National College of Ireland

Configuration Manual

MSc Internship
Cybersecurity

Joshua Nevilraj Yuva Kumar
Student ID: x18128106

School of Computing
National College of Ireland

Supervisor: Imran Khan

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name:	Joshua Nevilraj Yuva Kumar
Student ID:	X18128106
Programme:	MSc. Cybersecurity **Year:** 2019-2020
Module:	Academic Internship
Lecturer:	Imran Khan
Submission Due Date:	12 December 2019
Project Title:	Behavioural Based Threat Modelling to Increase The Efficiency in Breach Identification and Notification
Word Count:	693 **Page Count: 7**

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: ……

Date: ……

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Configuration Manual

Joshua Nevilraj Yuva Kumar
Student ID: x18128106

1 Introduction

This manual explains how the system and software are set up to produce the results of thesis "Behavioural based threat modelling to increase the efficiency in breach identification and notification" in relation to software and hardware requirements.

2 System Specifications:

Hardware Requirements:

Processor: 1.6 GHz Intel. Core i5
Memory: 8 GB 2133 MHz LPDDR3
Hard disk size: 121.02 GB

Software Used:

Operating System: macOS 10.14.6

Tools & Applications:

Visual Studio Code 1.40.2 : Code editor that is used to develop and debug modern web applications.

Xampp : Cross-platform web server used for testing and deployment which has apache HTTP Server and MySQL.

Postman: Tool used for testing API in various environments, helps us to simulate the user interaction with the system.

Angular CLI: Command line tool used to generate and modify applications

3 Execution

The steps followed for installing and execution are as follows

Step 1: Install Visual Studio Code in the system.

Step 2: Install Xampp to access MySQL database.

Step 3: Install the postman tool to generate API request

Step 4: Install Nodejs and Angular CLI.

Step 5: Check and validate token that has been passed as token

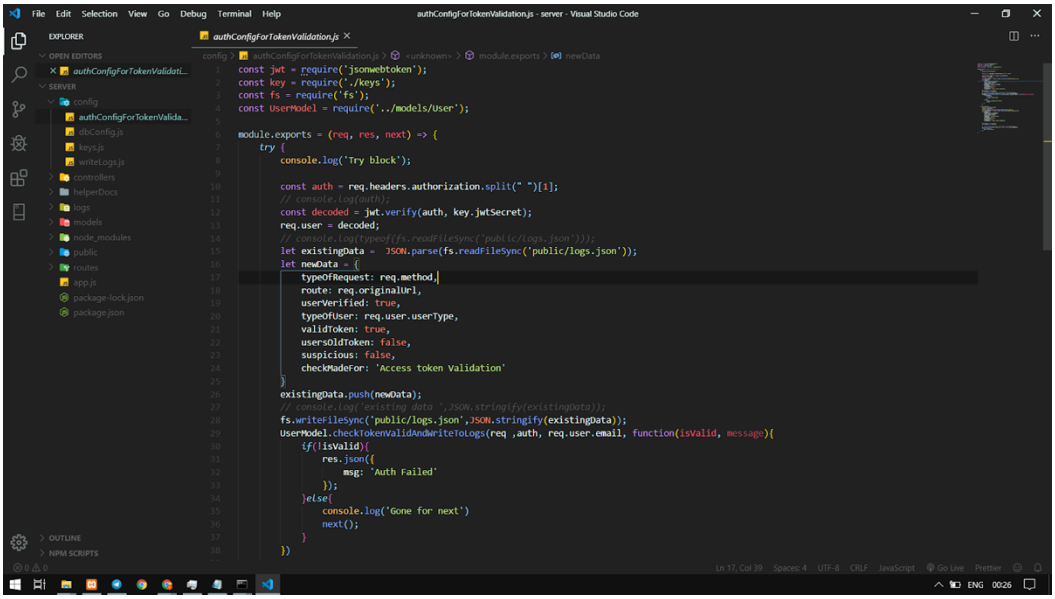

Figure – 1 *Validating Tokens*

Step 6: Controllers/logs.js is used to handle requests and response from postman application

