National College of Ireland

Cloud Security

MSc in Cybersecurity

MSCCYB1_JAN22I

Continuous Assessment

Prateek Pulastya – x21112541

Lecturer: Sean Heeney

Video Link -
https://studentncirl.sharepoint.com/:v:/s/GroupZyberwall/Ef3ehKevbT9JmgJb6RdrnZMBGudtc_1agN5_6yzxPzAciw?e=1e11gz

Presentation Link -
https://studentncirl-my.sharepoint.com/:p:/g/personal/x21112541_student_ncirl_ie/EeZ5yoY9V_FBnArOP-a5_lQBJAmB8ejlyAOyWj_UHkOcYQ?e=ByHuSD

Cloud Security Project

Prateek Pulastya
Msc. In Cybersecurity
National College of Ireland
Dublin, Ireland
x21112541@student.ncirl.ie

***Abstract*— Due to the increasing number of cloud platforms, it is important that the security measures that are implemented by the service providers are thoroughly reviewed and improved in order to prevent attacks. This report aims to provide a comprehensive understanding of the various security measures that are available to the consumers using Amazon Web Services.**

***Keywords*— DNS, AWS, EC2, Encryption, Cloud Security, WordPress.**

I. INTRODUCTION

Due to the increasing popularity of cloud computing, organizations are starting to realize the various advantages it offers. These include the ability to provide their customers with reliable and secure networks, as well as the lower cost of deployment. The competition between cloud providers is also fierce, as these firms are trying to provide their clients with the best possible security.

Cloud computing allows organizations to benefit from the various features and services that are offered by the platform. However, it also comes with a set of security controls and policies that are designed to ensure that the data and systems are protected. To ensure that the security measures are carried out properly, the providers should implement the necessary technologies and procedures. [1]

One of the most important advantages of cloud computing is its ability to provide a variety of services, such as a content delivery network (CDN) and load balancers. These two components work together to provide a faster and more reliable website. They can also prevent distributed denial of service (DDoS) attacks by directing traffic to a different server.

After conducting a comprehensive analysis of the various platforms available in Section III, Amazon Web Services was selected as the preferred cloud provider. The student account was activated, and a pre-built WordPress application was deployed to enhance the security of the cloud infrastructure. Following the implementation of the security measures, the solution was subjected to a dynamic analysis to evaluate its security standing. This method is used to measure the effectiveness of the security measures and identify areas where the solution can improve its security.

The report features four sections: introduction, overview, analysis, and conclusion. The first section covers the basics of cloud security, while the second section explores the multiple risks and vulnerabilities that come with it.

II. CLOUD SETUP

A. *Approach and Cloud Planning*

Amazon Web Services, Google Cloud, and Microsoft Azure are some of the most prominent cloud computing platforms that are known for their offerings. There are other players in the market that are not as well known, such as OpenStack.

These platforms offer various cloud computing services such as Software as a Service, Infrastructure as a Service, and Platform as a Service. They also provide hybrid approaches to address the needs of their customers.

Amazon Web Services, Microsoft Azure, and Google Cloud are the top three cloud providers when it comes to offering their services on a pay-per-minute basis. Organizations can pay for the minutes that they use by using the service, while Google Cloud provides a pay-per-second billing option.

This type of billing option was very beneficial for our research as it allowed us to reduce the number of credits that we have to use for the services. It also prolonged the usage of our resources. The other important factor that we considered when it came to choosing a cloud provider was the market share of these platforms.

Market Share of Cloud Providers in 2022:

Table 1 Market Share

Cloud Provider	Market Share
AWS	34%
Microsoft Azure	22%
Google Cloud	9.5%
Other Providers	34.5%

Figure 1 Market Share of Cloud Providers 2022

After conducting a comprehensive analysis of the various security tools available on Amazon Web Services, it was concluded that implementing security on the platform will be beneficial for most organizations. The tools that were compared were Microsoft Azure, Google Cloud, and AWS. They were able to provide a clear understanding of the tools and their performance.

For this assignment, I am using Amazon Web Services as the platform for my research. In addition to being a cloud platform, AWS also provides a student account.

B. *Tool Selection*

We initially deployed our web application using Amazon Web Services. During the process of deployment, we set up a root account and a user account. We were then presented with various applications and services that could help our application work more effectively.

Amazon EC2 (Elastic Compute Cloud)

Amazon EC2 is a web-based service that enables businesses to run their applications on the Amazon Web Services platform. Developers can also create virtual machines (VMs) that can run on top of Amazon EC2. This allows them to take advantage of the cloud's compute capacity and run their applications on a global scale. [2]

Amazon EC2 offers various features for managing your instances. These include the ability to create and manage multiple types of instances, storage, and networking capacity.

- Amazon EC2 instances are pre-configured with a variety of features, such as the operating system and software. These templates can be used to package the necessary bits for our server. [3]
- We can also use key pairs to secure your login information for Amazon EC2. These are used to store the public and private keys for your instances.
- Amazon EC2 instances can also store volumes for temporary data that can be deleted or changed when you stop, hibernate, or otherwise terminate the service.

Identity and Access management

Amazon Web Services (AWS) Identity and Access Management is a web service that enables you to control the access to your resources. It can be used to create and manage services that restrict the access to certain groups or individuals. This is the most widely used security service in AWS, as it is used to manage the multiple levels of access that users have to the company's services. Having a variety of access controls is very important for organizations as there are many tools and services that require a certain level of access. [4]

We used an identity and access management system known as IAM to configure the accounts for our users. This allows us to control and restrict the access to the application. It also helps us maintain the security of the system. One of the most important factors that we considered when implementing this system was the ability to hold the attacker accountable for any changes that might harm the application. [5]

- Password policies were created to make it harder for users to access accounts.
- They require a minimum of eight characters, and users are not allowed to continue using a default one.
- The length of the password is set to eight characters, and it must include at least one special character and a number.
- The password will remain valid for 90 days.

Encryption

Amazon Web Services (AWS) e-commerce platform (EBS) encryption is a straightforward way to protect your EC2 instances' resources. Unlike other solutions, it doesn't require you to build, maintain, and secure a dedicated key management infrastructure. With Amazon EBS encryption, you can create and manage volumes and backups using the Amazon Key Management Service (KMS).

The servers that host EC2 instances are equipped with encryption capabilities. This ensures that the data-at-rest and the data-in-transit between the instances are secure.

Instances

Amazon EC2 is a fast and easy way to build and deploy applications. Unlike other platforms, it doesn't require you to spend a lot of money on hardware to get started. You can launch as many virtual servers as you need, manage storage, and secure your networks.

Amazon EC2 has a wide variety of instance types that are designed to meet different needs. These types of instances can be used for various applications. You can choose the appropriate combination of resources for your needs.

