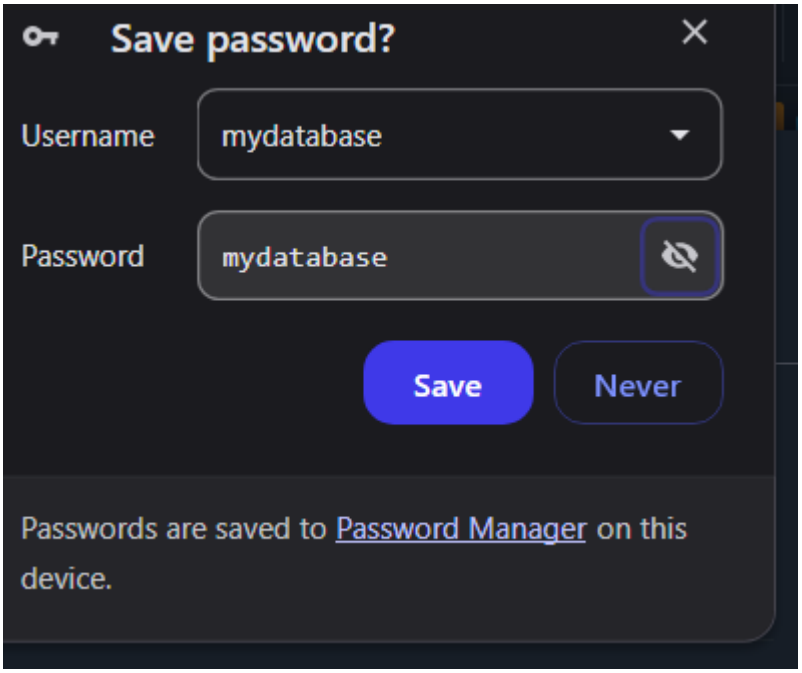
DAY FINAL PROJECT

```
#!/bin/bash
yum update -y
sudo yum install php -y
sudo yum install php-mysqli -y
sudo yum install httpd -y
amazon-linux-extras install -y php7.3
cd /var/www/html
echo "healthy" > healthy.html
wget https://wordpress.org/latest.tar.gz
tar -xzf latest.tar.gz
cp -r wordpress/* /var/www/html/
rm -rf wordpress
rm -rf latest.tar.gz
chmod -R 755 wp-content
chown -R apache:apache wp-content
wget https://project-htaccess.s3.ap-south-1.amazonaws.com/htaccess.txt
mv htaccess.txt .htaccess
chkconfig httpd on
service httpd start
```



be on your way to using the most extendable and powerful personal publishing platform in the world.

Information needed

Please provide the following information. Do not worry, you can always change these settings later.

Site Title portfolio

Username prathamesh2005

Usernames can have only alphanumeric characters, spaces, underscores, hyphens, periods, and the @ symbol.

Password prathamesh@2005 Hide

Strong

Important: You will need this password to log in. Please store it in a secure location.

