Sri Lanka Institute of Information Technology

Final Project Report

ISP Project Report

Information Security Project 2021

Project ID: ISP-21-REG-02

Submitted by:

IT Number	Name
IT19056012	Meeriyagalla P.Y.
IT19147192	K.A.P.P. Wickramarathne

Date of submission: 14/11/2021

Abstract

Transportation systems are critical infrastructures in every country. IoT and cloud computing systems are rapidly growing in today's world and those systems are also used to provide some services on transportation sector. The main purpose to create this CTF box is to elevate the need of having a good security system in cloud base transportation systems. This CTF box completely developed on AWS (Amazon Web Service) cloud platform. By playing this CTF box the professionals in the industry and the developers who develop cloud base web systems, can gain knowledge about security vulnerabilities and misconfigurations of website development and cloud platform configurations.

Acknowledgement

We would like to express our gratitude for the Sri Lanka Institute of Information Technology for giving this opportunity to get professional experiences about a development and implementing project of a CTF (Capture the Flag) Box. We would like to convey our profound thanks to Information Security Project (ISP) lecture in charge Dr.Lakmal Rupasinghe , and the subject instructor Miss. Menaka Moonamaldeniya, Miss. Chathuri Udagedara for their excitement, patience, insightful remarks, valuable information, practical guidance, and never-ending ideas, all of which have greatly aided us during our CTF creating project.

We are grateful for every individual and organization who helped us throughout the creation of the CTF box by providing cloud services (AWS), domain services (Domain.com), and tutorials (Mr. Neal Davis - YouTube).

Declaration

We declare that this project report or part of it was not a copy of a document done by any organization, university any other institute or a previous student project group at SLIIT and was not copied from the Internet or other sources.

Project Details

Project Title	Trip-To-Hell CTF Box
Project ID	ISP-21-REG-02

Group Members

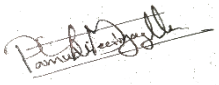
Reg. No	Name	Signature
IT19056012	Meeriyagalla P.Y.	
IT19147192	K.A.P.P. Wickramarathne	

Table of Contents

List of Figures

List of Tables

List of Acronyms and Abbreviations

IoT: Internet of Things

AWS: Amazon Web Service (Cloud Service Providing Platform)

CTF: Capture the Flag (Game that can play to improve cyber security skills)

RDS: Relational Database Service

VPC: Virtual Private Cloud

1. Introduction

1.1 Problem Statement

In most of industries cloud computing is more popular today. Transportation system is a critical infrastructure in every country. Most of the countries in the world use IoT technologies and web base systems with cloud computing in nowadays to improve the comfort and with the purpose of time saving. When a transportation system improvises with IoT, cloud base systems, and web technologies it can lead to critical cyber security threats. Even a smaller threat can be cause serious consequences in transportation sector. The main intention of creating this CTF box is to give a hand on experience of the security threats that can occur with above mentioned technologies.

To develop this Trip-To-Hell CTF box mainly used platform is AWS. For this CTF project a whole fully functioning website (www.travelmatetth.com) was developed using WordPress. The main reason to use WordPress for the development of the website is because, it is commonly used by professional developers to create and design websites. To get the real-life experiences about these services all the tools and services that used to build this project are up to date. There can be critical information security threats even the systems are up to date. That is the main reason to use latest versions of services and systems. To improve the realism, a domain name was purchased from Domain.com.

There is main 09 levels in this Trip-To-Hell CTF box. Each level has sublevels. This CTF box is fully built in AWS cloud platform. Because of that there is no image file that need to be installed by the players when playing this CTF. Players can easily open the website (www.travelmatetth.com) and play the CTF by joining with www.tryhackme.com (CTF url: tryhackme.com/jr/triptohellctf).

1.2 Product Scope

In Trip-to-Hell CTF box, the players can gather knowledge about new systems which contains vulnerabilities on transportation schedule and reservation management system. There will be

cloud base servers, web-based systems, and vulnerabilities that players can exploit and gather information which is related to railway scheduling and reservation system. By this project, people who are related to railway management systems and information security professionals will be able to identify real-life types of attacks with the knowledge that gain through the CTF box.

1.3 Project Report Structure

The implementation of the CTF box back-end and the website creating details will be explain in the methodology sector separately. Details about the levels, achievements and future development areas explained in the evaluation sector.

2. Methodology

2.1 Requirements and Analysis

The vulnerable website contains railway management details including railway path details, train scheduling details and it only shows the details about train seats reservations. The player can investigate the railway scheduling details and seat reservation details. Players need to find vulnerable loopholes to break into the website, scheduling system and to connect to the hidden servers.

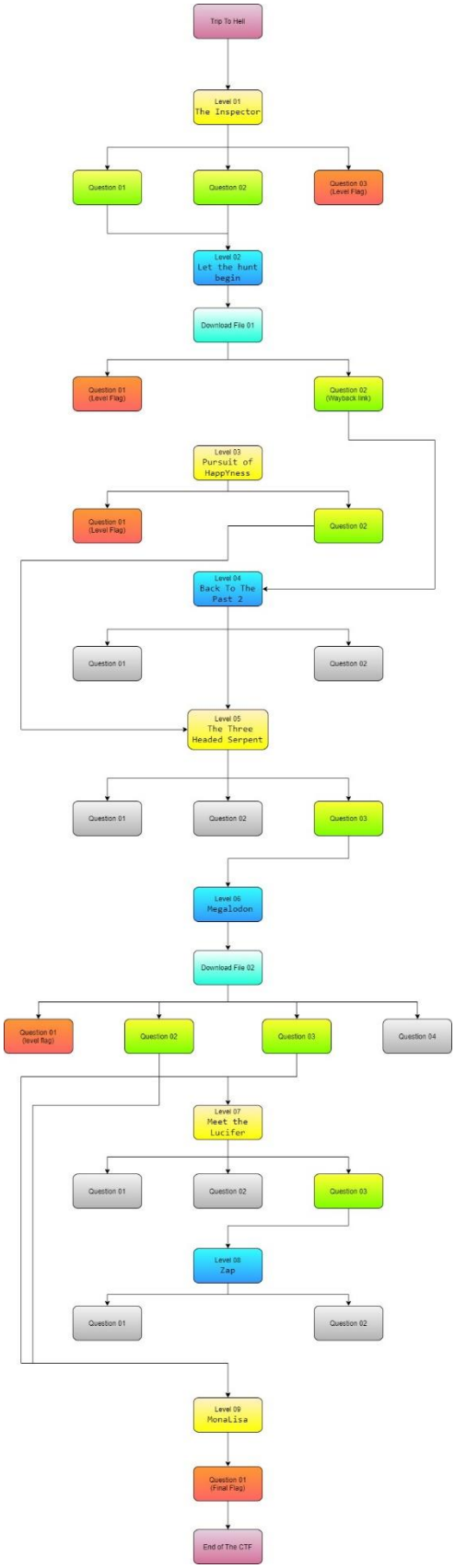
As the CTF player he or she will not need to download an image file and host it locally. The complete CTF is developed on AWS cloud. This CTF can play with both Linux and Windows operating systems (Linux OS is highly recommended). To play this CTF box player need to have security tools. According to the tasks that must play in this CTF the recommended tools:

- Wireshark
- Nmap
- OWASP ZAP
- Deepsound
- CryptTool
- STool
- Web Browser
- Winrar
- PuTTY (for Windows users)
- Nikto or any scanner
- Hydra

Player also need to register to the Try Hack Me website.

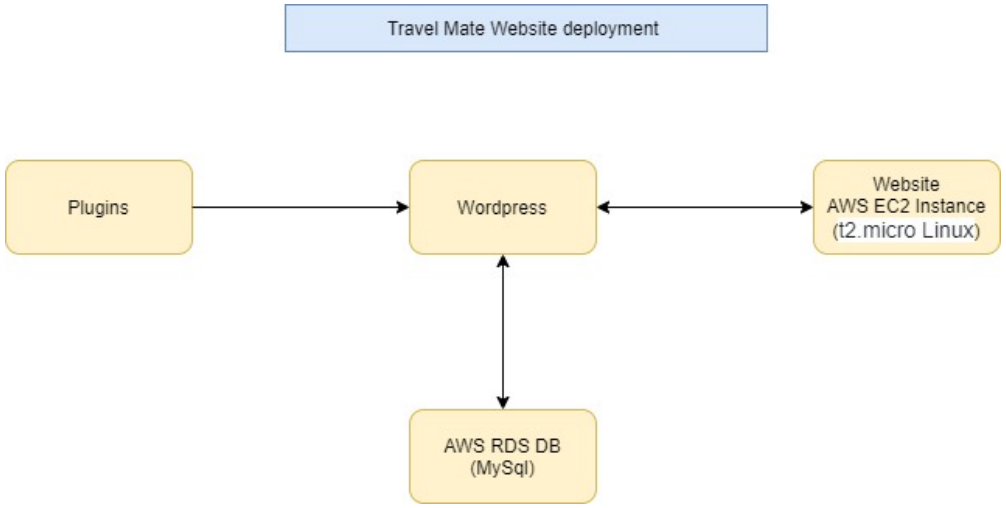
2.2 Design

The workflow of the CTF box is as below.


Trip To Hell
Level 01
The Inspector
Question 01
Question 02
Question 03
(Level Flag)
Level 02
Let the hunt
begin
Download File 01
Question 01
(Level Flag)
Question 02
(Wayback link)
Level 03
Pursuit of
HappYness
Question 01
(Level Flag)
Question 02
Level 04
Back To The
Past 2
Question 01
Question 02
Level 05
The Three
Headed Serpent
Question 01
Question 02
Question 03
Level 06
Megalodon
Download File 02
Question 01
(level flag)
Question 02
Question 03
Question 04
Level 07
Meet the
Lucifer
Question 01
Question 02
Question 03
Level 08
Zap
Question 01
Question 02
Level 09
MonaLisa
Question 01
(Final Flag)
End of The CTF

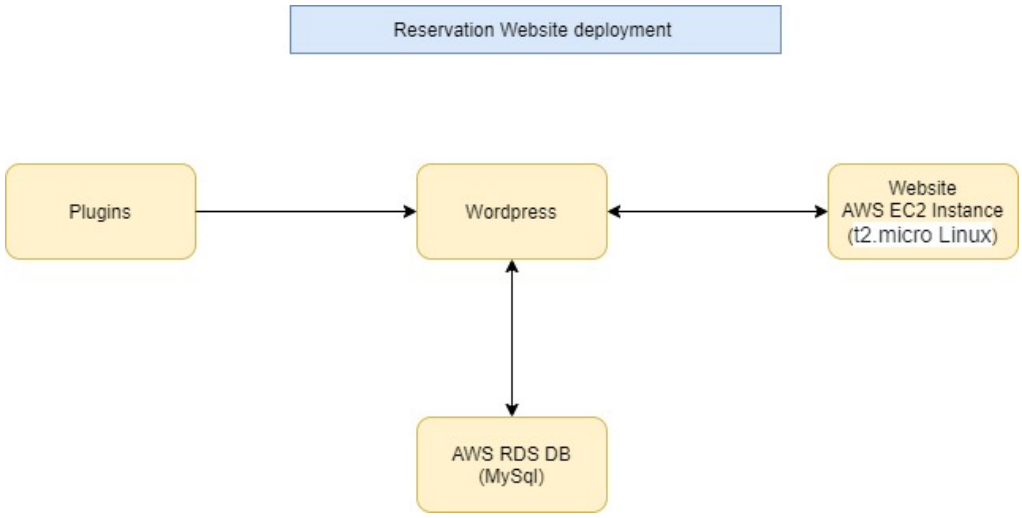
[Figure 01-CTF flow chart]

The basic deployment chart of the Travel Mate (www.travelmatetth.com) website.



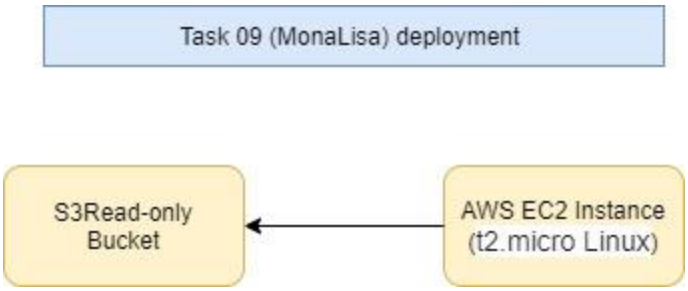
[Figure 02-TravelMate Deployment]

Reservation page deployment.



