Sri Lanka Institute of Information Technology

Final Project Report

ISP Project Report

Information Security Project 2022

Project ID: ISP-22-REG-10

Submitted by:

IT Number	Name
IT19065236	Maddumage M.
IT19172088	Kodagoda K. G. S. S. K

Date of submission : 7/6/2022

Abstract

Nova 6 – hybrid (virtual machine and web) based Capture The Flag challenge, which has the storyline of agent of Nova 6 trying to protect and defend against enemy virus attacks. Main aim of this CTF is to create awareness about cyber attacks in our community and agents, and to train students interested in CTF challenges. There are wide range of cyber-attacks used in Nova 6 CTF (i.e. bruteforce, steganography, exploiting backdoors, privilege escalation, encryption and decryption, etc). This CTF challenge is hosted on tryhackme platforms.

Acknowledgement

To Dr.Lakmal Rupasinghe, Ms. Laneesha Ruggahakotuwa and Miss. Chathuri Udagedara who gave using us the opportunity to create CTF challenge and earn specialized experience in building and implementing CTF challenges. To every literature, forums, AWS platform, tryhackme platform, 000webhost platform and all the other colleagues and services helped us is building Nova 6 CTF challenge.

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	Project NOVA 6
Project ID	ISP-22-REG-10

Group Members

Reg. No	Name	Signature
IT19172088	Kodagoda K. G. S. S. K	
IT19065236	Maddumage M.	

Table of Contents

List of Figures

List of Acronyms and Abbreviations

AWS - Amazon Web Service

CTF - Capture the Flag

OVA – Open Virtual Appliance

MD5 - message-digest algorithm

3DES - Triple Data Encryption Algorithm

DES - Data Encryption Standard

AES - Advanced Encryption Standard

1. Introduction

1.1 Problem Statement

In the modern world, Information Technology is used by every sector. With the rapid development of modern technology with IoT, Cloud computing and AI, the possibility of exposure to cyber-attacks are higher. This Nova6CTF provides hands-on experience with using pen testing tools to analyze data and vulnerability exploitations in web-based and OS based cloud bases vulnerability exploitation. The Nova6CTF is developed based on a hypothetical scenario, the user has to access a website that belongs to terrorists as an agent and find CTF flags by exploiting vulnerabilities and analyzing source codes and escalating privilege from agent to operator. There are 3 sub military bases and 1 main secret base, user need to access all 4 bases and find CTF flags to complete the game successfully, the main intention is to give experience on ethical hacking to cyber security beginners and persons who are at an intermediate level in cyber security.

To create this Nova6CTF mainly used platforms are AWS, WordPress and 000webhost and virtual machines of Ubuntu and Windows 7 operating systems because the CTF box includes both Operating system and web exploitations, therefore web exploitations vulnerabilities are included in the website and OS based exploitation vulnerabilities are contained in two virtual machines that mentioned above. The website is developed using WordPress. The main reason to select WordPress as the website developer is many organizations commonly use WordPress as their website developer and playing a CTF in a website that is developed using WordPress will improve the experience of real-life web exploitations. And also, the CTF box contains two virtual machines i.e. Ubuntu, and Windows 7, the main intention to use these Operating systems is to demonstrate the criticality of using outdated systems and software in the system. The reason to use 000webhost is to isolate those websites from the main website that develops on the AWS platform because the 000webhost web pages are in another military base and the first 2 military bases are in the AWS based website.

There are 17 steps in this CTF box. Players can easily play this CTF by accessing the Tryhackme website. Players don’t need to download virtual machines to their host machines, they can easily access the two virtual machines by entering the VM IP address that is given by the Tryhackme website and accessing it through OpenVPN. Players can easily access the website by simply entering the IP address of the website http://13.233.103.145/.

1.2 Product Scope

Players can get a hands-on experience with brute force attacks, web exploitations, program code analysing, backdoor exploitations, cryptography, using pen testing tools and Open Source Intelligence techniques. There are Virtual Machines, Web pages, program codes and operating system vulnerabilities in the Nova6CTF. This CTF box was developed based on the Jeopardy approach. The Jeopardy method contains different techniques i.e. cryptography, reverse engineering, data forensics, and web-based exploitations. Users should find flags by exploiting and breaking vulnerabilities to score marks. The user who gets the highest marks won. This CTF box contains cryptography, Steganography, Data forensics, web-based exploitations, and reverse engineering techniques. There will be a server and databases that users should exploit to gain information about the attacks and virus information from secret military bases.

1.3 Project Report Structure

The Implementation of the CTF box by creating the websites and configuring virtual machines are explained in the methodology section and the explanations about levels and future developments are explained in the evaluation section.

2. Methodology

2.1 Requirements and Analysis

The vulnerable website contains the first 2 military bases that belong to terrorists, and the other 2 bases are separately in the virtual machines, 3rd base is developed using windows 7 and 4th main base is developed using Ubuntu. All 3 secret bases include fragments of attack place information, virus version information, and main secret base information and the main secret base contains the cure to the virus. Users need to access all the 3 military bases to get the cure to the virus from the main secret base. In order to play the CTF, the following tools are needed.

- Quickstego
- S tool
- Wireshark
- FTK Imager
- John the Ripper
- WP scan
- Sherlock
- Wayback Machine

And also users must have knowledge about the following technologies.

- MD5
- 3DES
- DES
- Assembly
- C language
- AES

2.2 Design

The following diagram shows the workflow of the CTF

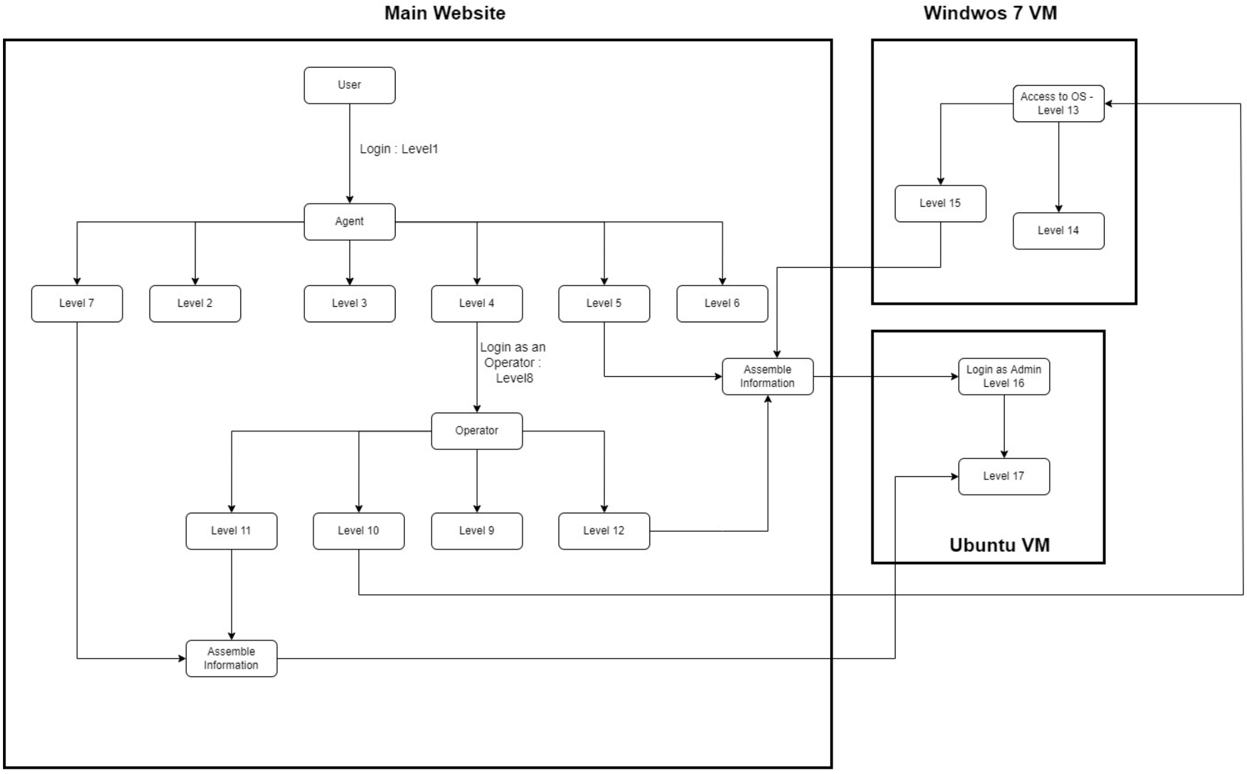


Figure 1

Website Deployment

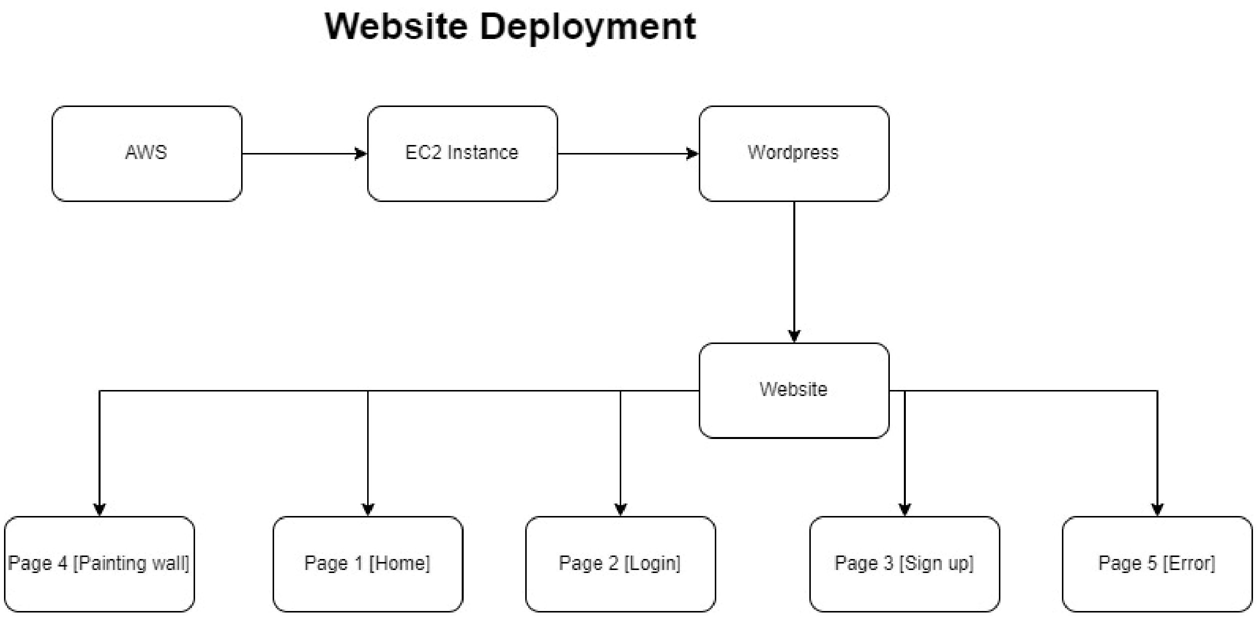


Figure 2

The Data and Read/Write access Diagram

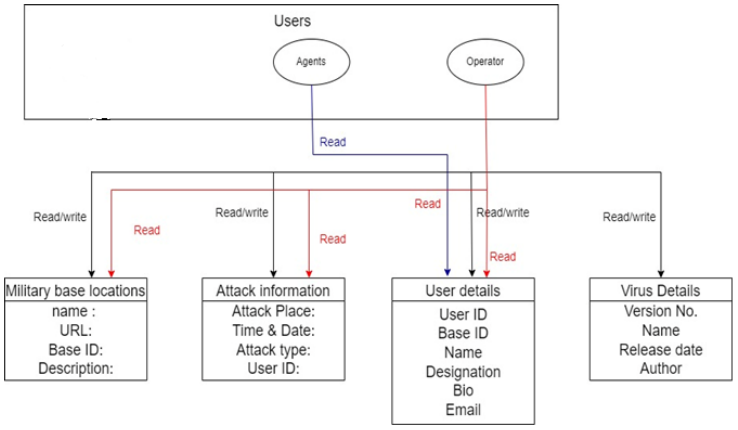
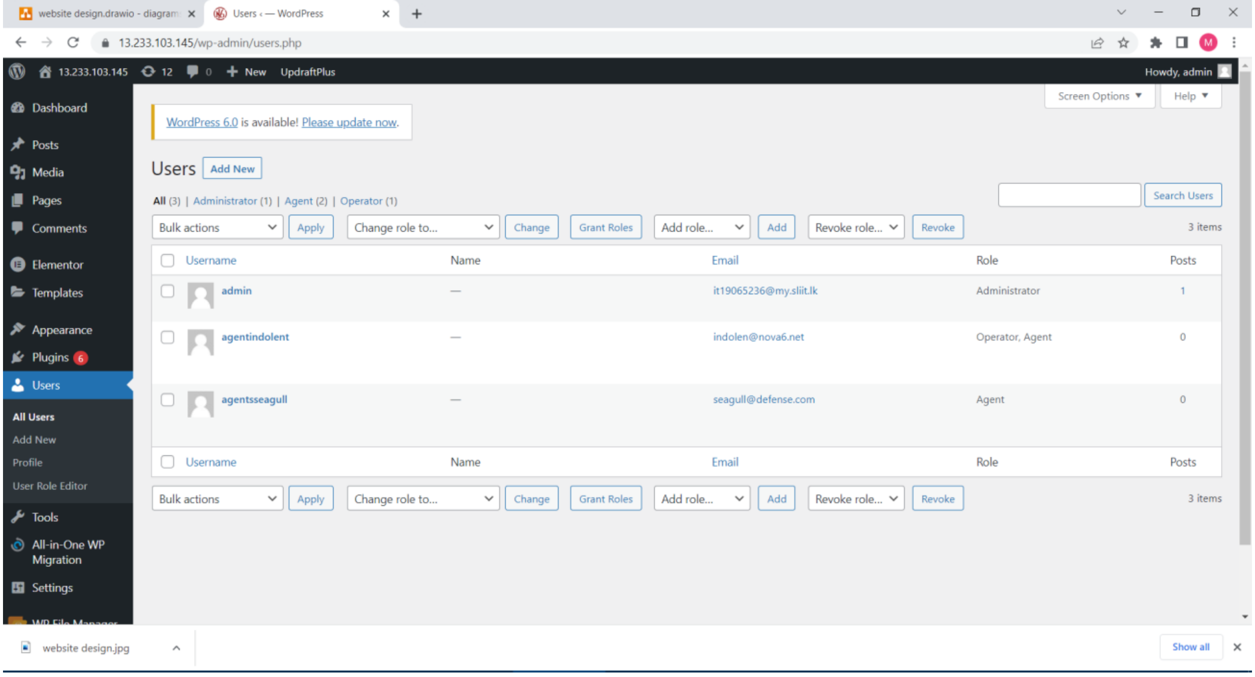


Figure 3

Backend of Wordpress



WordPress 6.0 is available! Please update now.

Users

All (3) | Administrator (1) | Agent (2) | Operator (1)

3 items

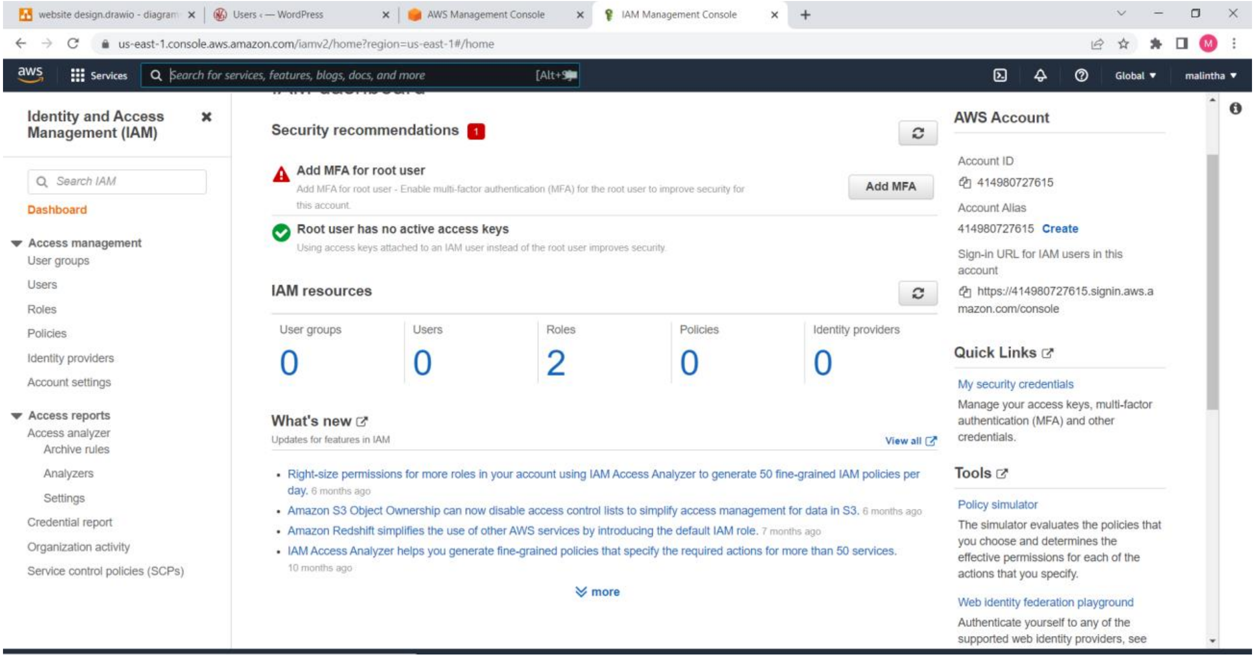
Username	Name	Email	Role	Posts
admin	—	it19065236@my.sliit.lk	Administrator	1
agentindolent	—	indolen@nova6.net	Operator, Agent	0
agentsseagull	—	seagull@defense.com	Agent	0

3 items

Figure 4

2.3 Implementation

This whole CTF Project consist of 2 virtual machines and one main website and one small website that used to develop a 7 web page.. The main reason to take 2 virtual machine is to isolate each bases from others. The reason to develop website and install 2 virtual machines is to implement level with both OS based exploitation and Web based exploitations. The website developed using AWS and wordpress. First created an account in wordpress and create EC2 instance for wordpress.



Security recommendations 1

Add MFA for root user

Add MFA for root user - Enable multi-factor authentication (MFA) for the root user to improve security for this account.

Root user has no active access keys

Using access keys attached to an IAM user instead of the root user improves security.

IAM resources

User groups	Users	Roles	Policies	Identity providers
0	0	2	0	0

What's new

Updates for features in IAM

- Right-size permissions for more roles in your account using IAM Access Analyzer to generate 50 fine-grained IAM policies per day. 6 months ago
- Amazon S3 Object Ownership can now disable access control lists to simplify access management for data in S3. 6 months ago
- Amazon Redshift simplifies the use of other AWS services by introducing the default IAM role. 7 months ago
- IAM Access Analyzer helps you generate fine-grained policies that specify the required actions for more than 50 services. 10 months ago

AWS Account

Account ID
414980727615

Account Alias
414980727615 Create

Sign-in URL for IAM users in this account
https://414980727615.signin.aws.amazon.com/console

Quick Links

My security credentials

Manage your access keys, multi-factor authentication (MFA) and other credentials.

