

КОМИСИЈИ ЗА СТУДИЈЕ II СТЕПЕНА ЕЛЕКТРОТЕХНИЧКОГ ФАКУЛТЕТА У БЕОГРАДУ

Комисија за студије II степена, Електротехничког факултета у Београду, на својој седници одржаној 10.01.2023. године именovalo нас је у Комисију за преглед и оцену мастер рада дипл. инж. Душана Станивуковића под насловом „Развој апликације за демонстрацију рањивости лажирања захтева на серверској страни”. Након прегледа материјала Комисија подноси следећи

ИЗВЕШТАЈ

1. Биографски подаци кандидата

Душан Станивуковић је рођен 09.11.1998. године у Крушевцу. Гимназију је завршио у Крушевцу са одличним успехом. Електротехнички факултет у Београду уписао је 2017. године. Дипломирао је на одсеку за Софтверско инжењерство 2021. године са просечном оценом 7.96. Дипломски рад на тему „Имплементација Java апликације за визуелну репрезентацију Whirlpool хеш алгорита” одбранио је у септембру 2021. године са оценом 10. Дипломске академске – мастер студије на Електротехничком факултету у Београду, на модулу за Софтверско инжењерство, уписао је у октобру 2021. године. Положио је све испите са просечном оценом 9,40.

2. Извештај о студијском истраживачком раду

Кандидат Душан Станивуковић је као припрему за израду мастер рада урадио истраживање релевантне литературе која се односи на област којој припада тема мастер рада. У оквиру израде рада анализирана је SSRF (енг. *Served Side Request Forgery*) рањивост са OWASP (енг. *Open Web Application Security Project*) листе десет најчешћих рањивости из 2021. године. Анализиране су различите врсте напада, технике превенције, као и последице постојања рањивости. Истраживањем је утврђено да постоје апликације које се користе за демонстрацију SSRF рањивости, од којих су у раду описане: *PortSwigger Web Security Academy* и *Server-Side Request Forgery (SSRF) vulnerable Lab*, као репрезентативне.

3. Опис мастер рада

Мастер рад обухвата 62 стране (од чега прилог обухвата 9), са укупно 55 слика, 1 табелом и 42 референце. Рад садржи увод, 4 поглавља и закључак (укупно 6 поглавља), списак коришћене литературе, списак скраћеница, списак слика, списак табела и прилог.

Прво поглавље представља увод у коме су описани предмет и циљ рада. Представљена је улога и значај веб апликација, као и значај безбедности истих, са освртом на OWASP пројекат и SSRF рањивост. Описан је значај система за демонстрацију рањивости апликација.

У другом поглављу је детаљно представљена SSRF рањивост. Приказани су различити типови рањивости и различите врсте напада. Објашњене су технике превенције рањивости и начини заобилажења заштите.

Треће поглавље приказује постојеће системе за демонстрацију рањивости лажирања захтева на страни сервера. Разматране су функционалности и особине одабраних система.

У четвртом поглављу је дат детаљан опис реализованог система. Приказан је начин експлоатације рањивости, као и имплементираних технике заштите.

У оквиру петог поглавља је описана имплементација система. Приказана је основна архитектура система, уз опис коришћених технологија. Дати су детаљи имплементације

сопствене рањиве апликације за демонстрацију SSRF рањивости. На крају се разматра и начин испоруке система у виду контејнера.

У шестом поглављу је дат закључак у оквиру кога се даје осврт на испуњење захтева постављених у овом раду, као и предлози за даљи рад.

4. Анализа рада са кључним резултатима

Мастер рад дипл. инж. Душана Станивуковића се бави проблематиком експлоатисања рањивости веб апликација и заштитом истих од потенцијалних напада. У оквиру рада анализирани су постојећи системи и на основу резултата анализе предложено је и имплементирано ново решење. Серверска страна је реализована помоћу .NET технологије. Клијентска страна је имплементирана помоћу *Angular* технологије, док је база података реализована као релациона *SQL server* база података.

Основни доприноси рада су: 1) анализа SSRF рањивости и приказ последица постојања ове рањивости у софтверу; 2) анализа постојећих система за демонстрацију SSRF рањивости; 3) имплементација сопствене рањиве апликације за демонстрацију техника напада на SSRF рањивост, као и техника заштите од истих.

5. Закључак и предлог

Кандидат Душан Станивуковић је у свом мастер раду успешно спровео анализу SSRF рањивости у веб апликацијама. На основу спроведене анализе кандидат је успешно имплементирао сопствену рањиву апликацију за демонстрацију рањивости лажирања захтева на серверској страни.

Кандидат је исказао самосталност и систематичност у своме поступку.

На основу изложеног, Комисија предлаже Комисији за студије II степена Електротехничког факултета у Београду да рад дипл. инж. Душана Станивуковића под насловом „Развој апликације за демонстрацију рањивости лажирања захтева на серверској страни” прихвати као мастер рад и кандидату одобри јавну усмену одбрану.

Београд, 31.08.2023. године

Чланови комисије:



др Жарко Станисављевић, ванредни професор



др Павле Вулећић, ванредни професор