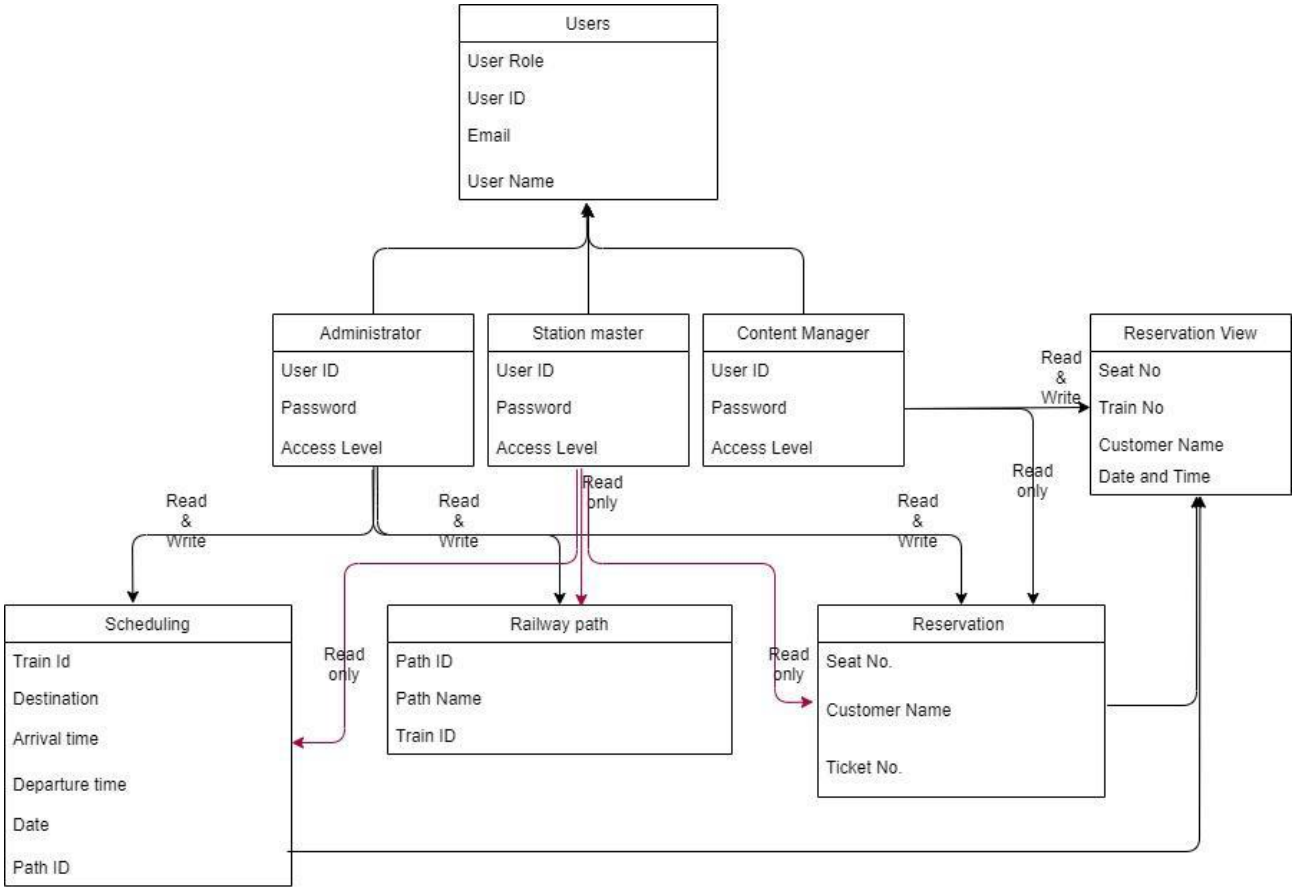
[Figure 03-Reservation Deployment]

Task 09 deployment.



[Figure 04-Task 09 Deployment]

The ER-Diagram for the database.

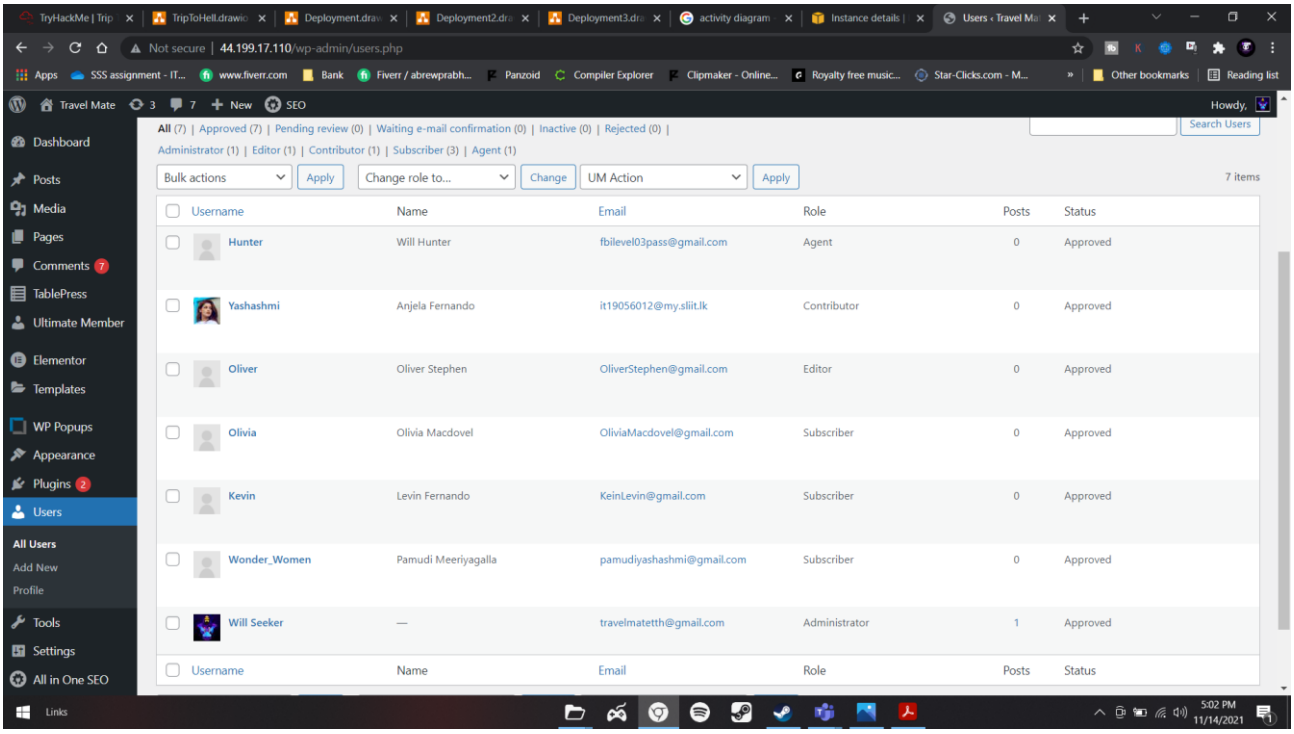


[Figure 05-ER Diagram]

Administrator: Administrator

Station master: Contributor

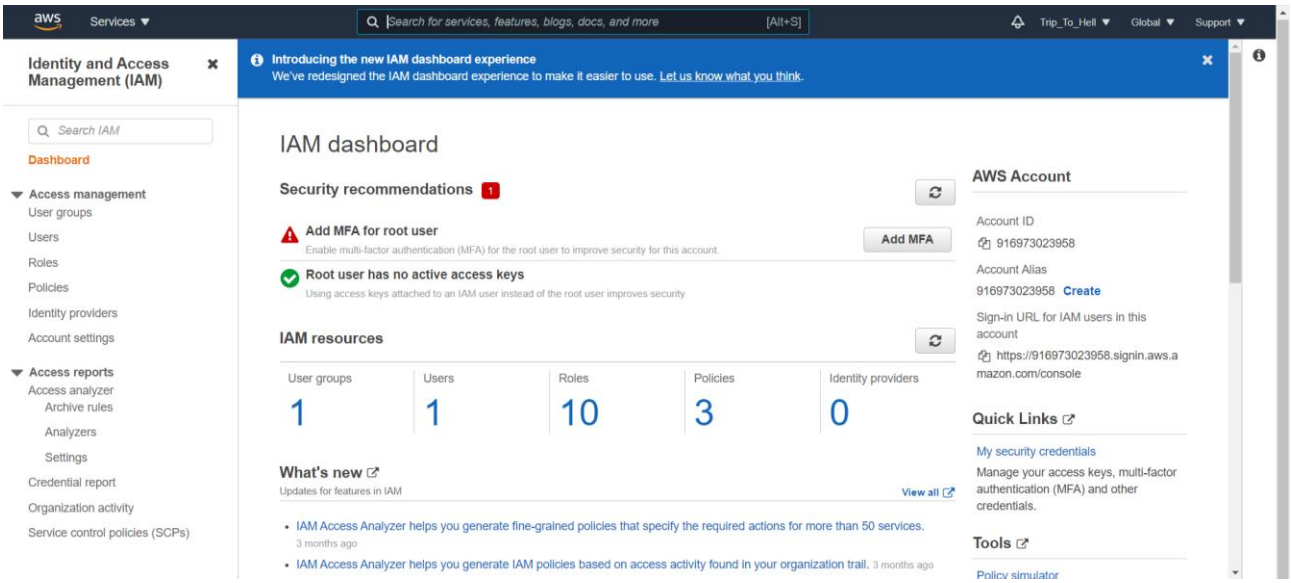
Content Manager: Editor



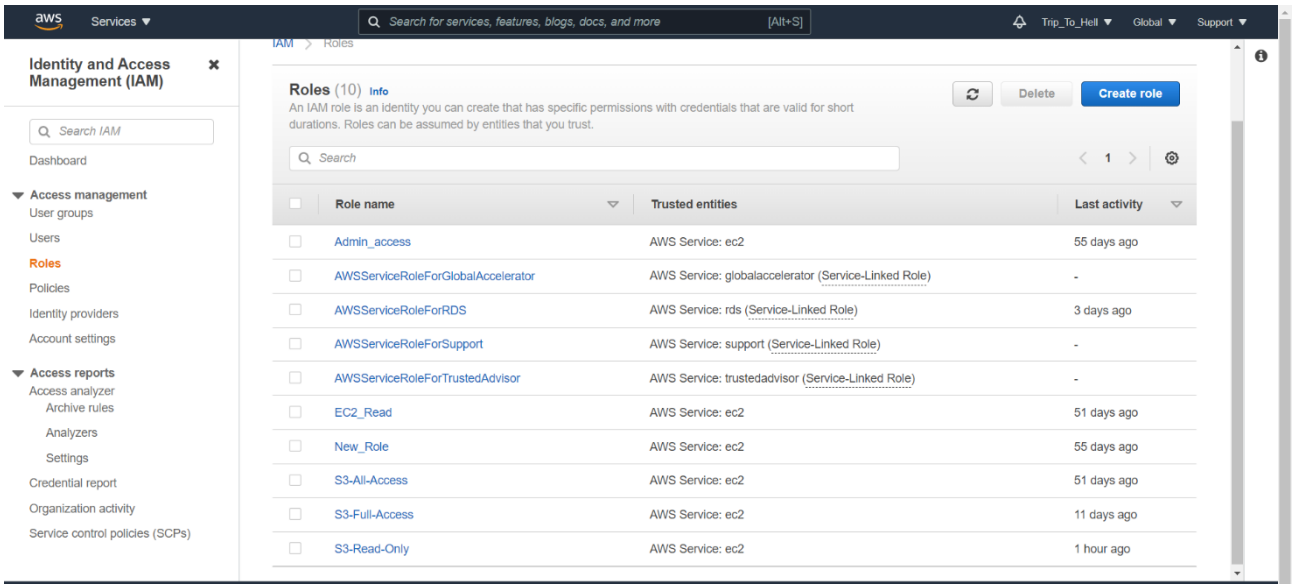
[Figure 06-WordPress Backend]

2.3 Implementation

The whole project was developed on the AWS cloud platform because when creating the project, the mainly focused areas were cloud computing and web security. As the starting point of the project, created an AWS account. After that created a user role as I am user.