Tools

Policy simulator

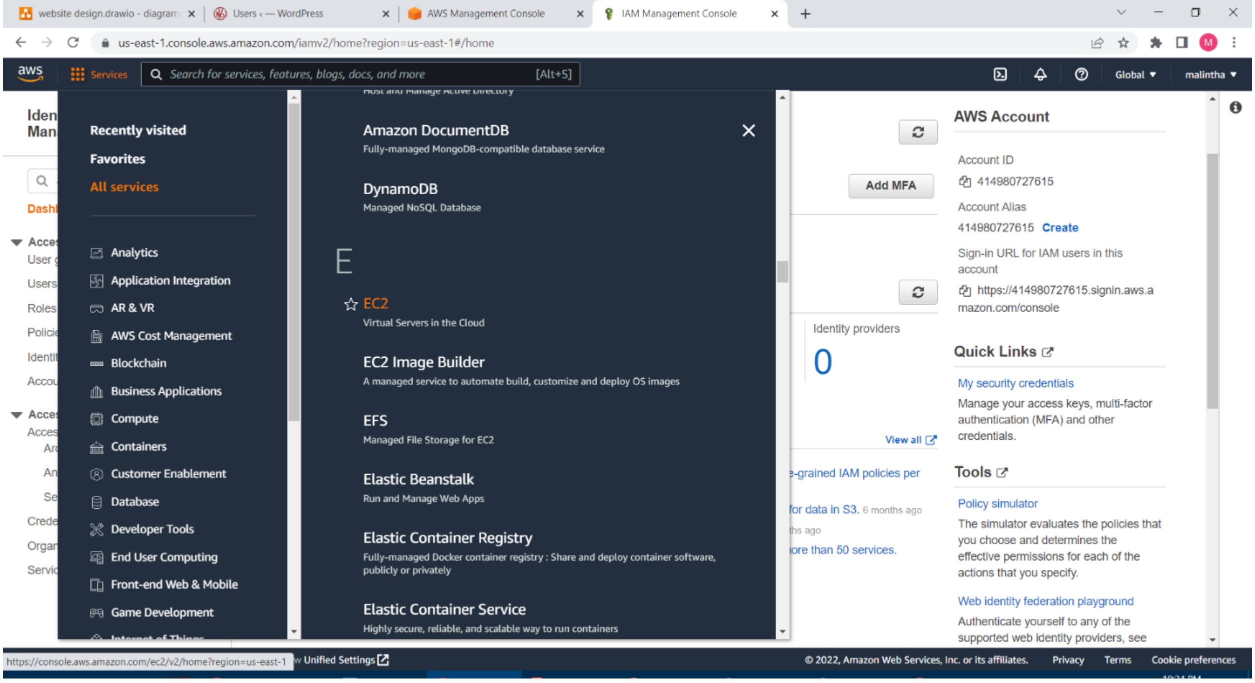
The simulator evaluates the policies that you choose and determines the effective permissions for each of the actions that you specify.

Web identity federation playground

Authenticate yourself to any of the supported web identity providers, see

Figure 5

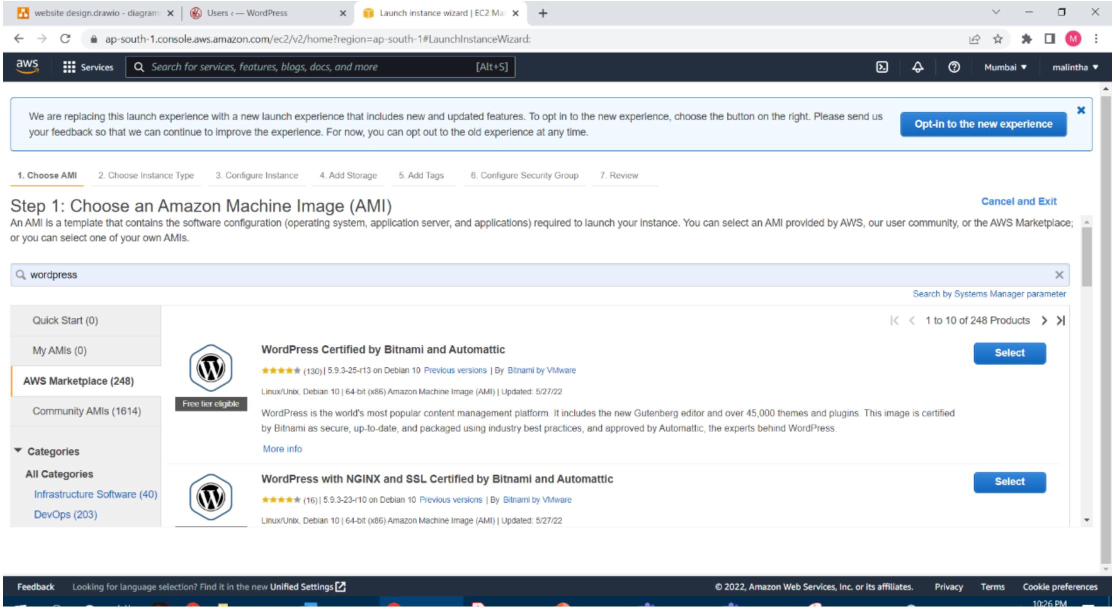
Then accessed the service tab and entered into the EC2 instance



website design.drawio - diagram
Users ‹ — WordPress
AWS Management Console
IAM Management Console
us-east-1.console.aws.amazon.com/iamv2/home?region=us-east-1#/home
aws
Services
Search for services, features, blogs, docs, and more
[Alt+S]
Global
malintha
Recently visited
Favorites
All services
Analytics
Application Integration
AR & VR
AWS Cost Management
Blockchain
Business Applications
Compute
Containers
Customer Enablement
Database
Developer Tools
End User Computing
Front-end Web & Mobile
Game Development
Internet of Things
Host and Manage Active Directory
Amazon DocumentDB
Fully-managed MongoDB-compatible database service
DynamoDB
Managed NoSQL Database
E
EC2
Virtual Servers in the Cloud
EC2 Image Builder
A managed service to automate build, customize and deploy OS images
EFS
Managed File Storage for EC2
Elastic Beanstalk
Run and Manage Web Apps
Elastic Container Registry
Fully-managed Docker container registry : Share and deploy container software, publicly or privately
Elastic Container Service
Highly secure, reliable, and scalable way to run containers
Add MFA
Identity providers
0
View all
AWS Account
Account ID
414980727615
Account Alias
414980727615 Create
Sign-in URL for IAM users in this account
https://414980727615.signin.aws.amazon.com/console
Quick Links
My security credentials
Manage your access keys, multi-factor authentication (MFA) and other credentials.
Tools
Policy simulator
The simulator evaluates the policies that you choose and determines the effective permissions for each of the actions that you specify.
Web identity federation playground
Authenticate yourself to any of the supported web identity providers, see
https://console.aws.amazon.com/ec2/v2/home?region=us-east-1
Unified Settings
© 2022, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

Figure 6

Search for wordpress in the search bar and entered into the wordpress Certified by Bitnami and Automatic


website design.drawio - diagram
Users ‹ — WordPress
Launch instance wizard | EC2 Ma
ap-south-1.console.aws.amazon.com/ec2/v2/home?region=ap-south-1#LaunchInstanceWizard:
aws
Services
Search for services, features, blogs, docs, and more
[Alt+S]
Mumbai ▾
malintha ▾
Opt-in to the new experience
Select
Select
Feedback
Looking for language selection? Find it in the new Unified Settings
© 2022, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

We are replacing this launch experience with a new launch experience that includes new and updated features. To opt in to the new experience, choose the button on the right. Please send us your feedback so that we can continue to improve the experience. For now, you can opt out to the old experience at any time.

1. Choose AMI | 2. Choose Instance Type | 3. Configure Instance | 4. Add Storage | 5. Add Tags | 6. Configure Security Group | 7. Review

Step 1: Choose an Amazon Machine Image (AMI)

Cancel and Exit

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. You can select an AMI provided by AWS, our user community, or the AWS Marketplace; or you can select one of your own AMIs.

wordpress

Search by Systems Manager parameter

Quick Start (0)
My AMIs (0)
AWS Marketplace (248)
Community AMIs (1614)

Categories
All Categories
Infrastructure Software (40)
DevOps (203)

1 to 10 of 248 Products

WordPress Certified by Bitnami and Automattic

Free tier eligible

★★★★★ (130) | 5.9.3-25-r13 on Debian 10 Previous versions | By Bitnami by VMware

Linux/Unix, Debian 10 | 64-bit (x86) Amazon Machine Image (AMI) | Updated: 5/27/22

WordPress is the world's most popular content management platform. It includes the new Gutenberg editor and over 45,000 themes and plugins. This image is certified by Bitnami as secure, up-to-date, and packaged using industry best practices, and approved by Automattic, the experts behind WordPress.

More info

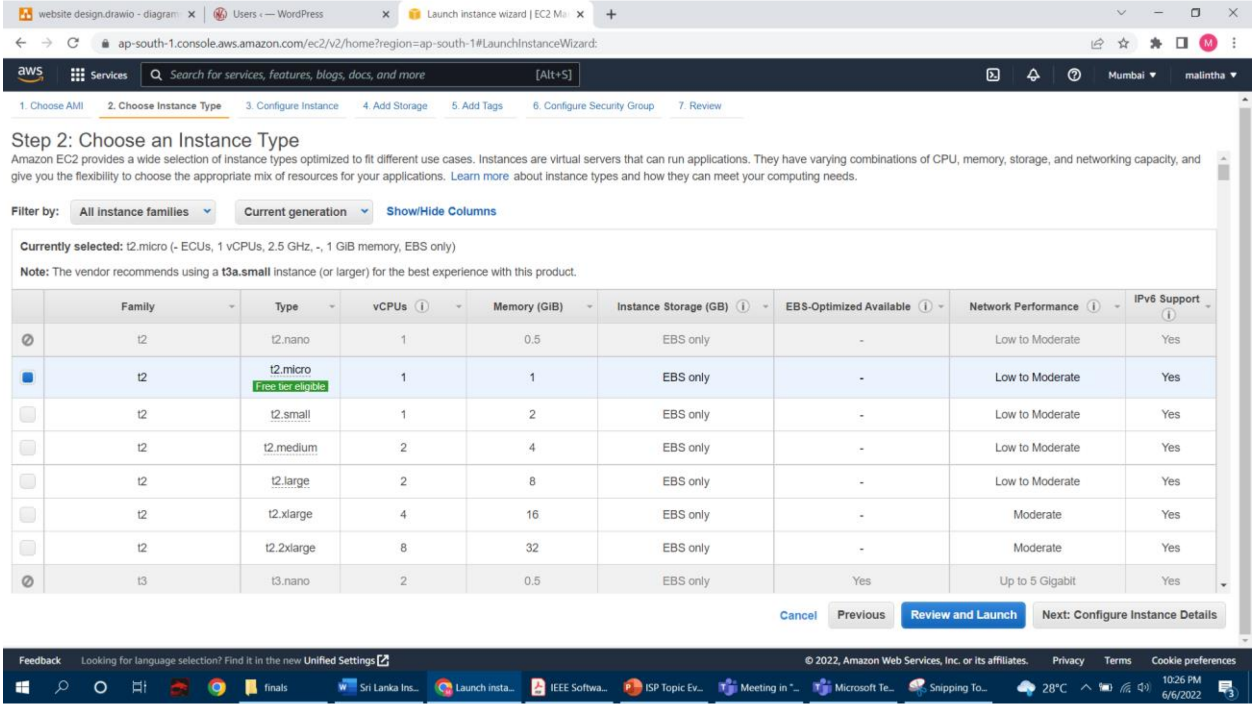
WordPress with NGINX and SSL Certified by Bitnami and Automattic

★★★★★ (16) | 5.9.3-23-r10 on Debian 10 Previous versions | By Bitnami by VMware

Linux/Unix, Debian 10 | 64-bit (x86) Amazon Machine Image (AMI) | Updated: 5/27/22

Figure 7

Selected free tier t2.micro as the instance type


website design.drawio - diagram
Users ‹ — WordPress
Launch instance wizard | EC2 Ma
ap-south-1.console.aws.amazon.com/ec2/v2/home?region=ap-south-1#LaunchInstanceWizard:
aws
Services
Search for services, features, blogs, docs, and more
[Alt+S]
Mumbai ▾
malintha ▾
Cancel
Previous
Review and Launch
Next: Configure Instance Details
Feedback
Looking for language selection? Find it in the new Unified Settings
© 2022, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
finals
Sri Lanka Ins...
Launch insta...
IEEE Softwa...
ISP Topic Ev...
Meeting in "...
Microsoft Te...
Snipping To...
28°C
10:26 PM
6/6/2022

1. Choose AMI | 2. Choose Instance Type | 3. Configure Instance | 4. Add Storage | 5. Add Tags | 6. Configure Security Group | 7. Review

Step 2: Choose an Instance Type

Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instances are virtual servers that can run applications. They have varying combinations of CPU, memory, storage, and networking capacity, and give you the flexibility to choose the appropriate mix of resources for your applications. Learn more about instance types and how they can meet your computing needs.

Filter by: All instance families ▾ Current generation ▾ Show/Hide Columns

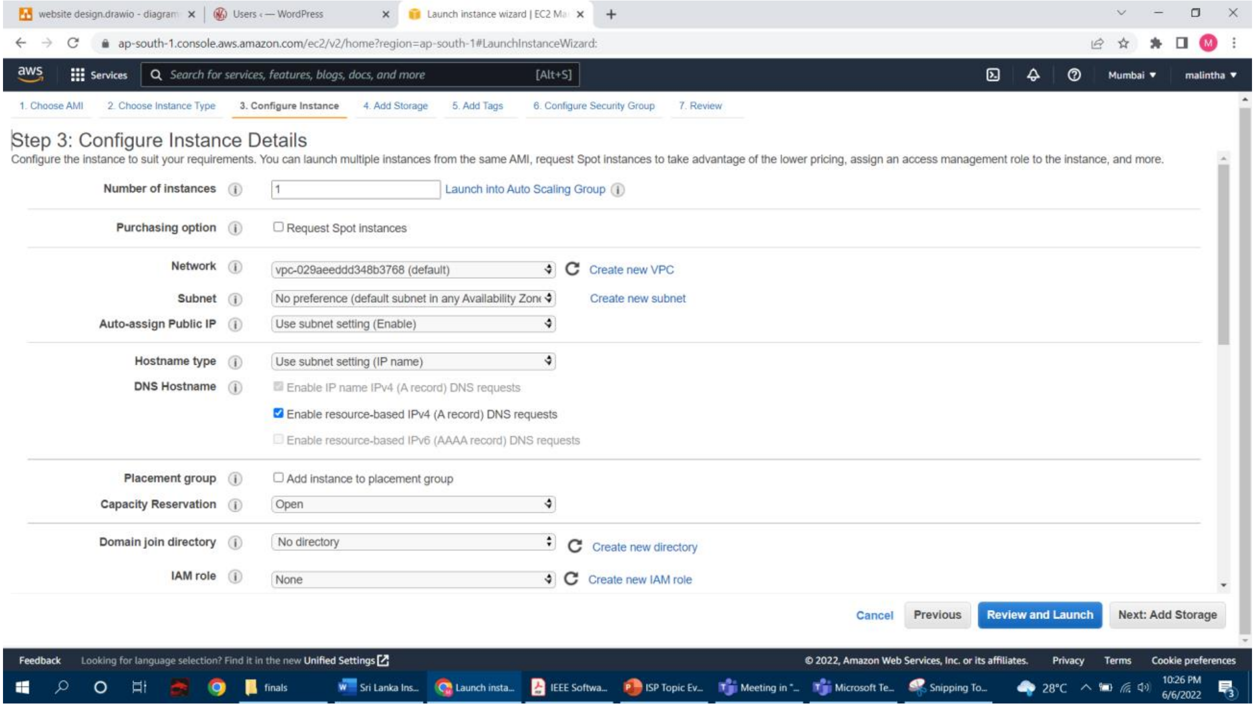
Currently selected: t2.micro (- ECUs, 1 vCPUs, 2.5 GHz, -, 1 GiB memory, EBS only)

Note: The vendor recommends using a **t3a.small** instance (or larger) for the best experience with this product.

	Family	Type	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance	IPv6 Support
⊘	t2	t2.nano	1	0.5	EBS only	-	Low to Moderate	Yes
■	t2	t2.micro Free tier eligible	1	1	EBS only	-	Low to Moderate	Yes
□	t2	t2.small	1	2	EBS only	-	Low to Moderate	Yes
□	t2	t2.medium	2	4	EBS only	-	Low to Moderate	Yes
□	t2	t2.large	2	8	EBS only	-	Low to Moderate	Yes
□	t2	t2.xlarge	4	16	EBS only	-	Moderate	Yes
□	t2	t2.2xlarge	8	32	EBS only	-	Moderate	Yes
⊘	t3	t3.nano	2	0.5	EBS only	Yes	Up to 5 Gigabit	Yes

Figure 8

Leave default settings in 3,4,5 and 6 stages.



Step 3: Configure Instance Details

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, assign an access management role to the instance, and more.

Number of instances: 1 — Launch into Auto Scaling Group

Purchasing option: □ Request Spot instances

Network: vpc-029aeeddd348b3768 (default) — Create new VPC

Subnet: No preference (default subnet in any Availability Zone) — Create new subnet

Auto-assign Public IP: Use subnet setting (Enable)

Hostname type: Use subnet setting (IP name)

DNS Hostname: ☑ Enable IP name IPv4 (A record) DNS requests

☑ Enable resource-based IPv4 (A record) DNS requests

□ Enable resource-based IPv6 (AAAA record) DNS requests

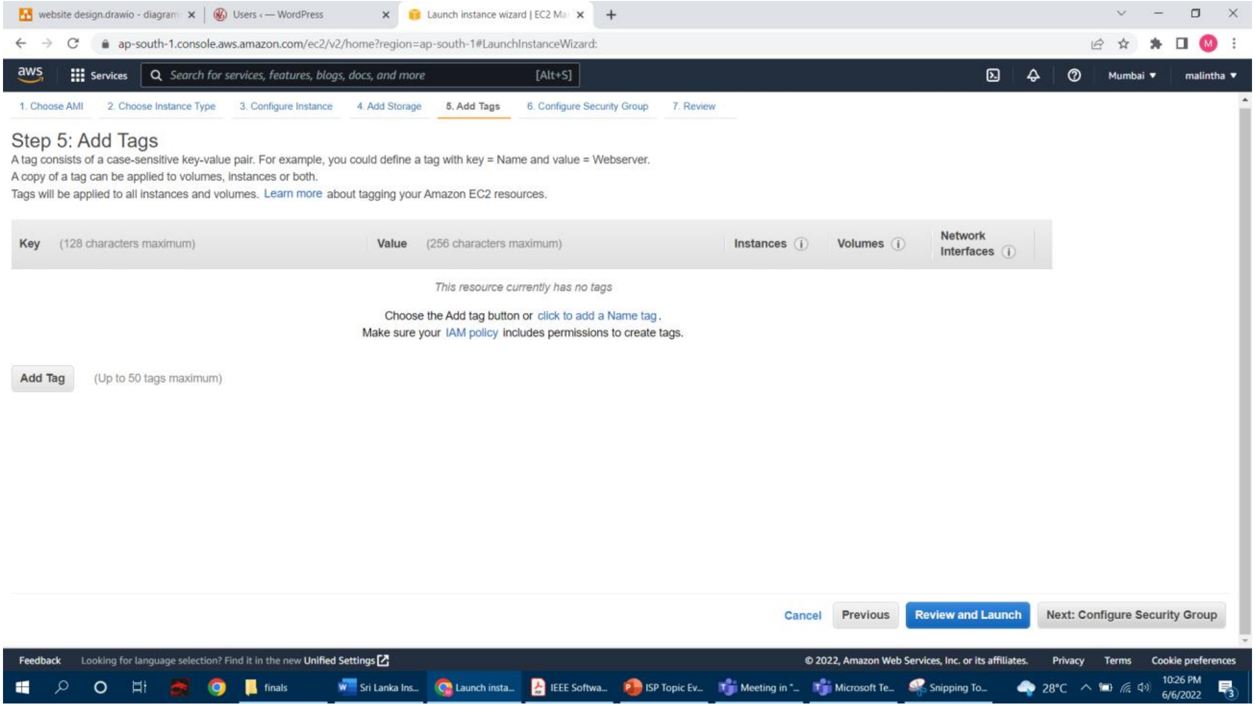
Placement group: □ Add instance to placement group

Capacity Reservation: Open

Domain join directory: No directory — Create new directory

IAM role: None — Create new IAM role

Figure 9


website design.drawio - diagram
Users ‹ — WordPress
Launch instance wizard | EC2 Ma
ap-south-1.console.aws.amazon.com/ec2/v2/home?region=ap-south-1#LaunchInstanceWizard:
aws
Services
Search for services, features, blogs, docs, and more
[Alt+S]
Mumbai ▼
malintha ▼
1. Choose AMI
2. Choose Instance Type
3. Configure Instance
4. Add Storage
5. Add Tags
6. Configure Security Group
7. Review
Cancel
Previous
Review and Launch
Next: Configure Security Group
Feedback
Looking for language selection? Find it in the new Unified Settings
© 2022, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
finals
Sri Lanka Ins...
Launch insta...
IEEE Softwa...
ISP Topic Ev...
Meeting in "...
Microsoft Te...
Snipping To...
28°C
10:26 PM
6/6/2022

Step 5: Add Tags

A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver.
A copy of a tag can be applied to volumes, instances or both.
Tags will be applied to all instances and volumes. Learn more about tagging your Amazon EC2 resources.

