ASSIGNMENT 2 FRONT SHEET

Qualification	**BTEC Level 5 HND Diploma in Computing**		
Unit number and title	Unit 9: Cloud Computing		
Submission date		**Date Received 1st submission**	
Re-submission Date		**Date Received 2nd submission**	
Student Name	Phan Ba Hung	**Student ID**	GCH17622
Class	GCH0711	**Assessor name**	Do Quoc Binh

Student declaration

I certify that the assignment submission is entirely my own work and I fully understand the consequences of plagiarism. I understand that making a false declaration is a form of malpractice.

Student's signature	Hung.P

Grading grid

P5	P6	P7	P8	M3	M4	D2	D3

❒ Summative Feedback:	❒ Resubmission Feedback:

Grade:	Assessor Signature:	Date:

Internal Verifier's Comments:

Signature & Date:

Contents

I. INTRODUCTION.

Continue with the first report. The report will outline how to perform code management, configuration and deployment of the web application. Also report if some common problem and security issues of cloud computing platform and solution for each case.

II. ATN.

a. Github.

To manage the source code for this scenario, I used Github. To make it easier, I used GitHub Desktop. Here are some basic operations to manage source code with Github.

First you need to create an account and log into the Github Desktop .

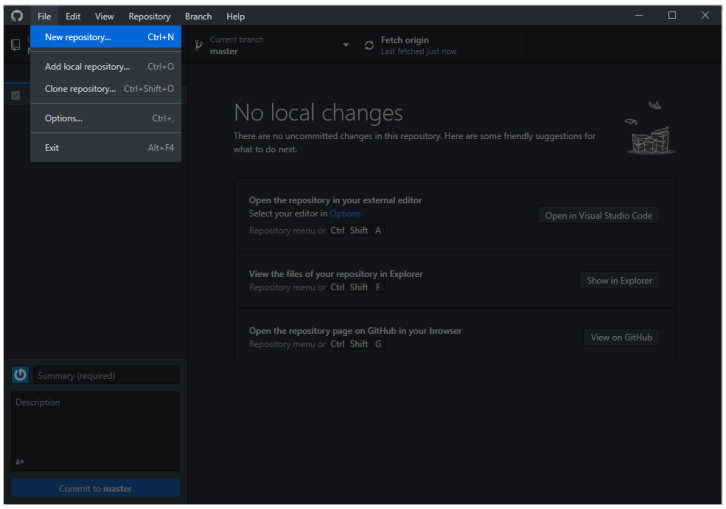

Figure 1

Next select File -> New respository to create a new archive. Next you name and choose the address to save for it and then select Create respository.

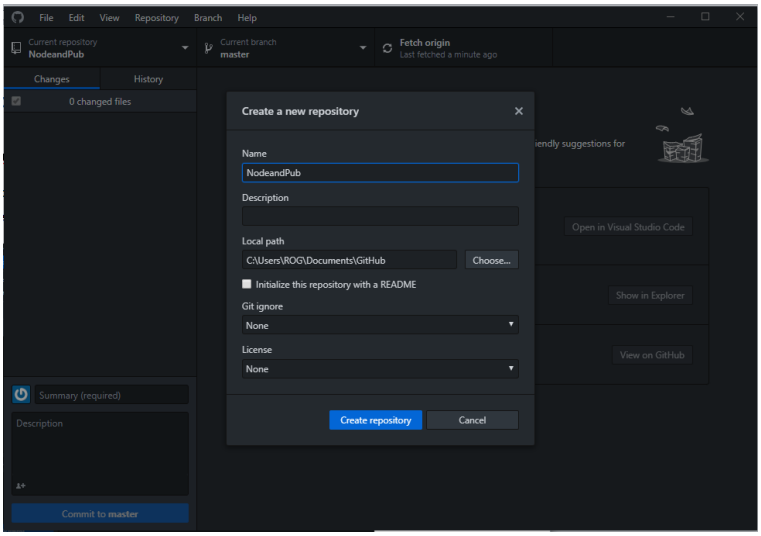

Figure 2

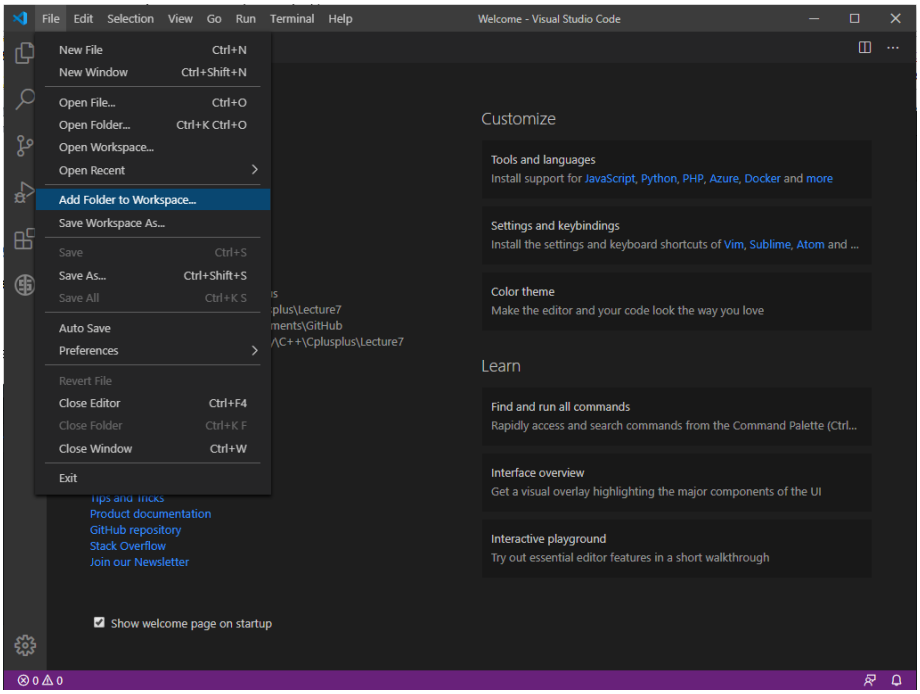

Figure 3

Next in the Visual Studio Code interface (VSC) select File -> Add Folder to Workspace then select the address you just saved on Github Desktop (in my case NodeandPub is stored in C: \ Users \ ROG \ Documents \ GitHub)

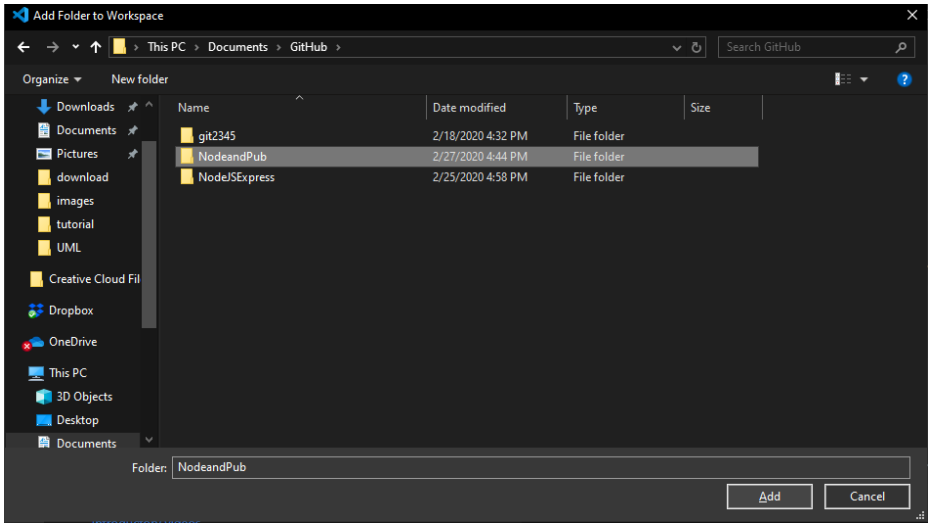

Figure 4

You can then create code files and start writing code in the folder that is added to the workspace.