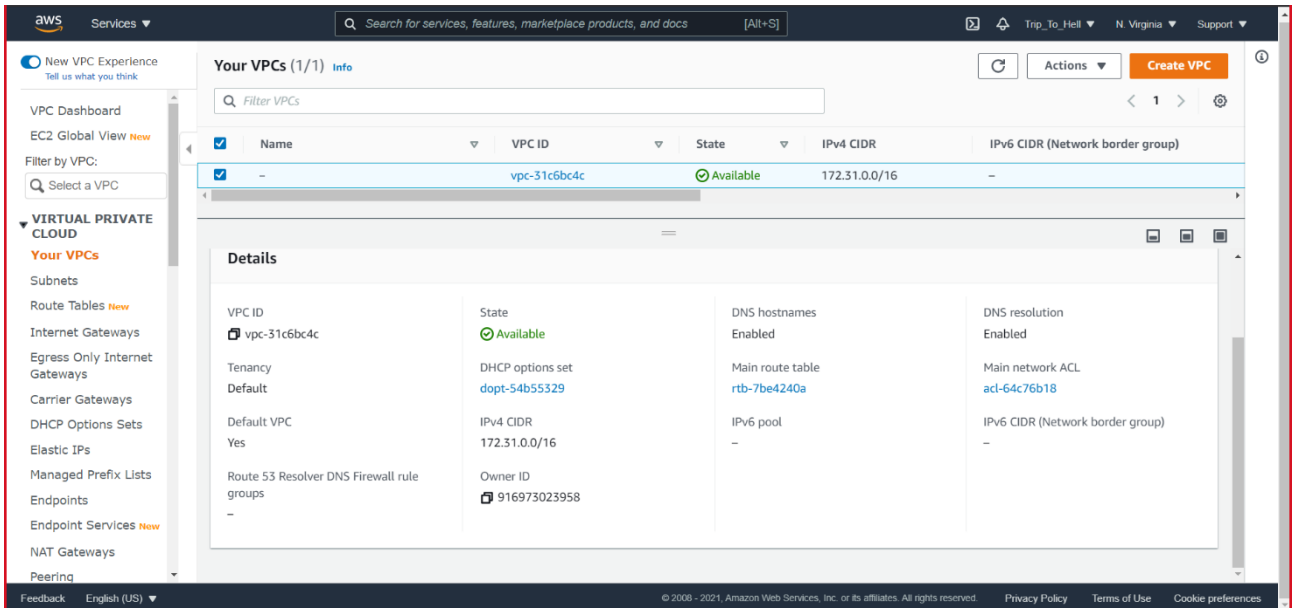


[Figure 07-I Am User Dashboard]

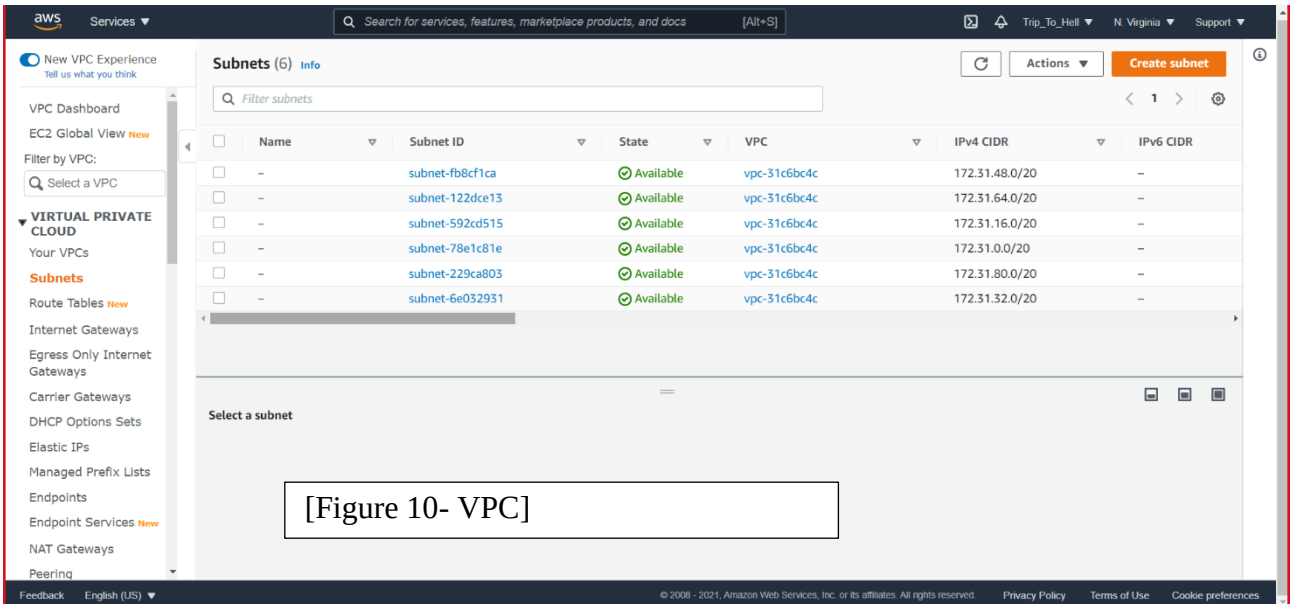


[Figure 08-I Am user]

Then created a VPC (Virtual Private Cloud) on AWS platform.

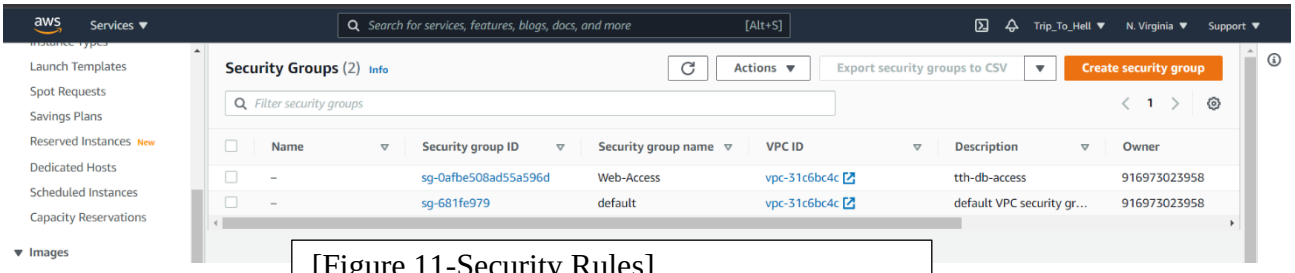


[Figure 09-VPC]

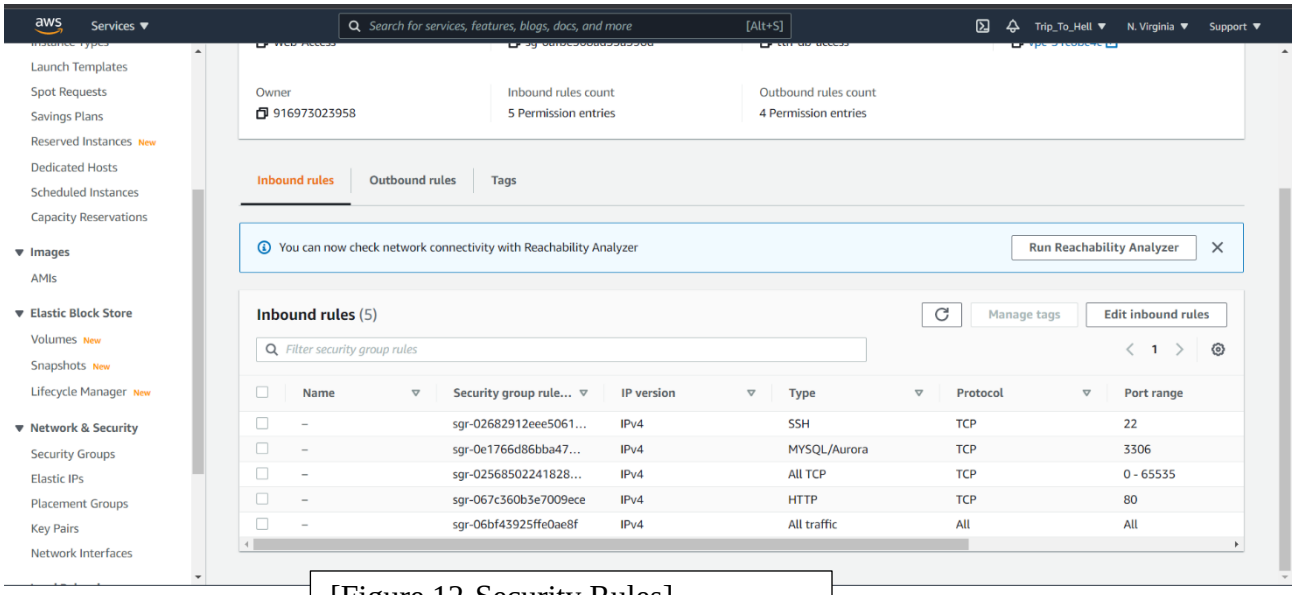


[Figure 10- VPC]

Then created security rules (Rule name: web-access) for the VPC using security group.

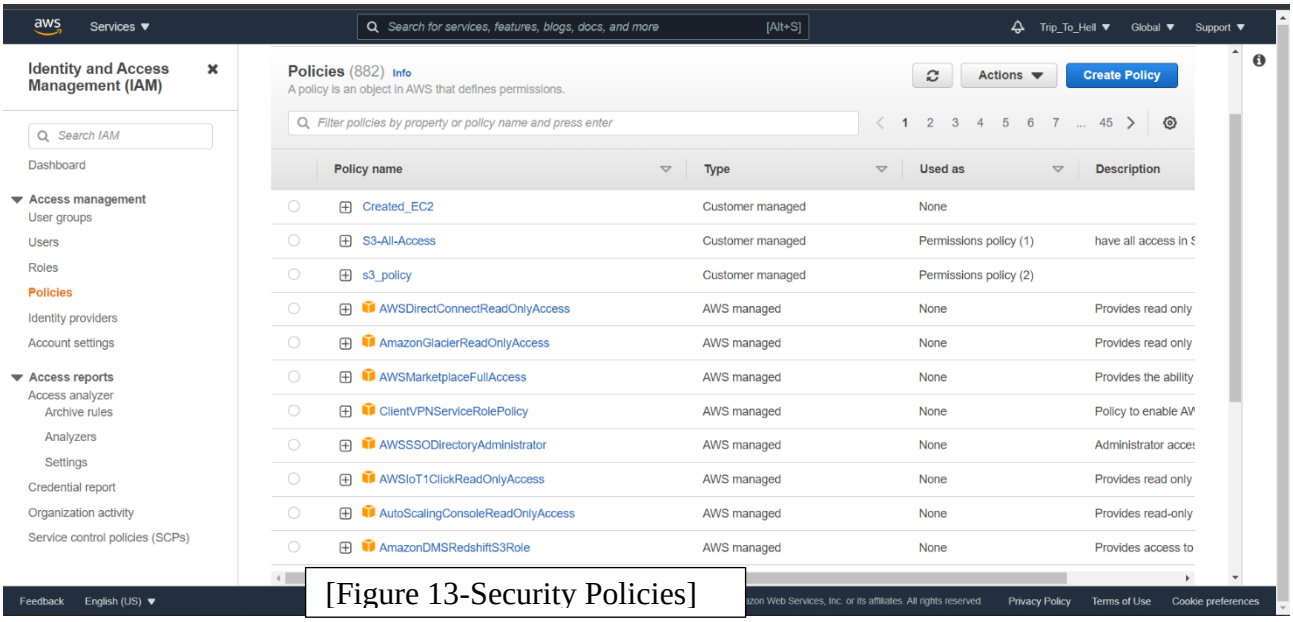


[Figure 11-Security Rules]



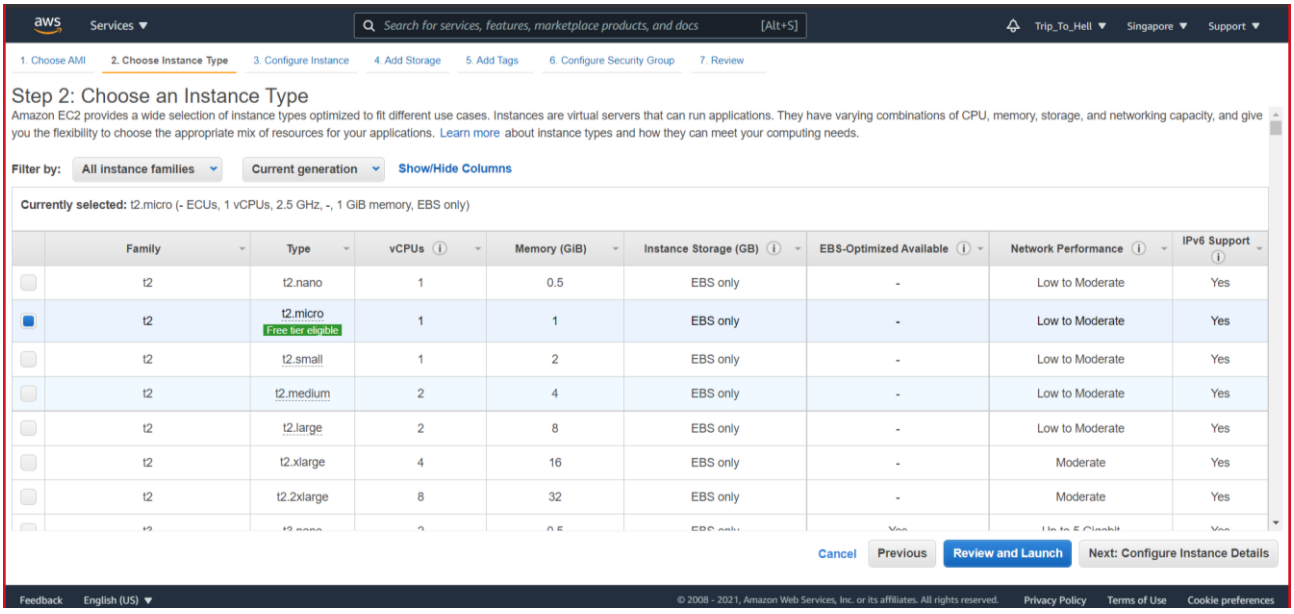
[Figure 12-Security Rules]

To add more security for the VPC created security policies.