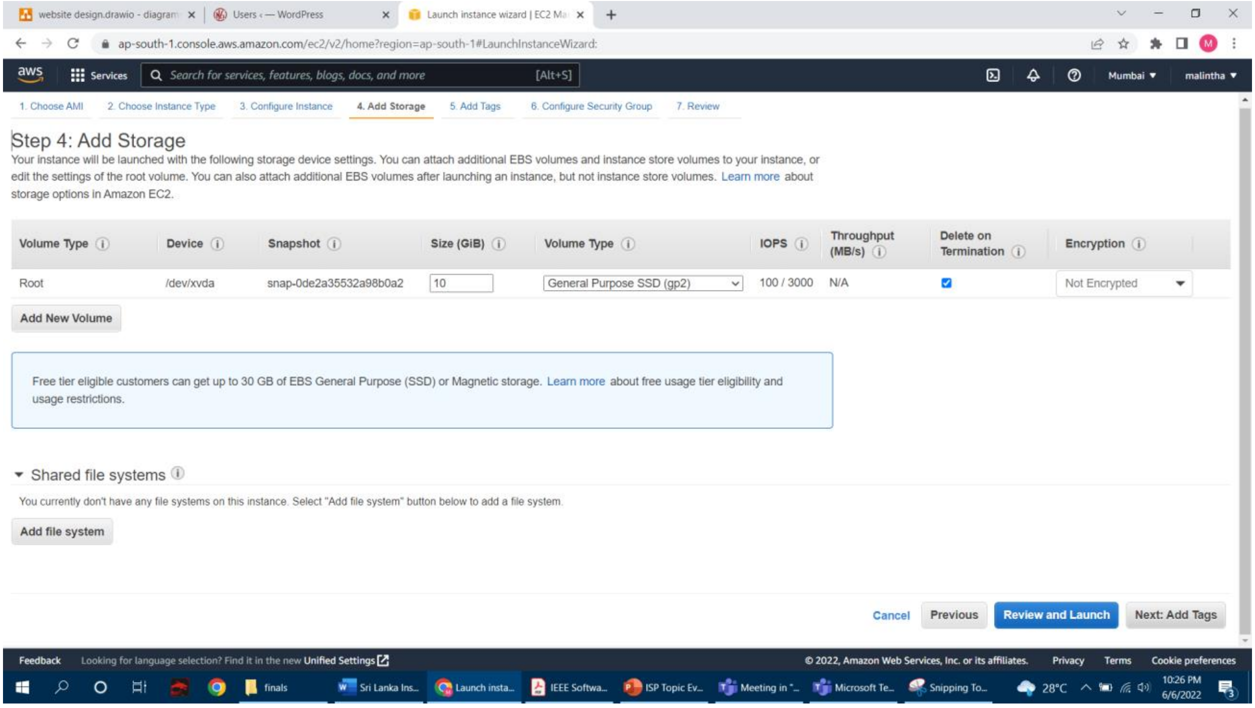
Key (128 characters maximum)	Value (256 characters maximum)	Instances	Volumes	Network Interfaces

This resource currently has no tags

Choose the Add tag button or click to add a Name tag.
Make sure your IAM policy includes permissions to create tags.

Add Tag (Up to 50 tags maximum)

Figure 10



website design.drawio - diagram
Users ‹ — WordPress
Launch instance wizard | EC2 Ma
ap-south-1.console.aws.amazon.com/ec2/v2/home?region=ap-south-1#LaunchInstanceWizard:
Services
Search for services, features, blogs, docs, and more
[Alt+S]
Mumbai
malintha
1. Choose AMI
2. Choose Instance Type
3. Configure Instance
4. Add Storage
5. Add Tags
6. Configure Security Group
7. Review

Step 4: Add Storage

Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes. Learn more about storage options in Amazon EC2.

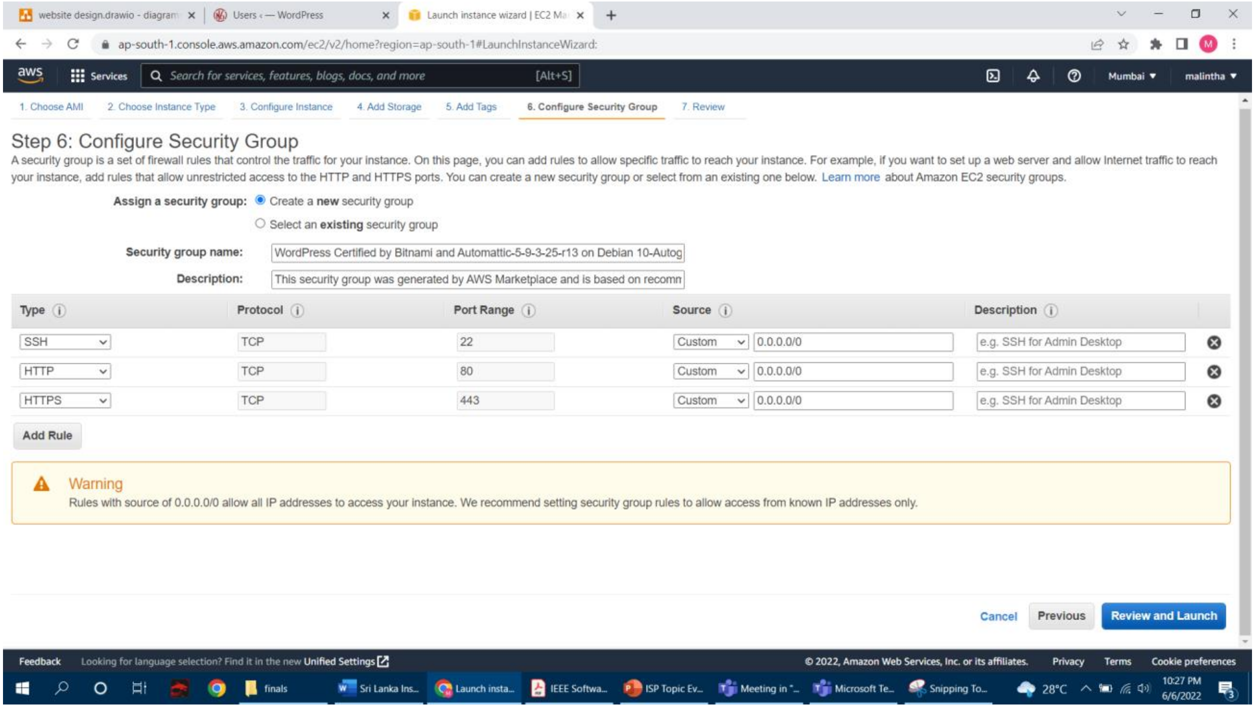
Volume Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Throughput (MB/s)	Delete on Termination	Encryption
Root	/dev/xvda	snap-0de2a35532a98b0a2	10	General Purpose SSD (gp2)	100 / 3000	N/A	☑	Not Encrypted

Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage. Learn more about free usage tier eligibility and usage restrictions.

Shared file systems

You currently don't have any file systems on this instance. Select "Add file system" button below to add a file system.

Figure 11



website design.drawio - diagram
Users ‹ — WordPress
Launch instance wizard | EC2 Ma
ap-south-1.console.aws.amazon.com/ec2/v2/home?region=ap-south-1#LaunchInstanceWizard:
Services
Search for services, features, blogs, docs, and more
[Alt+S]
Mumbai
malintha
1. Choose AMI
2. Choose Instance Type
3. Configure Instance
4. Add Storage
5. Add Tags
6. Configure Security Group
7. Review

Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. Learn more about Amazon EC2 security groups.

Assign a security group: ● Create a **new** security group

○ Select an **existing** security group

Security group name: WordPress Certified by Bitnami and Automattic-5-9-3-25-r13 on Debian 10-Autog

Description: This security group was generated by AWS Marketplace and is based on recomm

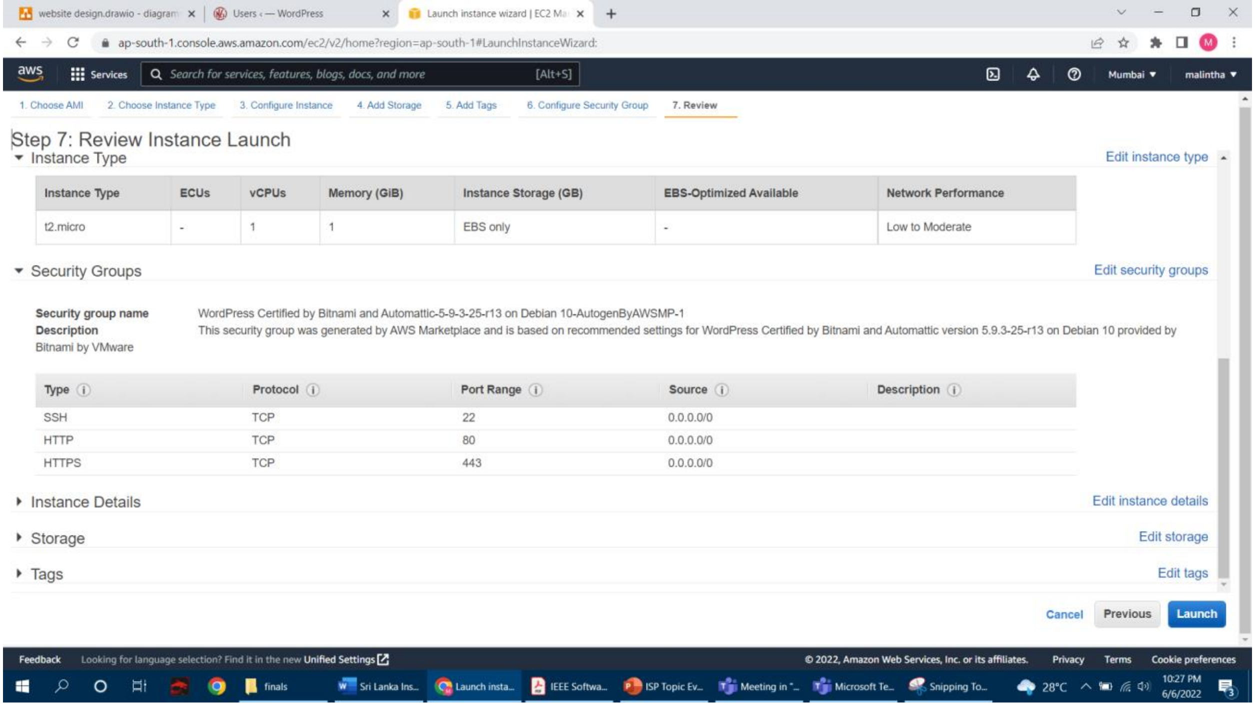
Type	Protocol	Port Range	Source		Description
SSH	TCP	22	Custom	0.0.0.0/0	e.g. SSH for Admin Desktop
HTTP	TCP	80	Custom	0.0.0.0/0	e.g. SSH for Admin Desktop
HTTPS	TCP	443	Custom	0.0.0.0/0	e.g. SSH for Admin Desktop

Warning

Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

Figure 12

Launched the instance



Step 7: Review Instance Launch

▾ Instance Type

Instance Type	ECUs	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance
t2.micro	-	1	1	EBS only	-	Low to Moderate

▾ Security Groups

Security group name WordPress Certified by Bitnami and Automattic-5-9-3-25-r13 on Debian 10-AutogenByAWSMP-1

Description This security group was generated by AWS Marketplace and is based on recommended settings for WordPress Certified by Bitnami and Automattic version 5.9.3-25-r13 on Debian 10 provided by Bitnami by VMware

Type	Protocol	Port Range	Source	Description
SSH	TCP	22	0.0.0.0/0	
HTTP	TCP	80	0.0.0.0/0	
HTTPS	TCP	443	0.0.0.0/0	

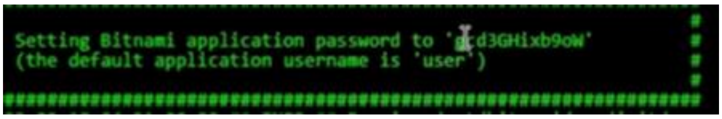
‣ Instance Details

‣ Storage

‣ Tags

Figure 13

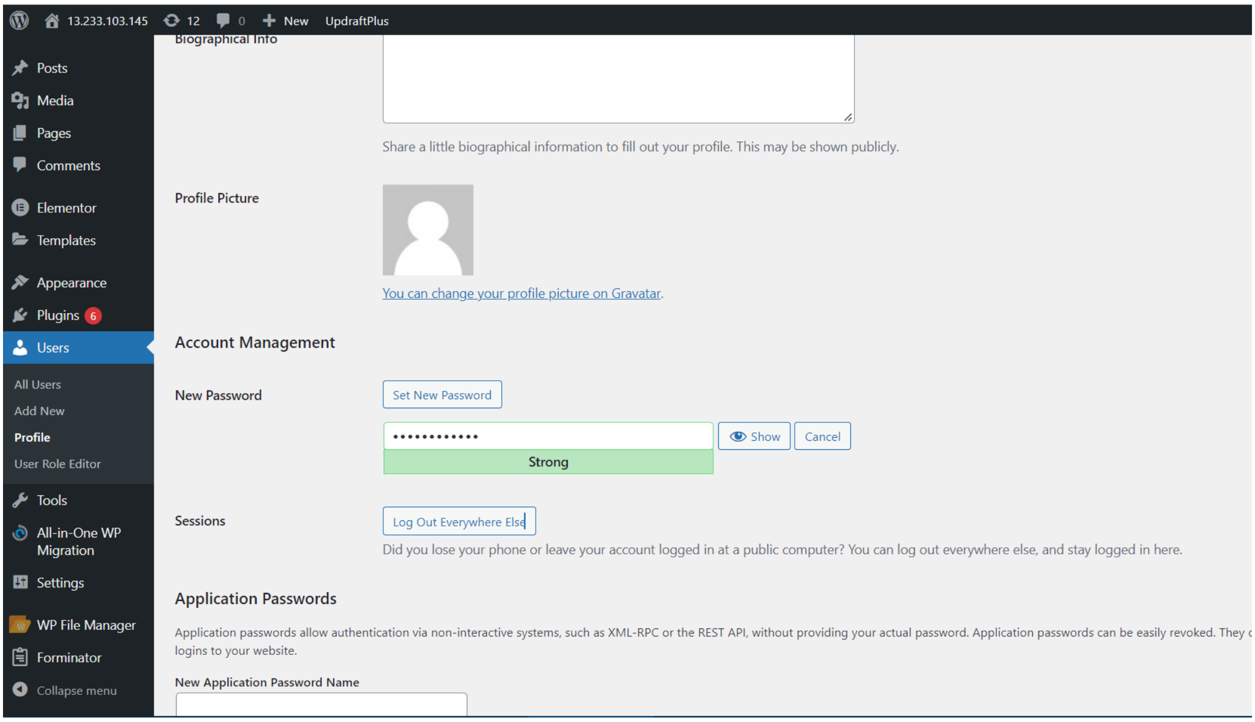
Then get the default username and password in system logs



```
#                                                                      #
# Setting Bitnami application password to 'gcd3GHixb9oW'               #
# (the default application username is 'user')                         #
#                                                                      #
########################################################################
```

Figure 14

And then entered the default username password into the WordPress site and change default username and password.



Biographical Info

Share a little biographical information to fill out your profile. This may be shown publicly.

Profile Picture

You can change your profile picture on Gravatar.

Account Management

New Password

••••••••••••

Strong

Sessions

Did you lose your phone or leave your account logged in at a public computer? You can log out everywhere else, and stay logged in here.

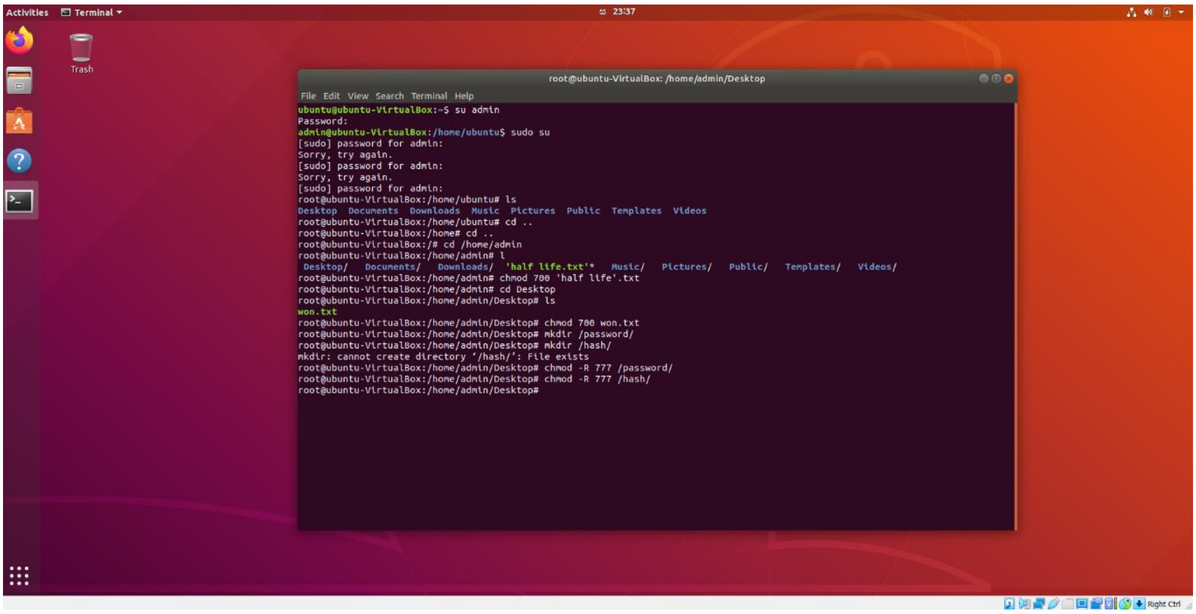
Application Passwords

Application passwords allow authentication via non-interactive systems, such as XML-RPC or the REST API, without providing your actual password. Application passwords can be easily revoked. They c logins to your website.

New Application Password Name

Figure 15

Also installed virtual machines into the virutalbox and created access privileges to users and exported the virtual machines as ova files and uploaded them to the tryhackme.


