

УНИВЕРЗИТЕТ У БЕОГРАДУ - ЕЛЕКТРОТЕХНИЧКИ ФАКУЛТЕТ

Булевар краља Александра 73, 11000 Београд, Србија

Тел. 011/324-8464, Факс: 011/324-8681

КОМИСИЈА ЗА СТУДИЈЕ II СТЕПЕНА ЕЛЕКТРОТЕХНИЧКОГ ФАКУЛТЕТА У БЕОГРАДУ

Комисија за студије II степена, Електротехничког факултета у Београду, на својој седници одржаној 05.09.2023. године именовала нас је у Комисију за преглед и оцену мастер рада дипл. инж. Петра Мاستиловића под насловом „Слабости контроле приступа и ескалација привилегија код веб апликација“. Након прегледа материјала Комисија подноси следећи

ИЗВЕШТАЈ

1. Биографски подаци кандидата

Петар Мاستиловић је рођен 15.03.1997. године у Аранђеловцу. Завршио је Основну школу „Милан Илић - Чича“ у Аранђеловцу као вуковац. Уписао је Гимназију „Милош Савковић“ коју је завршио са одличним успехом. Током школовања учествовао је на такмичењима из математике, физике и хемије, где је остварио запажене резултате на републичком нивоу. Електротехнички факултет уписао је 2016. године. Дипломирао је на одсеку за рачунарску технику и информатику 2021. године са просечном оценом 7.53. Дипломски рад одбранио је у септембру 2021. године са оценом 10. Дипломске академске – мастер студије на Електротехничком факултету у Београду, на Модулу за рачунарску технику и информатику уписао је у октобру 2021. године. Запослен као софтверски инжењер у компанији *Byteout Software d.o.o.* од јула 2019. године.

2. Извештај о студијском истраживачком раду

Кандидат Петар Мастиловић је као припрему за израду мастер рада урадио истраживање релевантне литературе која се односи на анализу и методе напада на веб апликације из области контроле приступа и ескалација привилегија. Истражене су и анализиране основне слабости веб апликација. У складу са овим истраживањем имплементирано је демонстрационо окружење које има за циљ да омогући практичан пример за имплементацију основних слабости веб апликација.

3. Опис мастер рада

Мастер рад обухвата 43 стране са укупно 33 слике и 9 референци. Рад садржи увод, 3 поглавља и закључак (укупно 5 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 веб апликација, структура и архитектура истих, неки статистички подаци везани за коришћење и слабости веб апликација. Уведени су и термини контрола приступа, хоризонтална и вертикална ескалација привилегија.

У другом поглављу је дат опис архитектуре веб апликација, историјат напада из наведене области, неки актуелни трендови, као и опис свих напада који ће се наћи у демонстрационом окружењу.

У трећем поглављу се налази детаљан опис свих замишљених сценарија напада који се могу практично извести у демонстрационом окружењу. Уз сваки сценарио постоје додатна објашњења за појмове који се користе и део који представља поставку сценарија. Сви сценарији су тестирани ЗАР алатом за динамичку анализу сигурности веб апликација, како би се показала ова методологија за проналажење слабости. На крају, последњи део представља решење сценарија у коме се детаљно пролазе кораци за проналажење слабости.

У четвртном поглављу је описан код којим је реализовано демонстрационо окружење. Такође, у овом поглављу је објашњен код за покретање самог пројекта у виду *docker* контејнера, као и све компоненте које се заправо инсталирају приликом првог покретања чиме

је омогућена лака репродукција реализованог пројекта. На крају су објашњени алати и технологије коришћене у прављењу демонстрационог окружења.

Пето поглавље је закључак у оквиру кога су побројани сви сценарији напада из демонстрационог окружења. Истакнута је важност учења основних слабости у овој области и наглашено је да се већина *framework* алата подразумевано штити од сценарија наведених у овом раду.

4. Анализа рада са кључним резултатима

Мастер рад дипл. инж. Петра Мاستиловића се бави слабостима контроле приступа и ескалација привилегија код веб апликација. Успешно је реализовано демонстрационо окружење са циљем на практичан начин корисницима представи основне слабости веб апликација за ову врсту напада. У оквиру рада су приказани детаљни сценарији како се напади могу извршити на овом окружењу.

Основни доприноси рада су: 1) развој и имплементација демонстрационог окружења, 2) детаљан приручник који омогућава коришћење овог окружења у образовне сврхе

5. Закључак и предлог

Кандидат Петар Мастиловић је у свом мастер раду успешно имплементирао демонстрационо окружење, као и приручник са сценаријима за нападе из ове области који се могу извести на поменутом окружењу. Кандидат је исказао самосталност и систематичност у своје 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 Мастиловића под насловом „Слабости контроле приступа и ескалација привилегија код веб апликација“ прихвати као мастер рад и кандидату одобри јавну усмену одбрану.

Београд, 14.09.2023. године

Чланови комисије:



Др Павле Вулетић, ванредни професор



Др Жарко Станисављевић, ванредни професор