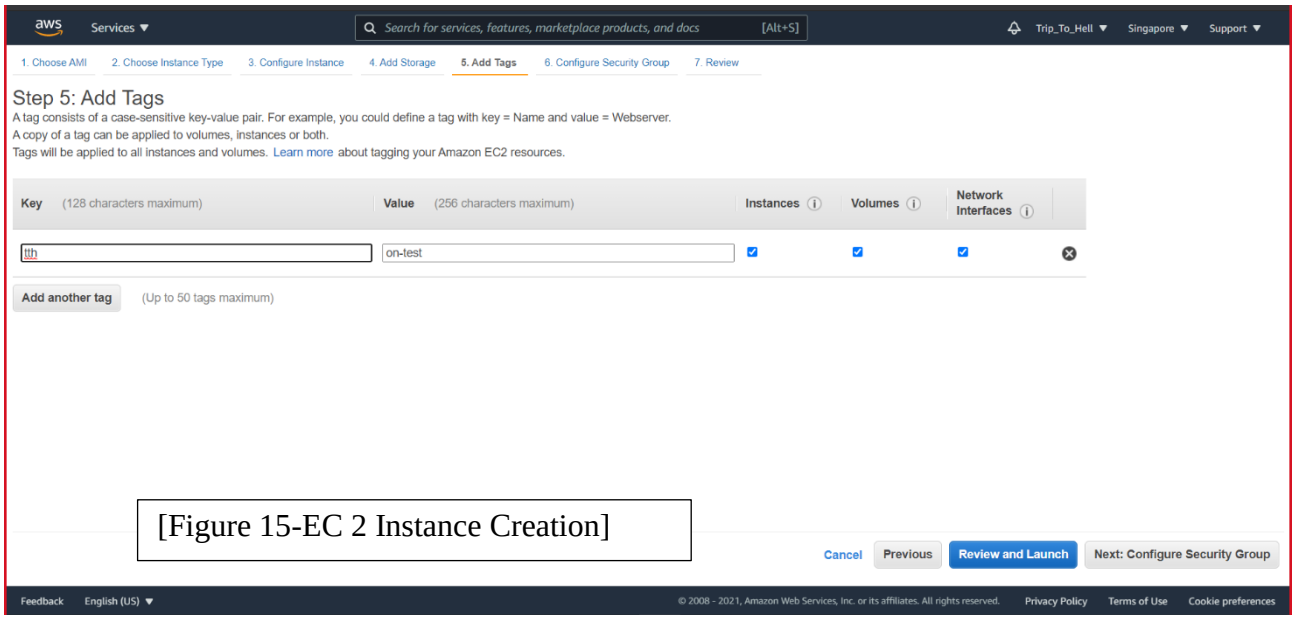


[Figure 13-Security Policies]

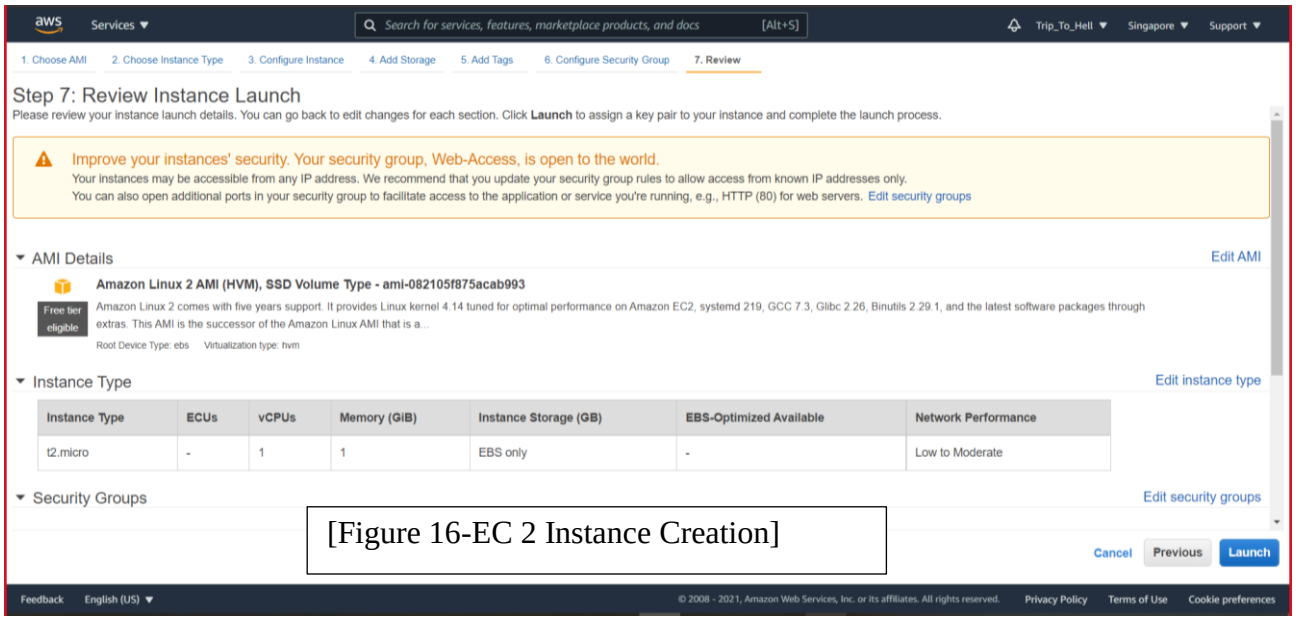
To create the main website (www.travelmatetth.com) and the reservation website created a t2.micro EC2 Linux instance on AWS. To make the IP address a static one, added an elastic IP to the EC2 instance.



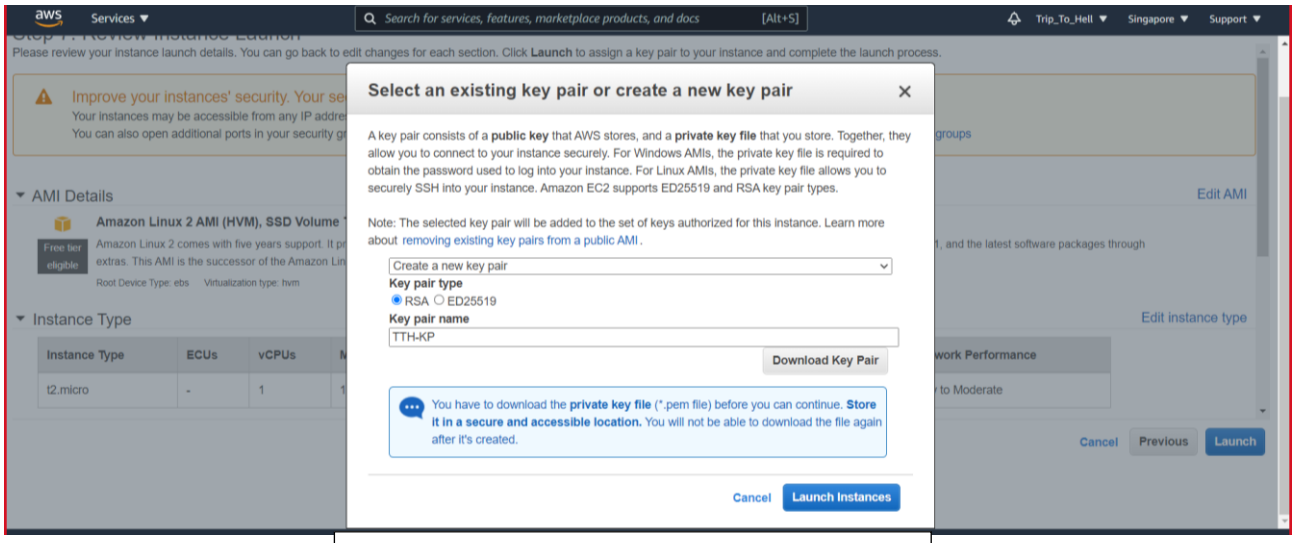
[Figure 14-EC 2 Instance Creation]



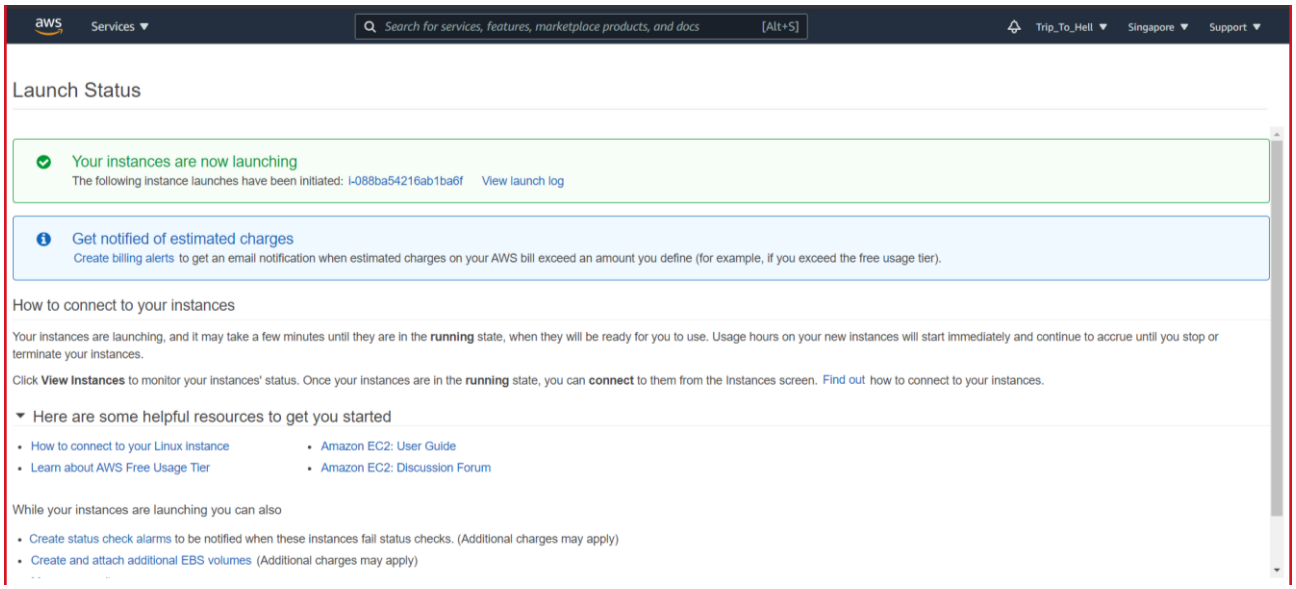
[Figure 15-EC 2 Instance Creation]



[Figure 16-EC 2 Instance Creation]

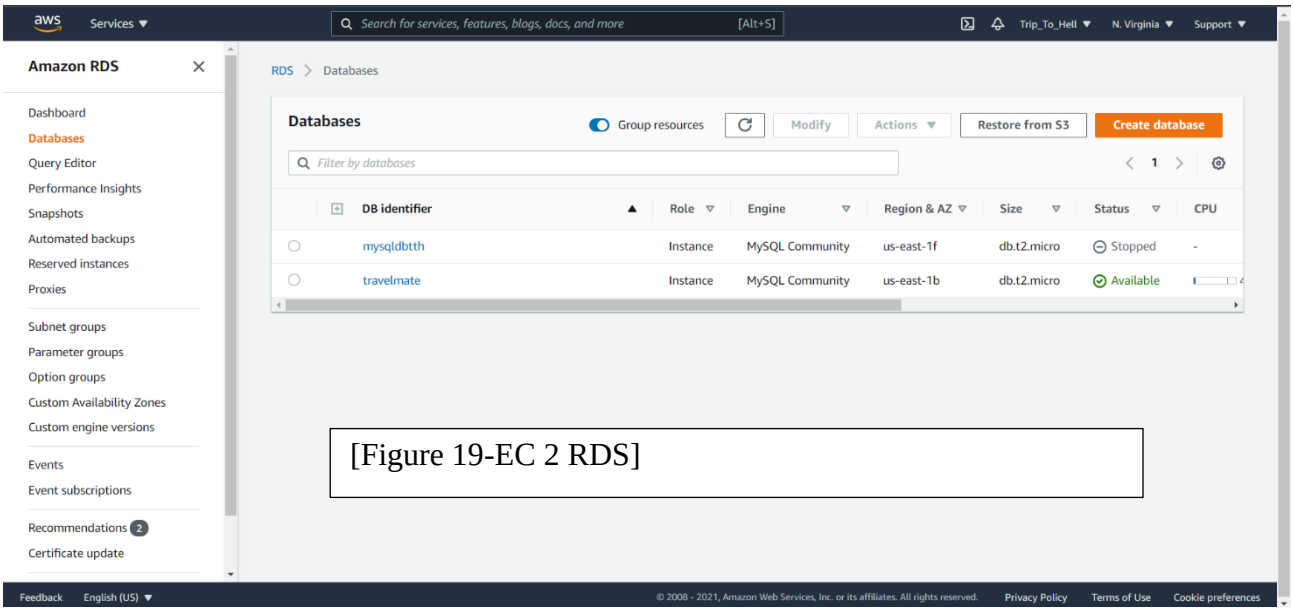


[Figure 17-EC 2 Instance Creation]