Activities
Terminal
23:37
Trash
root@ubuntu-VirtualBox: /home/admin/Desktop
File Edit View Search Terminal Help
Right Ctrl

```
ubuntu@ubuntu-VirtualBox:~$ su admin
Password:
admin@ubuntu-VirtualBox:/home/ubuntu$ sudo su
[sudo] password for admin:
Sorry, try again.
[sudo] password for admin:
Sorry, try again.
[sudo] password for admin:
root@ubuntu-VirtualBox:/home/ubuntu# ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos
root@ubuntu-VirtualBox:/home/ubuntu# cd ..
root@ubuntu-VirtualBox:/home# cd ..
root@ubuntu-VirtualBox:/# cd /home/admin
root@ubuntu-VirtualBox:/home/admin# l
 Desktop/   Documents/   Downloads/  'half life.txt'*   Music/   Pictures/   Public/   Templates/   Videos/
root@ubuntu-VirtualBox:/home/admin# chmod 700 'half life'.txt
root@ubuntu-VirtualBox:/home/admin# cd Desktop
root@ubuntu-VirtualBox:/home/admin/Desktop# ls
won.txt
root@ubuntu-VirtualBox:/home/admin/Desktop# chmod 700 won.txt
root@ubuntu-VirtualBox:/home/admin/Desktop# mkdir /password/
root@ubuntu-VirtualBox:/home/admin/Desktop# mkdir /hash/
mkdir: cannot create directory '/hash/': File exists
root@ubuntu-VirtualBox:/home/admin/Desktop# chmod -R 777 /password/
root@ubuntu-VirtualBox:/home/admin/Desktop# chmod -R 777 /hash/
root@ubuntu-VirtualBox:/home/admin/Desktop#
```

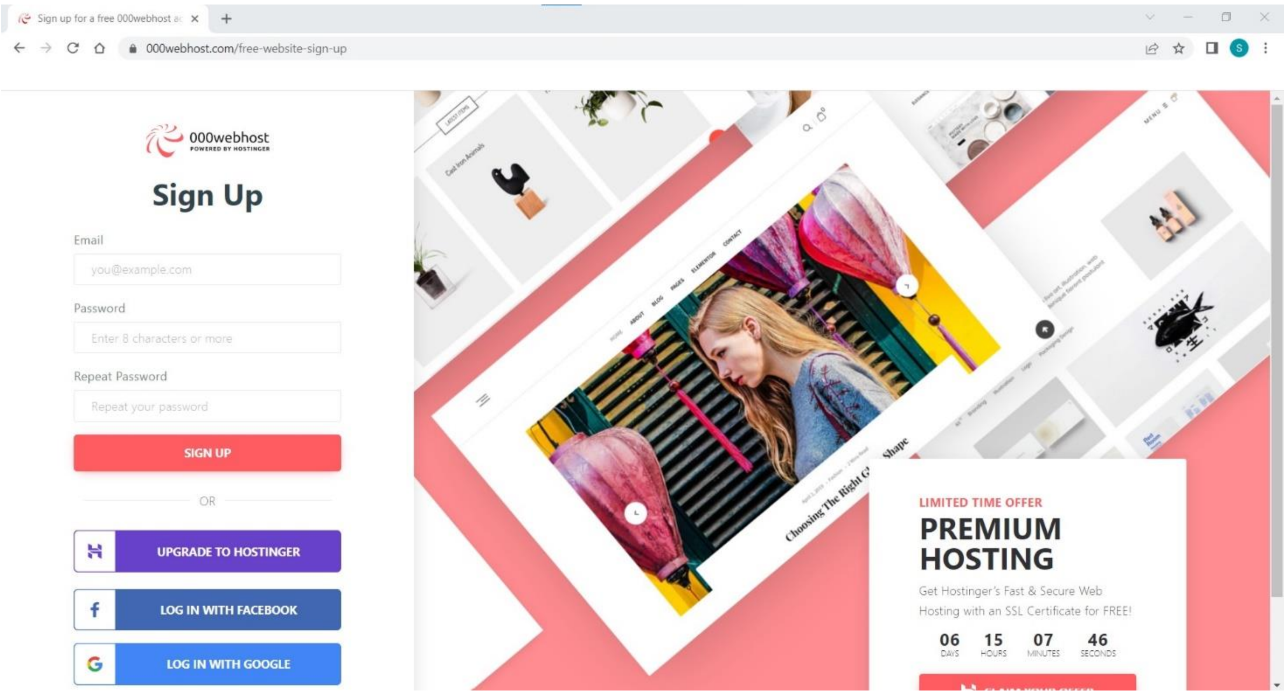
Figure 16

Installed ubuntu 18.04, because tryhackme doesn't supports latest versions, and created users and

Configured file read and write privileges for different users and made directories to put necessary files for player when playing the CTF and add permissions for players to add files to those directories.

000Webhost

Seven webpages and one java script file is hosted on 000webhost to isolate it from the other webpages in AWS. First an account is created in 000webhost (google account used).



Sign up for a free 000webhost ac

000webhost.com/free-website-sign-up

000webhost
POWERED BY HOSTINGER

Sign Up

Email
you@example.com

Password
Enter 8 characters or more

Repeat Password
Repeat your password

SIGN UP

OR

UPGRADE TO HOSTINGER

LOG IN WITH FACEBOOK

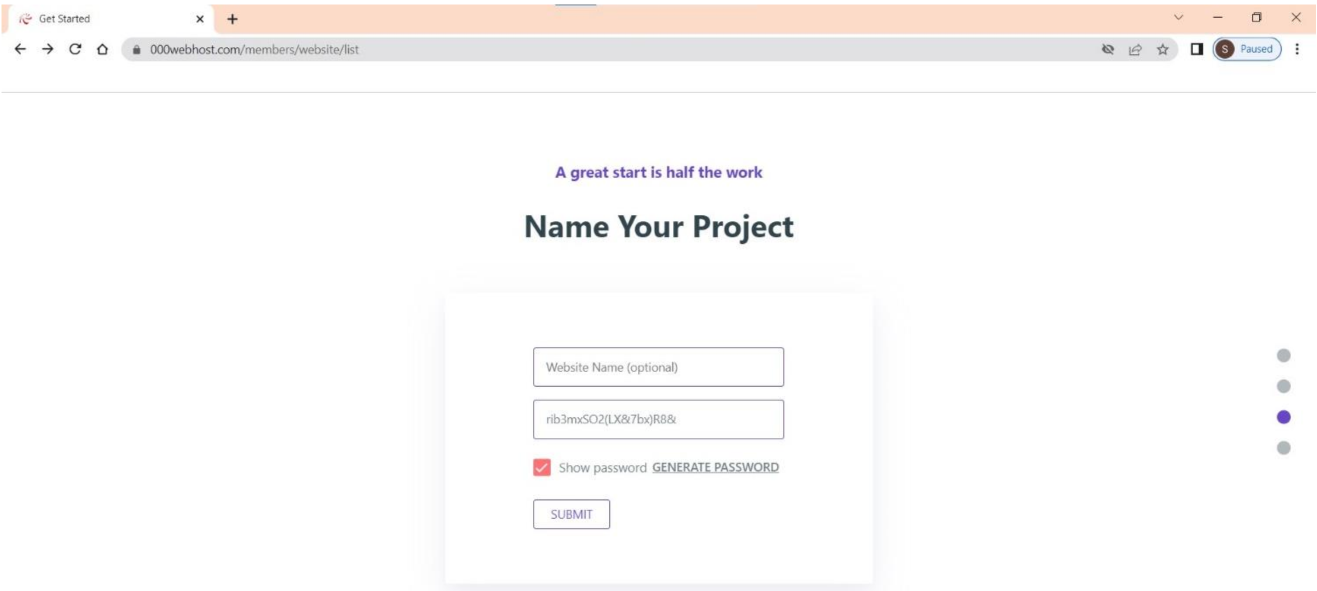
LOG IN WITH GOOGLE

LIMITED TIME OFFER
PREMIUM HOSTING
Get Hostinger's Fast & Secure Web Hosting with an SSL Certificate for FREE!

06	15	07	46
DAYS	HOURS	MINUTES	SECONDS

Figure 17

Next the webpage name and the password is added



Get Started

000webhost.com/members/website/list

A great start is half the work

Name Your Project

Website Name (optional)

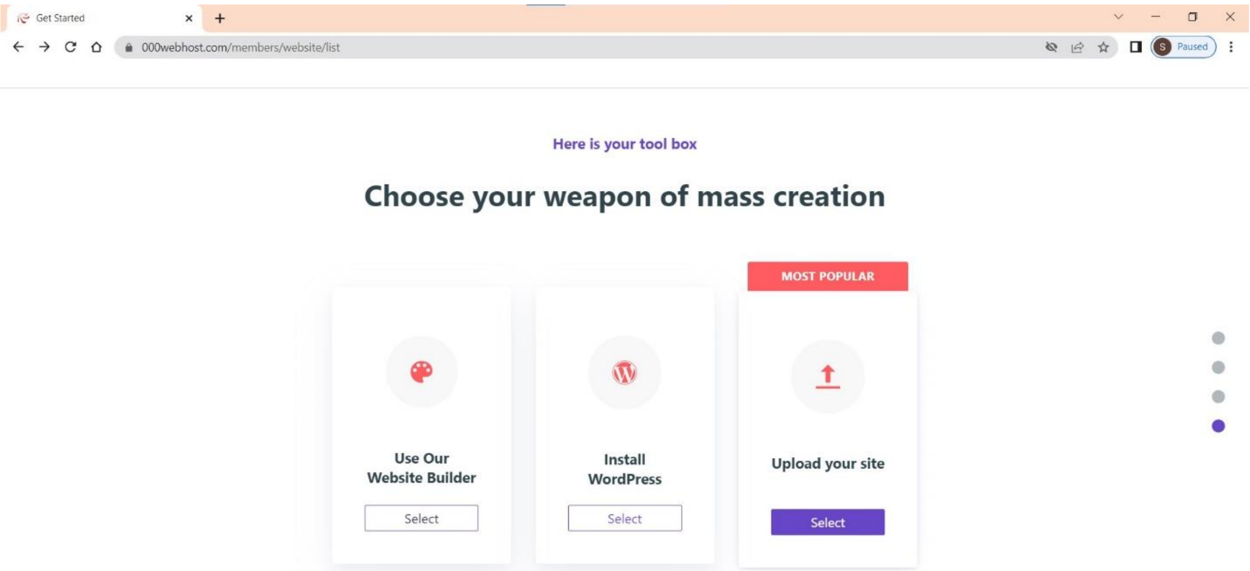
rib3mxSO2(LX&7bx)R8&

☑ Show password GENERATE PASSWORD

SUBMIT

Figure 18

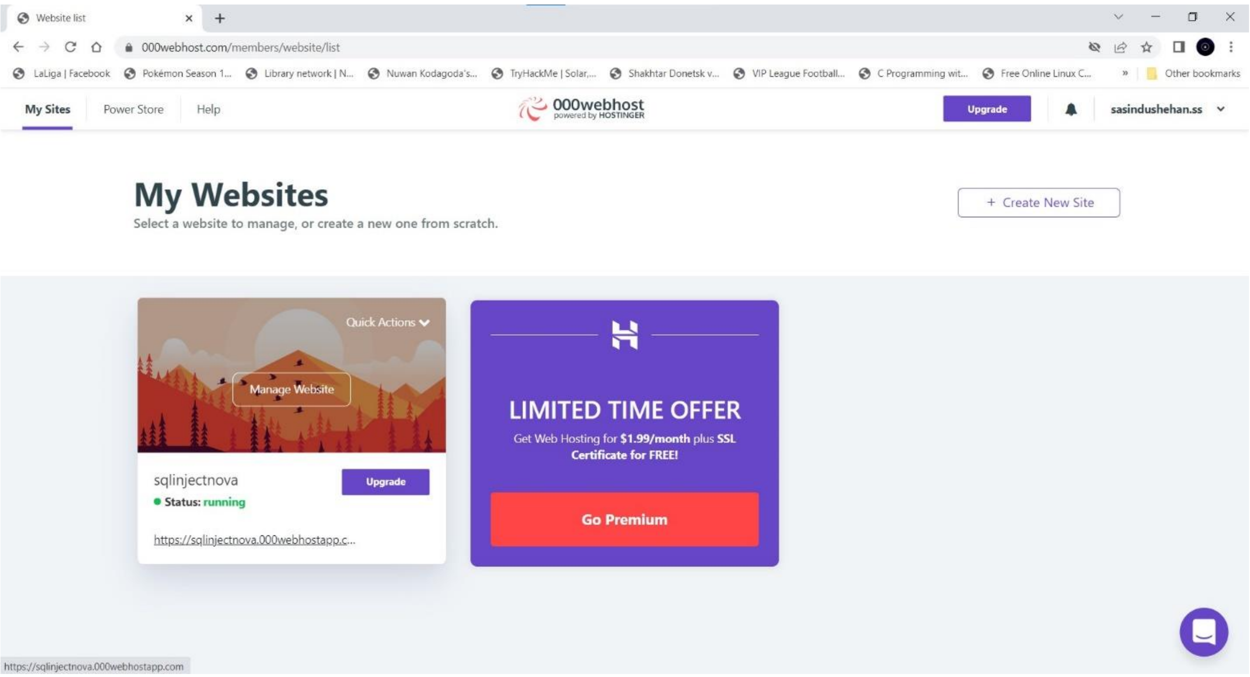
Then using their upload webpage service, the creation of webpages are done manually.


000webhost.com/members/website/list

Here is your tool box

Choose your weapon of mass creation

Figure 19


000webhost.com/members/website/list

My Websites

Select a website to manage, or create a new one from scratch.

sqlinjectnova

● Status: running

https://sqlinjectnova.000webhostapp.c...

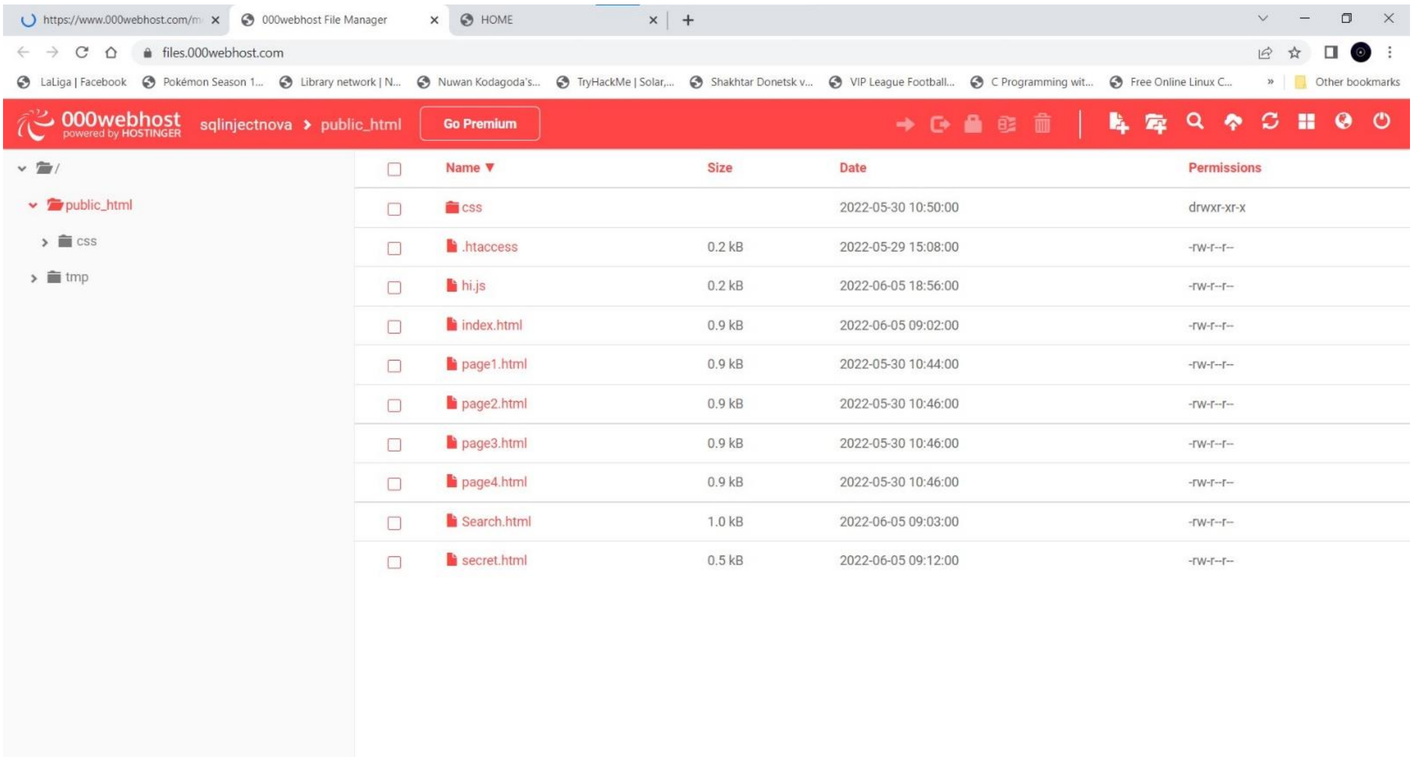
LIMITED TIME OFFER

Get Web Hosting for **$1.99/month** plus **SSL Certificate for FREE!**

https://sqlinjectnova.000webhostapp.com

Figure 20

Seven html pages and one java script page is created.



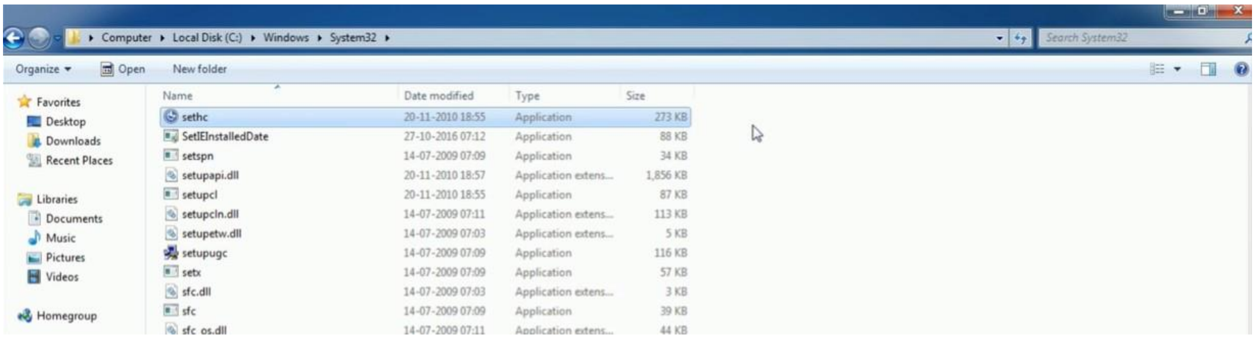
□	Name ▼	Size	Date	Permissions
□	css		2022-05-30 10:50:00	drwxr-xr-x
□	.htaccess	0.2 kB	2022-05-29 15:08:00	-rw-r--r--
□	hi.js	0.2 kB	2022-06-05 18:56:00	-rw-r--r--
□	index.html	0.9 kB	2022-06-05 09:02:00	-rw-r--r--
□	page1.html	0.9 kB	2022-05-30 10:44:00	-rw-r--r--
□	page2.html	0.9 kB	2022-05-30 10:46:00	-rw-r--r--
□	page3.html	0.9 kB	2022-05-30 10:46:00	-rw-r--r--
□	page4.html	0.9 kB	2022-05-30 10:46:00	-rw-r--r--
□	Search.html	1.0 kB	2022-06-05 09:03:00	-rw-r--r--
□	secret.html	0.5 kB	2022-06-05 09:12:00	-rw-r--r--

Figure 21

Windows 7

Windows 7 is used to implement the back door vulnerability in the CTF. The sticky key function on windows is replaced by a command prompt here

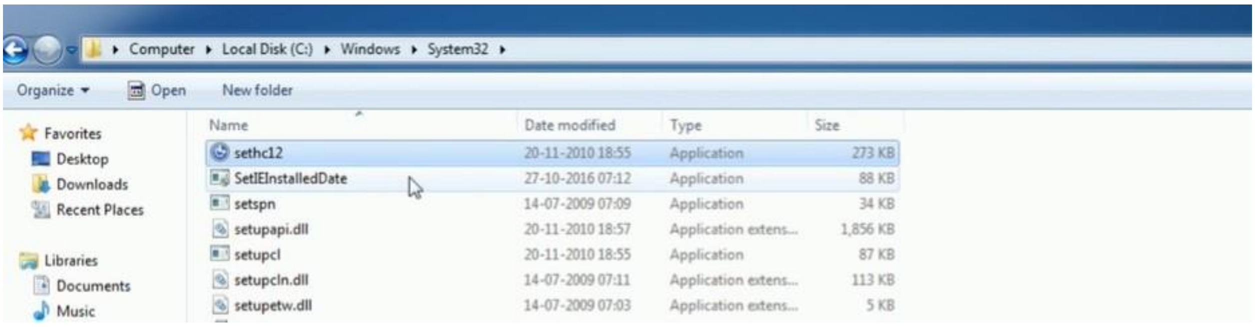
First the “sethc.exe” file in System32 folder (in windows folder) is copied to C drive



Name	Date modified	Type	Size
sethc	20-11-2010 18:55	Application	273 KB
SetIEInstalledDate	27-10-2016 07:12	Application	88 KB
setspn	14-07-2009 07:09	Application	34 KB
setupapi.dll	20-11-2010 18:57	Application extens...	1,856 KB
setupcl	20-11-2010 18:55	Application	87 KB
setupcln.dll	14-07-2009 07:11	Application extens...	113 KB
setupetw.dll	14-07-2009 07:03	Application extens...	5 KB
setupugc	14-07-2009 07:09	Application	116 KB
setx	14-07-2009 07:09	Application	57 KB
sfc.dll	14-07-2009 07:03	Application extens...	3 KB
sfc	14-07-2009 07:09	Application	39 KB
sfc_os.dll	14-07-2009 07:11	Application extens...	44 KB

Figure 22

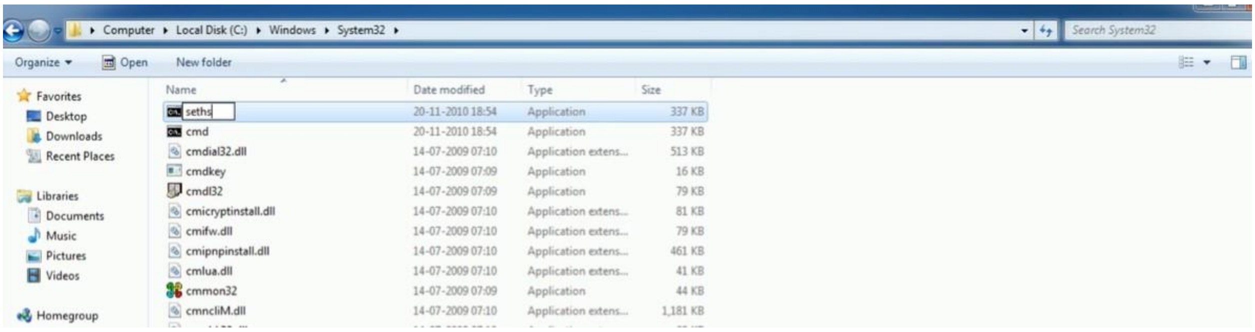
Then rename the “sethc.exe” file to any name (sethc12), the permission to this must be granted before renaming (full control).