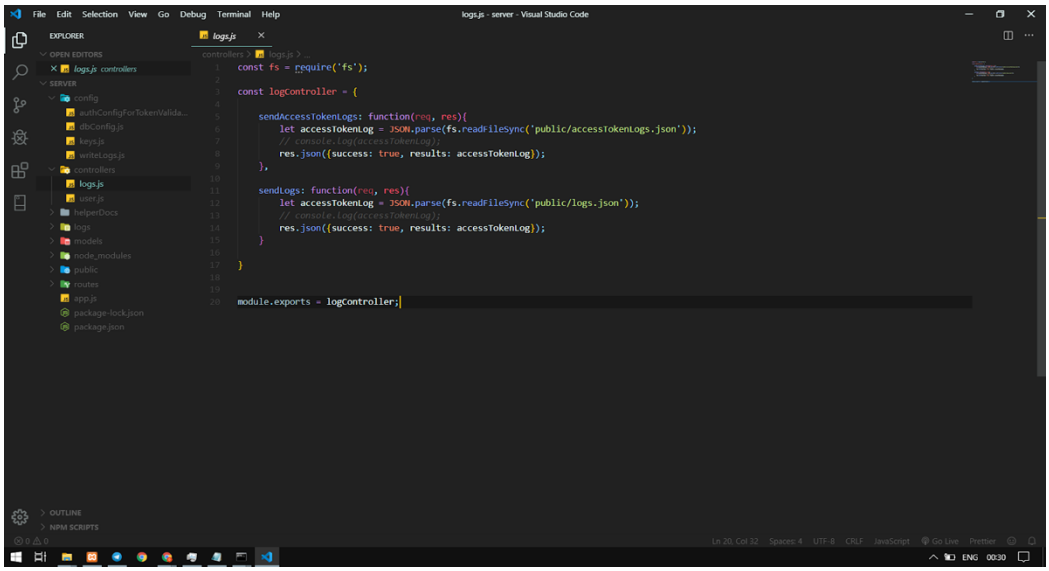

Figure –2 *Handling API Requests*

Step 7: Checking the login attempts to identify Brute Force.