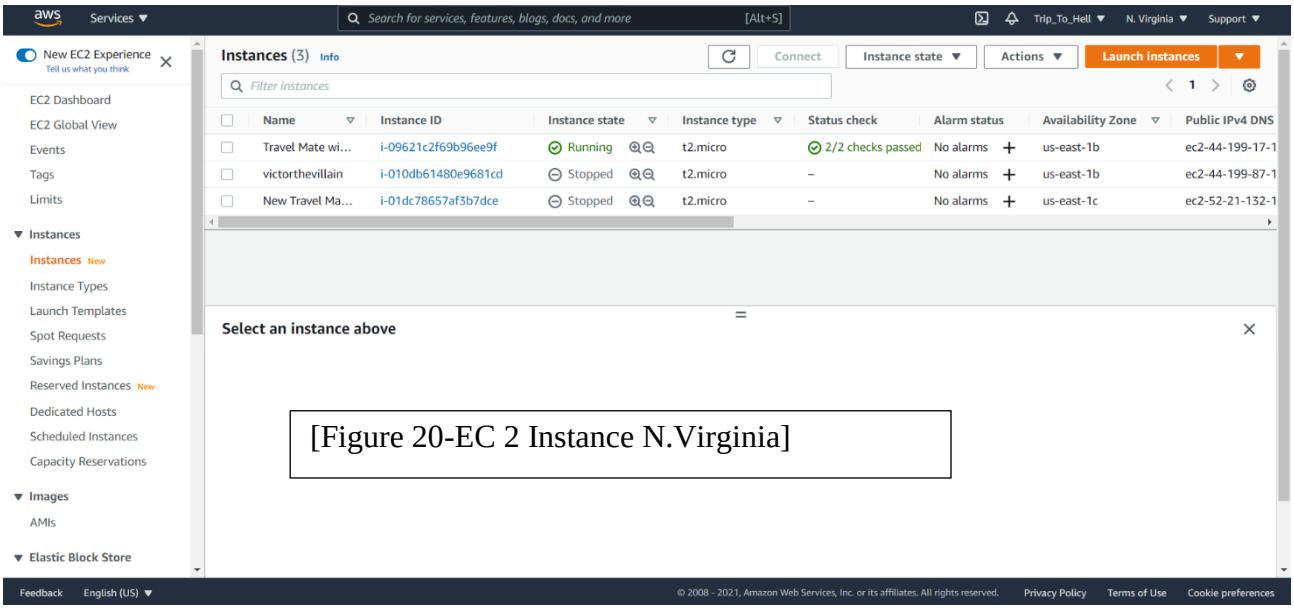
[Figure 18-EC 2 Instance Creation]

For the database system created a RDS (Relational Database Service) MySQL database on AWS.

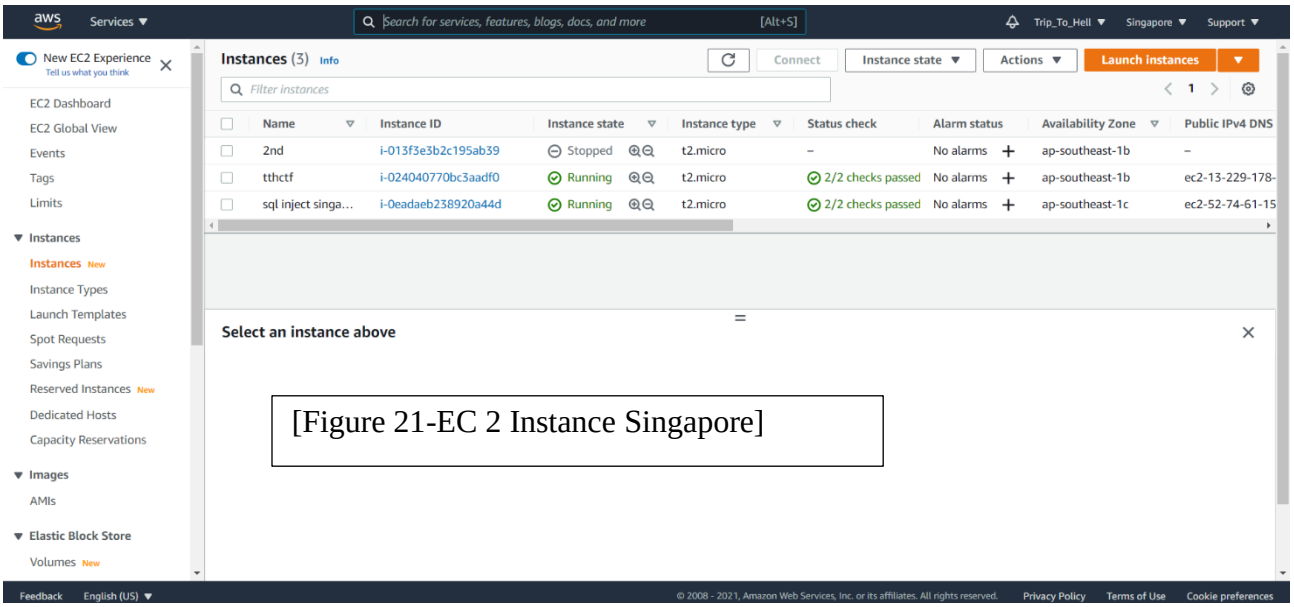


[Figure 19-EC 2 RDS]

Selected region for the Travel Mate website implementation is North Virginia. For the reservation website page selected Singapore region.

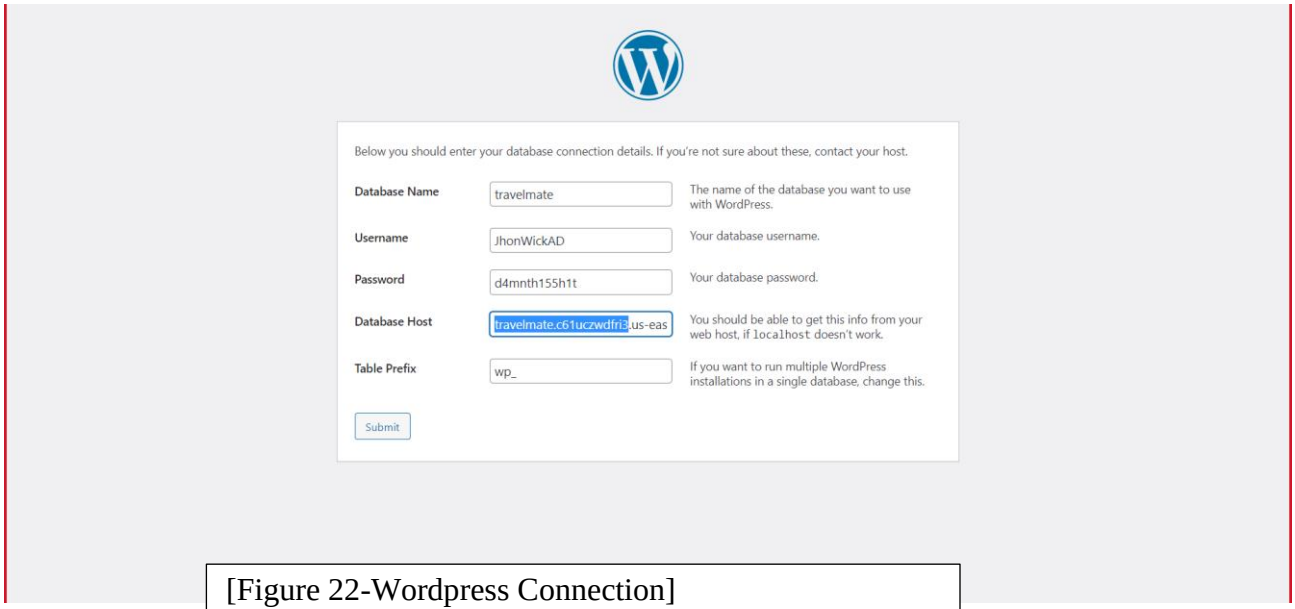


[Figure 20-EC 2 Instance N.Virginia]

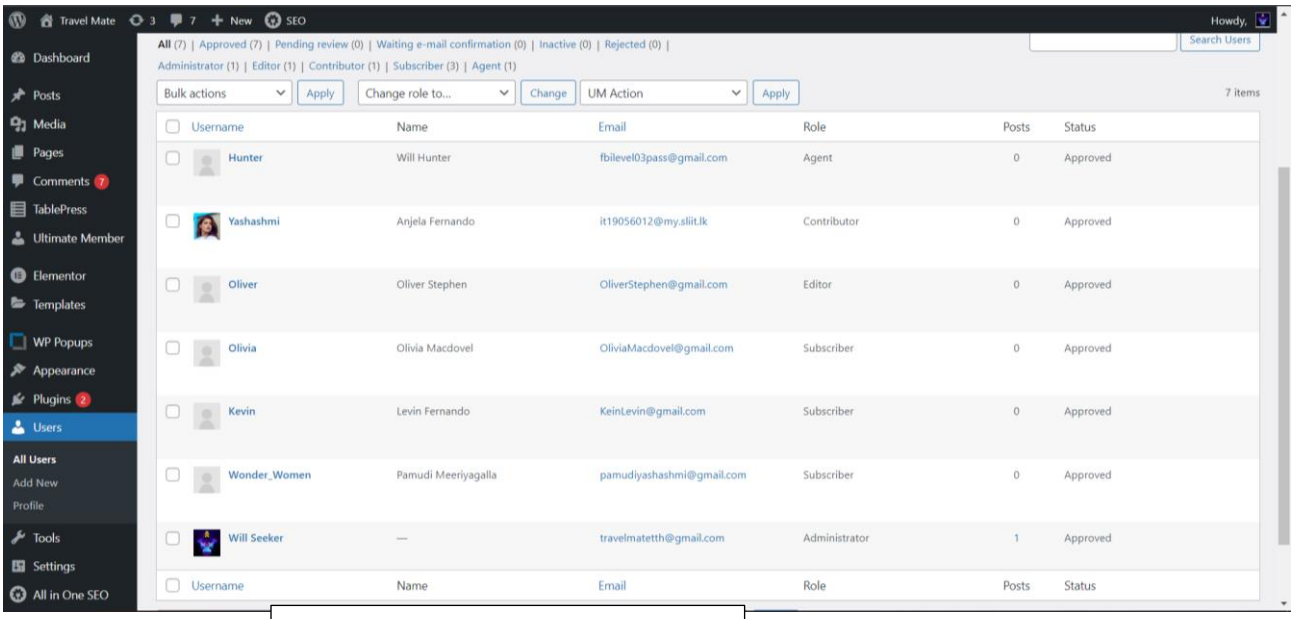


[Figure 21-EC 2 Instance Singapore]

To connect the database and the instance used WordPress.



[Figure 22-Wordpress Connection]



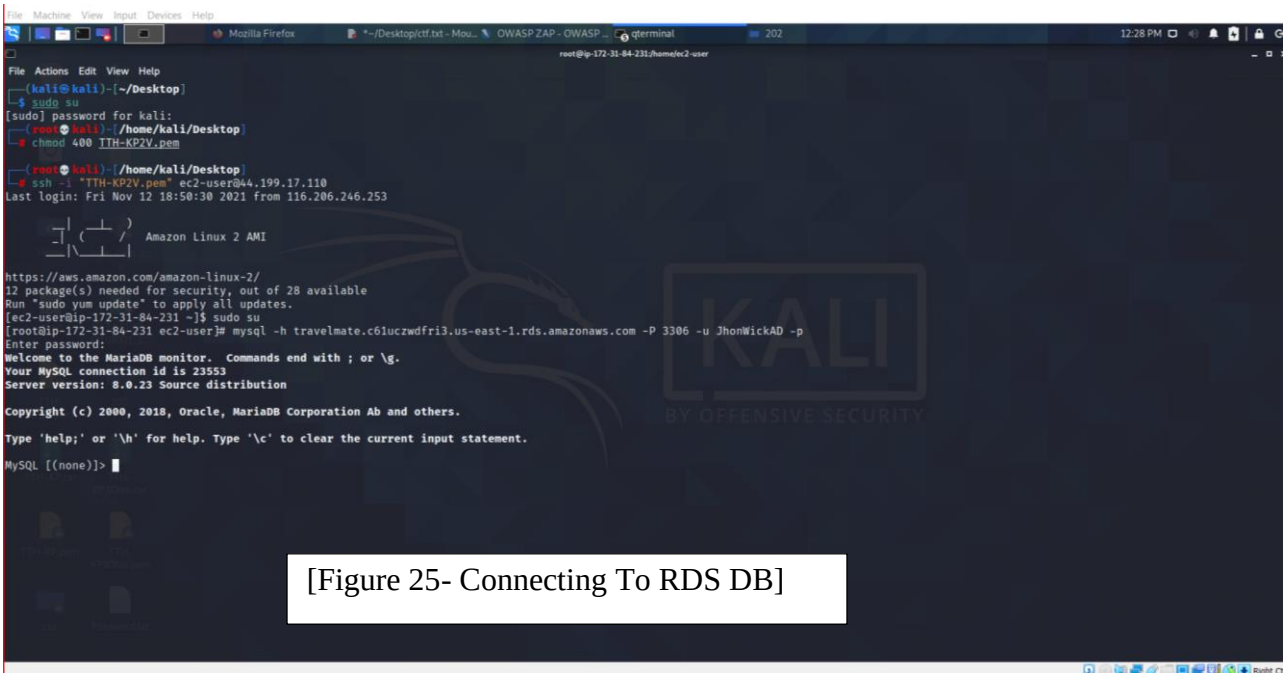
[Figure 23- Wordpress Backend]

When connecting the databases there were configuration commands that needed to run on the Linux instance.