Name	Date modified	Type	Size
sethc12	20-11-2010 18:55	Application	273 KB
SetIEInstalledDate	27-10-2016 07:12	Application	88 KB
setspn	14-07-2009 07:09	Application	34 KB
setupapi.dll	20-11-2010 18:57	Application extens...	1,856 KB
setupcl	20-11-2010 18:55	Application	87 KB
setupcln.dll	14-07-2009 07:11	Application extens...	113 KB
setupetw.dll	14-07-2009 07:03	Application extens...	5 KB

Figure 23

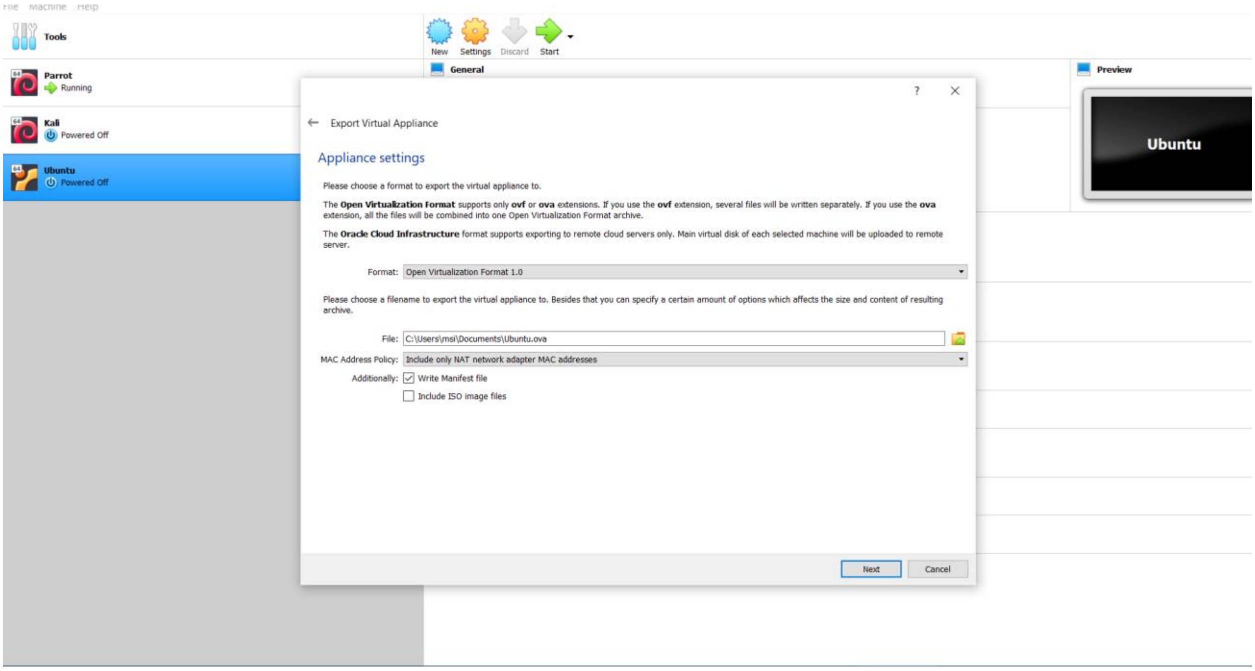
Next create another copy of the “cmd.exe” file and rename it as “sethc.exe”



Name	Date modified	Type	Size
seths	20-11-2010 18:54	Application	337 KB
cmd	20-11-2010 18:54	Application	337 KB
cmdial32.dll	14-07-2009 07:10	Application extens...	513 KB
cmdkey	14-07-2009 07:09	Application	16 KB
cmdl32	14-07-2009 07:09	Application	79 KB
cmicryptinstall.dll	14-07-2009 07:10	Application extens...	81 KB
cmifw.dll	14-07-2009 07:10	Application extens...	79 KB
cmipnpinstall.dll	14-07-2009 07:10	Application extens...	461 KB
cmlua.dll	14-07-2009 07:10	Application extens...	41 KB
cmmon32	14-07-2009 07:09	Application	44 KB
cmncliM.dll	14-07-2009 07:10	Application extens...	1,181 KB

Figure 24

Exported virtual machines in ova format



Export Virtual Appliance

Appliance settings

Please choose a format to export the virtual appliance to.

The **Open Virtualization Format** supports only **ovf** or **ova** extensions. If you use the **ovf** extension, several files will be written separately. If you use the **ova** extension, all the files will be combined into one Open Virtualization Format archive.

The **Oracle Cloud Infrastructure** format supports exporting to remote cloud servers only. Main virtual disk of each selected machine will be uploaded to remote server.

Format: Open Virtualization Format 1.0

Please choose a filename to export the virtual appliance to. Besides that you can specify a certain amount of options which affects the size and content of resulting archive.

File: C:\Users\msi\Documents\Ubuntu.ova

MAC Address Policy: Include only NAT network adapter MAC addresses

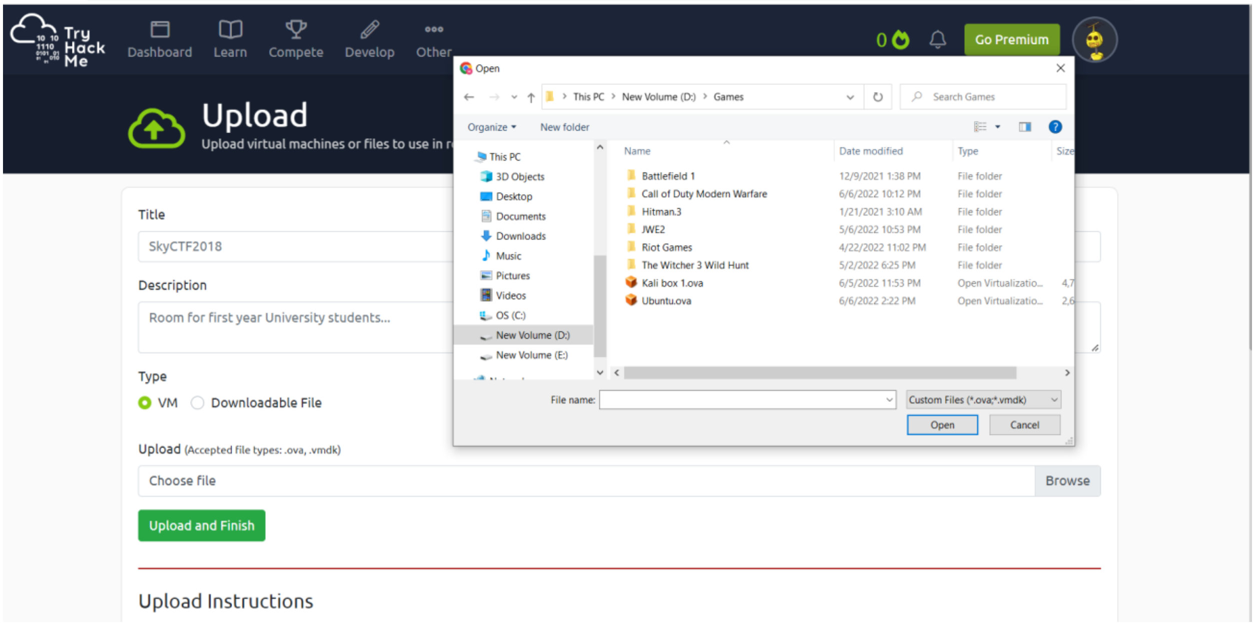
Additionally: ☑ Write Manifest file

□ Include ISO image files

Next Cancel

Figure 25

Then uploaded the ova files to the tryhackme



Upload

Upload virtual machines or files to use in r

Name	Date modified	Type	Size
Battlefield 1	12/9/2021 1:38 PM	File folder	
Call of Duty Modern Warfare	6/6/2022 10:12 PM	File folder	
Hitman.3	1/21/2021 3:10 AM	File folder	
JWE2	5/6/2022 10:53 PM	File folder	
Riot Games	4/22/2022 11:02 PM	File folder	
The Witcher 3 Wild Hunt	5/2/2022 6:25 PM	File folder	
Kali box 1.ova	6/5/2022 11:53 PM	Open Virtualizatio...	4,7
Ubuntu.ova	6/6/2022 2:22 PM	Open Virtualizatio...	2,6

File name:

Custom Files (*.ova;*.vmdk)

Title: SkyCTF2018

Description: Room for first year University students...

Type: ● VM ○ Downloadable File

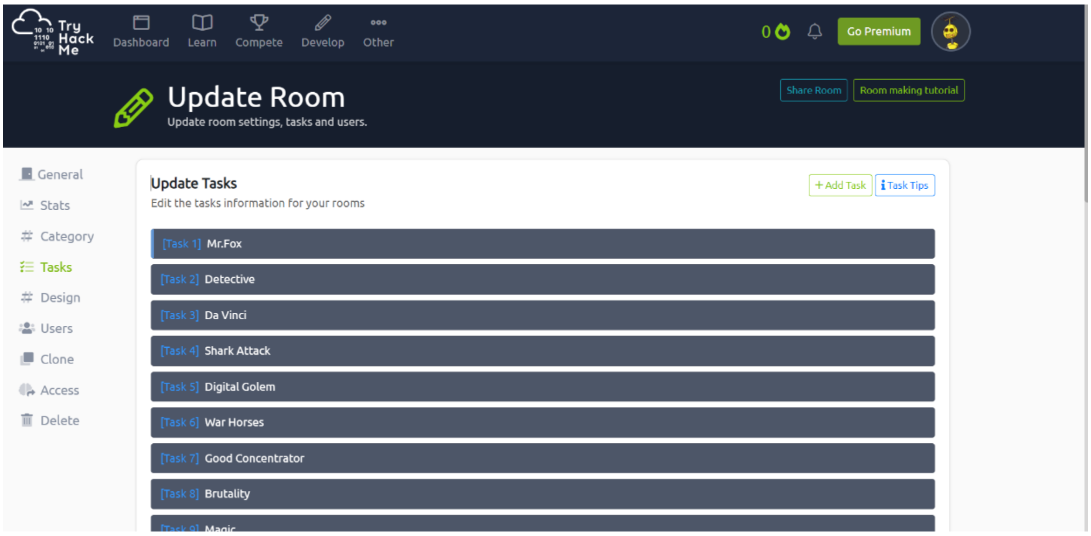
Upload (Accepted file types: .ova, .vmdk)

Choose file

Upload Instructions

Figure 26

Created tasks in tryhackme in early developed room



Update Room

Update room settings, tasks and users.

Update Tasks

Edit the tasks information for your rooms

[Task 1] Mr.Fox

[Task 2] Detective

[Task 3] Da Vinci

[Task 4] Shark Attack

[Task 5] Digital Golem

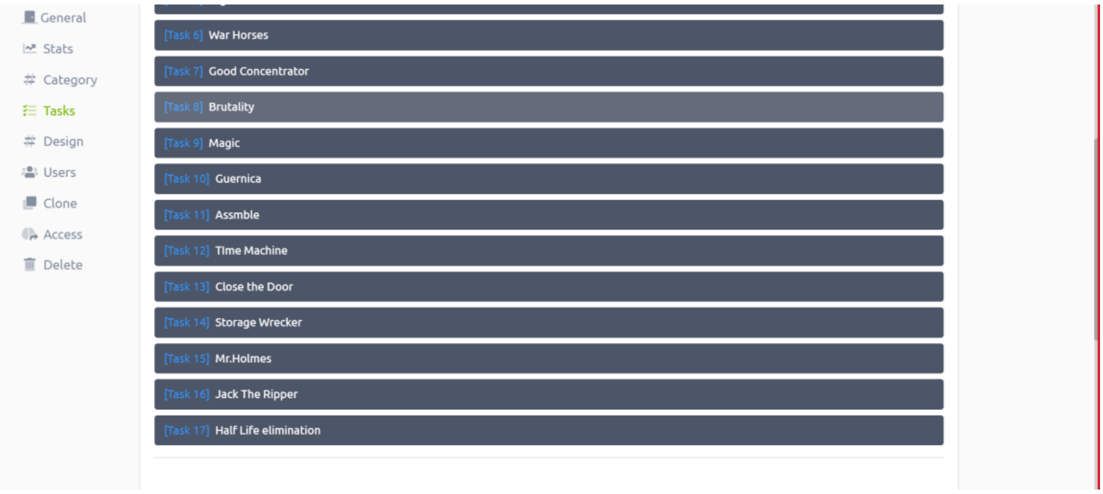
[Task 6] War Horses

[Task 7] Good Concentrator

[Task 8] Brutality

[Task 9] Magic

Figure 27



- General
- Stats
- Category
- Tasks
- Design
- Users
- Clone
- Access
- Delete

[Task 6] War Horses

[Task 7] Good Concentrator

[Task 8] Brutality

[Task 9] Magic

[Task 10] Guernica

[Task 11] Assmble

[Task 12] Time Machine

[Task 13] Close the Door

[Task 14] Storage Wrecker

[Task 15] Mr.Holmes

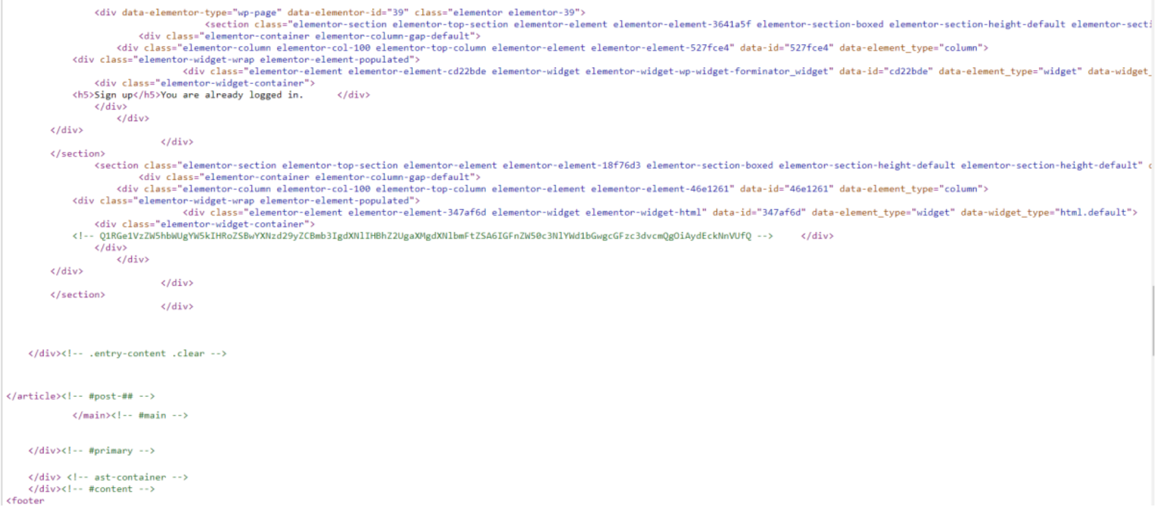
[Task 16] Jack The Ripper

[Task 17] Half Life elimination

Figure 28

Step1 implementation

Encoded the username and passwords for the agent user and hide the encoded text in the signup page source by adding the text as a comment.



```
                <div data-elementor-type="wp-page" data-elementor-id="39" class="elementor elementor-39">
                                <section class="elementor-section elementor-top-section elementor-element elementor-element-3641a5f elementor-section-boxed elementor-section-height-default elementor-secti
                        <div class="elementor-container elementor-column-gap-default">
                    <div class="elementor-column elementor-col-100 elementor-top-column elementor-element elementor-element-527fce4" data-id="527fce4" data-element_type="column">
            <div class="elementor-widget-wrap elementor-element-populated">
                            <div class="elementor-element elementor-element-cd22bde elementor-widget elementor-widget-wp-widget-forminator_widget" data-id="cd22bde" data-element_type="widget" data-widget_
                <div class="elementor-widget-container">
            <h5>Sign up</h5>You are already logged in.      </div>
                </div>
                    </div>
        </div>
                            </div>
        </section>
                <section class="elementor-section elementor-top-section elementor-element elementor-element-18f76d3 elementor-section-boxed elementor-section-height-default elementor-section-height-default" c
                        <div class="elementor-container elementor-column-gap-default">
                    <div class="elementor-column elementor-col-100 elementor-top-column elementor-element elementor-element-46e1261" data-id="46e1261" data-element_type="column">
            <div class="elementor-widget-wrap elementor-element-populated">
                            <div class="elementor-element elementor-element-347af6d elementor-widget elementor-widget-html" data-id="347af6d" data-element_type="widget" data-widget_type="html.default">
                <div class="elementor-widget-container">
            <!-- Q1RGe1VzZW5hbWUgYW5kIHRoZSBwYXNzd29yZCBmb3IgdXNlIHBhZ2UgaXMgdXNlbmFtZSA6IGFnZW50c3NlYWd1bGwgcGFzc3dvcmQgOiAydEckNnVUfQ -->     </div>
                </div>
                    </div>
        </div>
                            </div>
        </section>
                            </div>


    </div><!-- .entry-content .clear -->


</article><!-- #post-## -->
            </main><!-- #main -->


    </div><!-- #primary -->

    </div> <!-- ast-container -->
    </div><!-- #content -->
<footer
```

Figure 29

Step 2 implementation

Hide the link to the base location map in the background image of the home page using quickstego tool.