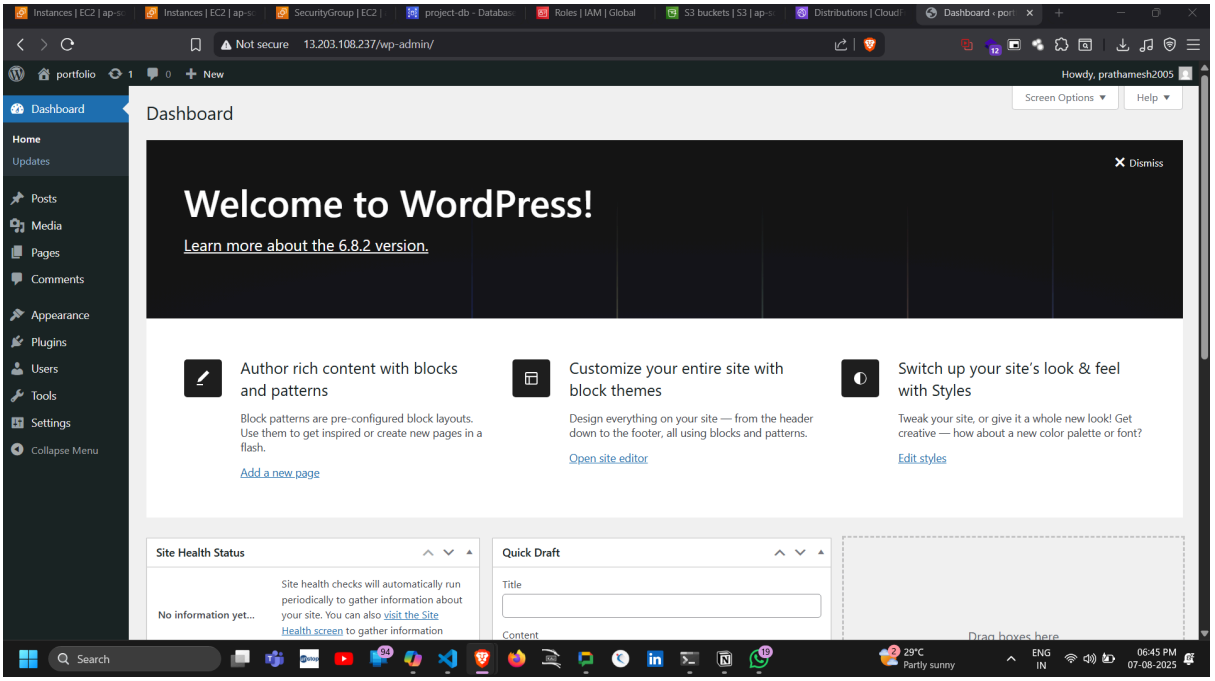
Your Email prathameshpendkar@gmail.com

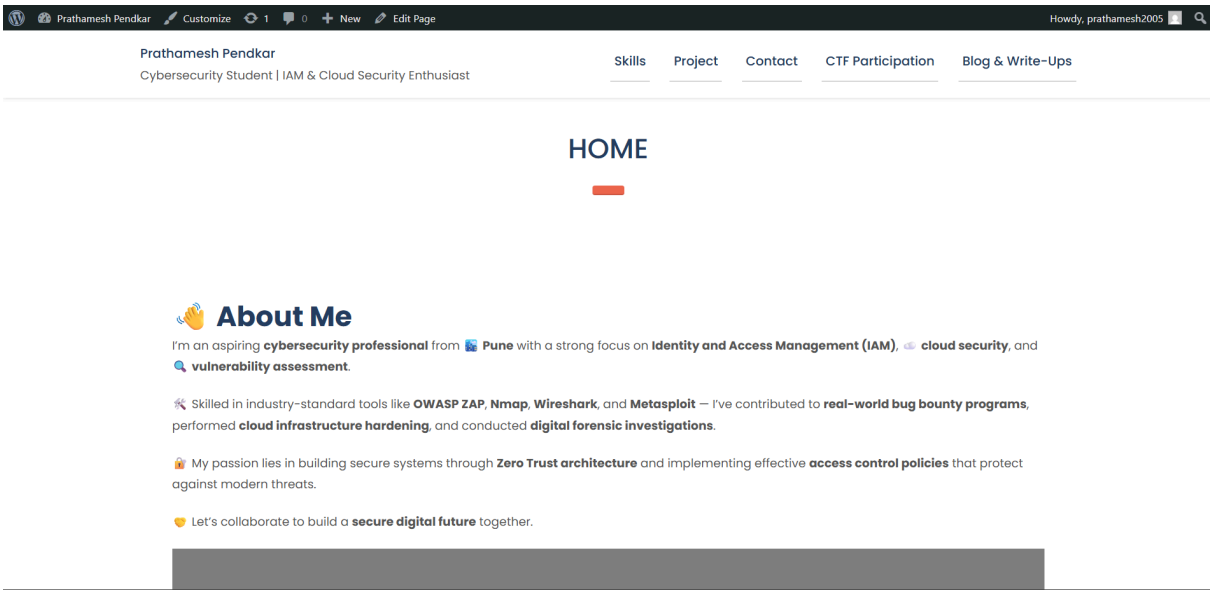
Double-check your email address before continuing.