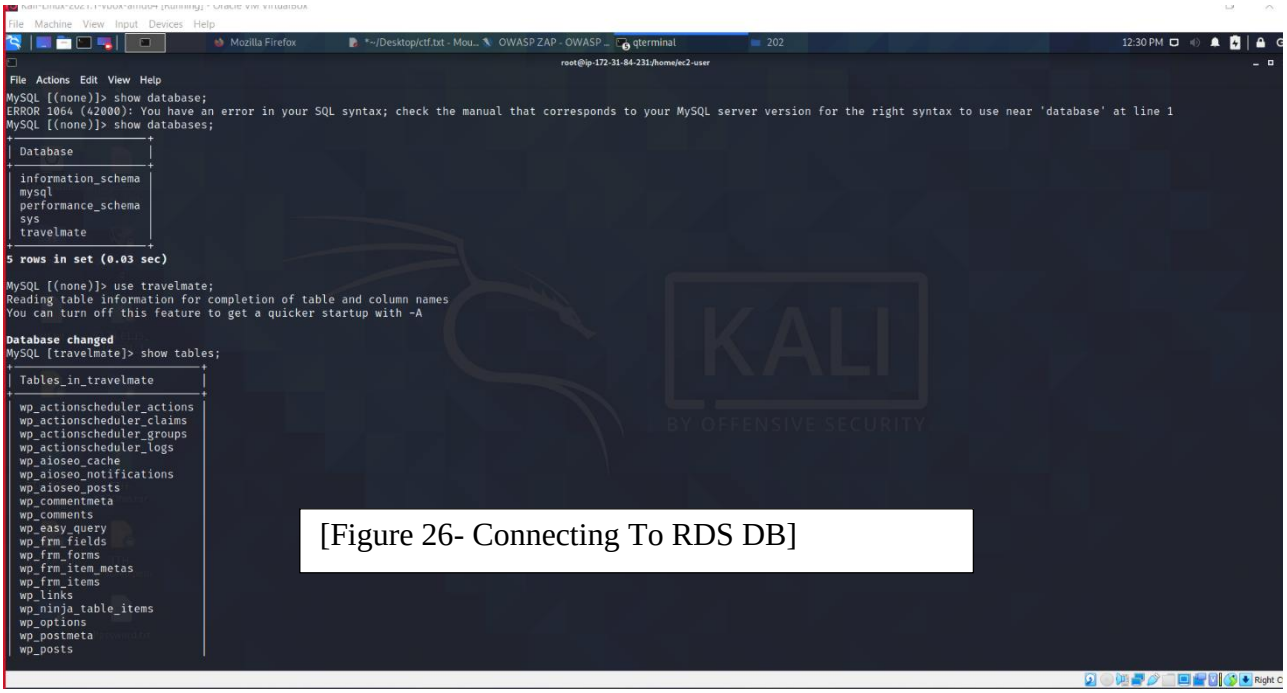
```
# Install WordPress on EC2 using RDS MySQL DB
# Either add "sudo" before all commands or use "sudo su" first
yum update -y
amazon-linux-extras install -y php7.2
yum install -y httpd
systemctl start httpd
systemctl enable httpd
cd /var/www/html
wget https://wordpress.org/latest.tar.gz
tar -xzf latest.tar.gz
cp -r wordpress/* ./
chmod -R 755 wp-content
```

To do that, connected to the Linux instance using security key pair with Kali Linux terminal. Connect to the database using linux:

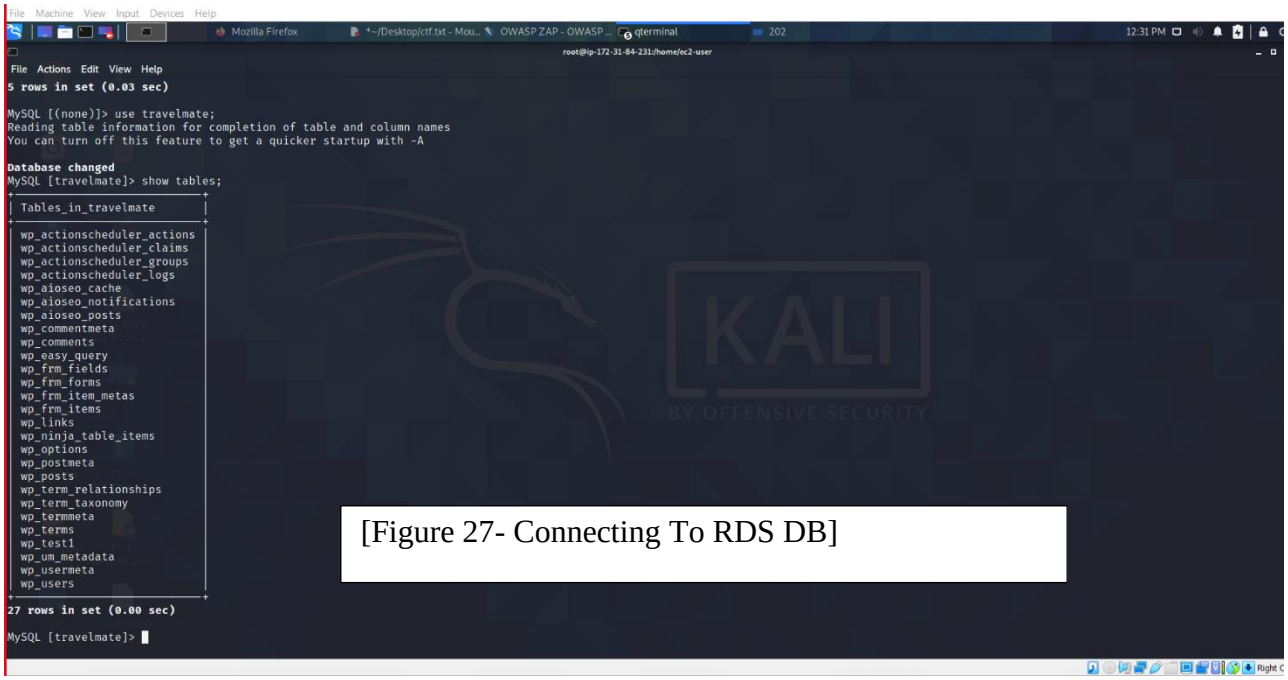
[Figure 24-Wordpress Install Code]



[Figure 25- Connecting To RDS DB]

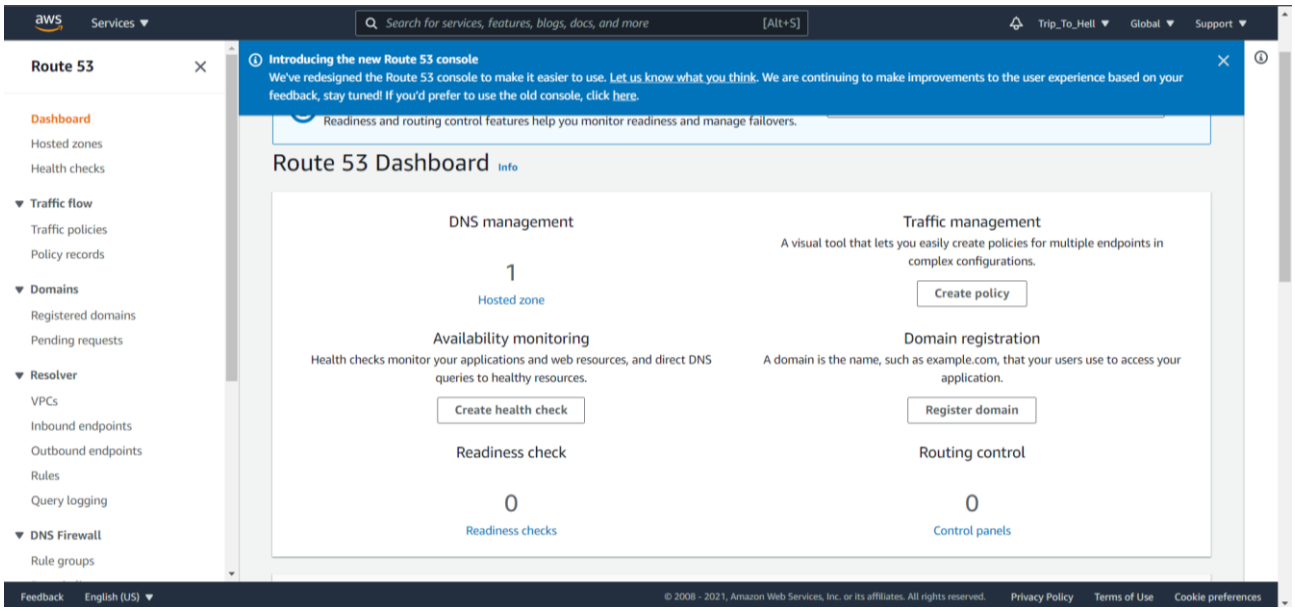


[Figure 26- Connecting To RDS DB]

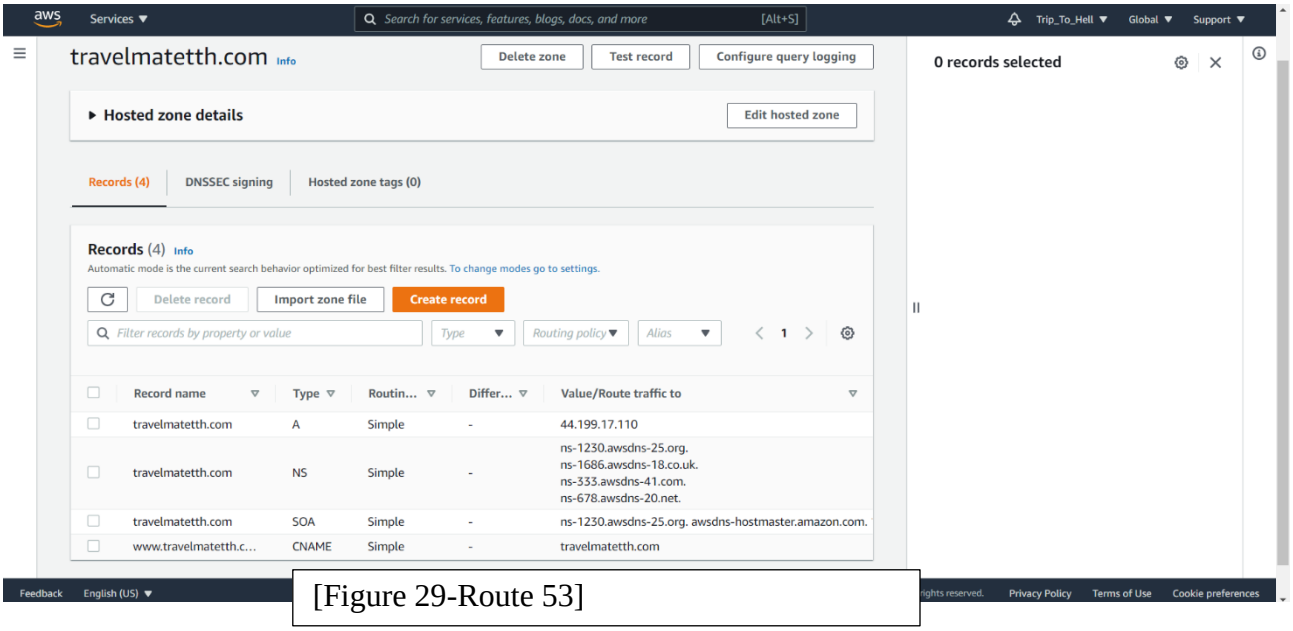


[Figure 27- Connecting To RDS DB]

To make the CTF project more realistic, purchased a domain from Domain.com and added it using route 53 feature.