Step 3 Implementation

Hide the exact flag for location map using quickstego tool in the image that previously downloaded.

Step 4 Implementation

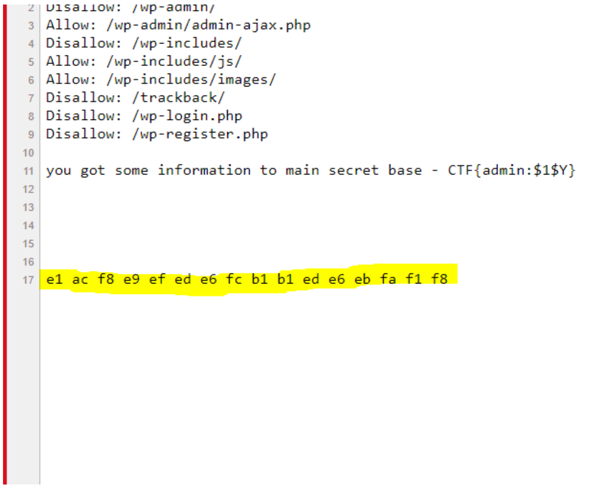
Captured the sent email via SMTP using wireshark.

Step 5 Implementation

Created a robotx.txt and configured the file and hide data in that file.

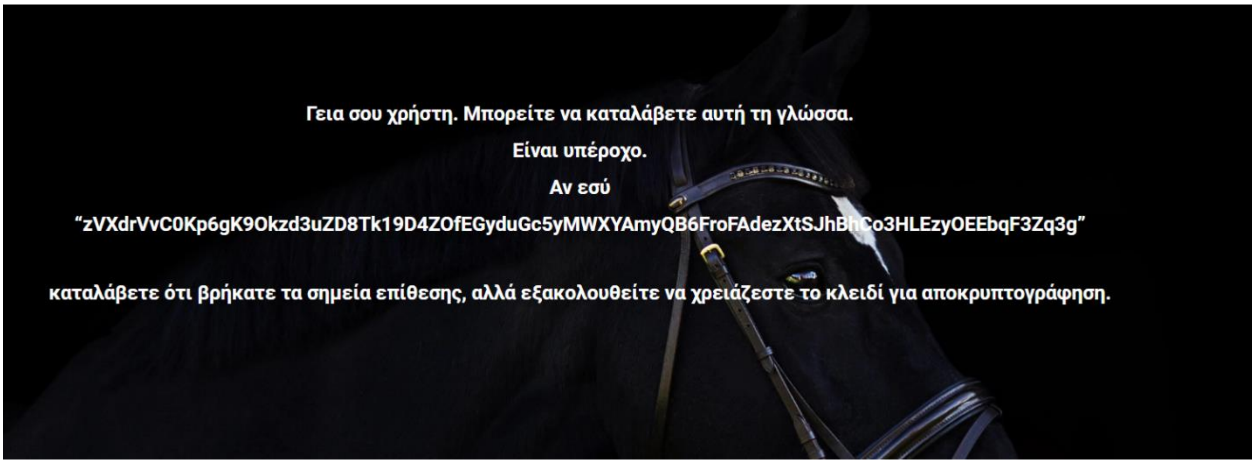
Step 6 Implementation

Encrypted the data using AES and hide the encrypted message in the middle of a paragraph that written in Greek language and put the paragraph and encrypted text in “war horses” web page and converted the key into the hexadecimal and shifted the key by 8 and stored the key in the robots.txt file.



```
Disallow: /wp-admin/
Allow: /wp-admin/admin-ajax.php
Disallow: /wp-includes/
Allow: /wp-includes/js/
Allow: /wp-includes/images/
Disallow: /trackback/
Disallow: /wp-login.php
Disallow: /wp-register.php

you got some information to main secret base - CTF{admin:$1$Y}





e1 ac f8 e9 ef ed e6 fc b1 b1 ed e6 eb fa f1 f8
```

Figure 30 key



Γεια σου χρήστη. Μπορείτε να καταλάβετε αυτή τη γλώσσα.

Είναι υπέροχο.

Αν εσύ

“zVXdrVvC0Kp6gK9Okzd3uZD8Tk19D4ZOfEGyduGc5yMWXYAmyQB6FroFAdezXtSJhBhCo3HLEzyOEEbqF3Zq3g”

καταλάβετε ότι βρήκατε τα σημεία επίθεσης, αλλά εξακολουθείτε να χρειάζεστε το κλειδί για αποκρυπτογράφηση.

Figure 31 encrypted text

Step 7 Implementation

Created a file that contain the CTF flag data in a pen drive and captured the memory from FTK Imager, and stored the mem file in war horses web page. The file names are given to users.

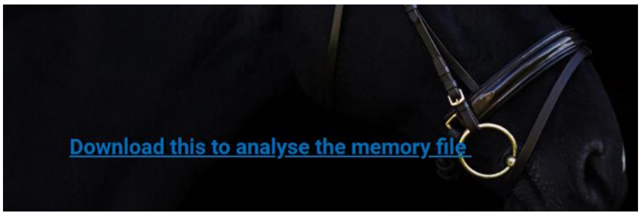
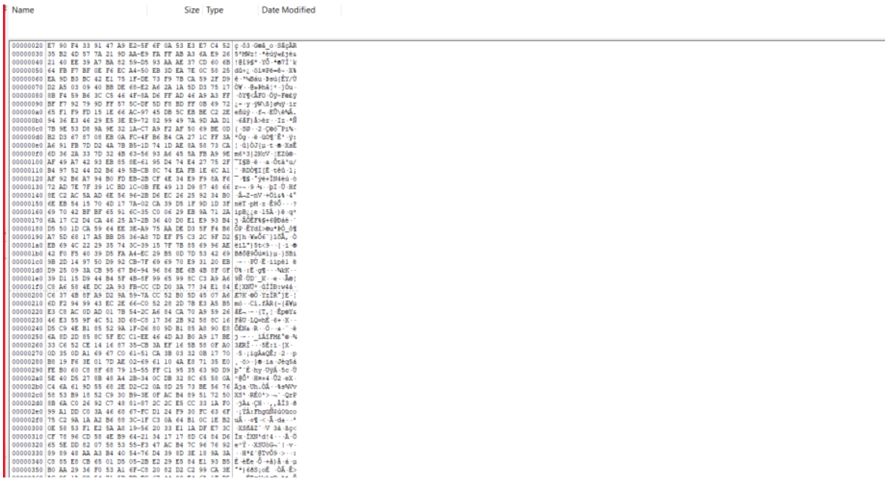


Figure 32 link to mem file



```
00000020 E7 90 F4 33 91 47 A9 E2-5F 6F 0A 53 E3 E7 C4 52 ç·ô3·Gâ_o·SãçÄR
00000030 35 B2 4D 57 7A 21 9D AA-E9 FA FF AB A3 6A E9 26 5²MWz!·ªéúÿ«£jé&
00000040 21 40 EE 39 A7 BA 82 59-D5 93 AA AE 37 CD 60 6B !@î9§º·YÕ·ª®7Í`k
00000050 64 FB F7 BF 0E F6 EC A4-50 EB 3D EA 7E 0C 58 25 dû÷¿·öì¤Pë=ê~·X%
00000060 EA 9D B3 BC 42 E1 75 1F-DE 73 F9 7B CA 59 2F D9 ê·³¼Báu·Þsù{ÊY/Ù
00000070 D2 A5 03 09 40 BB DE 68-E2 A6 2A 1A 5D D3 75 17 Ò¥··@»Þhâ¦*·]Óu·
00000080 8B F4 59 B6 3C C5 46 4F-8A D6 FF AD 46 A9 A3 FF ·ôY¶<ÅFO·ÖÿF©£ÿ
00000090 BF F7 92 79 9D FF 57 5C-DF 5D F8 BD FF 0B 69 72 ¿÷·y·ÿW\ß]ø½ÿ·ir
000000a0 65 F1 F9 FD 15 1E 66 AC-97 45 DB 5C EB BE C2 2E eñùý··f¬·EÛ\ë¾Â.
000000b0 94 36 E3 46 29 E5 3E E9-72 82 99 49 7A 9D AA D1 ·6ãF)å>ér··Iz·ªÑ
000000c0 7B 9E 53 D8 9A 9E 32 1A-C7 A9 F2 AF 50 69 BE 0D {·SØ··2·Ç©ò¯Pi¾·
000000d0 B2 D3 67 87 08 EB 0A FC-4F B6 B4 CA 27 1C FF 3A ²Óg··ë·üO¶´Ê'·ÿ:
000000e0 A6 91 FB 7D D2 4A 7B B5-1D 74 1D AE 8A 58 73 CA ¦·û}ÒJ{µ·t·®·XsÊ
000000f0 6D 36 2A 33 7D 32 4B 63-56 93 A6 45 5A FB A9 9E m6*3}2KcV·¦EZû©·
00000100 AF 49 A7 42 93 EB 85 8E-61 95 D4 74 E4 27 75 2F ¯I§B·ë··a·Ôtä'u/
00000110 B4 97 52 44 D2 B6 49 5B-CB 8C 74 EA FB 1E 6C A1 ´·RDÒ¶I[Ë·têû·l¡
00000120 AF 92 B6 A7 94 B0 FD EB-2B CF 4E 34 E9 F9 8A F6 ¯·¶§·°ýë+ÏN4éù·ö
00000130 72 AD 7E 7F 39 1C BD 1C-0B FE 49 13 D9 87 48 66 r~·9·½··þI·Ù·Hf
00000140 8E C2 AC 5A AD 6E 56 96-2B D6 EC 26 25 92 34 B0 ·Â¬ZnV·+Öì&%·4°
00000150 6E EB 54 15 70 4D 17 7A-02 CA 39 D5 1F 9D 1D 3F nëT·pM·z·Ê9Õ···?
00000160 69 70 42 BF BF 65 91 6C-35 C0 06 29 EB 9A 71 2A ipB¿¿e·l5À·)ë·q*
00000170 6A 17 C2 D4 CA 46 25 A7-2B 36 40 D0 E1 E9 93 B4 j·ÂÔÊF%§+6@Ðáé·´
00000180 D5 50 1D CA 59 64 EE 3E-A9 75 AA DE D3 5F F4 B6 ÕP·ÊYdî>©uªÞÓ_ô¶
00000190 A7 5D 68 17 A5 BB D5 36-A8 7D EF F5 C3 2C 9F D2 §]h·¥»Õ6¨}ïõÃ,·Ò
000001a0 EB 69 4C 22 29 35 74 3C-39 15 7F 7B 85 69 96 AE ëiL")5t<9··{·i·®
000001b0 42 F0 F5 40 39 D5 FA A4-EC 29 B5 0D 7D 53 42 69 Bðõ@9Õú¤ì)µ·}SBi
000001c0 9B 2D 14 97 50 D9 92 CB-7F 69 69 70 E9 31 20 EB ·-··PÙ·Ë·iipé1 ë
000001d0 D9 25 09 3A CB 95 67 B6-94 96 86 BE 6B 4B 8F 0F Ù%·:Ë·g¶···¾kK··
000001e0 39 D1 15 D9 44 B4 5F 4B-8F 99 65 99 8C C3 A9 A6 9Ñ·ÙD´_K··e··Ã©¦
000001f0 C8 A6 58 4E DC 2A 93 FB-CC CD D0 3A 77 34 E1 84 È¦XNÜ*·ûÌÍÐ:w4á·
00000200 C6 37 4B 8F A9 D2 9A 59-7A CC 52 B0 5D 45 07 A6 Æ7K·©Ò·YzÌR°]E·¦
00000210 6D F2 94 99 43 EC 2E 66-C0 52 28 2D 7B E3 A5 B5 mò··Cì.fÀR(-{ã¥µ
00000220 E3 C8 AC 0D AD 01 7B 54-2C A6 84 CA 70 A9 59 26 ãÈ¬··{T,¦·Êp©Y&
00000230 46 E3 55 9F 4C 51 3D 68-C8 17 36 2B 92 58 8C 16 FãU·LQ=hÈ·6+·X··
00000240 D5 C9 4E B1 85 52 9A 1F-D6 80 9D B1 85 A8 90 E8 ÕÉN±·R··Ö··±·¨·è
00000250 6A 8D 2D 85 8C 5F EC C1-EE 46 4D A3 B0 A9 17 BE j·-··_ìÁîFM£°©·¾
00000260 33 C6 52 CE 14 16 87 35-CB 3A EF 16 5B 58 0F A0 3ÆRÎ···5Ë:ï·[X· 
00000270 0D 35 0D A1 69 67 C0 61-51 CA 3B 03 32 0B 17 70 ·5·¡igÀaQÊ;·2··p
00000280 B8 19 F6 3E 01 7D AE 02-69 61 10 4A E8 71 35 E0 ¸·ö>·}®·ia·Jèq5à
00000290 FE B0 60 C8 8F 68 79 15-55 FF C1 95 35 63 9D D9 þ°`È·hy·UÿÁ·5c·Ù
000002a0 5E 40 D5 27 8B 48 A4 2B-34 0C DB 32 8C 65 58 0A ^@Õ'·H¤+4·Û2·eX·
000002b0 C4 6A 61 9D 55 68 2E D2-C2 0A 8D 25 73 BE 56 76 Äja·Uh.ÒÂ··%s¾Vv
000002c0 58 53 B9 18 52 C9 30 B9-3E 0F AC B4 89 51 72 50 XS¹·RÉ0¹>·¬´·QrP
000002d0 8B 6A C0 26 92 C7 48 81-87 2C 2C E5 CC 33 1A F0 ·jÀ&·ÇH··,,åÌ3·ð
000002e0 99 A1 DD C0 3A 46 68 67-FC D1 24 F9 30 FC 63 6F ·¡ÝÀ:FhgüÑ$ù0üco
000002f0 75 C2 9A 1A A2 B6 88 3C-1F C3 0A 64 B1 0C 1E B2 uÂ··¢¶·<·Ã·d±··²
00000300 0E 58 53 F1 E2 5A A8 19-56 20 33 E1 1A DF E7 3C ·XSñâZ¨·V 3á·ßç<
00000310 CF 78 96 CD 58 4E B9 64-21 34 17 17 8D C4 84 D6 Ïx·ÍXN¹d!4···Ä·Ö
00000320 65 5E DD 82 07 58 53 55-F3 47 AC B4 7C 96 76 92 e^Ý··XSUóG¬´|·v·
00000330 89 89 48 AA A3 B4 40 54-76 D4 39 8D 3E 18 9A 3A ··Hª£´@TvÔ9·>··:
00000340 C8 85 E8 CB 65 01 D5 05-2B E2 29 E5 84 E1 93 B5 È·èËe·Õ·+â)å·á·µ
00000350 B0 AA 29 36 F0 53 A1 6F-C8 20 82 D2 C2 99 CA 3E °ª)6ðS¡oÈ ·ÒÂ·Ê>
```

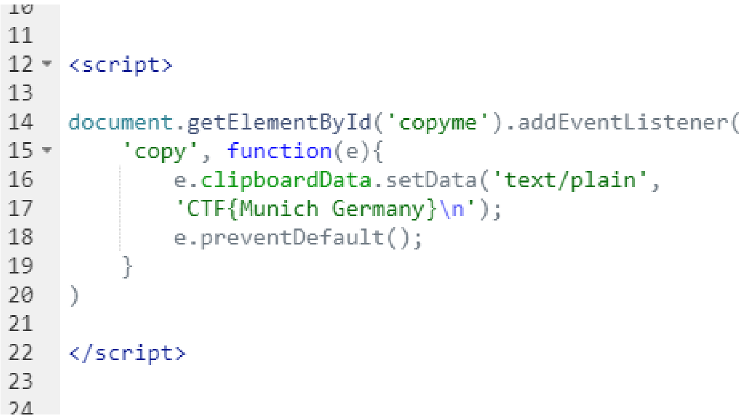
Figure 33 mem file analysys

Step 8 Implementation

Make user “Operative” and give privileges to specific pages and gave password and username files to users to bruteforce the login page of website using wp scan.

Step 9 Implementation

Created a Javascript file and hide the flag in that file, when a user copy the specific paragraph that is given by the Javascript program it pastes the Flag instead of copied text.



```


<script>

document.getElementById('copyme').addEventListener(
    'copy', function(e){
        e.clipboardData.setData('text/plain',
        'CTF{Munich Germany}\n');
        e.preventDefault();
    }
)

</script>

```

Figure 34 Js script

Step 10 Implementation

Hide the flag in an image using S tool and stored the image in the “Painting wall” page, user need to finde the correct painting by given hints and reveal the flag from given hints.

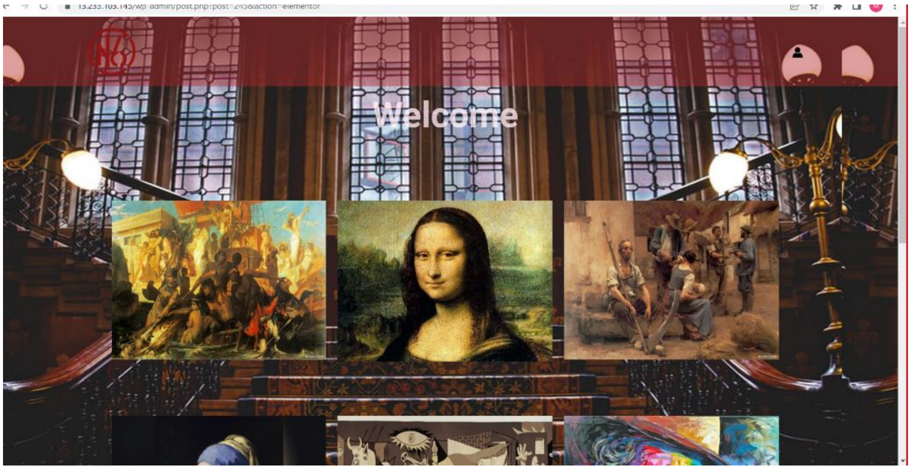
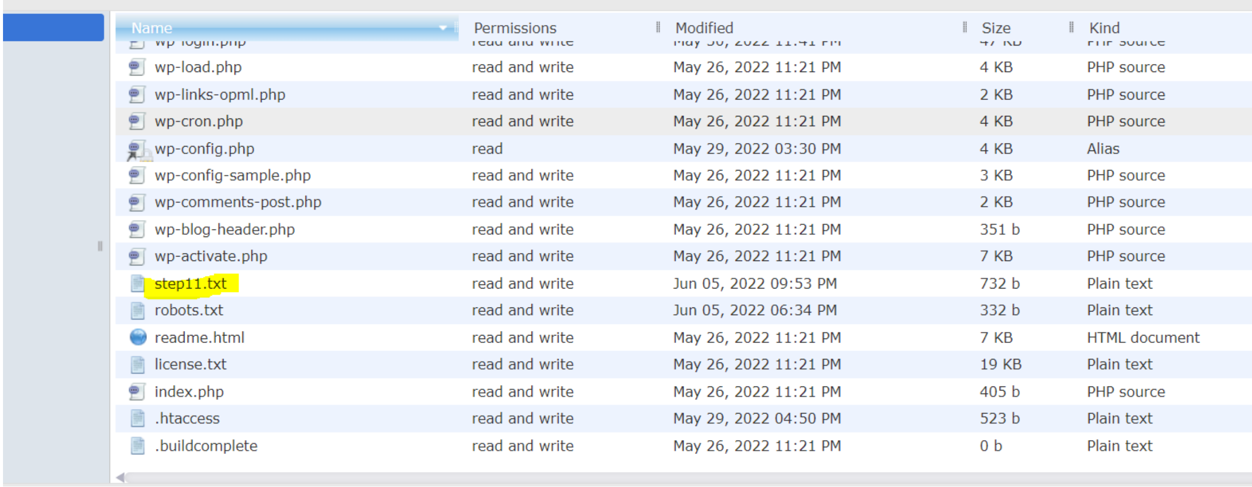


Figure 35 painting wall page

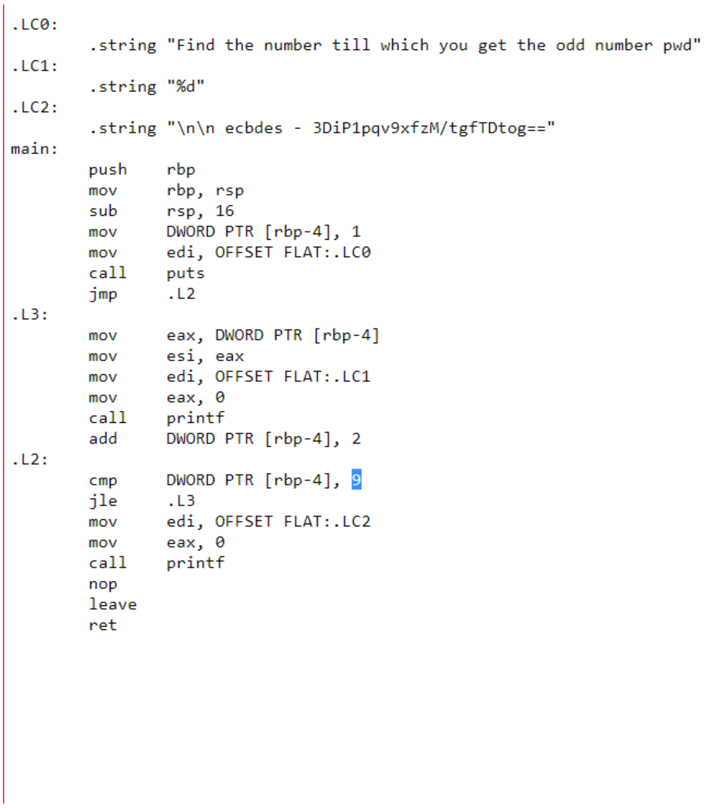
Step 11 implementation

Encrypted the flag using des and stored the flag in a C program as printf(“<flag>”) and created a while loop to generate a key that contains odd number from 1 to 10 and converted the code into assembly and stored the code in step11.txt in website folder.