Table 2 Description

Name	Wordpress Blog
Instance Type	t2.micro
CPU	1 vCPU
Storage	10 GiB SSD
Instance	Amazon Linux
Zone	North Virginia (us-east-1b)

Figure 2 Instance Details

The instance is hosted in North Virginia's US-EAST-1B region and is named as Wordpress Blog. It has 1 vCPU and 10 GiB of storage.

Table 3 Networking Config

IPv4 Networking	
Public Ip	3.92.101.70
Private IP	172.31.86.120

Figure 3 Configuration

I have a static IP of 3.92.101.70 for our application. This ensures that the developers can access the same IP for their instance while testing. After the testing is over, we will remove the Elastic IP from our environment. Having random Ip ensures that the application is secure.

Distribution and Load Balancer

A load balancer is a feature that helps in managing the flow of traffic between various servers. It can also prevent attacks from happening.

A load balancer is a single point of contact for a client. It distributes incoming traffic to various targets, such as EC2 instances, in order to increase the availability of an application. An SSL certificate is required to use this feature. The certificate can only be generated with a domain name. [6]

Table 4 Specification Table of Load Balancer

	DNS NAME	DNS ZONE
Load Balancer	Wall-1932820326.us-east-1.elb.amazonaws.com	North Virginia, allzones (us-east-1)

Figure 4 Properties of Load Balancer

2-Factor Authentication

Amazon Web Services (AWS) provides users with additional security when it comes to accessing their services. With Multi-Factor Authentication (MFA), users can log into their account with a combination of their name and password, as well as an additional factor of code that's generated on their device.

One-time password generation is a feature that's available on tablets and smartphones through the Amazon Web Services' TOTP feature. This method ensures that only the unique code is generated, and it's hard for an attacker to get hold of it since the code will expire in a short time. All of the code's details are stored in a real-time clock, which makes it harder for an attacker to access the account.

There are a variety of applications that support TOTP, such as Google Authenticator, Microsoft Authenticator, and Duo Mobile. These applications make it incredibly secure when it comes to accessing Amazon Web Services.

- To further improve the security of the system, the default password of the LightSail instance has been changed. This is because the company doesn't allow users to set up a password.
- The default WordPress password was also changed as soon as the instance was created. An SSL certificate was additionally not added to the system due to the requirement for a domain name to be generated.
- Google's reCAPTCHA is a tool that prevents malicious software from being installed on a website. When registering, a link is sent to the user's email address, which will allow them to set a password.
- They are also encouraged to use a strong password. To back up their files, users are additionally able to use a snapshot to automatically generate a new one.

C. Approach And Structure

In this project, we will be referring to the NIST Framework, which is a standard and technology framework that helps organizations to manage their cloud security. As the number of attacks and threats increases, every organization needs a robust framework to help them run its operations efficiently.

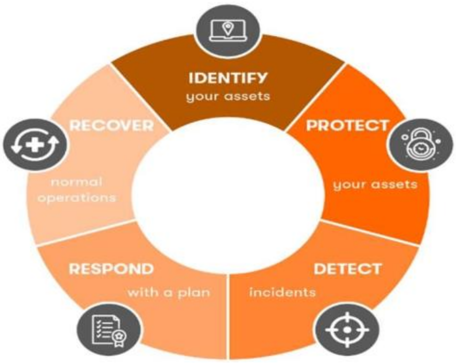


Figure 5 NIST Framework

- Identify: In order to effectively manage their cyber-security, organizations should regularly identify and measure their various parts of the business. This can help them identify the threats that are affecting their operations and develop a strategy to counteract them.
- Protect: A comprehensive security program is also required to protect an organization from various threats. This can be done through the establishment of policies and procedures that are designed to help employees manage their access and security.
- Detect: To effectively manage their cyber-security, organizations should regularly monitor their infrastructure. This can help them identify the threats that are affecting their operations and develop a strategy to counteract them. They should also regularly test their security measures.
- Respond: Before an attack can happen, an organization should also create a list of actions that it can take to minimize the impact of the damage it can cause. This can help them understand the nature of the attack and prevent it from happening in the future.
- Recover: After an organization has been hit by a cyber-attack, it is important that they immediately recover to prevent further damages. Having a recovery plan is also important to ensure that the organization can still operate.

D. BENCHMARKING

Amazon EC2 will allow us to monitor and benchmark the usage of our applications. This system will also help us keep track of our services.

We will be setting up alarms in different metrics to monitor our instances. They will be sent to us by Amazon Web Services using our registered email.

a) CPU Utilization:

We will be monitoring the CPU utilization of our instance for a period of 5 minutes. Whenever the usage exceeds 60%, we will notify the other users and continue to monitor the situation until the utilization drops below 60%.

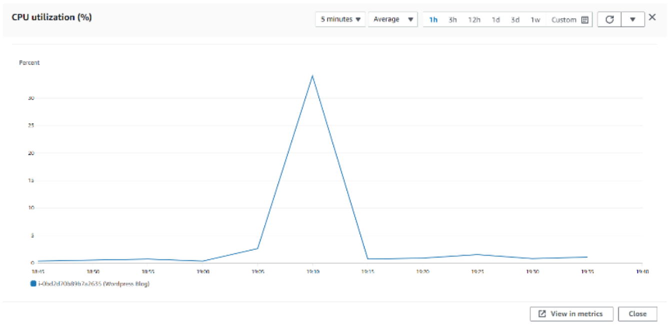


Figure 6 CPU Utilization

b) Incoming Traffic:

We will be monitoring the incoming traffic to our instance to ensure that it doesn't get affected by sudden surges. We can also identify if there's a denial-of-service attack.

Since our app is not heavy traffic-centric, we have decided to limit the amount of data that can be accessed by the application to 56MB per 5 minutes. This is the same as the cap that we would increase in the future if we see the traffic to be genuine.

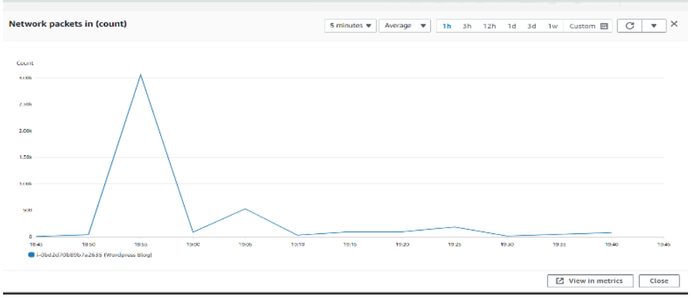


Figure 7 Incoming Traffic

c) Failed System Check Status:

Every minute, Amazon performs a virtual system check. The result of the check is either a failed or a passed. We will be notified if there is a failure in the system check, and we will be able to react quickly to prevent it from happening.