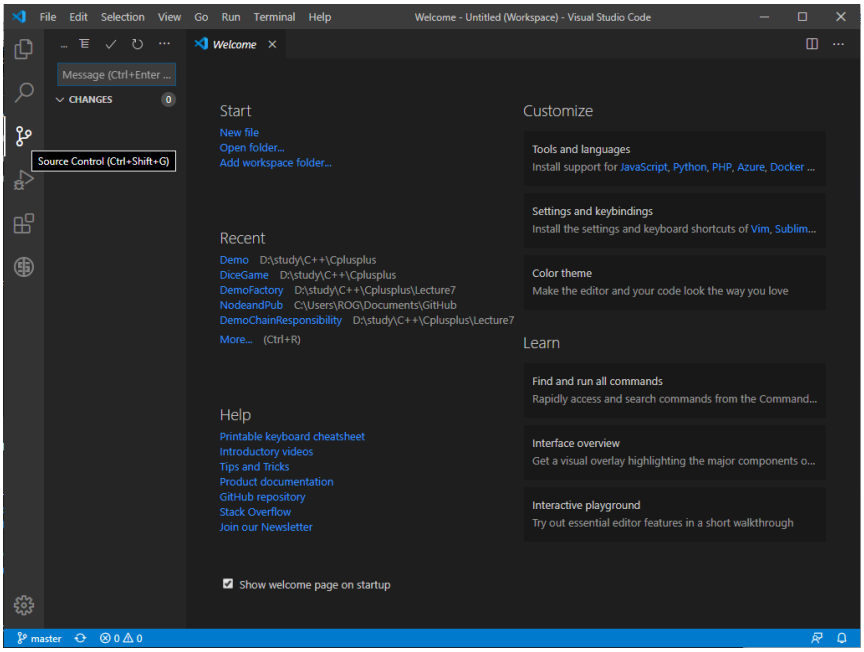

Figure 5

Next to synchronize the code on Github you need to go to Source Control -> Stage All Changes

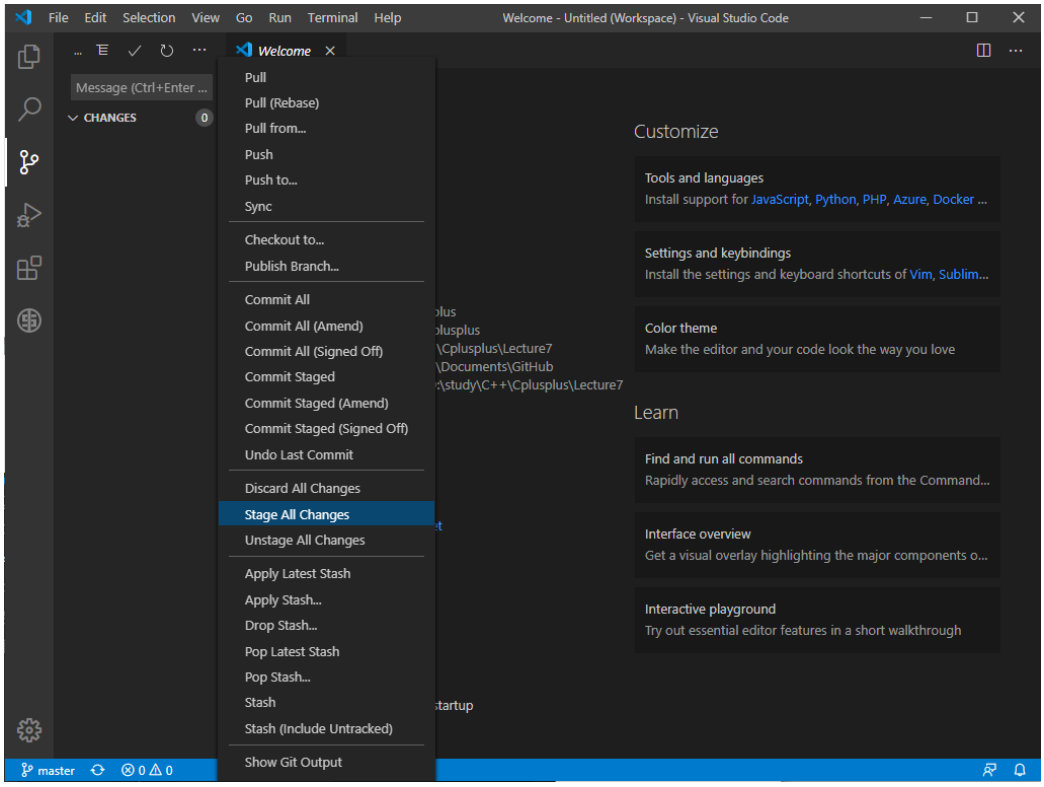

Figure 6

Then choose Commit All.

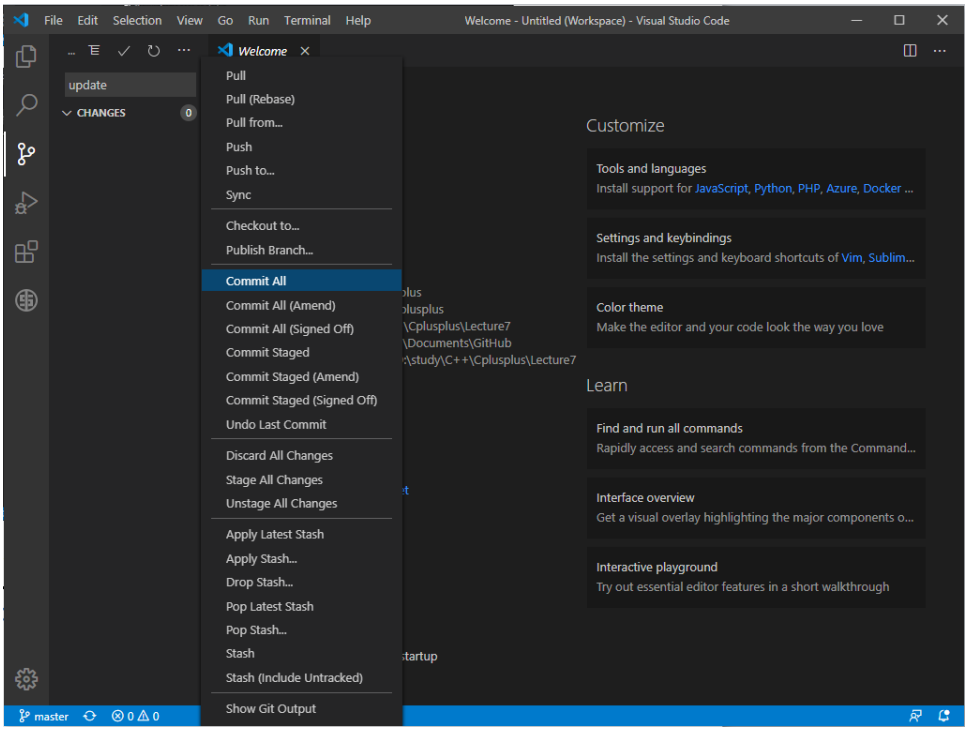

Figure 7

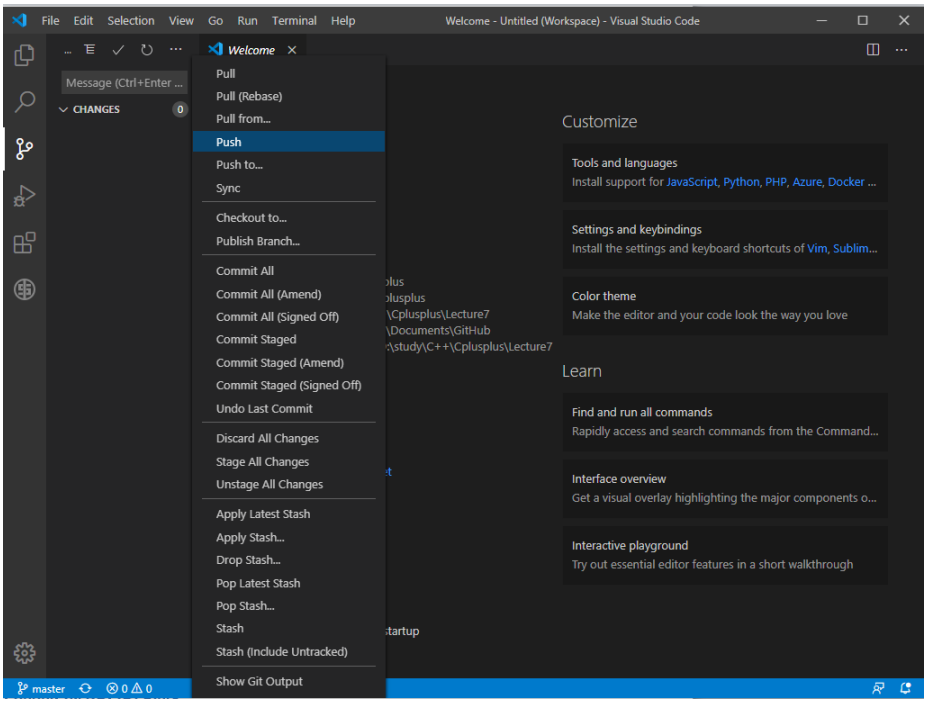

Figure 8

Finally, select push to complete the code synchronization on GitHub.