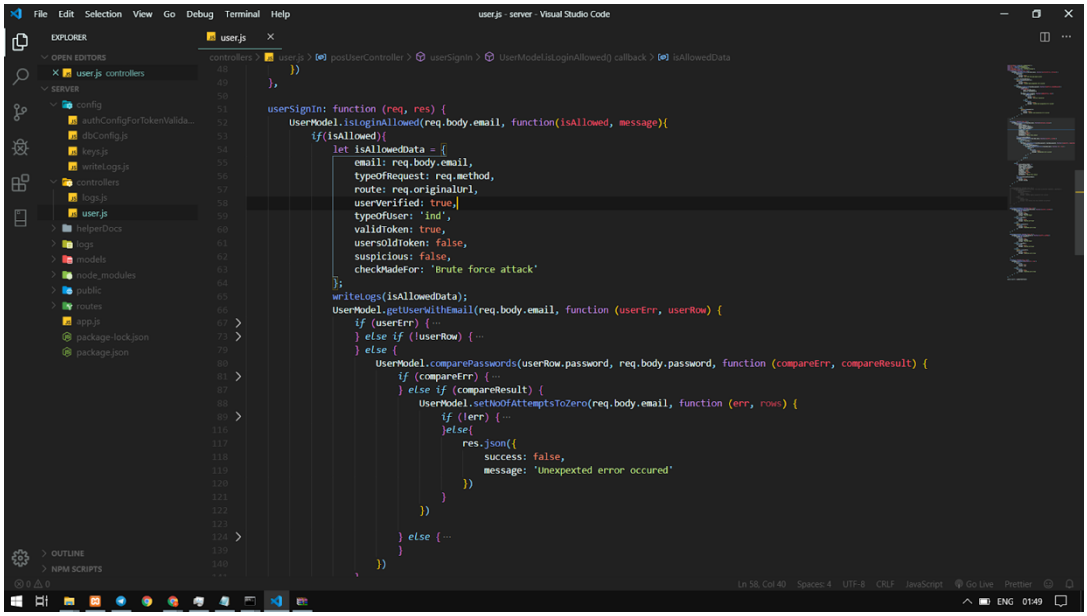

Figure –3 *Brute Force Identification*

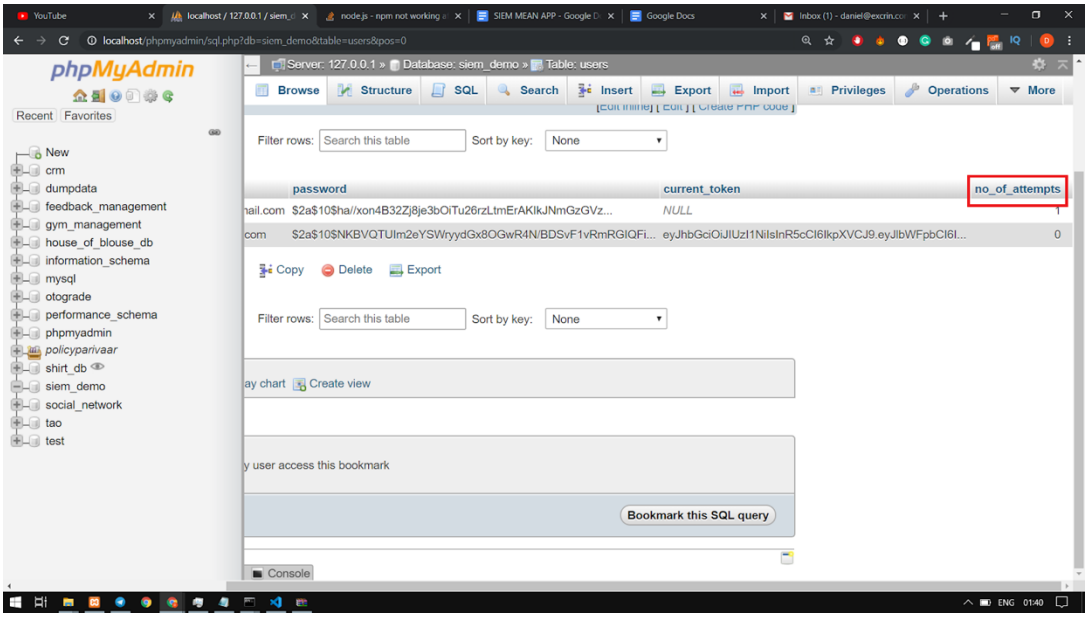

Figure –4 *Login attempts validation*

Step 8: Check tokens to identify Access Token Manipulation Technique.

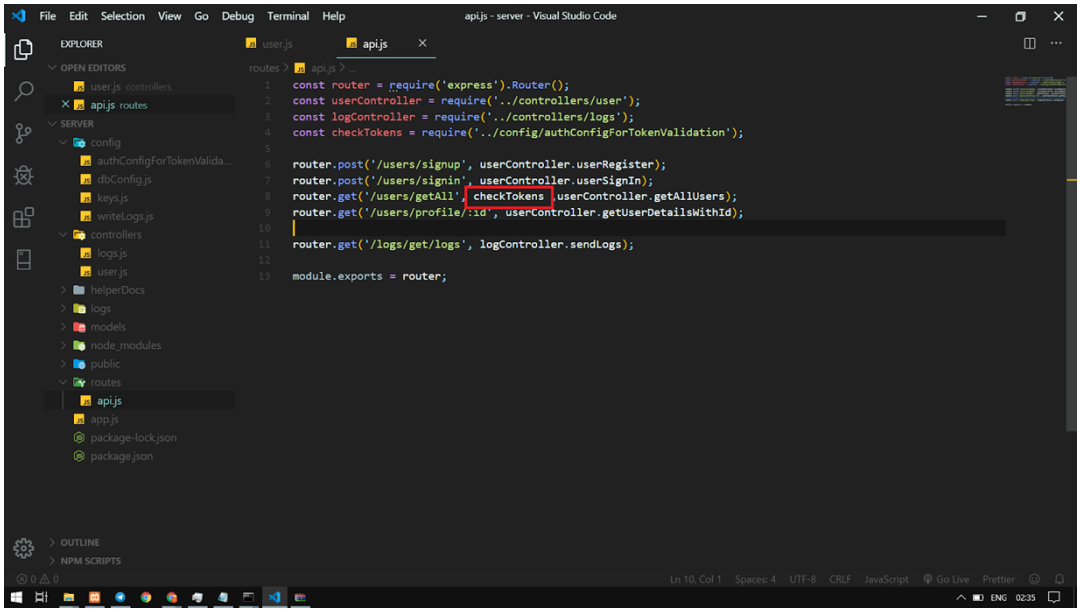

Figure – 5 *API routes Middleware*

Step 9: Validate new token and old token to check whether the sent token is valid or not.