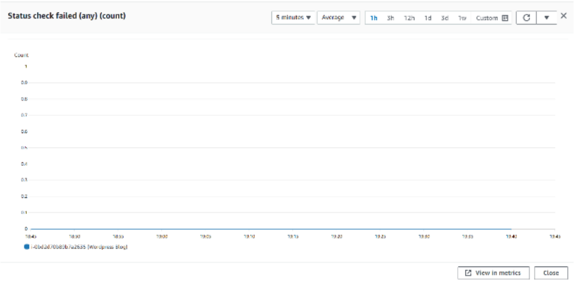


Figure 8 Failed System Check Status

E. TECHNICAL TESTING APPROACH

Technical testing is done for checking the website, if there are vulnerabilities present in the website.

Sr. No.	Test Cases	Negative/Positive Test Case
1.	Users can also create a password strength meter.	Positive. Passwords are only allowed to be created by users with at least 12 characters long.
2.	Check the comment functionality for XSS attacks.	Positive.
3.	Check if unknown UserID or email ID on wp-admin page works with known password.	Positive. If an unknown user ID or email address is associated with a known password, then it will not work.
4.	The password field should be tested to see if it will prompt you to use special characters or weak passwords.	Positive. After you generate a new password, a strength meter will be displayed.
5.	Test the uniqueness for username whether it is already taken or not.	Positive

III. Vulnerability Findings

Following a comprehensive review of the vulnerabilities in the securities market, we have identified several that need to be addressed in order to prevent them from happening in the future.

a) Brute force attack:

We discovered that our web app is prone to being attacked by brute force. This means that an attacker could perform various actions to try and access the application's login page. These actions could include performing a variety of passwords and trying to perform a trial and error.
CVE ID: CVE-2022-21661
Risk Rating: HIGH
CVSS Score: 5.0
Mitigation: To prevent brute force logins, we are planning on implementing an IP filtering feature that will prevent the application from accessing certain IP addresses. This method will allow us to restrict the number of attempts to login using an IP address.

b) XSS Cross-Site Scripting:

XSS is a type of security issue that can be caused by an attacker inserting malicious scripts into a web application. It can affect the future visitors and prevent them from accessing the application's features. Every time a user tries to access a particular field in the application, a request will be sent to the malicious script.
CVE ID: CVE-2022-21662
Risk Rating: HIGH
CVSS Score: 7.5
Mitigation: We can enable the Amazon Web Application Firewall (AWS WAF) for our web app. WAF helps us identify and prevent malicious scripts from attacking our web applications by creating filters that will inspect the requests sent by our web servers.

c) DDOS Attack:

A denial-of-service attack is a type of cyber-attack that uses a combination of methods to prevent a network or machine from working properly. It can affect a host's services for an indefinite amount of time.
CVE ID: CVE-2018-6389
Risk Rating: MEDIUM
CVSS Score: 5.0
Mitigation: A successful solution for addressing distributed denial-of-service attacks will intelligently route traffic to ensure that the remaining traffic is kept in manageable chunks.

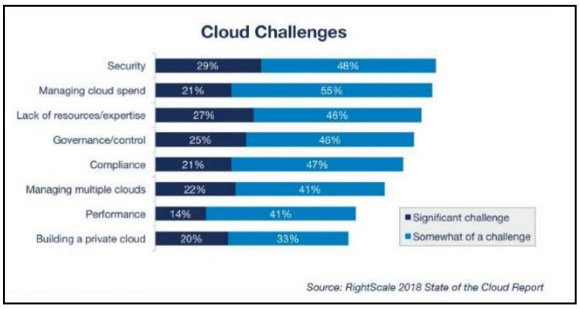
Some extra points regarding mitigations that can be apply to cloud:

- To manage the risks associated with web applications, Amazon Web Services (AWS) has a variety of security controls. These controls are designed to provide a minimum set of requirements for the organization.

- Through its business risk management program, Amazon Web Services has a variety of tools and security controls designed to help manage the risks associated with its operations.
- To ensure that its operations are conducted in a secure and effective manner, Amazon Web Services has a variety of security controls that are regularly monitored and evaluated.
- Through the cloud adoption risk assessment tool, customers can easily identify the potential risks associated with choosing a particular cloud service provider. It uses a combination of data and background information to analyze the various scenarios that can affect their operations.

IV. *CHALLENGES AND LIMITATIONS*

Due to the advent of cloud computing, there are various challenges and limitations that are typically encountered when creating web applications on a platform that uses cloud services. A survey conducted in 2022 revealed that there were many of these issues and limitations.



Source: RightScale 2018 State of the Cloud Report

Figure 9 Data from Survey

Identity and Access management (IAM)
Due to the limited access that the college account provides, the implementation of the Identity and Access management service could not be carried out in the web application. This service was not feasible to implement in the cloud without fully utilising the available functions.

HTTPS
An SSL certificate is used to protect a web application from unauthorized access. It ensures that the website can be accessed using HTTPS instead of HTTP, which would have prevented it from being affected by Man in the Middle attacks. However, since acquiring a domain name is a commercial activity, it was not integrated into the online application.

2-Factor Authentication
One-time password authentication was supposed to be implemented in an application to allow users to log in using their email address. Unfortunately, since this service is also paid, it was not able to be integrated into the app.

IP Address Blocking
This feature, which was not part of the application, was designed to allow administrators to prevent a specific IP address from being used during a failed login attempt.

V. *CONCLUSION*

In our project, we discussed about securing our web application using Amazon Web Services EC2 Cloud Platform. This report describes the various tools and techniques that we used to make our application secure and stable. It also shows the performance and security aspects of the application.

In the future, we would like to focus on providing a comprehensive view of our application's limitations using an integrated approach that includes hosting it with all of its root privileges and using services such as Amazon Web Services Config and CloudTrail Management Console.

The goal of the project was to help us thoroughly assess the various advantages of using cloud platforms and how they can be used to host our applications. It also helped us understand how to secure our applications and monitor their usage.

References

[1] "What is cloud computing?," Oracle, [Online]. Available: https://www.oracle.com/ie/cloud/what-is-cloud-computing/. [Accessed 15 07 2022].

[2] D. Carty, "Amazon EC2," Techtarget, [Online]. Available: https://www.techtarget.com/searchaws/definition/Amazon-Elastic-Compute-Cloud-Amazon-EC2. [Accessed 15 07 2022].

[3] "What is Amazon EC2?," AWS, [Online]. Available: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/concepts.html. [Accessed 15 07 2022].