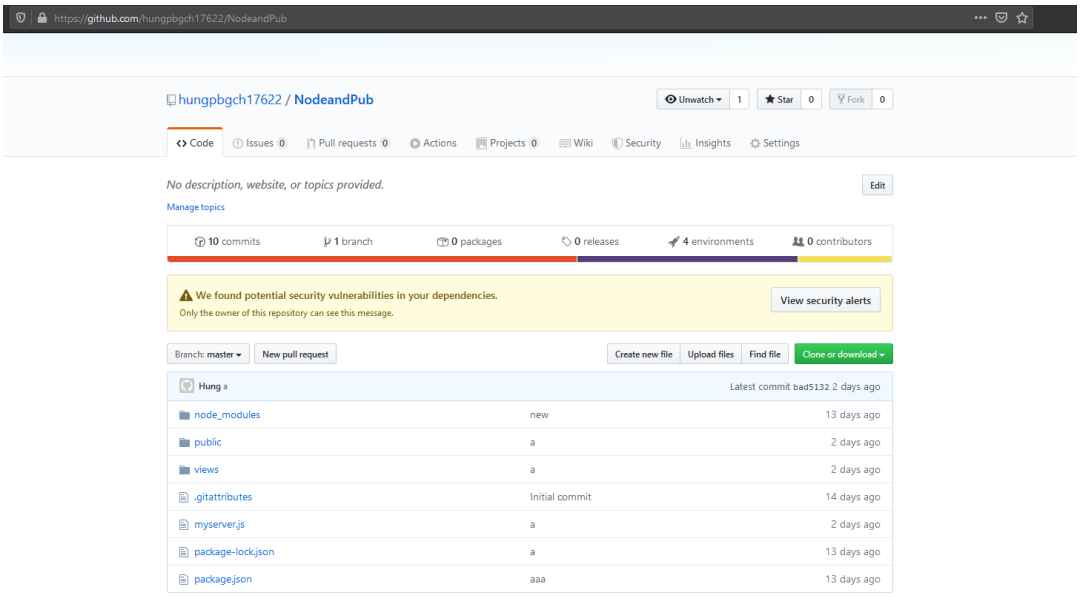

Figure 9

This is all my code for this program has been synchronized to GitHub.

b. Code.

```
PS C:\Users\ROG\Documents\GitHub\aaaaaa> npm init
This utility will walk you through creating a package.json file.
It only covers the most common items, and tries to guess sensible defaults.

See `npm help json` for definitive documentation on these fields
and exactly what they do.

Use `npm install <pkg>` afterwards to install a package and
save it as a dependency in the package.json file.

Press ^C at any time to quit.
package name: (aaaaaa)
version: (1.0.0)
description:
entry point: (index.js)
test command:
git repository:
keywords:
author:
license: (ISC)
About to write to C:\Users\ROG\Documents\GitHub\aaaaaa\package.json:

{
  "name": "aaaaaa",
  "version": "1.0.0",
  "description": "",
  "main": "index.js",
  "scripts": {
    "test": "echo \"Error: no test specified\" && exit 1"
  },
  "author": "",
  "license": "ISC"
}
```

Figure 10

First I use the npm init command in the terminal window to create the package.json file

Next, I installed 2 modules express and jade with the command npm install express and npm install jade.

- Express: Express is a minimal and flexible Node js web application framework that provides a robust set of features for the web and mobile applications.
- Jade: Jade is a high-performance template engine and implemented with JavaScript for node and browsers.

```
PS C:\Users\ROG\Documents\GitHub\NodeandPub> npm install express
```

Figure 11

```
PS C:\Users\ROG\Documents\GitHub\NodeandPub> npm install jade
```

Figure 12

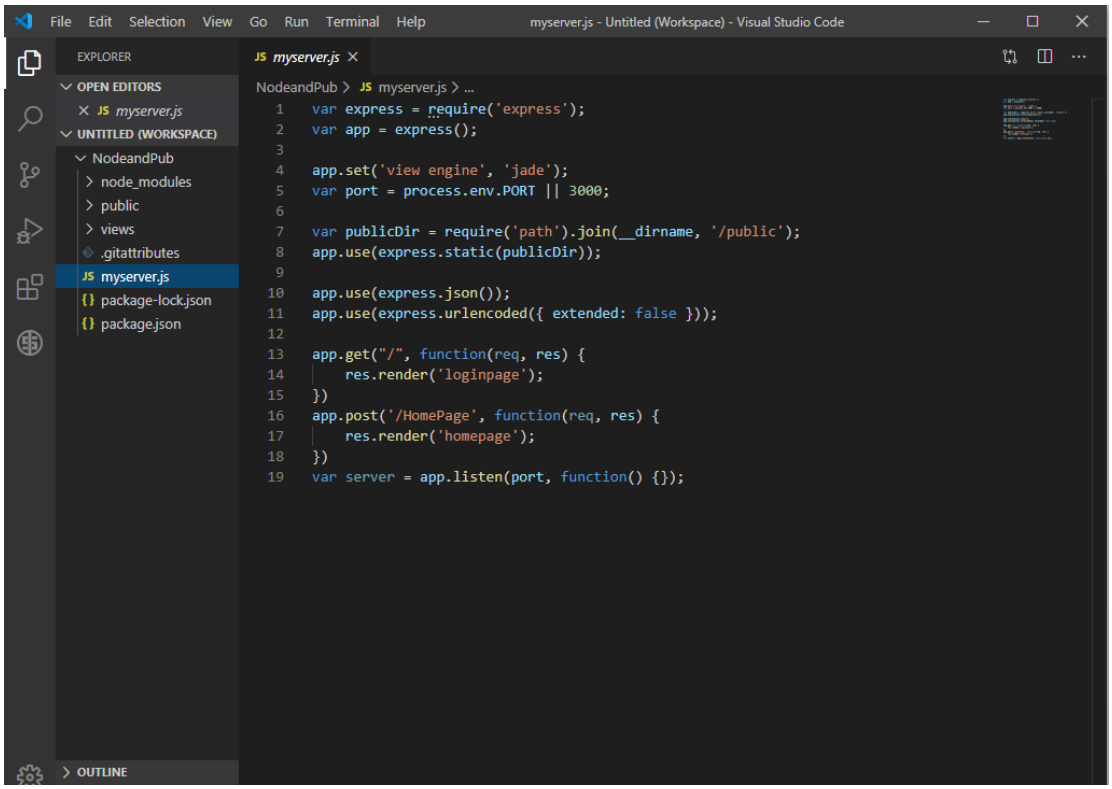

Figure 13

Next create the file myserver.js including:

Line 1 : use the express module

Line 2 : create an object of the express module

Line 4 : setting view engine to jade

Line 5 : cài đặt PORT tại cổng 3000

Line 13 : Create a call back function , This function will be called whenever anybody browses to the root of our web application which is http://localhost:3000.

Line 14 : rendering the loginpage template page

Similarly, the program will render the homepage jade template when someone visits http://localhost:3000/HomePage at line 16 17

line 19 : Using the listener function to make server application listen for client requests on the port PORT assigned at 3000