Name	Permissions	Modified	Size	Kind
wp-login.php	read and write	May 30, 2022 11:41 PM	47 KB	PHP source
wp-load.php	read and write	May 26, 2022 11:21 PM	4 KB	PHP source
wp-links-opml.php	read and write	May 26, 2022 11:21 PM	2 KB	PHP source
wp-cron.php	read and write	May 26, 2022 11:21 PM	4 KB	PHP source
wp-config.php	read	May 29, 2022 03:30 PM	4 KB	Alias
wp-config-sample.php	read and write	May 26, 2022 11:21 PM	3 KB	PHP source
wp-comments-post.php	read and write	May 26, 2022 11:21 PM	2 KB	PHP source
wp-blog-header.php	read and write	May 26, 2022 11:21 PM	351 b	PHP source
wp-activate.php	read and write	May 26, 2022 11:21 PM	7 KB	PHP source
step11.txt	read and write	Jun 05, 2022 09:53 PM	732 b	Plain text
robots.txt	read and write	Jun 05, 2022 06:34 PM	332 b	Plain text
readme.html	read and write	May 26, 2022 11:21 PM	7 KB	HTML document
license.txt	read and write	May 26, 2022 11:21 PM	19 KB	Plain text
index.php	read and write	May 26, 2022 11:21 PM	405 b	PHP source
.htaccess	read and write	May 29, 2022 04:50 PM	523 b	Plain text
.buildcomplete	read and write	May 26, 2022 11:21 PM	0 b	Plain text

Figure 36 step11.txt

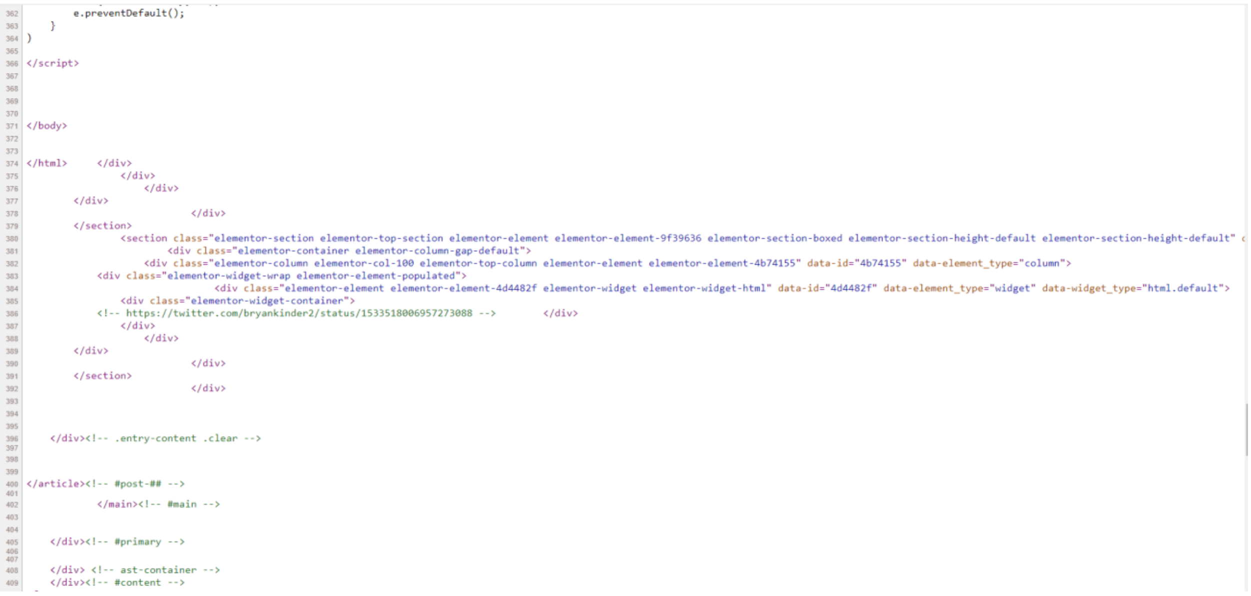


```
.LC0:
        .string "Find the number till which you get the odd number pwd"
.LC1:
        .string "%d"
.LC2:
        .string "\n\n ecbdes - 3DiP1pqv9xfzM/tgfTDtog=="
main:
        push    rbp
        mov     rbp, rsp
        sub     rsp, 16
        mov     DWORD PTR [rbp-4], 1
        mov     edi, OFFSET FLAT:.LC0
        call    puts
        jmp     .L2
.L3:
        mov     eax, DWORD PTR [rbp-4]
        mov     esi, eax
        mov     edi, OFFSET FLAT:.LC1
        mov     eax, 0
        call    printf
        add     DWORD PTR [rbp-4], 2
.L2:
        cmp     DWORD PTR [rbp-4], 9
        jle     .L3
        mov     edi, OFFSET FLAT:.LC2
        mov     eax, 0
        call    printf
        nop
        leave
        ret
```

Figure 37 assembly code

Step 12 Implementation

Uploaded a post in twitter that contains the flag and deleted the post and copied the link and stored it in the painting wall. Users need to retrieve the post using way back machine.



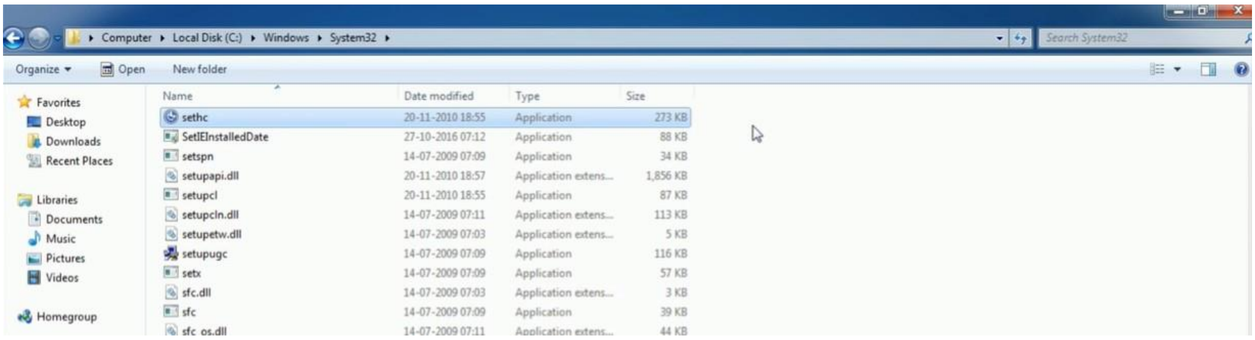
```
        e.preventDefault();
    }
)

</script>



</body>


</html>     </div>
                </div>
                    </div>
        </div>
                            </div>
        </section>
                <section class="elementor-section elementor-top-section elementor-element elementor-element-9f39636 elementor-section-boxed elementor-section-height-default elementor-section-height-default" c
                        <div class="elementor-container elementor-column-gap-default">
                    <div class="elementor-column elementor-col-100 elementor-top-column elementor-element elementor-element-4b74155" data-id="4b74155" data-element_type="column">
            <div class="elementor-widget-wrap elementor-element-populated">
                                <div class="elementor-element elementor-element-4d4482f elementor-widget elementor-widget-html" data-id="4d4482f" data-element_type="widget" data-widget_type="html.default">
                <div class="elementor-widget-container">
            <!-- https://twitter.com/bryankinder2/status/1533518006957273088 -->        </div>
                </div>
                    </div>
        </div>
                            </div>
        </section>
                            </div>



    </div><!-- .entry-content .clear -->



</article><!-- #post-## -->

            </main><!-- #main -->


    </div><!-- #primary -->

    </div> <!-- ast-container -->
    </div><!-- #content -->
```

Figure 38 source code in the painting wall contains deleted post's link

Step 13 Implementation

Windows 7 is used to implement the back door vulnerability in the CTF. The sticky key function on windows is replaced by a command prompt here

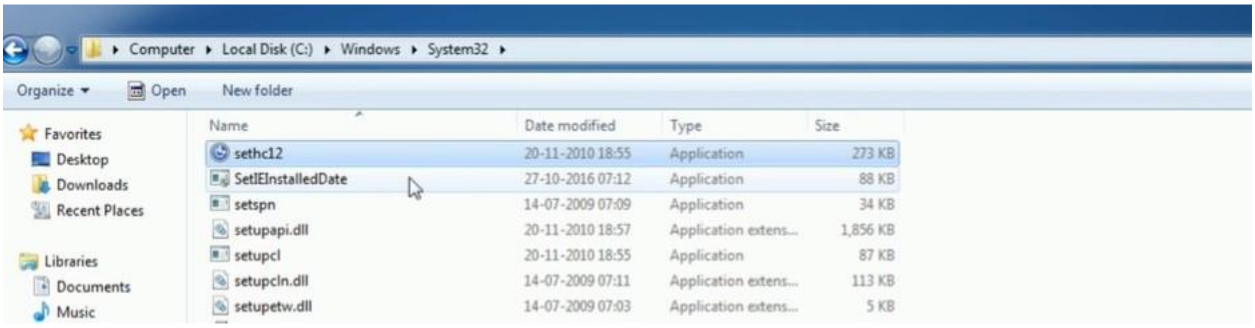
First the "sethc.exe" file in System32 folder (in windows folder) is copied to C drive



Name	Date modified	Type	Size
sethc	20-11-2010 18:55	Application	273 KB
SetIEInstalledDate	27-10-2016 07:12	Application	88 KB
setspn	14-07-2009 07:09	Application	34 KB
setupapi.dll	20-11-2010 18:57	Application extens...	1,856 KB
setupcl	20-11-2010 18:55	Application	87 KB
setupcln.dll	14-07-2009 07:11	Application extens...	113 KB
setupetw.dll	14-07-2009 07:03	Application extens...	5 KB
setupugc	14-07-2009 07:09	Application	116 KB
setx	14-07-2009 07:09	Application	57 KB
sfc.dll	14-07-2009 07:03	Application extens...	3 KB
sfc	14-07-2009 07:09	Application	39 KB
sfc_os.dll	14-07-2009 07:11	Application extens...	44 KB

Figure 39

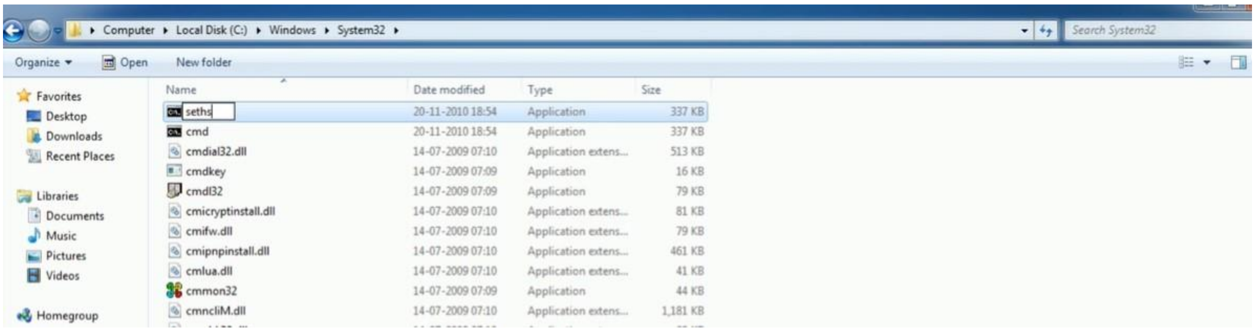
Then rename the “sethc.exe” file to any name (sethc12), the permission to this must be granted before renaming (full control).



Name	Date modified	Type	Size
sethc12	20-11-2010 18:55	Application	273 KB
SetIEInstalledDate	27-10-2016 07:12	Application	88 KB
setspn	14-07-2009 07:09	Application	34 KB
setupapi.dll	20-11-2010 18:57	Application extens...	1,856 KB
setupcl	20-11-2010 18:55	Application	87 KB
setupcln.dll	14-07-2009 07:11	Application extens...	113 KB
setupetw.dll	14-07-2009 07:03	Application extens...	5 KB

Figure 40

Next create another copy of the “cmd.exe” file and rename it as “sethc.exe”



Name	Date modified	Type	Size
seths	20-11-2010 18:54	Application	337 KB
cmd	20-11-2010 18:54	Application	337 KB
cmdial32.dll	14-07-2009 07:10	Application extens...	513 KB
cmdkey	14-07-2009 07:09	Application	16 KB
cmdl32	14-07-2009 07:09	Application	79 KB
cmicryptinstall.dll	14-07-2009 07:10	Application extens...	81 KB
cmifw.dll	14-07-2009 07:10	Application extens...	79 KB
cmipnpinstall.dll	14-07-2009 07:10	Application extens...	461 KB
cmlua.dll	14-07-2009 07:10	Application extens...	41 KB
cmmon32	14-07-2009 07:09	Application	44 KB
cmncliM.dll	14-07-2009 07:10	Application extens...	1,181 KB

Figure 41

Step 14 Implementation

Created a website and hosted in the 000webhost, website consist of 7 html files and 1 js file. Secret.html file contains the hidden information, which is not linked with other pages. Attacker should get the secret.html page using malicious query.

Step 15 Implementation

Created a Instagram account by adding flag information and information in main secret base. User should get the account using sherlock tool. Username is given to players.

\

Step 16 Implementation

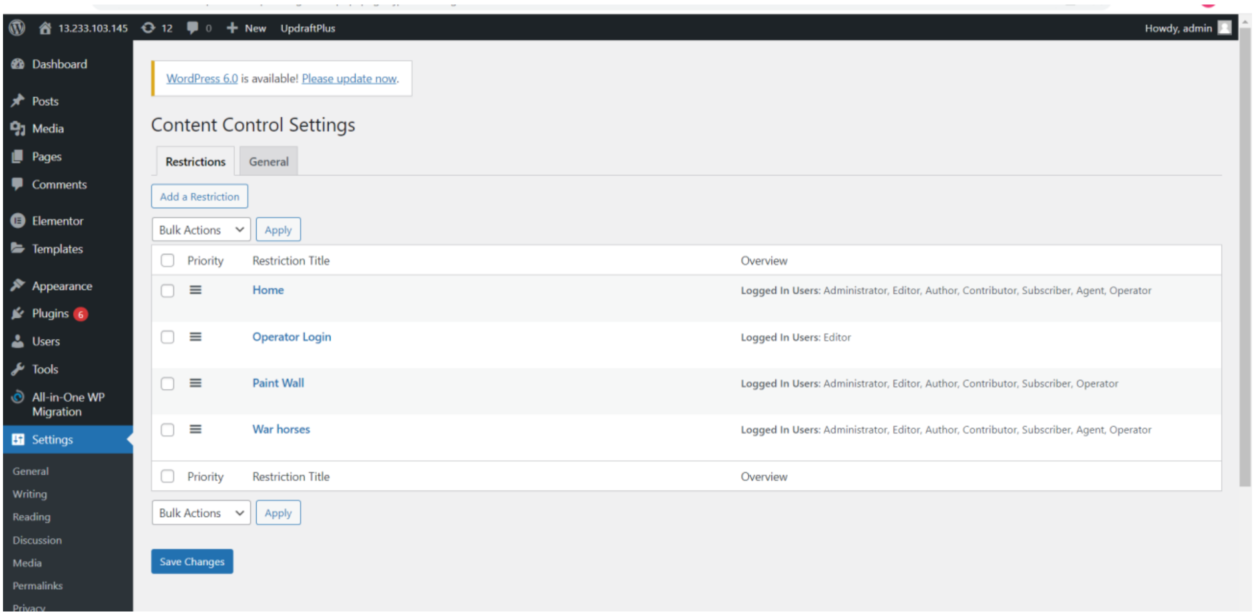
Created a ubuntu box as the main secret base, and guest user credential are given to the players, players need to get the admin login credentials by brute forcing the hash file of the admin’s password that was given in previous steps as fragments. User should use john the ripper tool to do the attack. password list is given to the user.

Step 17 Implementation

After user logged into the ubuntu box as admin they should find the file that contains encrypted text of the virus cure, users should decrypt the text using 3DES and they should use the virus version that was given in the previous steps as fragments as the key to decrypt.

2.4 Testing

As the test phase, checked al the content control mechanism are worked correctly and login pages are working correctly. Also, tested the error redirect page whether the page redirects to the correct location.



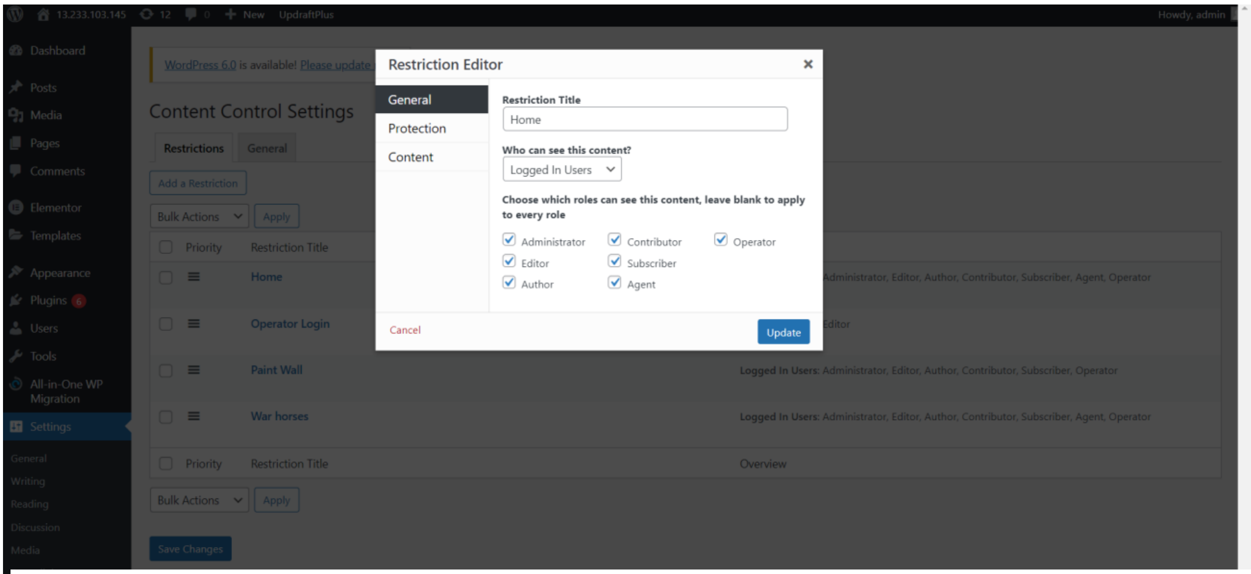
WordPress 6.0 is available! Please update now.