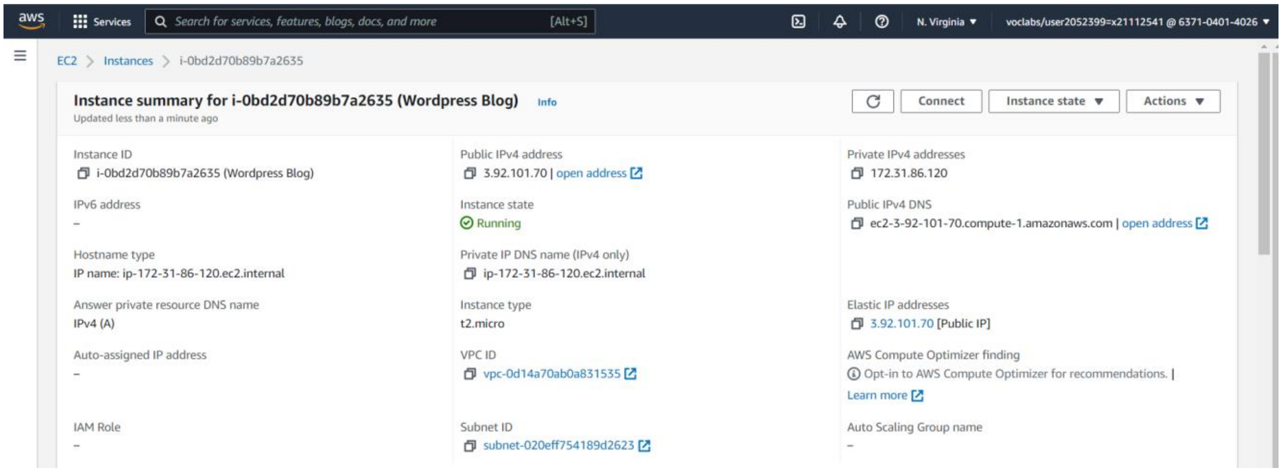
[4] "What is IAM?," AWS, [Online]. Available: https://docs.amazonaws.cn/en_us/IAM/latest/UserGuide/introduction.html. [Accessed 015 07 2022].

[5] Simplilearn, "AWS IAM: Working, Components, and Features Explained," Simplilearn, 04 04 2022. [Online]. Available: https://www.simplilearn.com/tutorials/aws-tutorial/aws-iam. [Accessed 16 07 2022].

[6] "What is an Application Load Balancer?," AWS, [Online]. Available: https://docs.aws.amazon.com/elasticloadbalancing/latest/application/introduction.html. [Accessed 16 07 2022].

Appendix

1. Instance



aws
Services
Search for services, features, blogs, docs, and more [Alt+S]
N. Virginia
voclabs/user2052399=x21112541 @ 6371-0401-4026
EC2 > Instances > i-0bd2d70b89b7a2635

Instance summary for i-0bd2d70b89b7a2635 (Wordpress Blog) Info

Updated less than a minute ago

Connect
Instance state
Actions

Instance ID
i-0bd2d70b89b7a2635 (Wordpress Blog)

IPv6 address
–

Hostname type
IP name: ip-172-31-86-120.ec2.internal

Answer private resource DNS name
IPv4 (A)

Auto-assigned IP address
–

IAM Role
–

Public IPv4 address
3.92.101.70 | open address

Instance state
Running

Private IP DNS name (IPv4 only)
ip-172-31-86-120.ec2.internal

Instance type
t2.micro

VPC ID
vpc-0d14a70ab0a831535

Subnet ID
subnet-020eff754189d2623

Private IPv4 addresses
172.31.86.120

Public IPv4 DNS
ec2-3-92-101-70.compute-1.amazonaws.com | open address

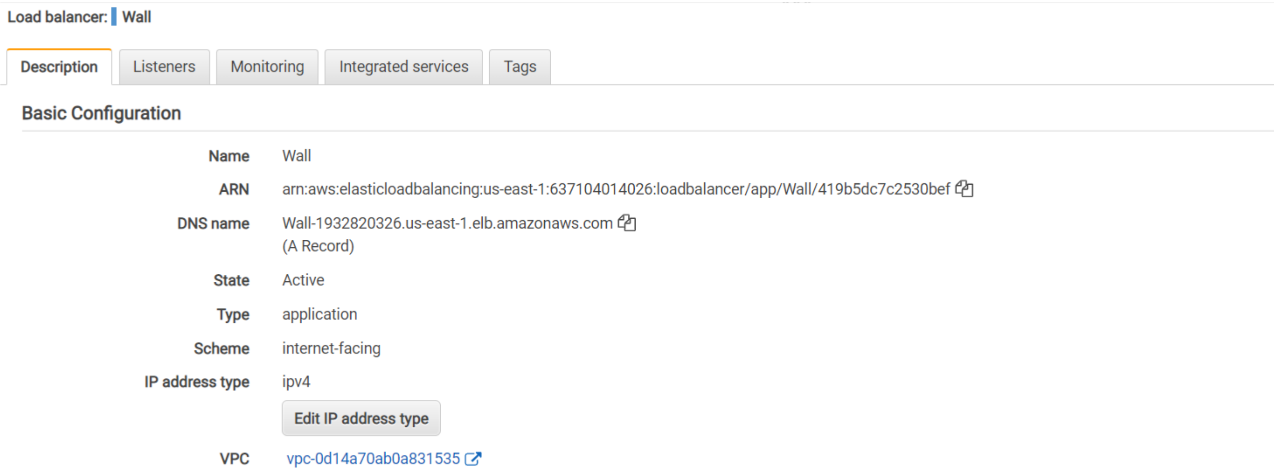
Elastic IP addresses
3.92.101.70 [Public IP]

AWS Compute Optimizer finding
Opt-in to AWS Compute Optimizer for recommendations. |
Learn more

Auto Scaling Group name
–

Figure 10 Instance Summary

2. Load Balancer



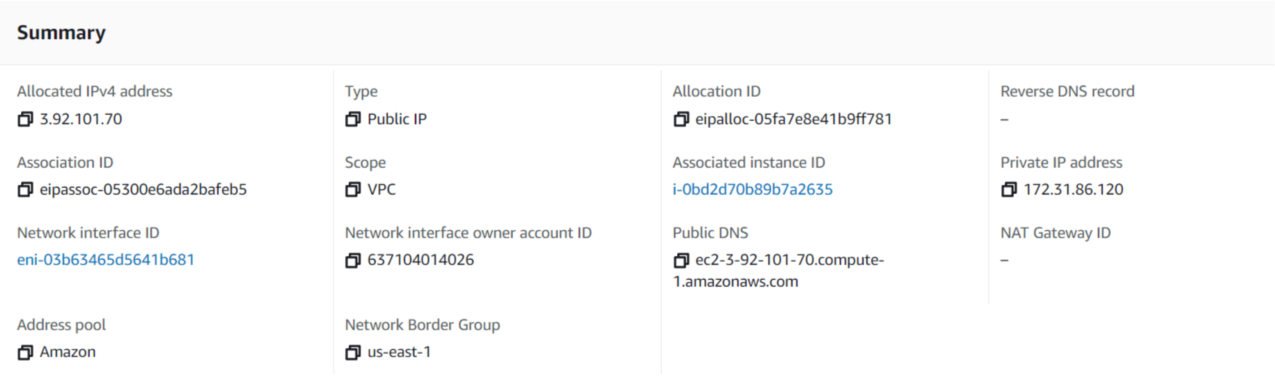
Load balancer: Wall

Basic Configuration

Name	Wall
ARN	arn:aws:elasticloadbalancing:us-east-1:637104014026:loadbalancer/app/Wall/419b5dc7c2530bef
DNS name	Wall-1932820326.us-east-1.elb.amazonaws.com (A Record)
State	Active
Type	application
Scheme	internet-facing
IP address type	ipv4 Edit IP address type
VPC	vpc-0d14a70ab0a831535