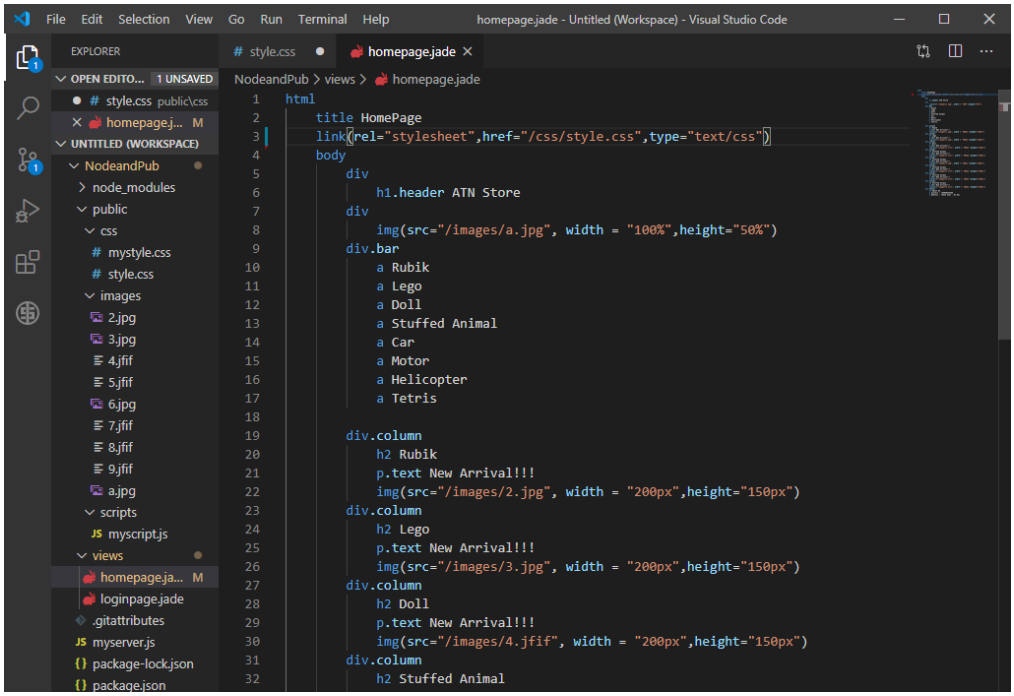

Figure 14

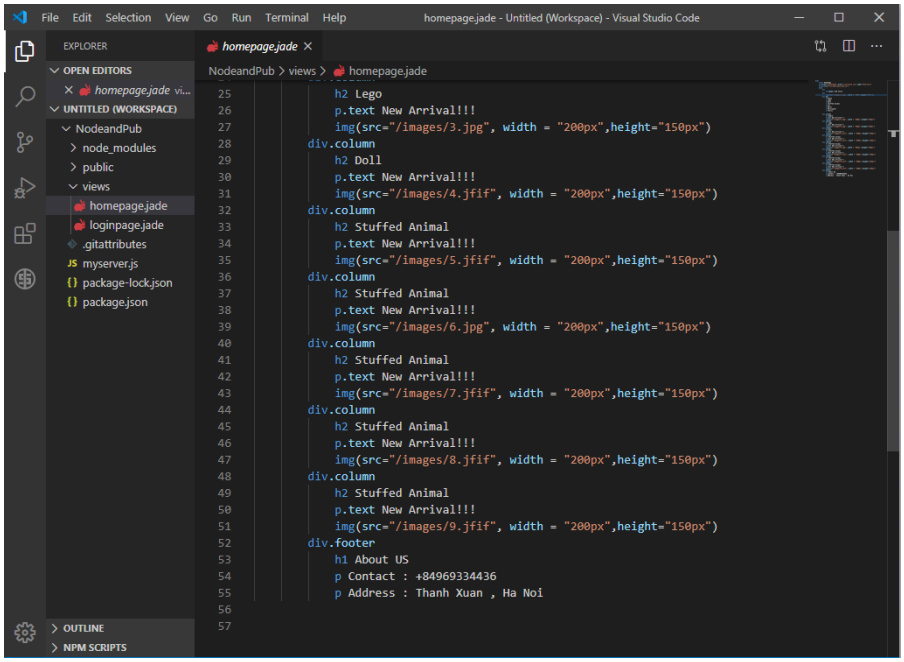

Figure 15

Above is the configuration source code of the homepage:

Inline 3 I declare using CSS in style.css stored in the public folder

Next is the source code for configuring the homepage using the jade template.

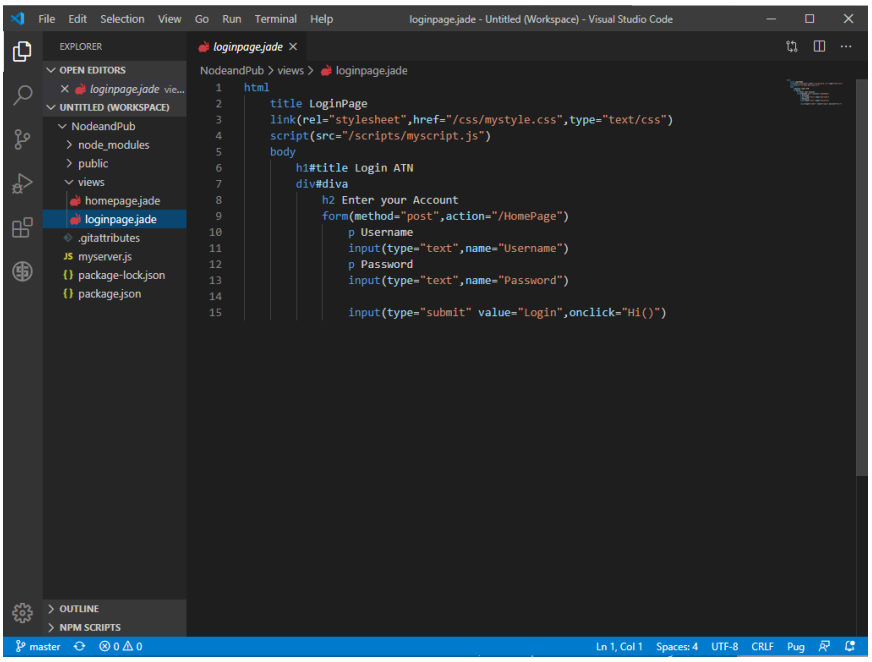

Figure 16

Here we also use jade template to configure loginpage interface. In addition, I use additional scripts declared in line 4. and used in line 15 with 1 button after clicking the button will run funtion Hi (); Installed in myscript.js is stored in public folder.

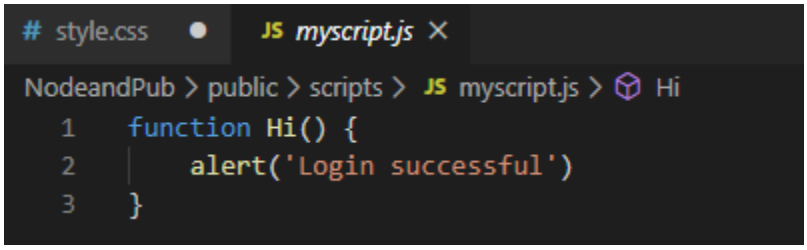

Figure 17

Install Hi() function with the function that alerts the "Login Successful" when called.