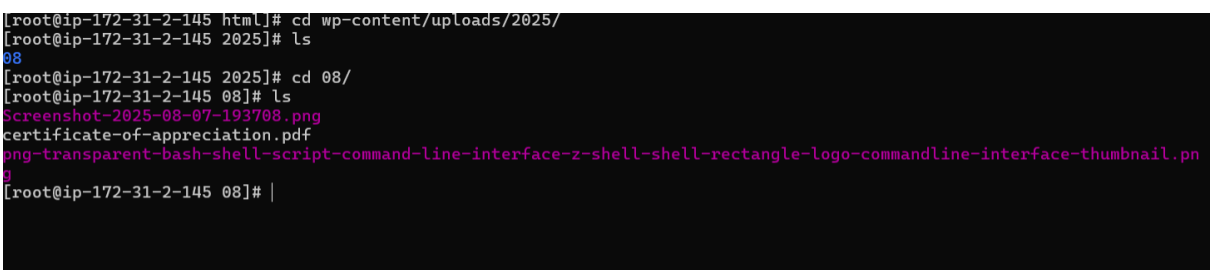
Search engine visibility Discourage search engines from indexing this site

It is up to search engines to honor this request.

Install WordPress


Not secure 13.203.108.237/wp-admin/
portfolio
New
Howdy, prathamesh2005
Dashboard
Home
Updates
Posts
Media
Pages
Comments
Appearance
Plugins
Users
Tools
Settings
Collapse Menu
Screen Options
Help
Dismiss
Welcome to WordPress!
Learn more about the 6.8.2 version.
Author rich content with blocks and patterns
Block patterns are pre-configured block layouts. Use them to get inspired or create new pages in a flash.
Add a new page
Customize your entire site with block themes
Design everything on your site — from the header down to the footer, all using blocks and patterns.
Open site editor
Switch up your site's look & feel with Styles
Tweak your site, or give it a whole new look! Get creative — how about a new color palette or font?
Edit styles
Site Health Status
No information yet...
Site health checks will automatically run periodically to gather information about your site. You can also visit the Site Health screen to gather information
Quick Draft
Title
Content
Drag boxes here
Search
29°C
Partly sunny
ENG
IN
06:45 PM
07-08-2025


Prathamesh Pendkar
Customize
New
Edit Page
Howdy, prathamesh2005
Prathamesh Pendkar
Cybersecurity Student | IAM & Cloud Security Enthusiast
Skills
Project
Contact
CTF Participation
Blog & Write-Ups
HOME
About Me
I'm an aspiring cybersecurity professional from Pune with a strong focus on Identity and Access Management (IAM), cloud security, and vulnerability assessment.
Skilled in industry-standard tools like OWASP ZAP, Nmap, Wireshark, and Metasploit — I've contributed to real-world bug bounty programs, performed cloud infrastructure hardening, and conducted digital forensic investigations.
My passion lies in building secure systems through Zero Trust architecture and implementing effective access control policies that protect against modern threats.
Let's collaborate to build a secure digital future together.


[root@ip-172-31-2-145 html]# cd wp-content/uploads/2025/
[root@ip-172-31-2-145 2025]# ls
08
[root@ip-172-31-2-145 2025]# cd 08/
[root@ip-172-31-2-145 08]# ls
Screenshot-2025-08-07-193708.png
certificate-of-appreciation.pdf
png-transparent-bash-shell-script-command-line-interface-z-shell-shell-rectangle-logo-commandline-interface-thumbnail.png
[root@ip-172-31-2-145 08]#