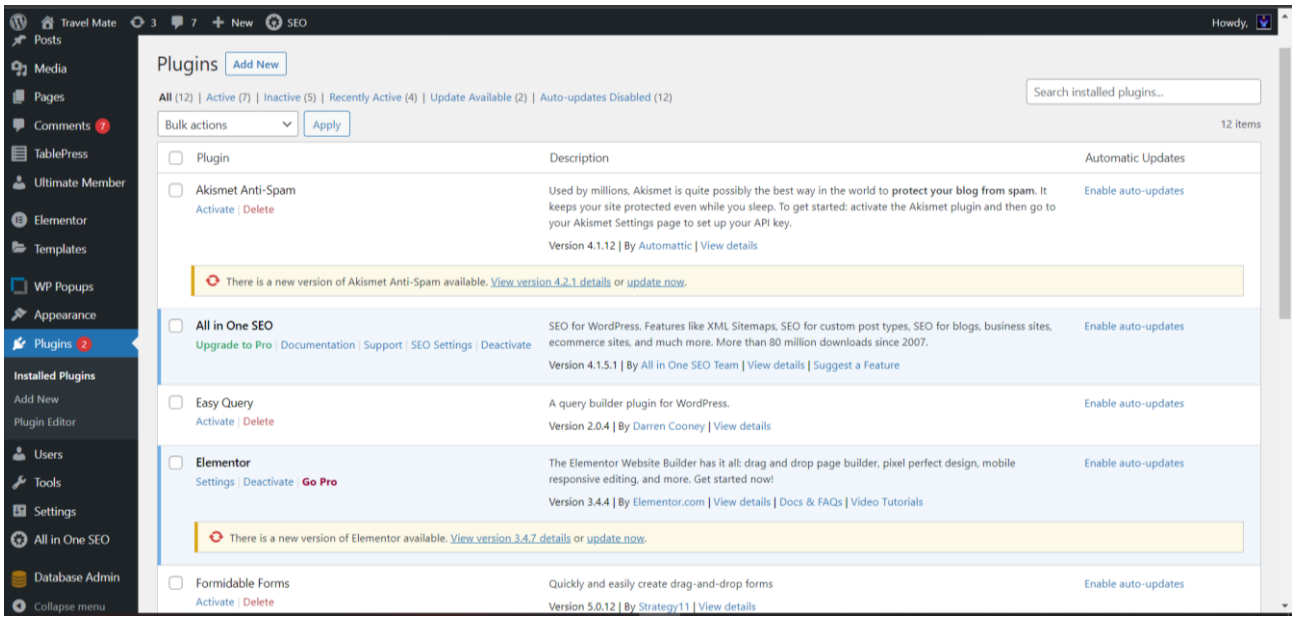


[Figure 28-Route 53]

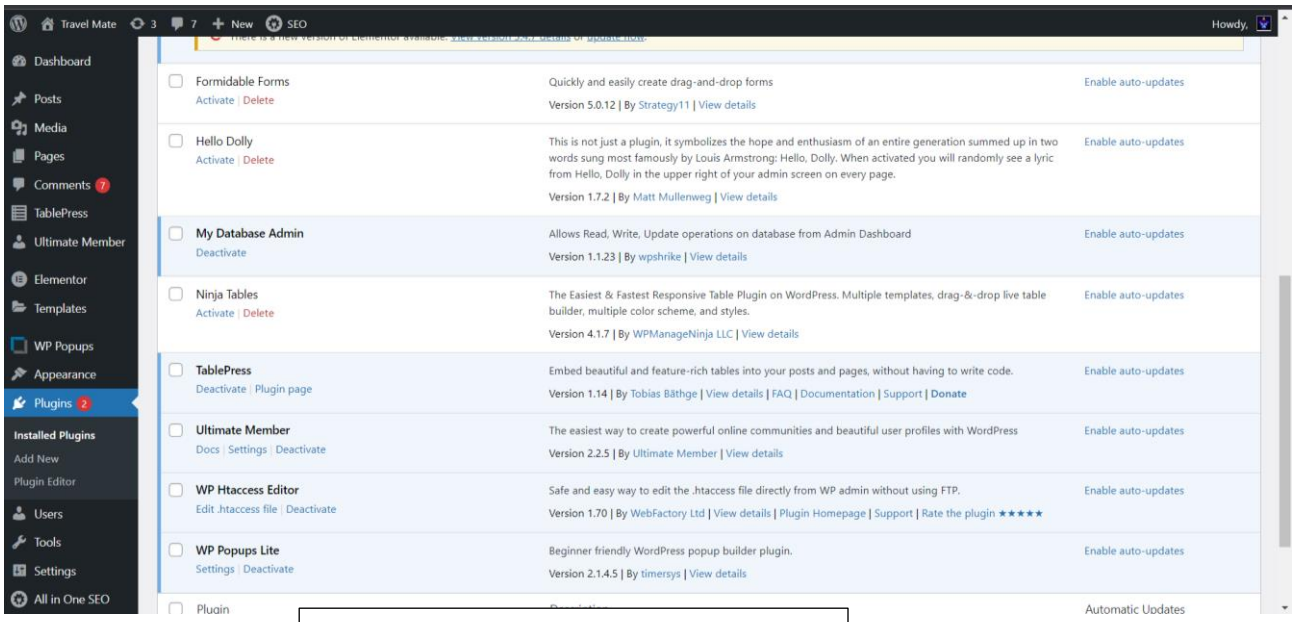


[Figure 29-Route 53]

For develop and design purposes of the Travel Mate website used WordPress and plugins. Not only for the Travel Mate website but also for the reservation web page used WordPress and plugins for development purposes.

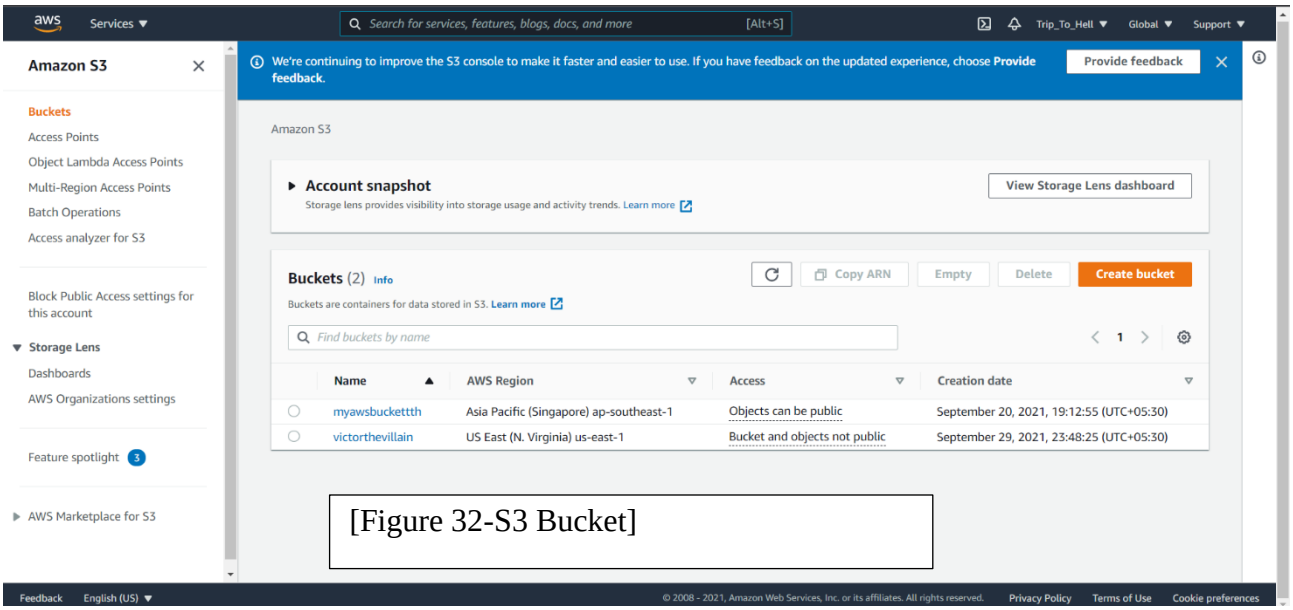


[Figure 30-Route Plugins]



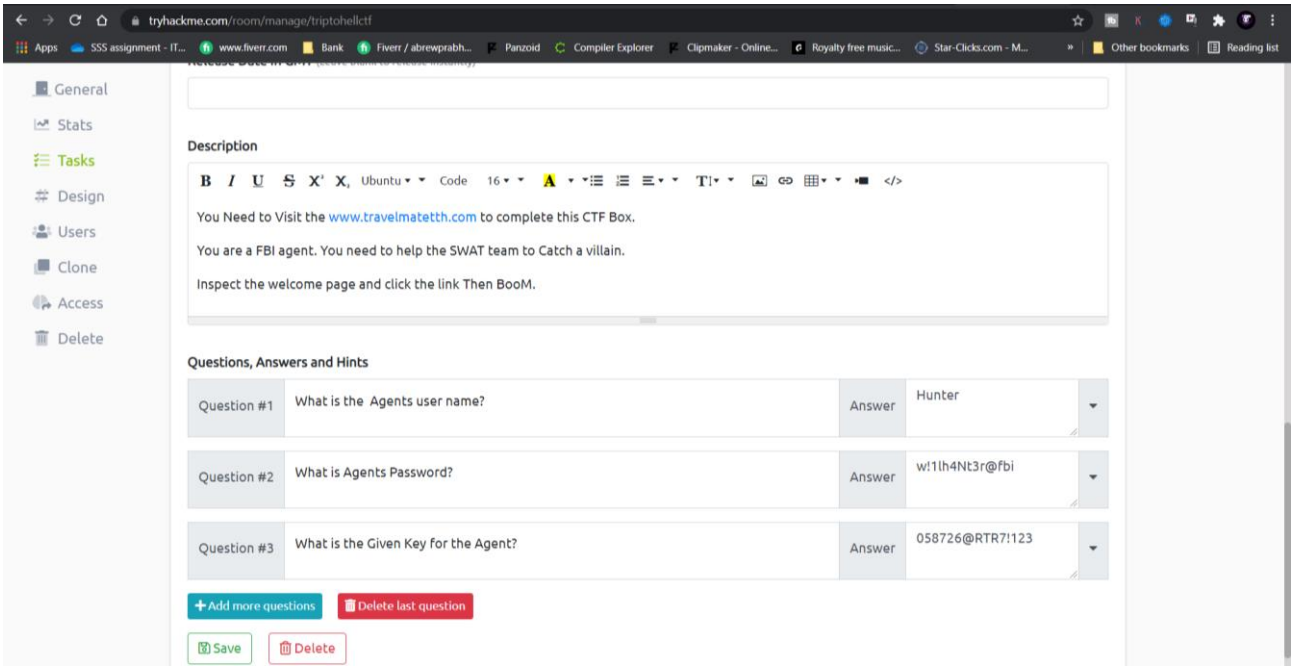
[Figure 31-Route Plugins]

In the Trip-To-Hell CTF box, to implement the task number 09, created a S3 bucket with read only permissions. S3 bucket is not in a region it is available for globally.

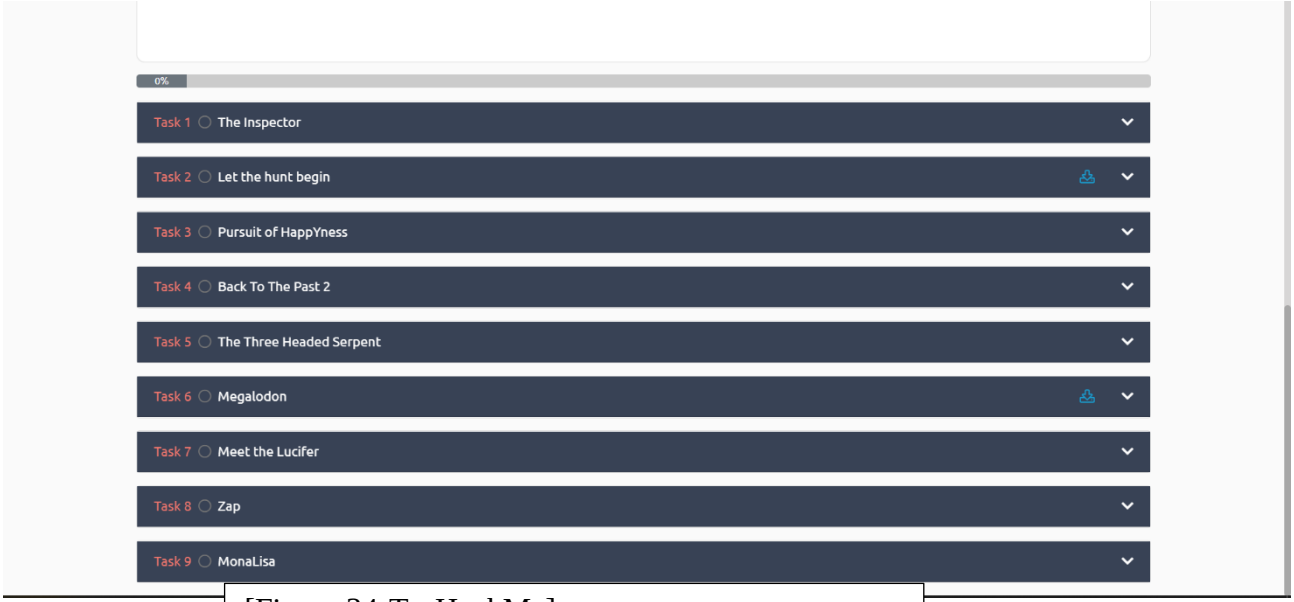


[Figure 32-S3 Bucket]

As the final level of the CTF project, created an account on tryhackme.com. After that created a room to host the CTF box and created 09 tasks related to the CTF box. In the first task players can join and visit the vulnerable website or they can easily google it.