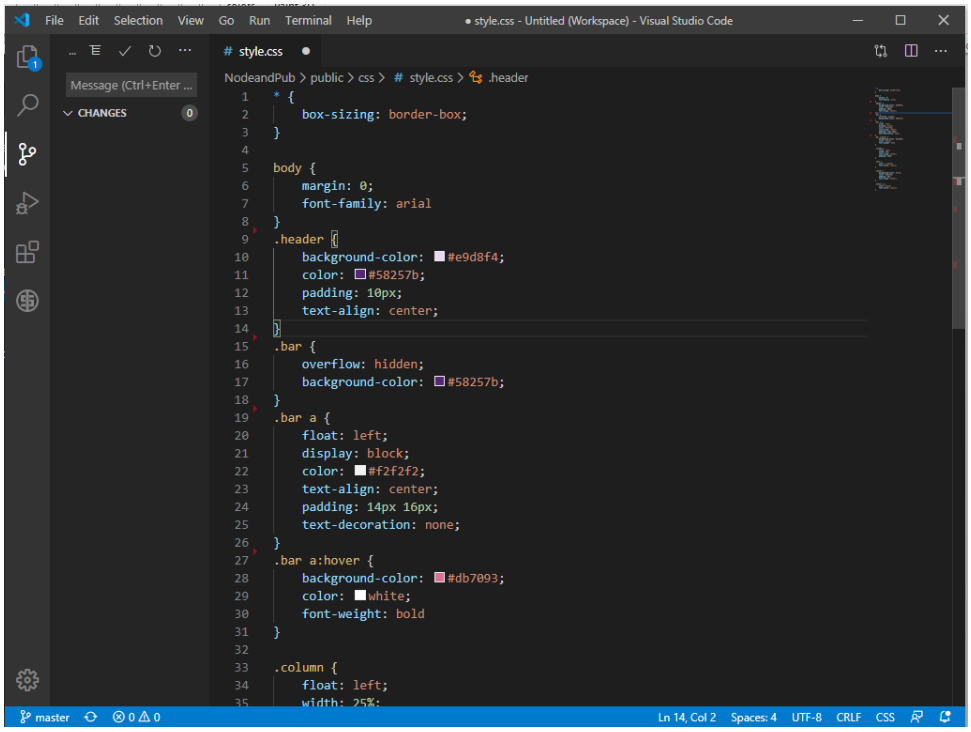

Figure 18

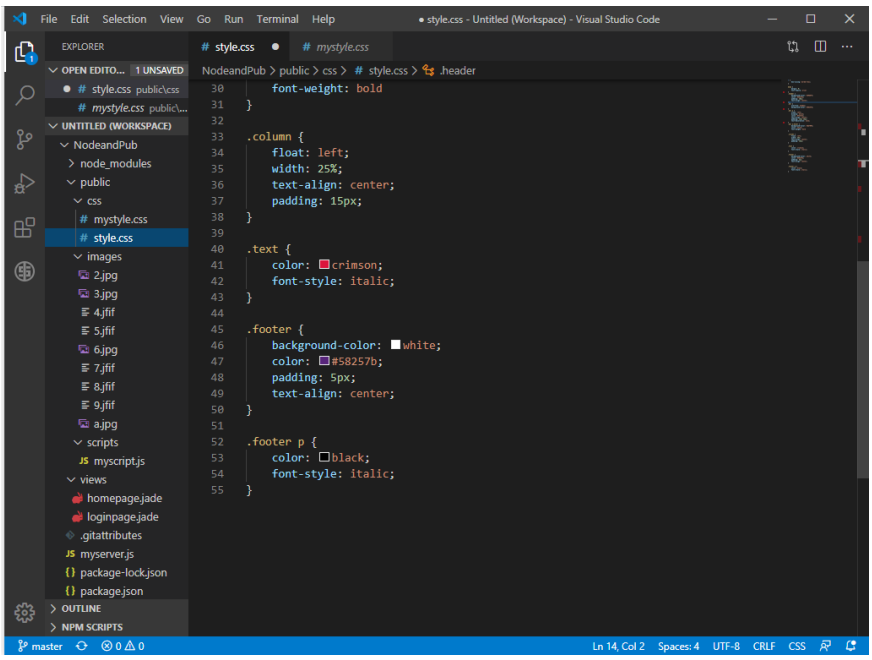

Figure 19

Figure 1 and Figure 2 are the CSS source code used to format the homepage.

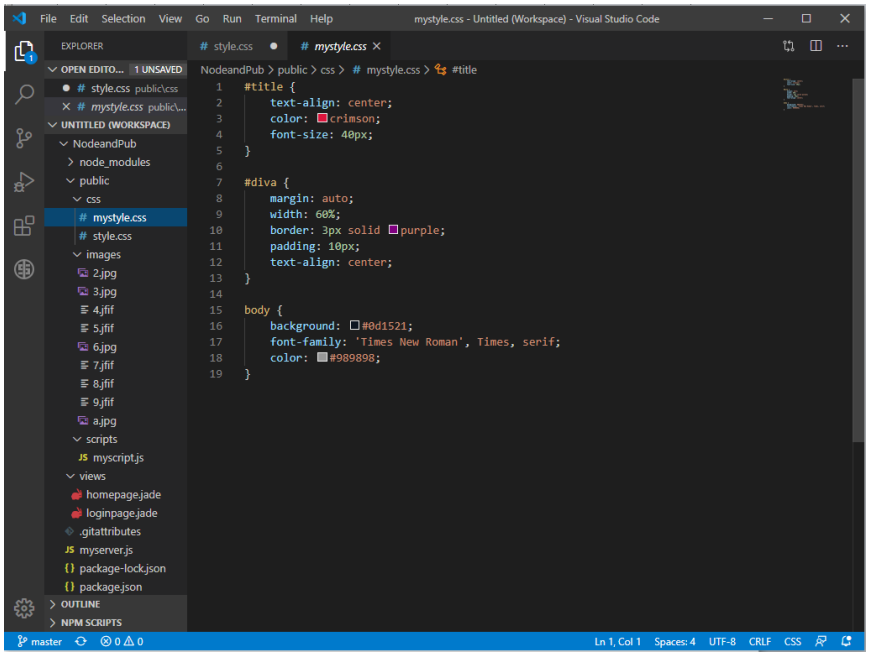

Figure 20

The image above is the CSS source code declared in the file mystyle.css used to format the loginpage.

c. Heroku.

Heroku is a cloud platform as a service that supports several programming languages. Here are some steps to deploy the system to Heroku

First, you need to create an account and log in to Heroku. Tiếp theo bạn chọn Create New App và đặt tên cho nó .

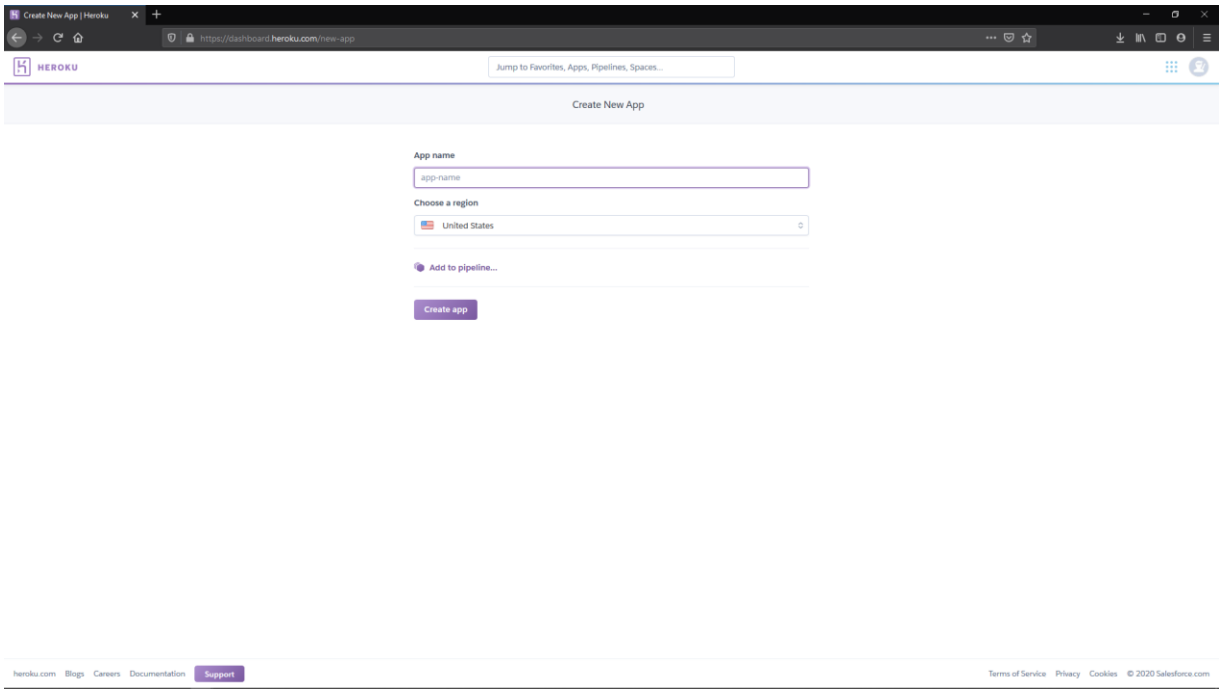

Figure 21

After creating the App, select Setting -> Add Buildpack, select NodeJS and click Save changes.

