1/3/2022

IO 6: ТУТОРИЈАЛ ЗА ПРОЈЕКТОВАЊЕ И ТЕХНИЧКУ ИМПЛЕМЕНТАЦИЈУ ВЕБ ЛАБОРАТОРИЈА – СИГУРНОСТ У КОМУНИКАЦИЈИ

Co-funded by
the European Union

1. УВОД

Лабораторијска опрема и ресурси у оквиру *WebLabs* су доступни свима преко интернета, на основу тога аутоматски постају рањиви јер су доступни и злонамерним корисницима. Групе аутора и универзитети који развијају и користе *WebLabs* обично не схватају превише озбиљно питање безбедности оваквих интернет платформи, а безбедност је заправо једна од најкритичнијих тачака на које треба обратити пажњу. У том смислу, комуникациони канали, протоколи и архитектура одабрани за реализацију вежби у оквиру *WebLabs-a* су од највеће важности, јер утичу на ниво остварене безбедности.

Овај документ даје преглед неких од најтипичнијих безбедносних претњи и решења за очување сигурности у процесу комуникације, а све у циљу објашњења и отклањања потенцијалних ризика.

2. ОПИС ПРЕТЊИ И НАЧИНИ ЗА ОЧУВАЊЕ БЕЗБЕДНОСТИ

У наставку је дат преглед најчешћих извора претњи *WebLab-a*, описани су и ризици повезани са њима:

- Опрема (камере, рачунари, прекидачи, итд.) користи јавне IP адресе. Када се лабораторијским уређајима приступа преко јавне IP адресе, они су видљиви и доступни свима. Иако је ово најпогодније решење за приступ и реализацију самих вежби у оквиру *WebLabs-a* , оно такође носи огроман ризик, јер сваки корисник или бот може да покуша да приступи таквим уређајима.
- *WebLabs* услуге не користе систем аутентификације. Понекад *WebLabs* дозвољава отворен приступ садржајима, односно дозвољава да му свако може приступити без корисничког имена и лозинке. Овакав приступ може бити реализован планирано или грешком од стране аутора, али у оба случаја, злонамерни корисници могу преузети контролу над лабораторијом и лоше је користити. Могуће је да дође до потенцијалног оштећења опреме што би имало последице на реализацију вежби, монополизације опреме чиме би се онемогућило да и други учесници користе опрему за реализацију вежби, или приступ одређеним уређајима (попут камера) које не би требали да буду доступи свима у било ком тренутку.
- Не користи се *https* сигурносни протокол. Чак и када постоји механизам за аутентификацију, ако се такав механизам не ослања на *https*, безбедност је угрожена јер се не користи шифровани комуникациони канал ни сертификати. Многе веб странице и услуге *WebLabs* - а и даље раде на *http* уместо *https* протоколу, што је далеко од идеалног у погледу остварене сигурности.
- Када корисници приступају *WebLab*–у они имају приступ и самом оперативном систему (ОС). Понекад су *WebLab* платформе засноване на удаљеном приступу радној површини. Када је то случај, особа која приступа ВебЛаб-у има приступ целом оперативном систему. Чак и ако корисник на *WebLab* рачунару има ограничене привилегије, што није увек случај, он опет представља велику опасност јер има могућност да, на пример, реализује phishing или да шаље непожељну е-пошту са удаљених адреса. И не само то, корисници *WebLab-a* који приликом рада вежби користе универзалне корисничке налоге могу пронаћи датотеке са лабораторијским подацима и резултатима које су добили други ученици који су претходно приступали *WebLab-y* , било да су они остављени тамо намерно или случајно.

Основне препоруке за избегавање наведених ризика и очување безбедности дати су у наставку:

- Користити приватне IP адресе унутар VLAN/VPN -а који је заштићен и који омогућава контролу приступа ресурсима у оквиру приватне мреже.
- Користити доступне системе за аутентификацију на нивоу комуникационог протокола. Најчешће, коришћење аутентификације за приступ веб страници није довољно јер овакав сценарио дозвољава кориснику приступ платформи, учитавање веб апликације која остаје отворена и активна приликом сваком приступа. На овај начин корисник преузету апликацију може користити кад год пожели без да се поново пријављује и идентификује на веб страници.
- Инсталирати и користити SSL сертификат који подржава реализацију https протокола а самим тим и шифровани комуникациони канал.

- Користити веб апликацију која комуницира са *WebLab* сервисима на ограничен начин (као што су приказани документи 2а, 2б и 3) Уколико се користи удаљени приступ радној површини:
    - 1) користити налог корисника на удаљеном рачунару који има ограничене привилегије као корисник.
    - 2) ограничити визуелни приступ удаљеном рачунару тако да се приказују само апликација која контролишу лабораторијску опрему.