[Figure 33-TryHackMe]



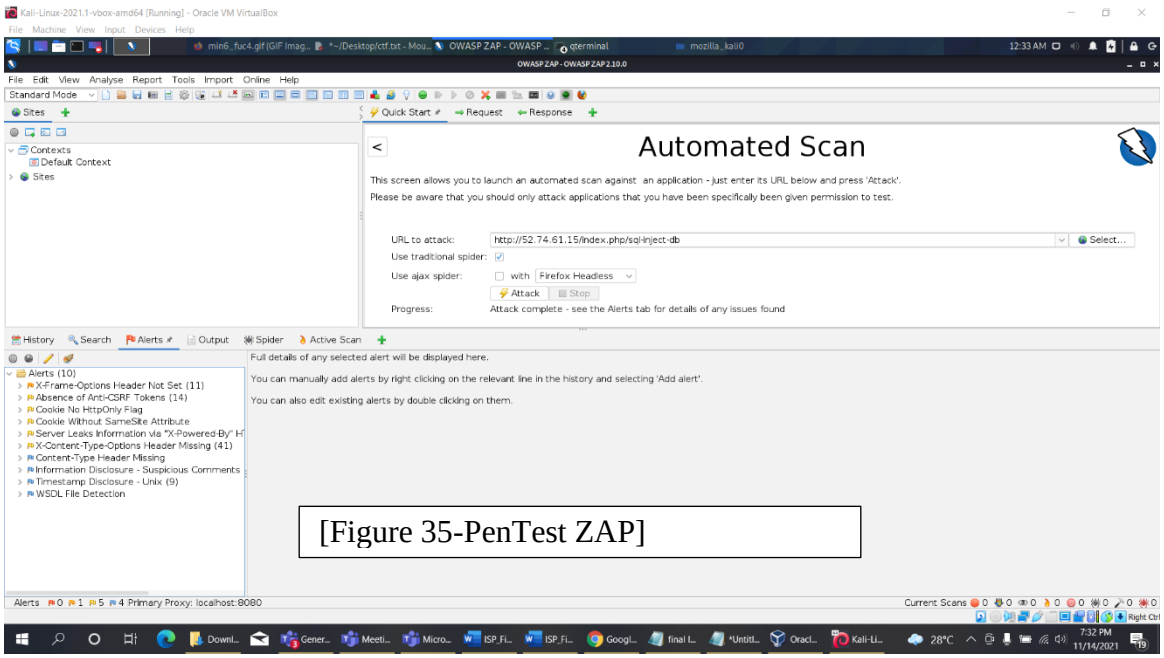
[Figure 34-TryHackMe]

2.4 Testing

As the first step after hosting the website, checked about its functions (ex: login function, register function, account maintaining). Those functions were successfully worked.

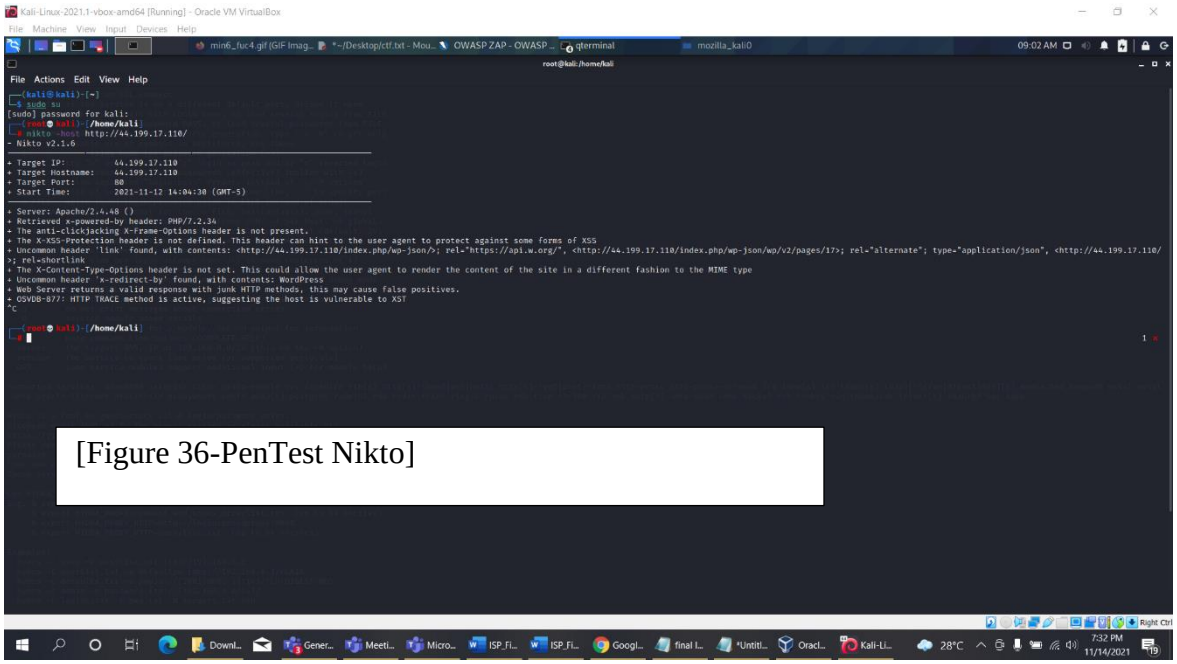
After the implementation of the cloud-based website, using security scanners the created web site was fully scanned. The main purpose of doing the security scan of the website was, needed to know is there any loopholes on the website than the created loopholes. By conducting the web scanning could analyze that there are no critical vulnerabilities except implemented ones. To penetrate the website used OWASP ZAP, Nmap, nikto, wapiti, skipfish, jSQL, scanQLi, SQLmap.

Scan results of OWASP ZAP



[Figure 35-PenTest ZAP]

Nikto results:

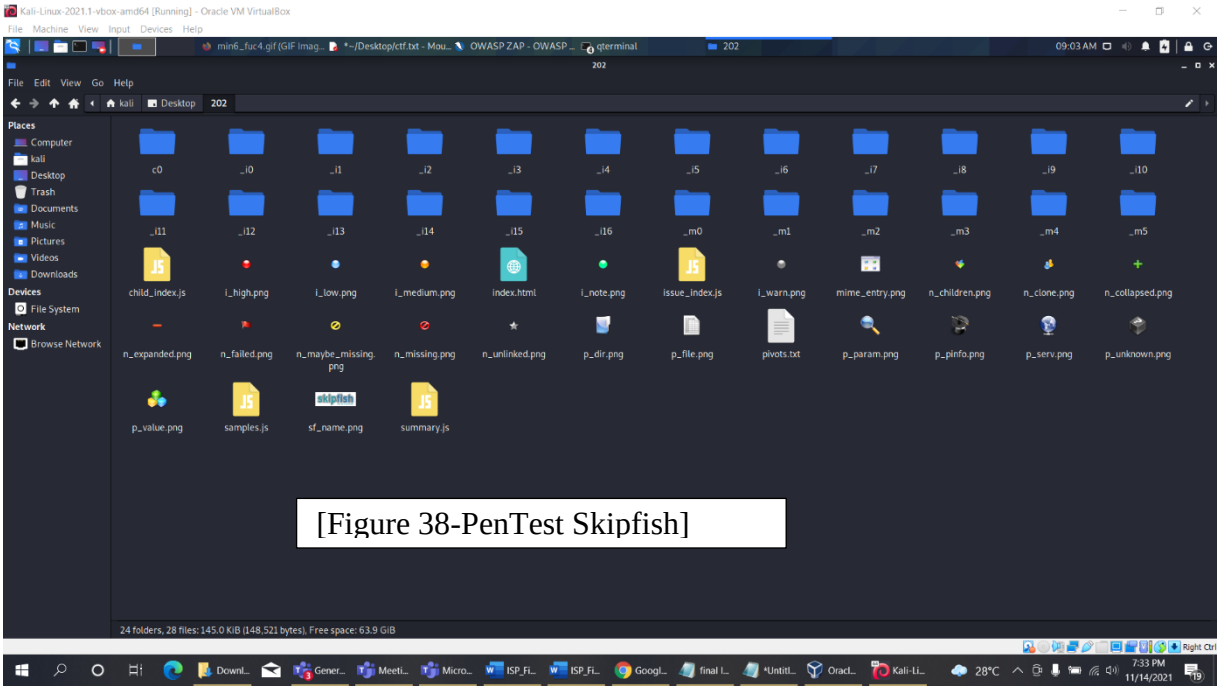


[Figure 36-PenTest Nikto]

Wapiti scan results:

[Figure 37-PenTest Wapiti]

Skipfish scan result results:



[Figure 38-PenTest Skipfish]

3. Evaluation

3.1 Assessment of the Project results

When starting the CTF project the team had zero knowledge about cloud computing. To improve the knowledge, had to follow tutorials and practical. After gaining finite amount of knowledge about the AWS cloud platform and it uses the team decided to start the implementation of Trip-To-Hell CTF box.

As mentioned above in methodology sector the implementation of the instances, databases and other requirements was the main task of the CTF box. The backend of the CTF box was firstly developed due to the necessity of the security requirements and other requirements that need to implement the CTF levels.

When implementing the first task of the CTF box, tried to make that level easier because the players need to adapt to the vulnerable website. As the first step, implemented it with hiding a secret link address in the coding part of the website home page. The second task is dependent on the first task's findings. In second task, player must download audio file and analyze it with a tool called Deepsound. Inside the audio file there is an old link of a twitter post of the website. Player must capture that. That level is based on cryptography. Third level is different from above two levels. At that level player need to run a nikto scan on website URL to analyze it. Nikto will give some information about the website. By collecting that information player has to find a comment section which is hided by the administrator and capture the flag and other link. Inside that link there will be a password file. As the fourth level of the CTF player had to analyze the old twitter link that found on the second level with way-back machine. As the fifth level, implemented a brute force task. In that task player need to know how to use hydra and how to create input files for the hydra. In the sixth level of the Trip-To-Hell CTF the player needs to analyze Wireshark packets and collect the details. For that analysis, as a small help to the player, uploaded a txt file on the tryhackme.com to collect the data for the analysis. That level is based on network analysis and cryptography. In the seventh task using the knowledge about the basic cryptography player need to capture the level flag. In task number eight player will get information about a hidden web page from the previous task and using OWASP ZAP or any advance scanning tool the player needs to find the admin name and the web page created date (There will not be any critical vulnerability alerts. However, player has to analyze every information

specially the feed information that disclosed with low level vulnerability alerts.). The main intention to implement this level is to mention that even with the low-level information disclosures that can be critical information leakages happened.

Task number nine is implemented with cloud computing basics. To capture the flag of this MonaLisa level player need to have basic knowledge about cloud computing. In this level player has to connect to the S3 via connecting EC2 instance with its DNS address and download an image file from the read only S3 bucket and analyze it with STool (steganography tool) and capture the final flag. In this level player will be needed to use Nmap tool too. Because he or she will need to find the open port details of the EC2 instance to connect to it.

With these backend, frontend web and CTF level implementations the team could successfully complete the CTF project. However, there were some failures happened when coming through this CTF building project. When trying to set the route 53 domain on the vulnerable website the web site was completely crashed due to misconfigurations. To overcome this issue, had to re-create the entire vulnerable website again. When creating the RDS database inside the Singapore region the MySQL database was unavailable due to technical failures of the Amazon server. After few research about the AWS server, found out that the Singapore region server face to technical failures commonly. Therefore, the RDS database region was changed to the North Virginia region and created it again to overcome that issue. In the testing phase, while doing the penetration testing on the created Travel Mate website, a system crash happened. jSQL tool was used at that time to pentest the web page to analyze for sql injection vulnerabilities. The penetration went wrong, and the web system completely crashed. However, after restarting the servers and databases the error was fixed by the system automatic repairing method. While configuring the permalinks on the website using WordPress that leaded to a system failure with website functioning errors. To resolve that the configuration details of the permalinks had to reset by manually.

3.2 Lessons Learned

By doing this CTF building project could gain knowledge about cloud computing basics and could learn about web site hosting on AWS platform. Also learned about the uses of WordPress and its security features. By hosting a web site on cloud, could learn number of security vulnerabilities and misconfigurations that can happen due to the lack of knowledge about security and configurations.

When configuring the latest version of WordPress with database found out that to install plugins the admin needs to give read, write, execute permission for wp-content directory and plugins folder. After doing research about it, could figure out that it is a kind of vulnerability that is only in the WordPress newest (10/11/2021) version 5.8.1.

3.3 Future Work

Expecting to fine tune the present version of the Trip-To-Hell CTF box and build an image file that players can host the website locally. However, the local hosting part might come out as an extended version of current CTF box. As a team, that plan to continue this CTF box with more features in future.

4. Conclusion

The CTF project created with web-based system that based on cloud computing. To implement the CTF box used AWS platform as cloud service provider and used WordPress as the website development tool. RDS Database and the EC2 instance of the website was connected with WordPress and with all these mechanisms developed a fully function vulnerable website. CTF box levels are implemented and based on the vulnerable Travel Mate website. There is main nine levels in the created CTF box. Try Hack Me website was selected to host this Trip-To-Hell CTF box.

5. References

[01]YouTube: https://www.youtube.com/watch?v=ulprqHHWlng&t=7963s

[02]WordPrss: https://wordpress.org/

[03]Try Hack Me: https://tryhackme.com/dashboard

[04]Contrast: https://www.contrastsecurity.com/security-influencers/tips-tactics-ctf-event

Appendix A: Test Results

Link to the walkthrough video: https://drive.google.com/drive/folders/1GR-c9JeRazk2N1wVwWXu2U_ORVsSZvcp?usp=sharing