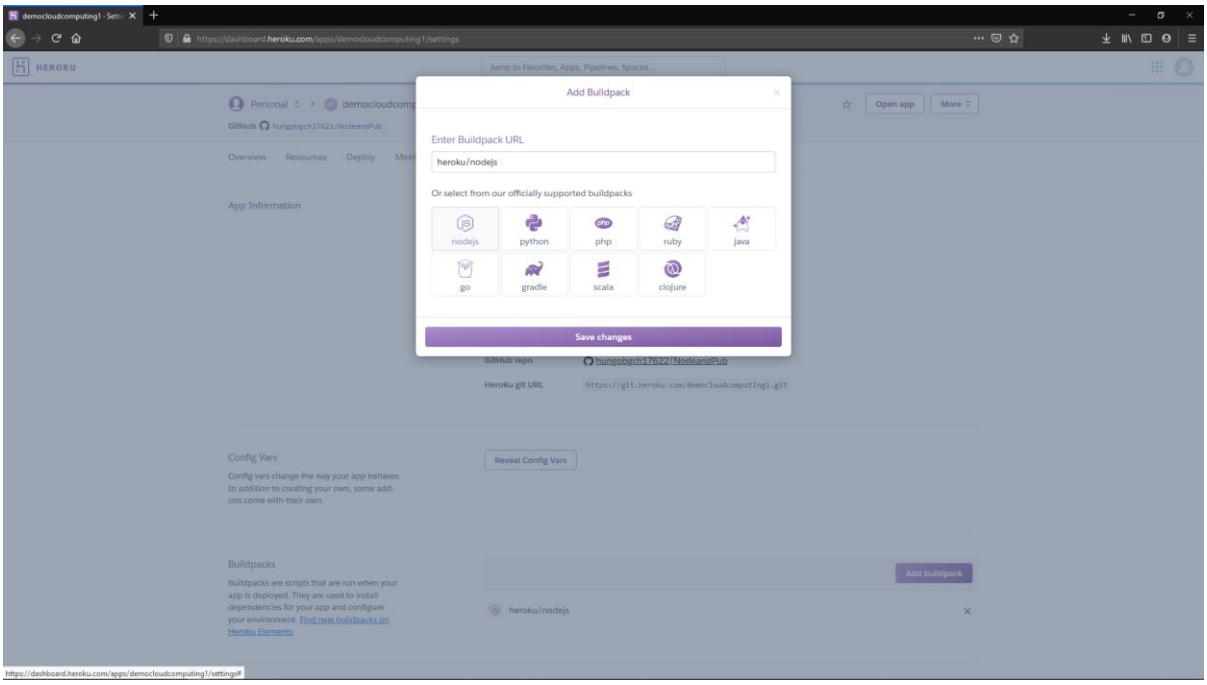

Figure 22

Next go to Deploy and select Github and connect to your Github account. Then you need to enter the name of the source folder and then select search (here the folder where my source code is stored is NodeandPub). When you have found the folder select connect.

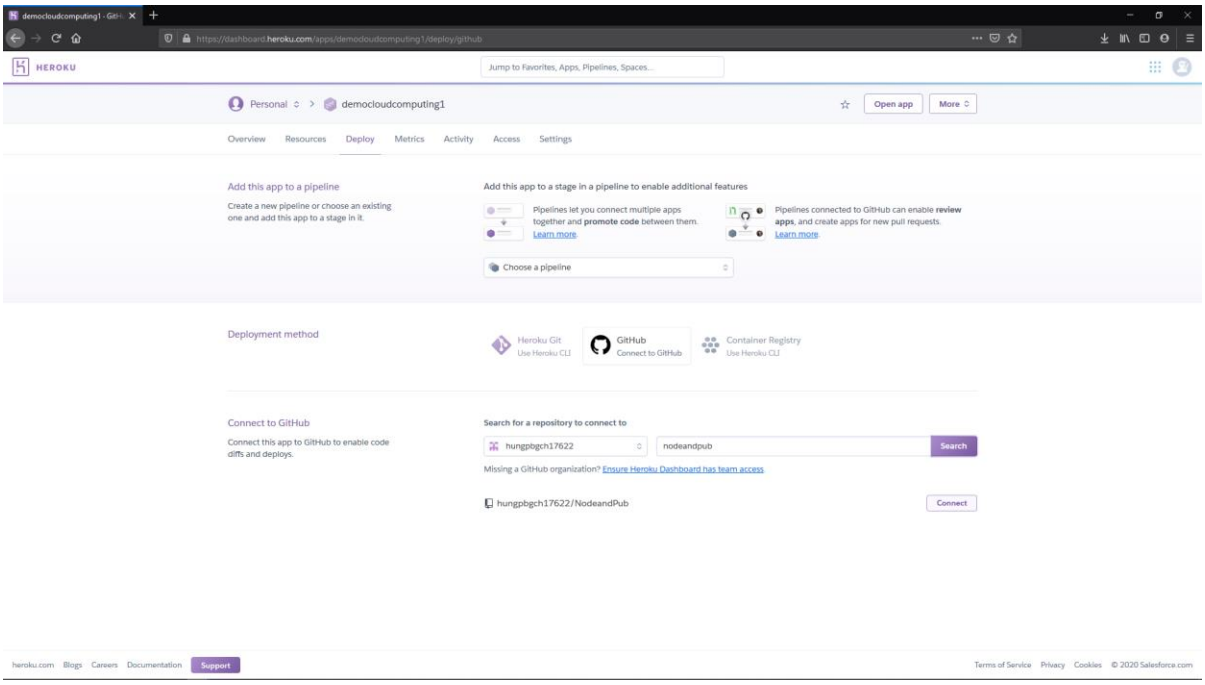

Figure 23

After connecting select Deploy Brand to deploy the source code to heroku.

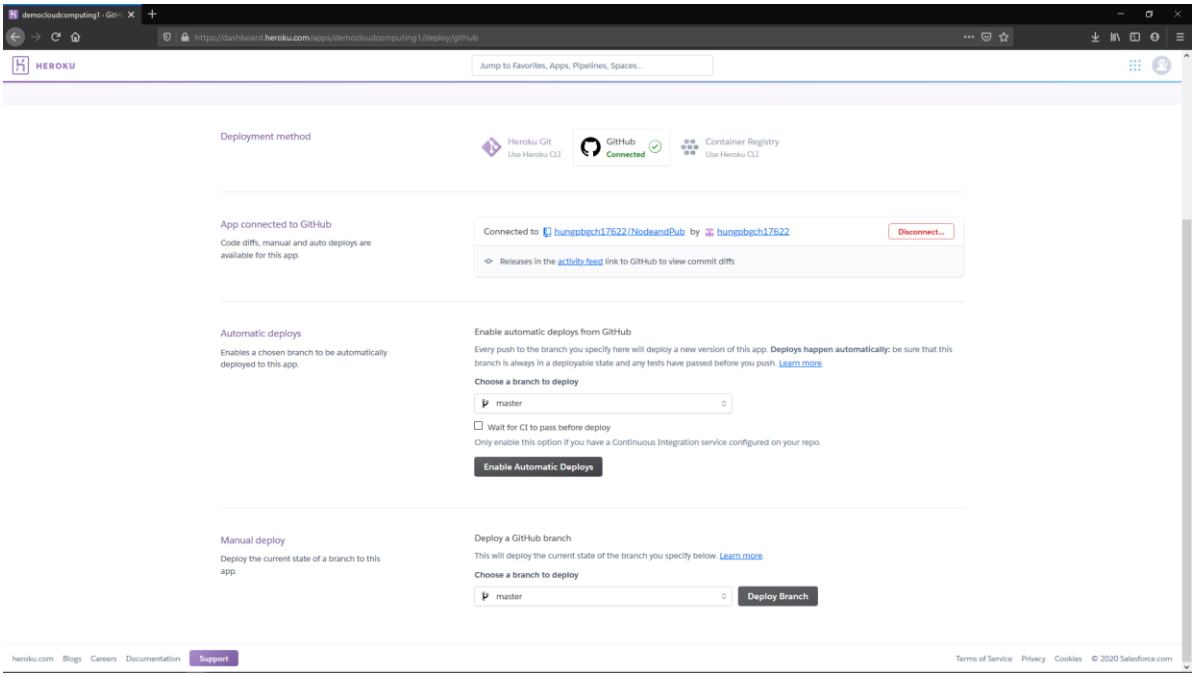

Figure 24

Next, when Deploy is successful, you will see a message of successfully deployed, you select the view to transfer to your App