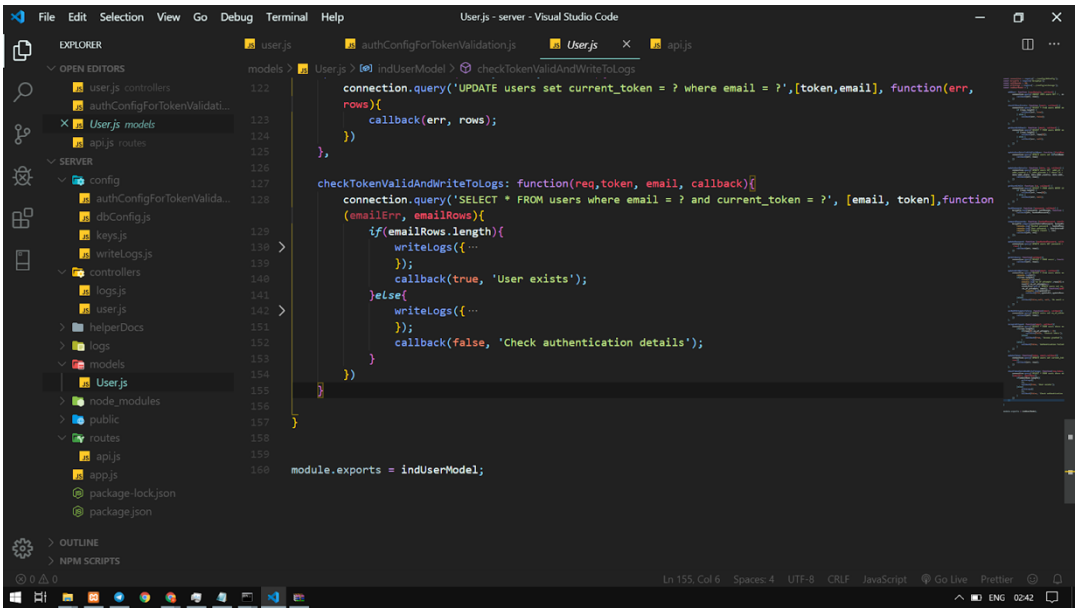

Figure – 6 *Steal Access Token Technique Idetification*

Output:

The Dashboard developed using pages template will show the suspicious activities from the API requests generated from Postman.

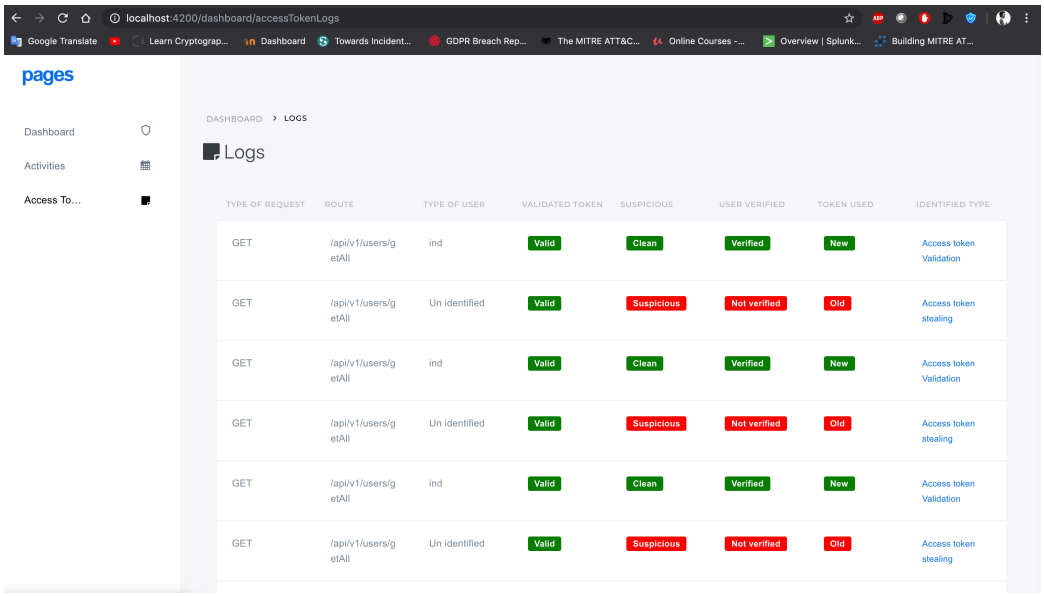

Figure – 7 *Dashboard displaying alerts for above techniques*