Content Control Settings

Priority	Restriction Title	Overview
≡	Home	**Logged In Users:** Administrator, Editor, Author, Contributor, Subscriber, Agent, Operator
≡	Operator Login	**Logged In Users:** Editor
≡	Paint Wall	**Logged In Users:** Administrator, Editor, Author, Contributor, Subscriber, Operator
≡	War horses	**Logged In Users:** Administrator, Editor, Author, Contributor, Subscriber, Agent, Operator

Figure 42 content manager plugin wordpress

Checked whether the user roles are assigned to users correctly and privileges are configured correctly.



Restriction Editor

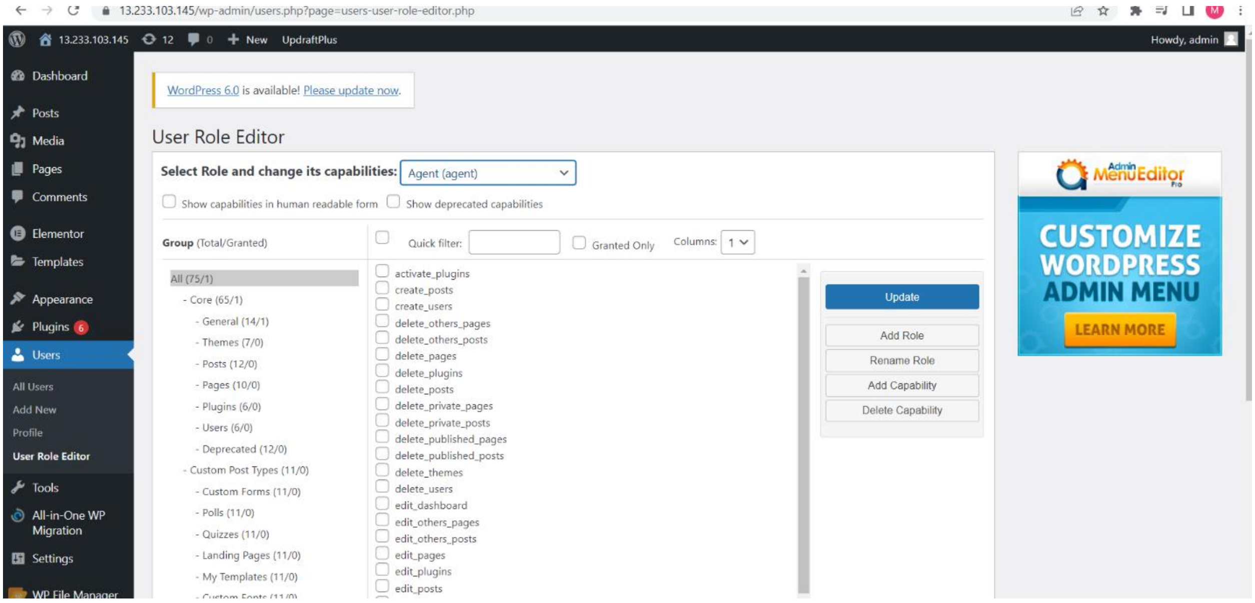
Restriction Title: Home

Who can see this content? Logged In Users

Choose which roles can see this content, leave blank to apply to every role

☑ Administrator ☑ Contributor ☑ Operator
☑ Editor ☑ Subscriber
☑ Author ☑ Agent

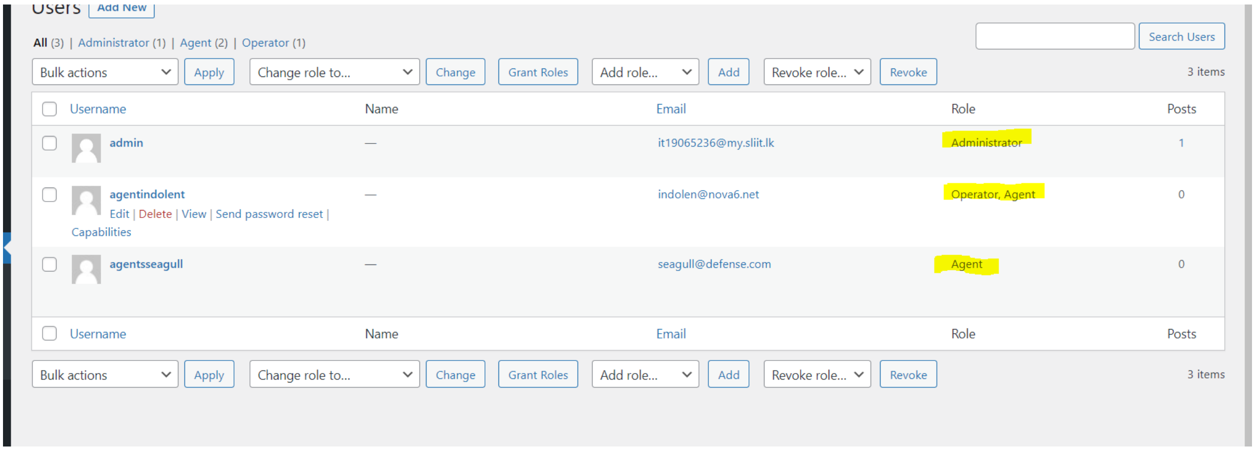
Figure 43 content manager plugin wordpress



Select Role and change its capabilities: Agent (agent)

- □ activate_plugins
- □ create_posts
- □ create_users
- □ delete_others_pages
- □ delete_others_posts
- □ delete_pages
- □ delete_plugins
- □ delete_posts
- □ delete_private_pages
- □ delete_private_posts
- □ delete_published_pages
- □ delete_published_posts
- □ delete_themes
- □ delete_users
- □ edit_dashboard
- □ edit_others_pages
- □ edit_others_posts
- □ edit_pages
- □ edit_plugins
- □ edit_posts

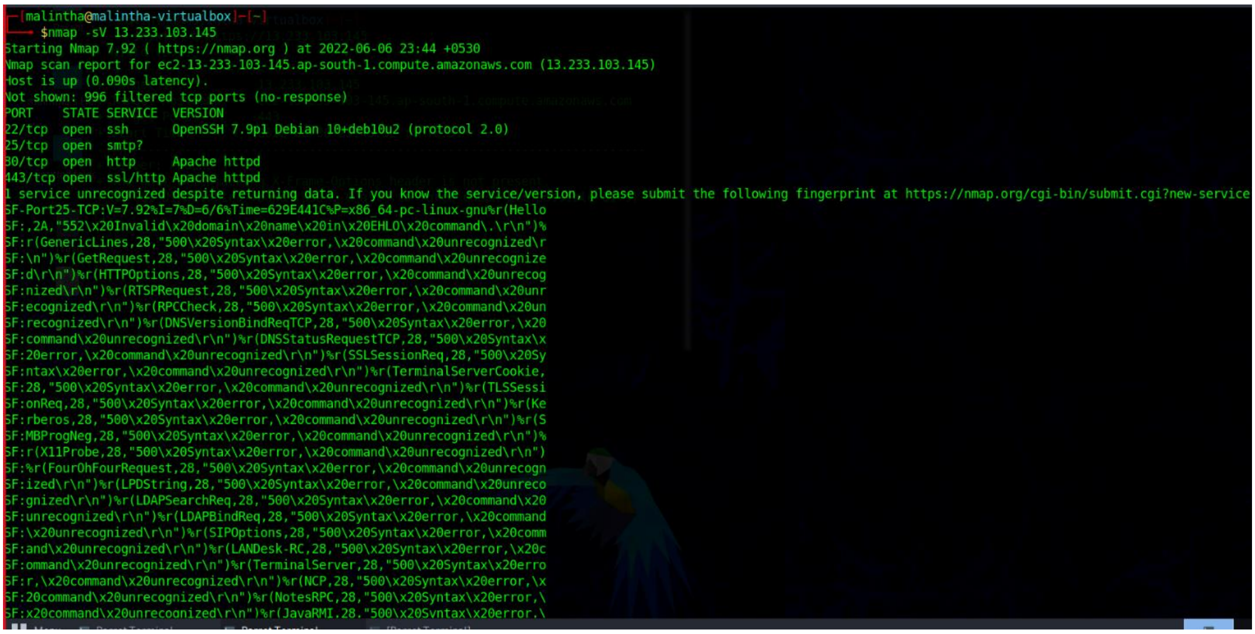
Figure 44



□ Username	Name	Email	Role	Posts
□ admin	—	it19065236@my.sliit.lk	Administrator	1
□ agentindolent	—	indolen@nova6.net	Operator, Agent	0
□ agentsseagull	—	seagull@defense.com	Agent	0
□ Username	Name	Email	Role	Posts

Figure 45

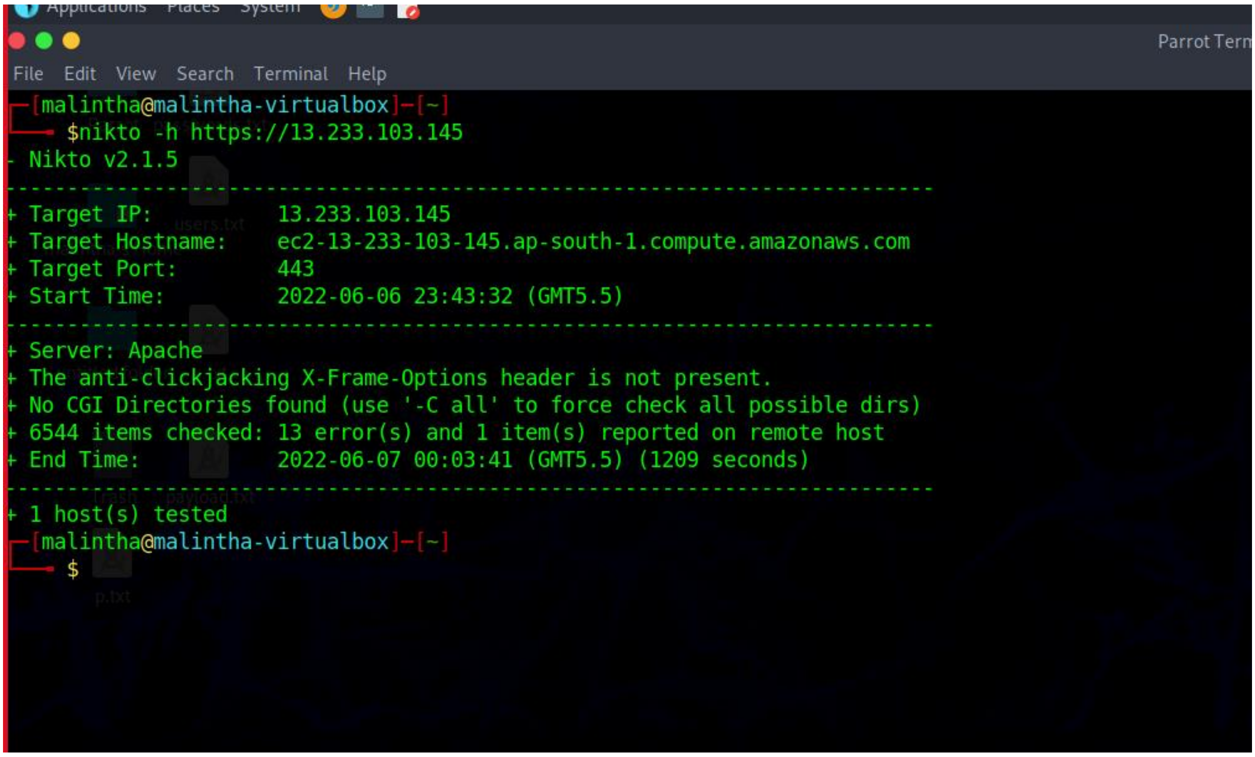
Scanned the website using nmap



```
┌─[malintha@malintha-virtualbox]─[~]
└──╼ $nmap -sV 13.233.103.145
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-06 23:44 +0530
Nmap scan report for ec2-13-233-103-145.ap-south-1.compute.amazonaws.com (13.233.103.145)
Host is up (0.090s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT    STATE SERVICE  VERSION
22/tcp  open  ssh      OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
25/tcp  open  smtp?
80/tcp  open  http     Apache httpd
443/tcp open  ssl/http Apache httpd
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service
SF-Port25-TCP:V=7.92%I=7%D=6/6%Time=629E441C%P=x86_64-pc-linux-gnu%r(Hello
SF:,2A,"552\x20Invalid\x20domain\x20name\x20in\x20EHLO\x20command\.\r\n")%
SF:r(GenericLines,28,"500\x20Syntax\x20error,\x20command\x20unrecognized\r
SF:\n")%r(GetRequest,28,"500\x20Syntax\x20error,\x20command\x20unrecognize
SF:d\r\n")%r(HTTPOptions,28,"500\x20Syntax\x20error,\x20command\x20unrecog
SF:nized\r\n")%r(RTSPRequest,28,"500\x20Syntax\x20error,\x20command\x20unr
SF:ecognized\r\n")%r(RPCCheck,28,"500\x20Syntax\x20error,\x20command\x20un
SF:recognized\r\n")%r(DNSVersionBindReqTCP,28,"500\x20Syntax\x20error,\x20
SF:command\x20unrecognized\r\n")%r(DNSStatusRequestTCP,28,"500\x20Syntax\x
SF:20error,\x20command\x20unrecognized\r\n")%r(SSLSessionReq,28,"500\x20Sy
SF:ntax\x20error,\x20command\x20unrecognized\r\n")%r(TerminalServerCookie,
SF:28,"500\x20Syntax\x20error,\x20command\x20unrecognized\r\n")%r(TLSSessi
SF:onReq,28,"500\x20Syntax\x20error,\x20command\x20unrecognized\r\n")%r(Ke
SF:rberos,28,"500\x20Syntax\x20error,\x20command\x20unrecognized\r\n")%r(S
SF:MBProgNeg,28,"500\x20Syntax\x20error,\x20command\x20unrecognized\r\n")%
SF:r(X11Probe,28,"500\x20Syntax\x20error,\x20command\x20unrecognized\r\n")
SF:%r(FourOhFourRequest,28,"500\x20Syntax\x20error,\x20command\x20unrecogn
SF:ized\r\n")%r(LPDString,28,"500\x20Syntax\x20error,\x20command\x20unreco
SF:gnized\r\n")%r(LDAPSearchReq,28,"500\x20Syntax\x20error,\x20command\x20
SF:unrecognized\r\n")%r(LDAPBindReq,28,"500\x20Syntax\x20error,\x20command
SF:\x20unrecognized\r\n")%r(SIPOptions,28,"500\x20Syntax\x20error,\x20comm
SF:and\x20unrecognized\r\n")%r(LANDesk-RC,28,"500\x20Syntax\x20error,\x20c
SF:ommand\x20unrecognized\r\n")%r(TerminalServer,28,"500\x20Syntax\x20erro
SF:r,\x20command\x20unrecognized\r\n")%r(NCP,28,"500\x20Syntax\x20error,\x
SF:20command\x20unrecognized\r\n")%r(NotesRPC,28,"500\x20Syntax\x20error,\
SF:x20command\x20unrecognized\r\n")%r(JavaRMI,28,"500\x20Syntax\x20error,\
```

Figure 46

Scanned the website using nikto



```
┌─[malintha@malintha-virtualbox]─[~]
└──╼ $nikto -h https://13.233.103.145
- Nikto v2.1.5
---------------------------------------------------------------------------
+ Target IP:          13.233.103.145
+ Target Hostname:    ec2-13-233-103-145.ap-south-1.compute.amazonaws.com
+ Target Port:        443
+ Start Time:         2022-06-06 23:43:32 (GMT5.5)
---------------------------------------------------------------------------
+ Server: Apache
+ The anti-clickjacking X-Frame-Options header is not present.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ 6544 items checked: 13 error(s) and 1 item(s) reported on remote host
+ End Time:           2022-06-07 00:03:41 (GMT5.5) (1209 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
┌─[malintha@malintha-virtualbox]─[~]
└──╼ $
```

Figure 47

3. Evaluation

3.1 Assessment of the Project results

Evaluation of the CTF project involved complete examination of all steps from 1 to 17. These steps were tested together and one at a time. Moreover, evaluation included retrieval of hidden flags and submission of flags dashboard for score computation.

There were few errors in steps that we sorted out and rectified. There were no errors in flag submission and score calculation.

The team had no knowledge about how to build a CTF at the initial stage of the project. Therefore, had to follow tutorials and read articles in internet to find how to build CTF and also had to play CTF boxes to get a knowledge about attacks and exploitations, used Pico CTF to practice CTF challenges. Then since there are both OS and Web based exploitations, choose to create both website and OS, to build the website first used azure but due to some issues mentioned below,

- High security measures
- Web host provides domain default instead of IP address

Therefore, chose AWS to host the website, the first stage was to create steps for the CTF and define how to implement those steps and implemented those steps

3.2 Lessons Learned

Through our project CTF we were able to get professional experience and knowledge on creating and implementing. Furthermore, we were able to learn and familiarize many vulnerability and penetration testing tools, backdoor attacks, brute forcing, website hosting in AWS and 000webhost, WordPress. We faced many challenges in implementing brute force in webpages and overcame them.

3.3 Future Work

Planning to fine tune the CTF and continue the CTF by maintaining the websites and other materials. And planning to create a system that can be hosted in localhost which can be used without AWS. As a team expecting to increase the levels and improve the quality and complexity of the CTF by using modern techniques and modern vulnerability exploitations.

4. Conclusion

The CTF box created with both web base systems and OS bases systems that give users to hand on experience in OS based and Web based hacking. The CTF box consists of 17 levels each levels are interconnected to each other. To get the results of the final level, user need to complete all other levels. The CTF box created based on a hypothetical scenario in Military based system that players are informed to find a cure to a virus called Nova 6.

5. References

[1] "Youtube," [Online]. Available: https://www.youtube.com/watch?v=5qxZj-PbAN0&t=329s. [Accessed 1 06 2022].

[2] "Youtube," [Online]. Available: https://www.youtube.com/watch?v=yynLeBlbujY. [Accessed 04 06 2022].

[3] marco97pa. [Online]. Available: https://marco97pa.github.io/copy-paste-hack-js/. [Accessed 2 05 2022].

[4] A. Gupta, "infosecwriteups.com," 18 01 2022. [Online]. Available: https://infosecwriteups.com/how-to-make-our-own-ctf-challenge-with-ease-6b15f76865b5. [Accessed 10 05 2022].

[5] A. Schaal, "Contrastsecurity.com," 23 04 2020. [Online]. Available: https://www.contrastsecurity.com/security-influencers/tips-tactics-ctf-event. [Accessed 11 05 2022].

[6] "medium.com," 23 09 2020. [Online]. Available: https://thehackersmeetup.medium.com/beginners-guide-to-capture-the-flag-ctf-71a1cbd9d27c. [Accessed 2 06 2022].

Appendix A: Test Results

Link to the walkthrough video :

https://drive.google.com/drive/folders/14DCCv2sThx9co3yF09mgQhMKpH6vehK5?usp=sharing