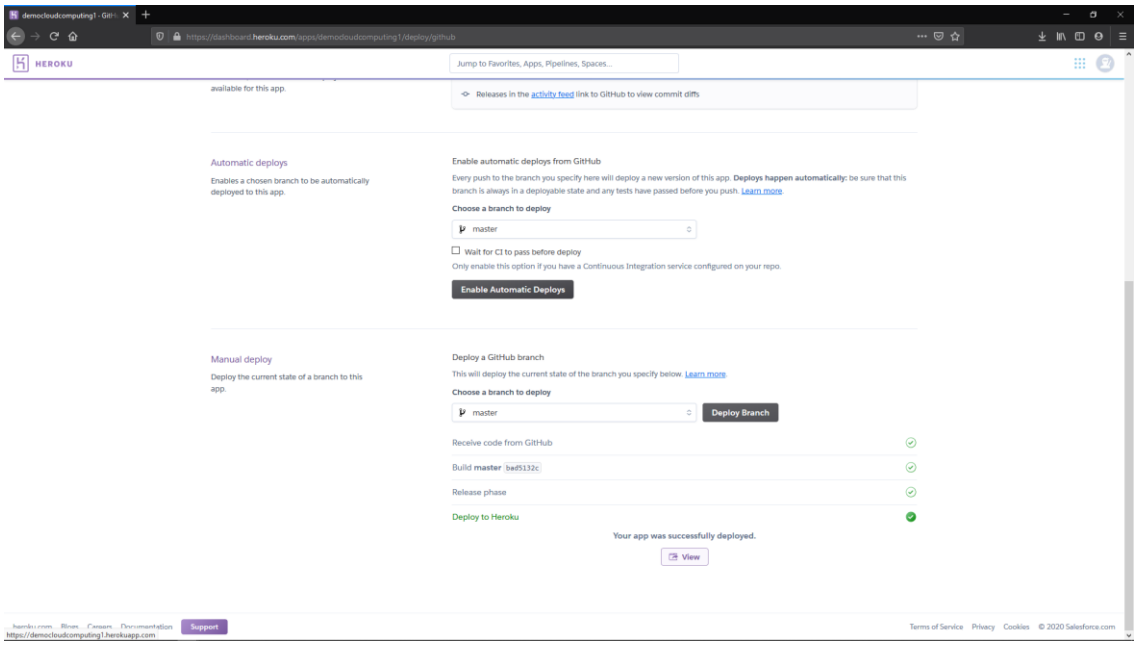

Figure 25

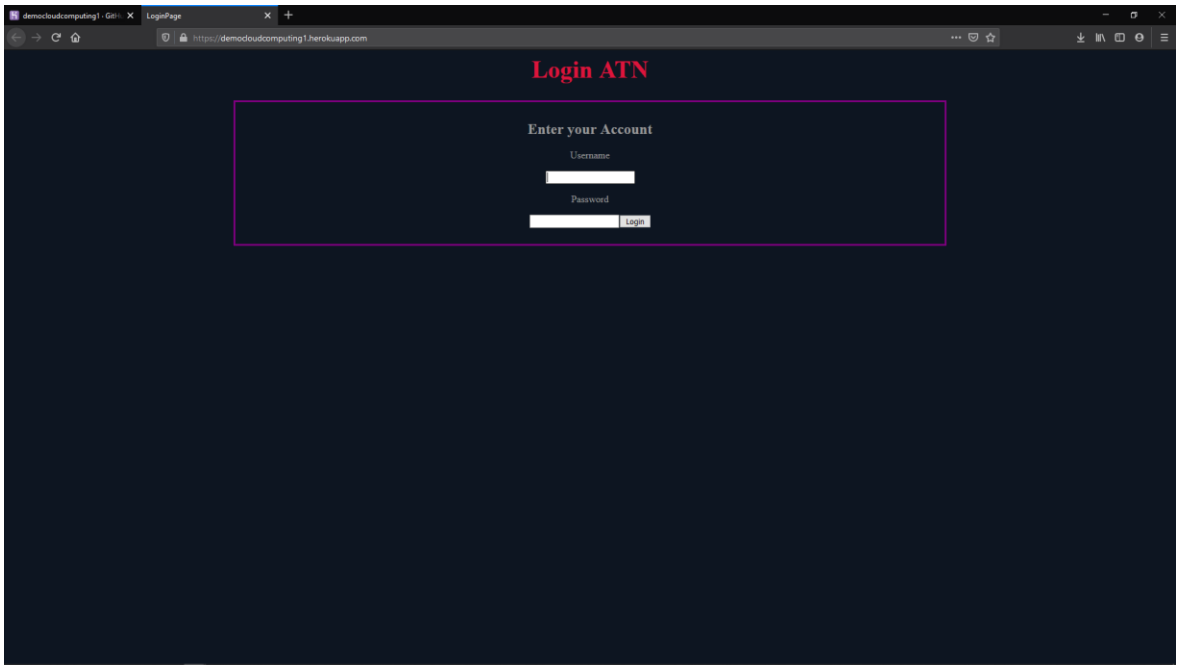

Figure 26

This is the login page interface that I have built. After entering information and clicking Login, the program will display a successful login

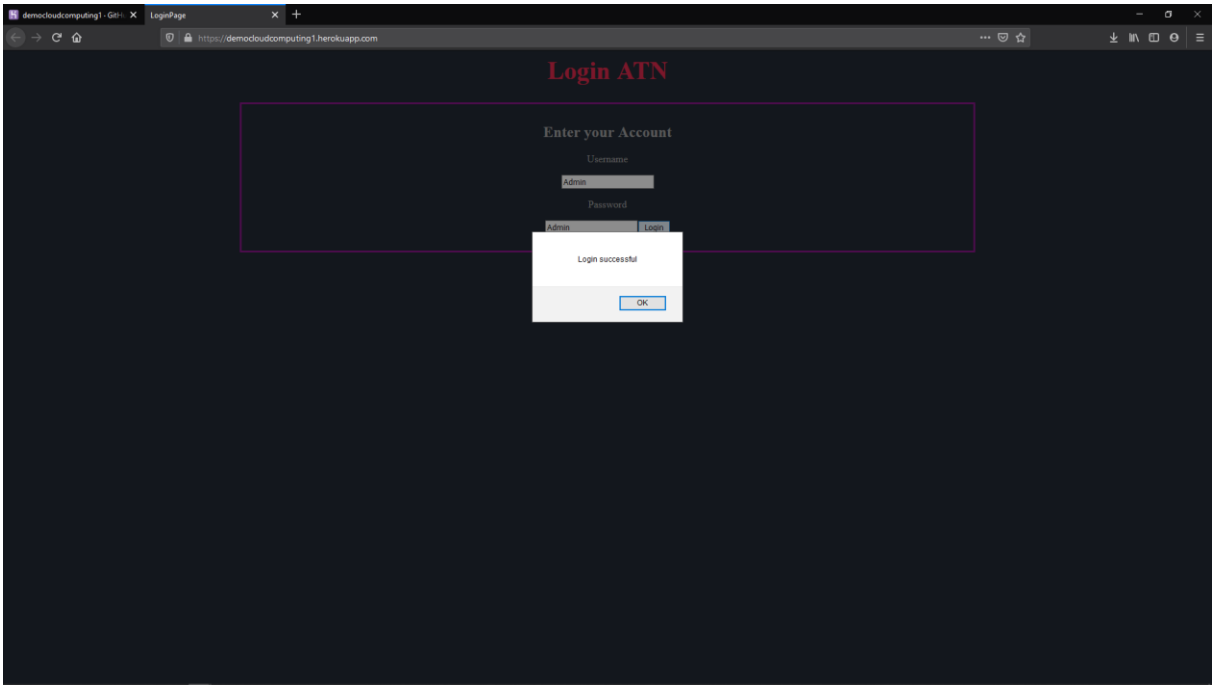

Figure 27

After you click OK, you will move to the home page.

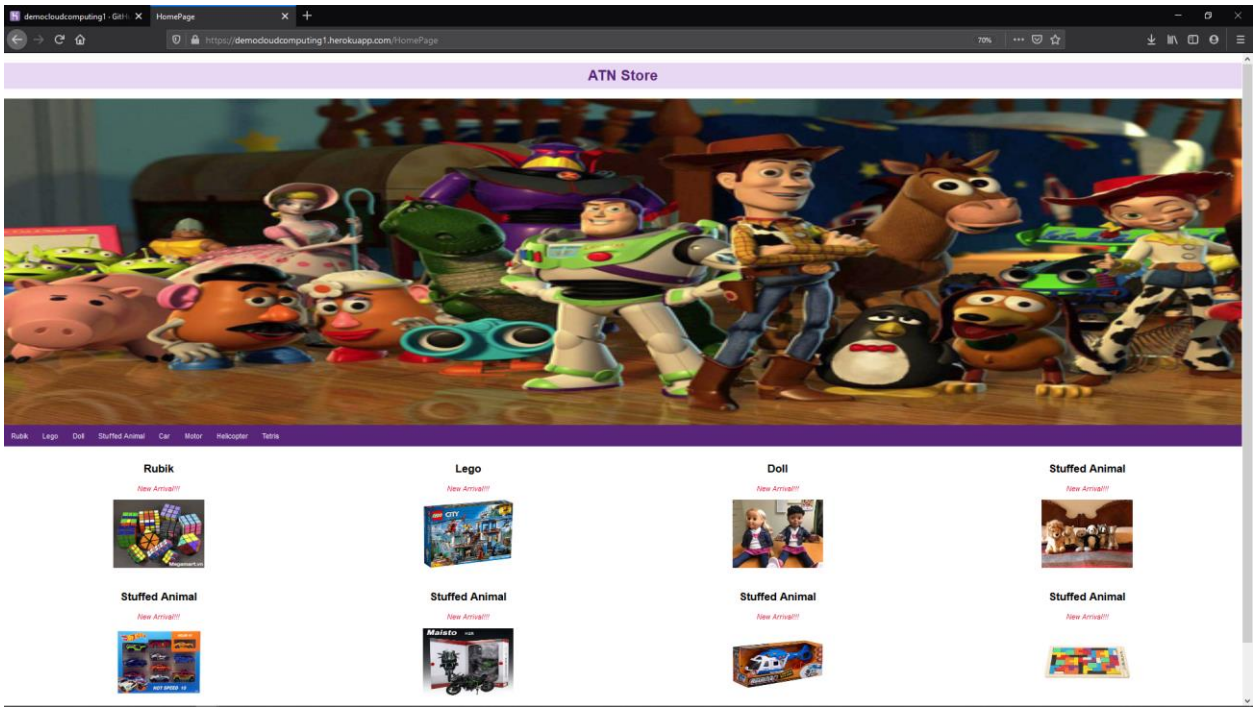

Figure 28

This is homepage interface.