Figure 11 Load Balancer Summary

3. Elastic IP



Summary

Allocated IPv4 address
3.92.101.70

Association ID
eipassoc-05300e6ada2bafeb5

Network interface ID
eni-03b63465d5641b681

Address pool
Amazon

Type
Public IP

Scope
VPC

Network interface owner account ID
637104014026

Network Border Group
us-east-1

Allocation ID
eipalloc-05fa7e8e41b9ff781

Associated instance ID
i-0bd2d70b89b7a2635

Public DNS
ec2-3-92-101-70.compute-1.amazonaws.com

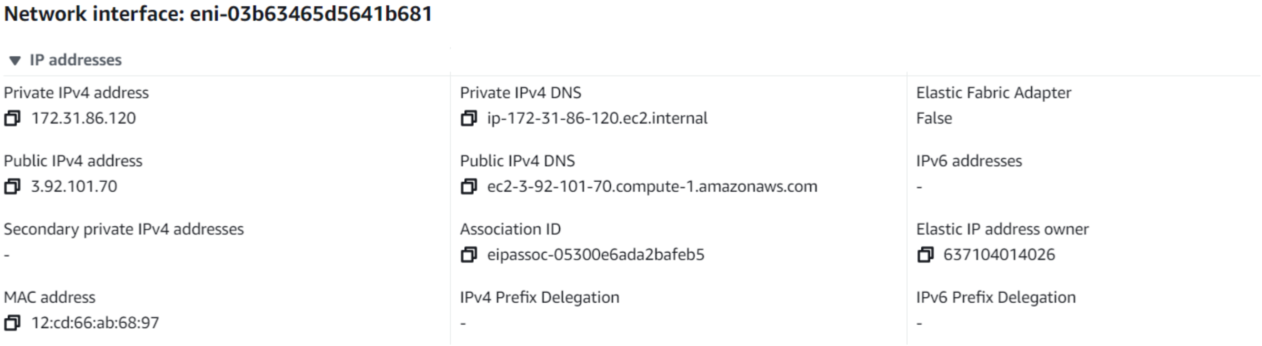
Reverse DNS record
–

Private IP address
172.31.86.120

NAT Gateway ID
–

Figure 12 Static IP Information

4. IPv4 Networking



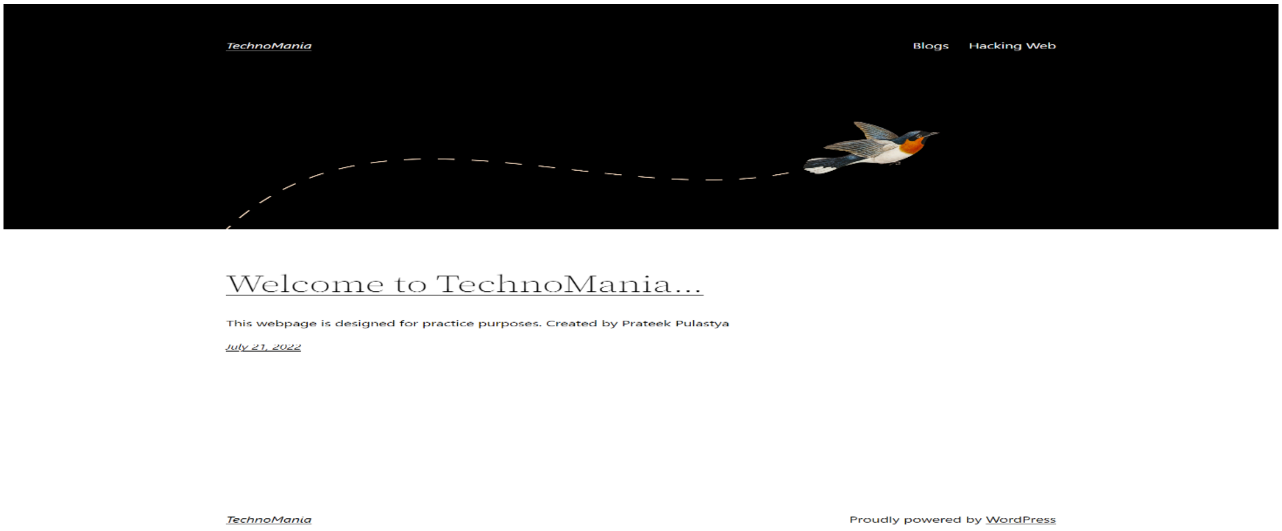
Network interface: eni-03b63465d5641b681

▼ IP addresses

Private IPv4 address 172.31.86.120	Private IPv4 DNS ip-172-31-86-120.ec2.internal	Elastic Fabric Adapter False
Public IPv4 address 3.92.101.70	Public IPv4 DNS ec2-3-92-101-70.compute-1.amazonaws.com	IPv6 addresses -
Secondary private IPv4 addresses -	Association ID eipassoc-05300e6ada2bafeb5	Elastic IP address owner 637104014026
MAC address 12:cd:66:ab:68:97	IPv4 Prefix Delegation -	IPv6 Prefix Delegation -

Figure 13 IPv4 information

5. Home page of my website http://3.92.101.70/



TechnoMania

Welcome to TechnoMania...