we got soa and name server

using crontab to automate and sync

✅ AWS WordPress Hosting Architecture Report

📦 Services Used

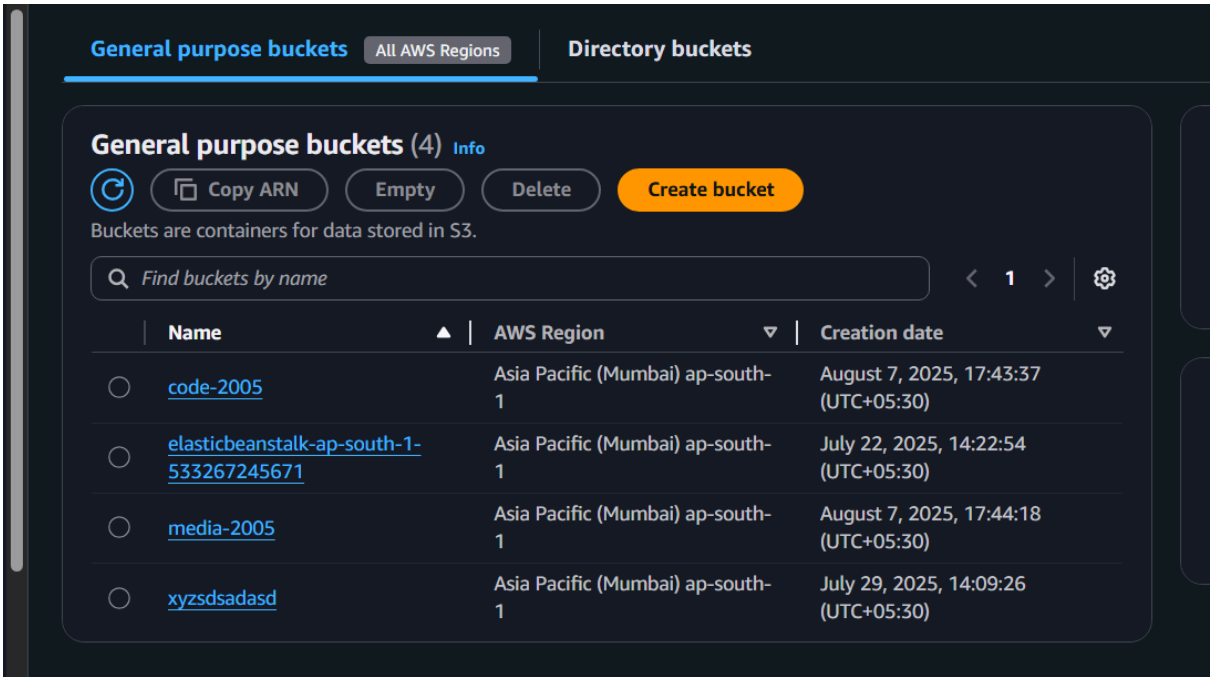
Service	Usage
S3	Bucket for media and code storage
CloudFront	CDN for faster content delivery
EC2	Hosting the WordPress instance
Elastic IP	Assigning static IP to EC2
IAM	Grant EC2 access to S3
RDS (MySQL)	Database backend
VPC	Networking
Security Groups	Inbound traffic rules
Route 53	DNS hosting
ALB (Application Load Balancer)	Load balancing across instances
Auto Scaling	Automatically scale instances
CloudWatch + Crontab	Monitoring + periodic sync with S3
AMI	EC2 instance image for scaling

🛠️ Step-by-Step Deployment Process

🗂️ 1. S3 Bucket Creation

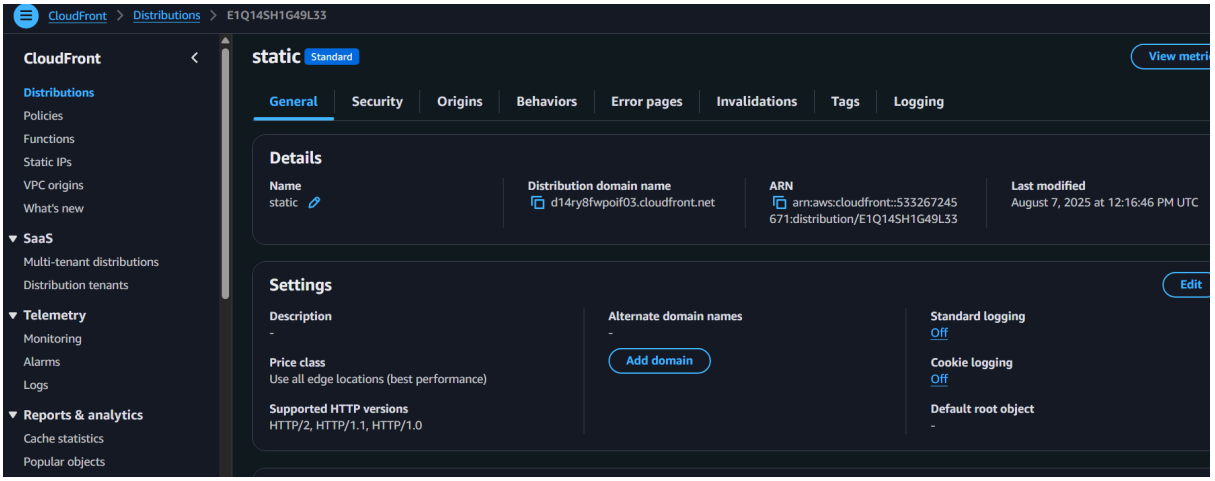
- Create two S3 buckets:
  - `code-2005`
  - `media-2005`

