНА ЕЛЕКТРОТЕХНИЧКОГ ФАКУЛТЕТА У БЕОГРАДУ

Комисија за студије II степена, Електротехничког факултета у Београду, на својој седници одржаној 23.05.2023. године именовала нас је у Комисију за преглед и оцену мастер рада дипл. инж. Петра Палибрка под насловом „Анализа и детекција XSS рањивости савремених веб страница“. Након прегледа материјала Комисија подноси следећи

ИЗВЕШТАЈ

1. Биографски подаци кандидата

Петар Палибрк је рођен 15.10.1997. године у Београду. Завршио је Основну школу „Свети Сава“ у Београду и Трећу београдску гимназију у Београду као вуковац. Електротехнички факултет уписао је 2016. године. Дипломирао је на одсеку за Софтверско инжењерство 2020. године са просечном оценом 9,91 и био је студент генерације на свом одсеку. Дипломски рад одбранио је у септембру 2020. године са оценом 10. Дипломске академске – мастер студије на Електротехничком факултету у Београду, на Модулу за софтверско инжењерство уписао је у октобру 2020. године. Положио је све испите са просечном оценом 9,60. Запослен је у струци на позицији софтвер инжењер 2.

2. Извештај о студијском истраживачком раду

Кандидат Петар Палибрк је као припрему за израду мастер рада урадио истраживање релевантне литературе која се односи на анализу и методе детекције XSS (енг. *Cross Site Scripting*) напада. Истражене и анализирани врсте XSS слабости, те одлике веб страница које су најважније за детекцију XSS напада. У складу са овим истраживањем имплементирани су скрипте које преузимају податке, рачунају жељене одлике, тренирају модел помоћу ког се ради детекција XSS напада и извлаче статистику која је омогућила анализу одлика која је приказана у раду.

3. Опис мастер рада

Мастер рад обухвата 45 страна, са укупно 21 сликом, 7 табела и 39 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. Такође је уведен појам XSS напада и описана је његова заступљеност у свету. У другом поглављу је дат кратак историјат и детаљан опис XSS напада. Поред дефиниције XSS напада дата је и њихова подела, где је за сваку категорију описан начин извођења напада, што укључује приказ ограничења и предности те категорије напада.

У трећем поглављу је дат опис начина детекције напада и рањивости на основу карактеристика веб страница у постојећим решењима. За свако постојеће решење је описан начин функционисања, његове предности и мане. Потом је дат разлог примене машинског учења при решавању проблема детекције XSS рањивости и напада, као и опис значајних одлика веб страница које су посматране у овом раду ради детектовања ових напада.

У четвртом поглављу је описана сама реализација *Python* и *JavaScript* скрипти које прикупљају скуп података, израчунавају одлике које укључују *HTML (Hyper Text Markup Language)*, *JavaScript* и *URL (Uniform Resource Locator)* одлике страница и тренирају *XGBoost* модел за класификацију. Такође су приказане и дефиниције метрика које су коришћене при мерењу перформанси класификације, као и метода избора најперформантнијих параметара модела.

У петом поглављу су приказани резултати овог рада, што укључује саме резултате тренирања модела и анализу одлика које највише утичу на добијене резултате. Првобитно је

урађена анализа која користи све одлике, где је приказан утицај величине скупа података на резултате, вредност посматраних метрика и анализа посматраних одлика које имају највећу важност унутар модела. За најважније одлике је и наведено пар примера из стварног света који описују новооткривене XSS рањивости у веб страницама које баш њих злоупотребљавају. Потом је одрађена слична анализа која уклања URL одлике које су биле најдоминантније у претходно истренираном моделу, где је приказани поновни избор параметара модела, утицај величине скупа података на резултате, вредност посматраних метрика и анализа посматраних одлика које имају највећу важност унутар модела. Такође је изведен и закључак за важност одлика при детекцији XSS напада и рањивости.

Шесто поглавље је закључак у оквиру кога су сумирани резултати анализе и тренирања XGBoost модела. Истакнута је важност појединих одлика, као и потенцијалне мане овог решења када су специфични напади у питању. Такође, наведен је и пример могуће примене ових модела у претраживачима, да би се омогућило безбедније коришћење интернета.

4. Анализа рада са кључним резултатима

Мастер рад дипл. инж. Петра Палибрка се бави анализом и детекцијом XSS рањивости модерних веб страница. Успешно је реализован XGBoost модел који може да детектује XSS напад на веб страницама који користи скуп од педесет девет HTML, JavaScript и URL одлика. У оквиру рада су приказани резултати класификације XGBoost модела који је у скорије време један од најпопуларнијих модела машинског учења. Такође је изведена и детаљна анализа одлика које утичу на резултате и детекцију XSS напада, као и потенцијални начини како нападач може заобићи главне одлике.

Основни доприноси рада су: 1) имплементација скрипти за прикупљање података, израчунавање одлика и тренирање модела; 2) формирање скупа података страница рањивих на XSS нападе и оних које нису рањиве; 3) тренирање XGBoost модела који може да детектује XSS нападе и анализа његових перформанси; 4) анализа одлика веб страница које највише утичу на рањивост и детекцију XSS напада.

5. Закључак и предлог

Кандидат Петар Палибрк је у свом мастер успешно анализирао одлике које утичу на рањивост на XSS нападе савремених веб страница, као и формирао скуп података и истренирао XGBoost класификатор који може да детектује XSS напад посматрањем различитих одлика веб странице. Кандидат је исказао 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. Петра Палибрка под насловом „Анализа и детекција XSS рањивости савремених веб страница“ прихвати као мастер рад и кандидату одобри јавну усмену одбрану.

Београд, 14.08.2023. године

Чланови комисије:



Др Павле Вулећић, ванредни професор



Др Жарко Станисављевић, ванредни професор



Ас. мс Михајло Огривовић, мастер инжењер електротехнике и рачунарства