This webpage is designed for practice purposes. Created by Prateek Pulastya

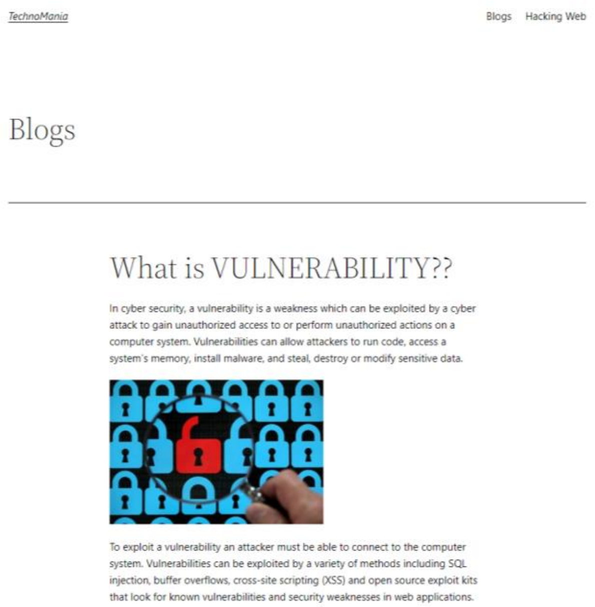
July 21, 2022

TechnoMania

Proudly powered by WordPress

Figure 14 Website homepage

6. Blog page of website http://3.92.101.70/blogs/



TechnoMania

Blogs

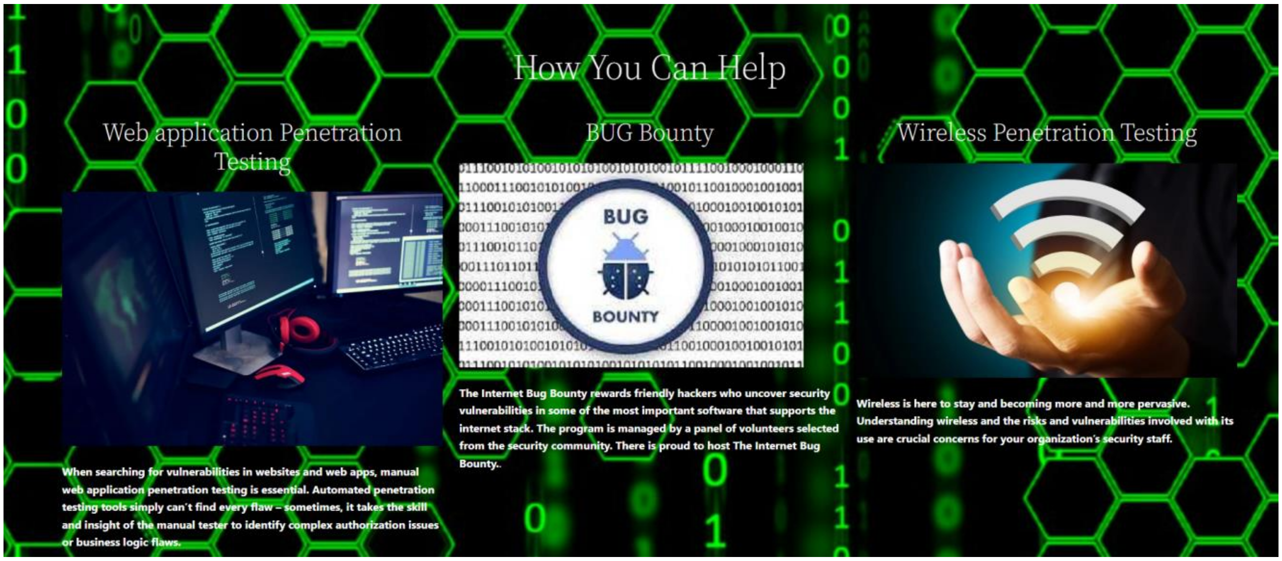
What is VULNERABILITY??

In cyber security, a vulnerability is a weakness which can be exploited by a cyber attack to gain unauthorized access to or perform unauthorized actions on a computer system. Vulnerabilities can allow attackers to run code, access a system's memory, install malware, and steal, destroy or modify sensitive data.

To exploit a vulnerability an attacker must be able to connect to the computer system. Vulnerabilities can be exploited by a variety of methods including SQL injection, buffer overflows, cross-site scripting (XSS) and open source exploit kits that look for known vulnerabilities and security weaknesses in web applications.

Figure 15 Blogs

7. Hacking Web page of website http://3.92.101.70/sample-page/


How You Can Help
Web application Penetration Testing
BUG Bounty
Wireless Penetration Testing
BUG
BOUNTY

When searching for vulnerabilities in websites and web apps, manual web application penetration testing is essential. Automated penetration testing tools simply can't find every flaw – sometimes, it takes the skill and insight of the manual tester to identify complex authorization issues or business logic flaws.

The Internet Bug Bounty rewards friendly hackers who uncover security vulnerabilities in some of the most important software that supports the internet stack. The program is managed by a panel of volunteers selected from the security community. There is proud to host The Internet Bug Bounty..

Wireless is here to stay and becoming more and more pervasive. Understanding wireless and the risks and vulnerabilities involved with its use are crucial concerns for your organization's security staff.