- ACL: **Disabled**
- Public Access: **Enabled**
- Versioning: **Disabled**
- Object Lock: **Disabled**
- Bucket Key: **Disabled**



🌐 2. Create CloudFront Distribution

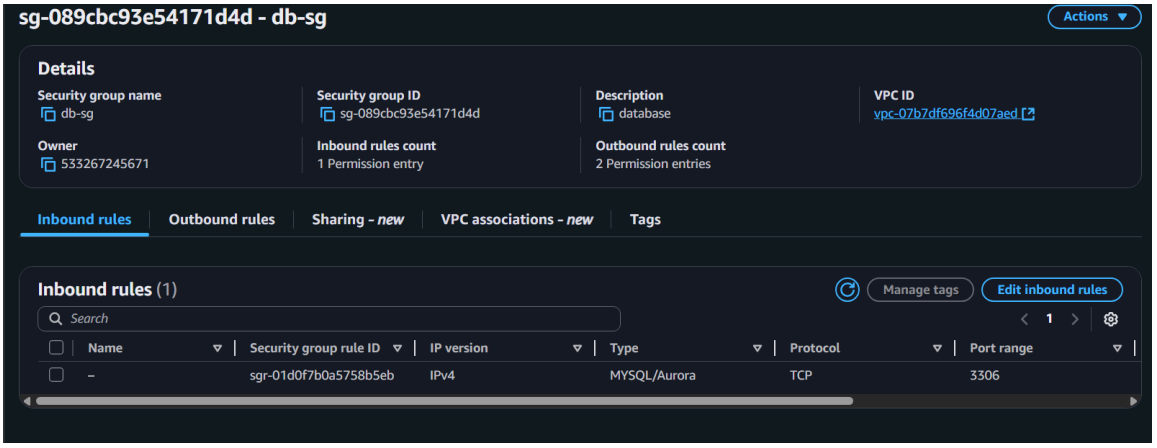
- Distribution type: **Web**
- Origin: **media-2005 S3 bucket**
- No WAF/Shield enabled



🔐 3. Configure Security Groups

- **website-sg**:
  - Inbound: SSH (22), HTTP (80)