III. COMMON PROBLEMS.

a. Public Cloud.

Low-security level: Because data often share a common location, not as secure as other Cloud models.

Solution: to increase security you can use private cloud

b. Private Cloud.

Higher costs: your business will have to spend a lot on equipment, licenses ... This is like buying your own home and having to buy all the furniture in the house.

Solution: if your finances are limited, you should consider the public cloud or hybrid cloud

c. Community Cloud.

Because community clouds are a cloud deployment model that includes many businesses linked together. So the data that can be accessed between businesses is always a problem with the public cloud, but management, security or cost is a challenge for this model

Solution: In this model companies should have policies and laws in place regarding service use. This will help make data access to each other more secure.

d. Hybrid Cloud.

Difficult to manage: Strategic management and deployment of hybrid cloud require commitment and skills; Companies will need to have a clear path before deploying a hybrid cloud solution. In addition, the Hybrid Cloud requires technical expertise.

Solution :

You can build or hire a team of dedicated cloud deployments.

IV. SECURITY ISSUES.

The fact that you are online is synonymous with threats of being attacked. So in cloud computing when data is done via the internet, security is one of the top concerns. According to (Anthony, Toby & Robert, 2010) ” Security is the number one issue when it comes to cloud computing”.

Since cloud computing also involves using public networks and then sending data to the world, cloud computing is expected to have network attacks of all kinds. And you need to be prepared to solve this problem.

However, denial of service attacks is just one of many cloud security risks. Cloud security risks are divided into five main categories (Physical Security, Organizational, Data Security, Technological, Compliance & Audit) (Figure 1)

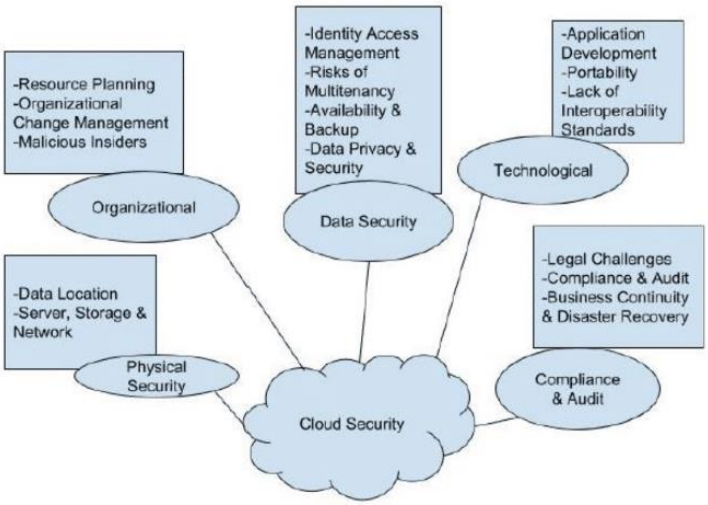

Figure 29 : Cloud Security (Source : Internet)

a. Physical Security.

Physical security is the defense of staff, equipment, software, networks and data from physical actions and events that could cause a business, organization or institution to suffer serious loss or damage

Solution:

The risk of intruders having physical access to devices will be reduced by physical security breaches such as armed protection, biometric scans, etc. Because CSP is responsible for infrastructure physical, they should deploy and operate infrastructure controls. Therefore, the solution to this problem is that we should use the service with a reputable, reliable supplier and have a reasonable backup plan.

b. Organizational.

Organizational risks can come from both sides (CSP and CSC) for example:

If a CSP is acquired or goes bankrupt, the internal operations of the CSP organization may change this, possibly affecting CSC.

Or the risk comes from CSC, for example, there could be the threat of malicious insiders in the organization

Solution:

The solution to this problem is to have contract terms between CSP and CSC. In addition, organizations should have reasonable policies for cloud computing. Finally, we should have a separate amount to maintain cloud computing. The risk of having malicious personnel in a CSPs staff can be mitigated by putting strict legal constraints in contracts when hiring personnel

c. Data Security.

There are several threats to data security that we need to keep in mind. Integrity, data security, and availability are the three main assets we need to protect.

Some risks can come up with your data such as:

Data attacks: This can happen when you lose your device and are hacked or some malicious person can also attack your data remotely.

Data loss: the fact that you can log into the system and accidentally delete the data is the case that very little gas happens but it is not impossible.

Solution :

In order to better protect data, we should have clear and reasonable security policies, decentralizing the system's accounts, authentication in the Cloud. Building staff and security classes for the system. Encrypt data when transferring to the system and have more than one data storage facility.

- **Data encryption**:

In fact, data encryption is a popular and effective method of data protection today. Data encryption is the transfer of data from one type to another that can only be read by the person accessing the decryption key or password. Encrypted data is often called ciphertext, data not encrypted called plaintext.

The data is encrypted with an encryption algorithm and encryption key. After decoding the data can only be viewed in its original form if it is decoded with the correct keys.

The purpose of data encryption is to protect the privacy of digital data when it is stored on computer systems and transmitted over the internet or other computer networks.

Some types of data encryption such as: classical encryption, symmetric encryption, and asymmetric encryption…

Some popular data encryption algorithms such as : Data Encryption Standard - DES, TripleDES, RSA, Advanced Encryption Standard - AES, Twofish…

- **Data Security Properties**:
    - Privacy : privacy guarantees that a CSC does not expose personal information and identification to unauthorized users
    - Confidentiality : This concerns the privacy of data since it is the property which ensures that data from CSC are not disclosed to unauthorized parties
    - Integrity : Data integrity refers to the trust that the data stored in the cloud will in no way be changed by unauthorized parties when it is retrieved
    - Availability: Availability guarantees that the CSC has access to its data and that no access is withheld by any party or by malicious attacks. Attacks like denial-of-service are typically used to deny the availability of data.

DOS and DDOS are one of the common forms of attack today:

- DOS (Denial Of Service) is a form of denial of service attacks. This is a fairly common form of attack today, it makes the target computer can not handle the tasks and lead to overload. These DOS attacks often target virtual servers (VPS) or Web Servers of large companies.

DOS attacks are usually only attacked from a single location that is, it will start at a point and only have an IP range. You can detect and prevent it.

- DDOS (Distributed Denial Of Service) is an attack to exhaust server resources and flood Internet bandwidth, causing access from users to the server to be interrupted. glitches, can't even access the internet, crashes the system. Or even an intranet system

DDOS attack is much stronger than DOS, the strength of this form is that it is dispersed from many different IP ranges, so the attacker will be very difficult to detect to prevent. Because hackers not only use their computers to launch an attack on a website or a network, but they also use millions of other computers to do this.

d. Technological.

Technological risk can be understood as risks related to hardware, technology, and services provided by CSP.

Solution:

Regular maintenance and inspection of infrastructure should be carried out by CSP. In addition, when choosing a service provider, we should also learn and choose a good provider in the market and may request to participate in periodic infrastructure testing if possible. This is the recommended solution in this case

e. Compliance & Audit.

This risk mainly refers to legal issues. Therefore CSP and CSC need to understand the rules and ensure all activities meet these requirements. In addition, CSP also needs to ensure the security and privacy of data.

Solution:

To avoid these risks for both parties (CSP and CSC), there is a need for clear laws and policies tailored to different locations (for example, U.S. and Vietnamese laws are different.) affects the scope and mode of operation of both parties). This makes it easy for both parties to follow the rules and requirements to minimize this risk.

V. SUMMARY.

The report shows how to manage code, configure and deploy the web application. In addition, the report also highlighted some common issues and security issues of the platform and cloud computing solutions for each case.

Bibliography

Anthony T. Velte, Toby J. Velte, Ph.D. Robert Elsenpeter. (2010) Cloud Computing: A Practical Approach. US, The McGraw-Hill Companies Publishing.