Figure 16 Sample web page

8. Wp-admin login page

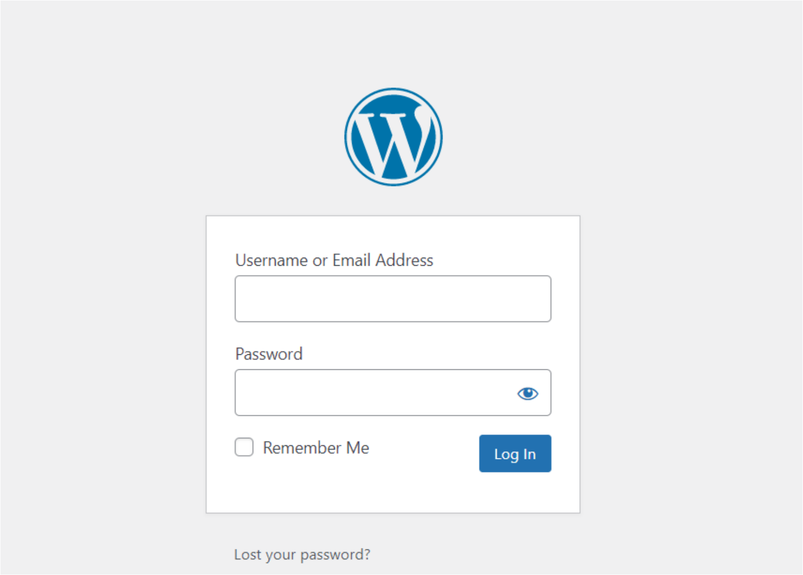


Figure 17 WordPress login page

9. Comment column in the website

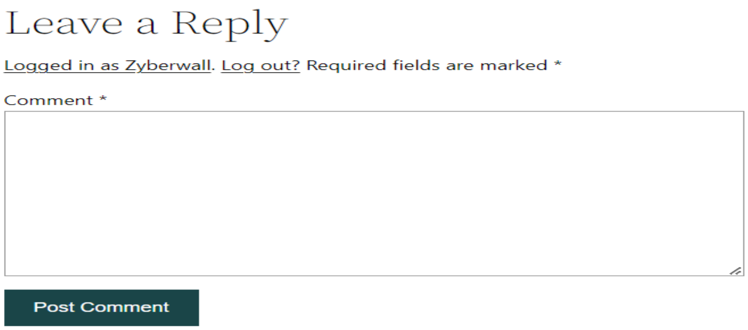
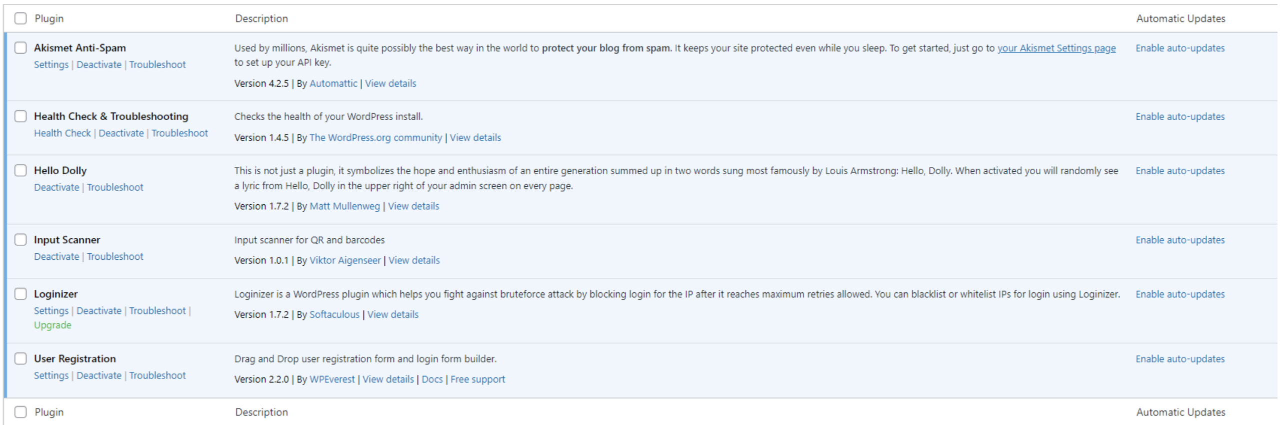

Leave a Reply
Logged in as Zyberwall. Log out? Required fields are marked *
Comment *
Post Comment

Figure 18 Comment option

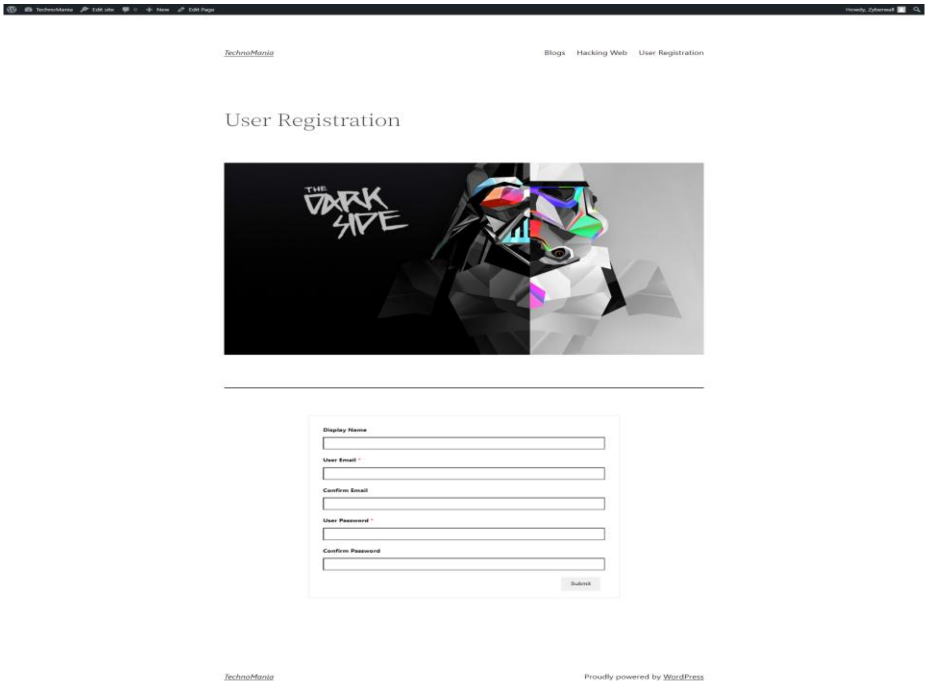
10. Security plugins in WordPress



☐ Plugin	Description	Automatic Updates
☐ **Akismet Anti-Spam** Settings | Deactivate | Troubleshoot	Used by millions, Akismet is quite possibly the best way in the world to **protect your blog from spam.** It keeps your site protected even while you sleep. To get started, just go to your Akismet Settings page to set up your API key. Version 4.2.5 | By Automattic | View details	Enable auto-updates
☐ **Health Check & Troubleshooting** Health Check | Deactivate | Troubleshoot	Checks the health of your WordPress install. Version 1.4.5 | By The WordPress.org community | View details	Enable auto-updates
☐ **Hello Dolly** Deactivate | Troubleshoot	This is not just a plugin, it symbolizes the hope and enthusiasm of an entire generation summed up in two words sung most famously by Louis Armstrong: Hello, Dolly. When activated you will randomly see a lyric from Hello, Dolly in the upper right of your admin screen on every page. Version 1.7.2 | By Matt Mullenweg | View details	Enable auto-updates
☐ **Input Scanner** Deactivate | Troubleshoot	Input scanner for QR and barcodes Version 1.0.1 | By Viktor Aigenseer | View details	Enable auto-updates
☐ **Loginizer** Settings | Deactivate | Troubleshoot | Upgrade	Loginizer is a WordPress plugin which helps you fight against bruteforce attack by blocking login for the IP after it reaches maximum retries allowed. You can blacklist or whitelist IPs for login using Loginizer. Version 1.7.2 | By Softaculous | View details	Enable auto-updates
☐ **User Registration** Settings | Deactivate | Troubleshoot	Drag and Drop user registration form and login form builder. Version 2.2.0 | By WPEverest | View details | Docs | Free support	Enable auto-updates
☐ Plugin	Description	Automatic Updates