- **db-sg**:
  - Inbound: MySQL (3306) from `website-sg`

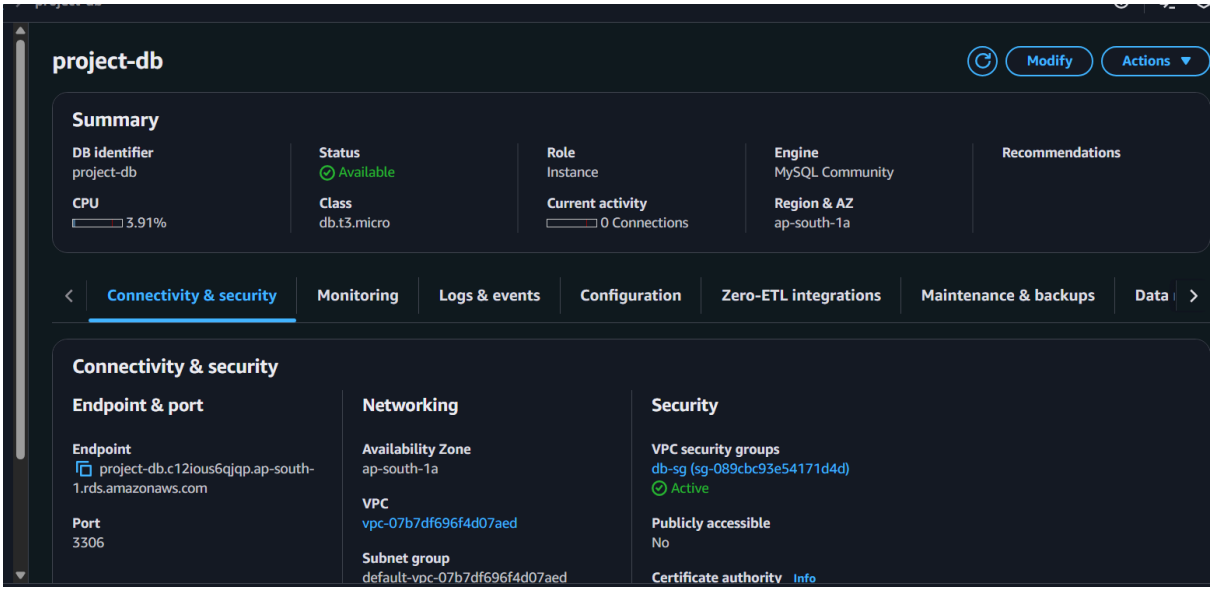


🗃️ 4. Setup RDS (MySQL)

- Engine: **MySQL Community**
- Tier: **Free Tier (Single AZ)**
- Identifier: `project-db`
- Username: `mydatabase`
- Password: `mydatabase`
- Endpoint:

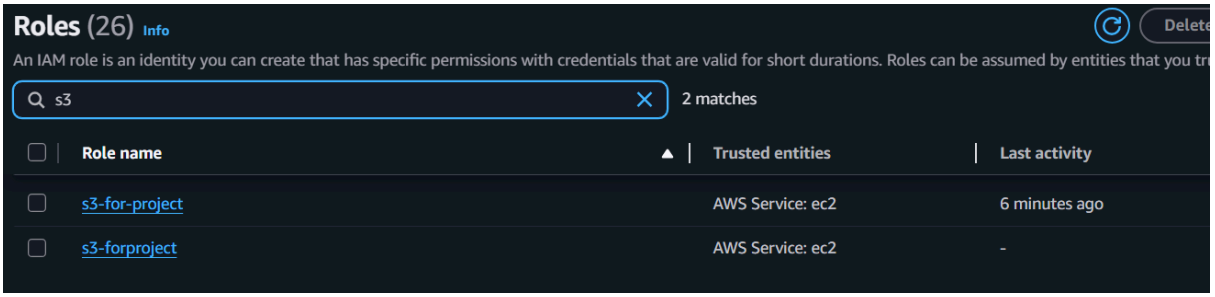
  ```
  project-db.c12ious6qjqp.ap-south-1.rds.amazonaws.com
  ```

- VPC: **Default**
- Subnet: **Default**
- Security Group: **db-sg**



🔑 5. IAM Role and Policy

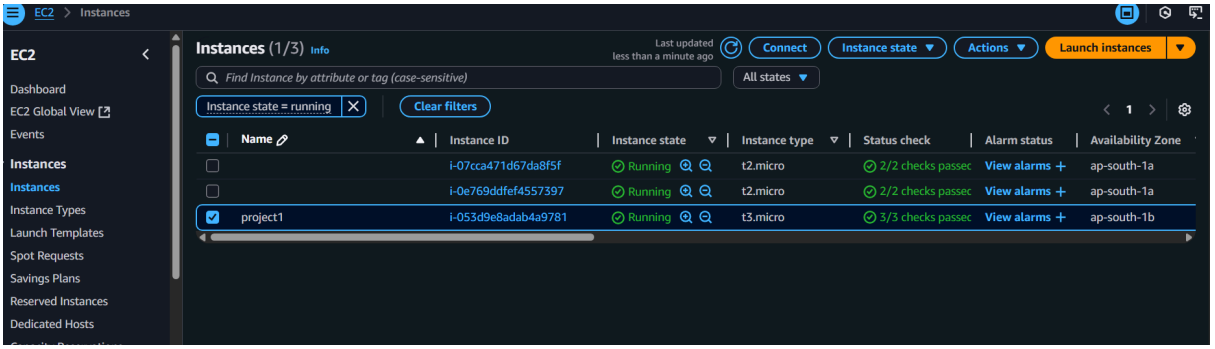
- Create IAM Role: `s3-forproject`
- Attach managed policy: `AmazonS3FullAccess`
- Assign role to EC2 at launch