Figure 19 Installed Plugins in WordPress

11. User Registration Page



User Registration

Display Name

User Email *

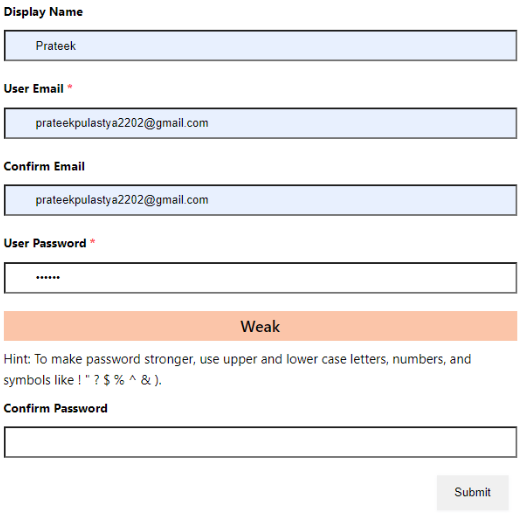
Confirm Email

User Password *

Confirm Password

Figure 20 User Registration page

12. Shows the strength of the password



Display Name

Prateek

User Email *

prateekpulastya2202@gmail.com

Confirm Email

prateekpulastya2202@gmail.com

User Password *

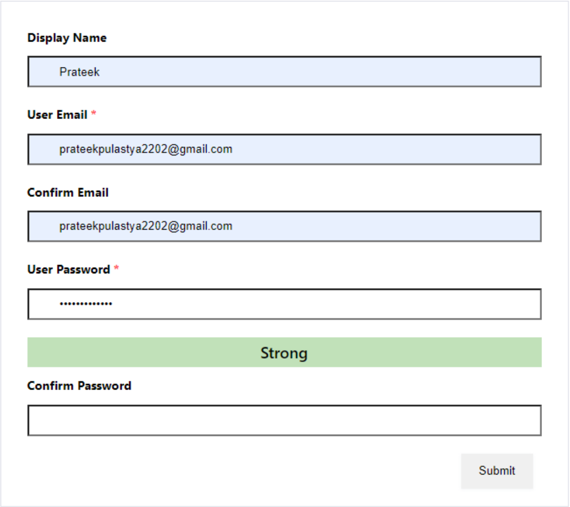
••••••

Weak

Hint: To make password stronger, use upper and lower case letters, numbers, and symbols like ! " ? $ % ^ &).

Confirm Password

Figure 21 Shows weak password strength



Display Name

Prateek

User Email *

prateekpulastya2202@gmail.com

Confirm Email

prateekpulastya2202@gmail.com

User Password *

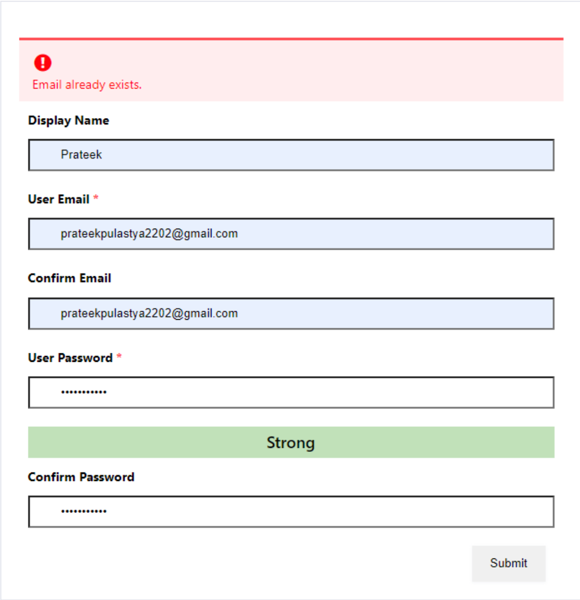
•••••••••••••

Strong

Confirm Password

Figure 22 Shows strong password strength

13. Shows email already exists



Email already exists.

Display Name

Prateek

User Email *

prateekpulastya2202@gmail.com

Confirm Email

prateekpulastya2202@gmail.com

User Password *

•••••••••••

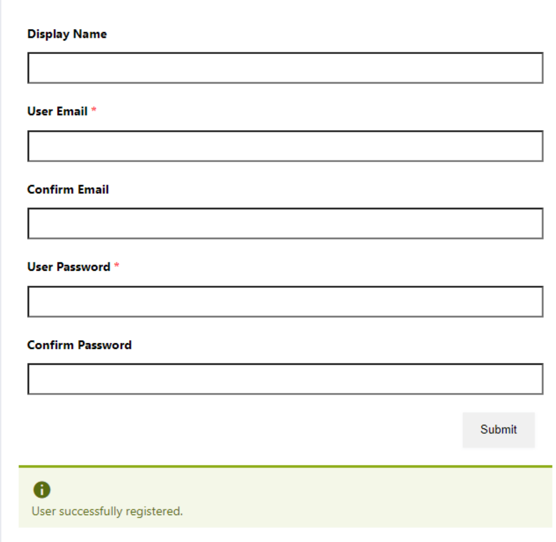
Strong

Confirm Password

•••••••••••

Figure 23 Email already exists

14. User successfully registered



Display Name

User Email *

Confirm Email

User Password *

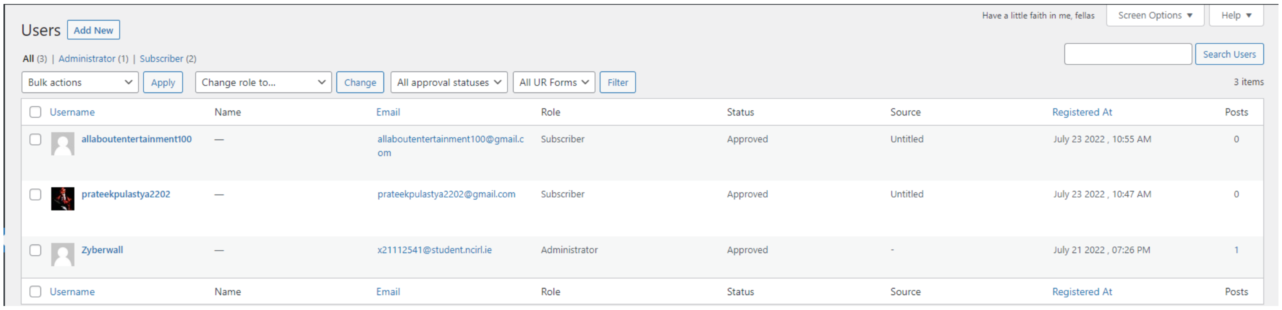
Confirm Password

Submit

User successfully registered.

Figure 24 Successfully registered user

15. Users tab to see all the registered users



All (3) | Administrator (1) | Subscriber (2)

3 items

□	Username	Name	Email	Role	Status	Source	Registered At	Posts
□	allaboutentertainment100	—	allaboutentertainment100@gmail.com	Subscriber	Approved	Untitled	July 23 2022 , 10:55 AM	0
□	prateekpulastya2202	—	prateekpulastya2202@gmail.com	Subscriber	Approved	Untitled	July 23 2022 , 10:47 AM	0
□	Zyberwall	—	x21112541@student.ncirl.ie	Administrator	Approved	-	July 21 2022 , 07:26 PM	1
□	Username	Name	Email	Role	Status	Source	Registered At	Posts

Figure 25 Admin page to see all the registered user