💻 6. Launch EC2 Instance

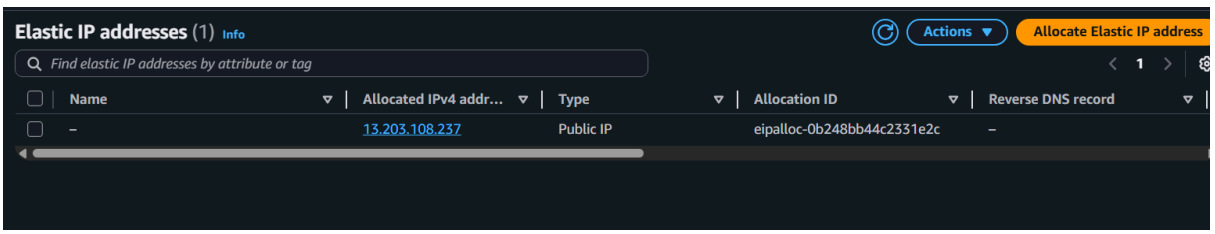
- OS: **Amazon Linux 2**
- Attach:
  - Security Group: `website-sg`
  - IAM Role: `s3-forproject`
- Bootstrap Script:

```
#!/bin/bash
yum update -y
sudo yum install php -y
sudo yum install php-mysqli -y
sudo yum install httpd -y
amazon-linux-extras install -y php7.3
cd /var/www/html
echo "healthy" > healthy.html
wget https://wordpress.org/latest.tar.gz
tar -xzf latest.tar.gz
cp -r wordpress/* /var/www/html/
rm -rf wordpress latest.tar.gz
chmod -R 755 wp-content
chown -R apache:apache wp-content
wget https://project-htaccess.s3.ap-south-1.amazonaws.com/htaccess.txt
mv htaccess.txt .htaccess
chkconfig httpd on
service httpd start
```



📌 7. Attach Elastic IP

- Allocate and associate Elastic IP to the EC2 instance.



📸 8. Sync EC2 with S3

- One-time sync:

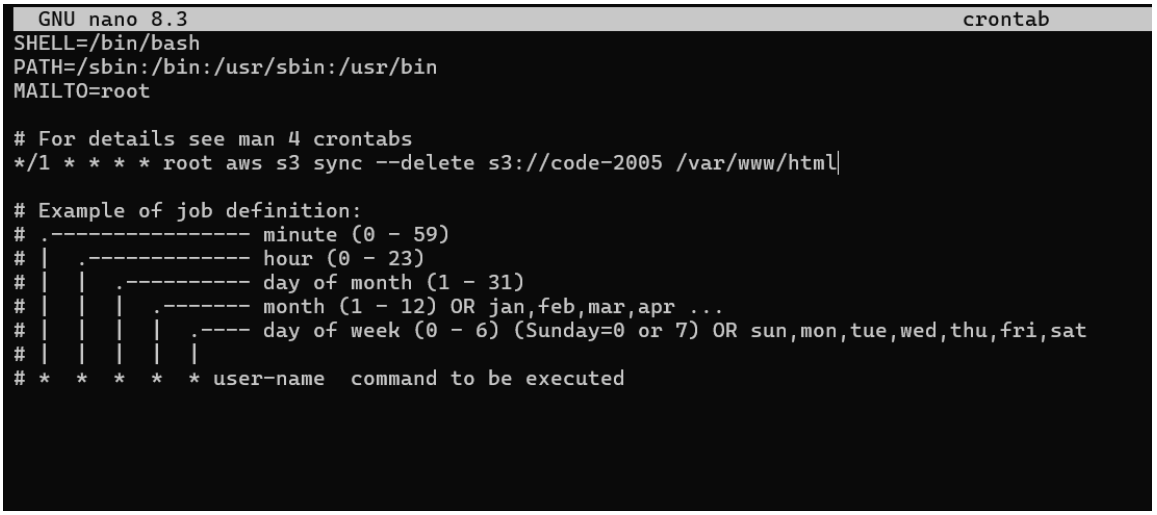
```
aws s3 sync /var/www/html s3://code-2005
```

- Crontab to automate:

```
crontab -e
```

Add:

```
*/5 * * * * aws s3 sync /var/www/html s3://code-2005
```



🌍 9. Make `media-2005` Bucket Public

Add this bucket policy:

```
{
"Version": "2012-10-17",
"Statement": [
{
"Sid": "PublicReadGetObject",
"Effect": "Allow",
"Principal": "",
"Action": [
"s3:GetObject"
],
"Resource": [
"arn:aws:s3:::media-2005/"
]
}
]
}
```

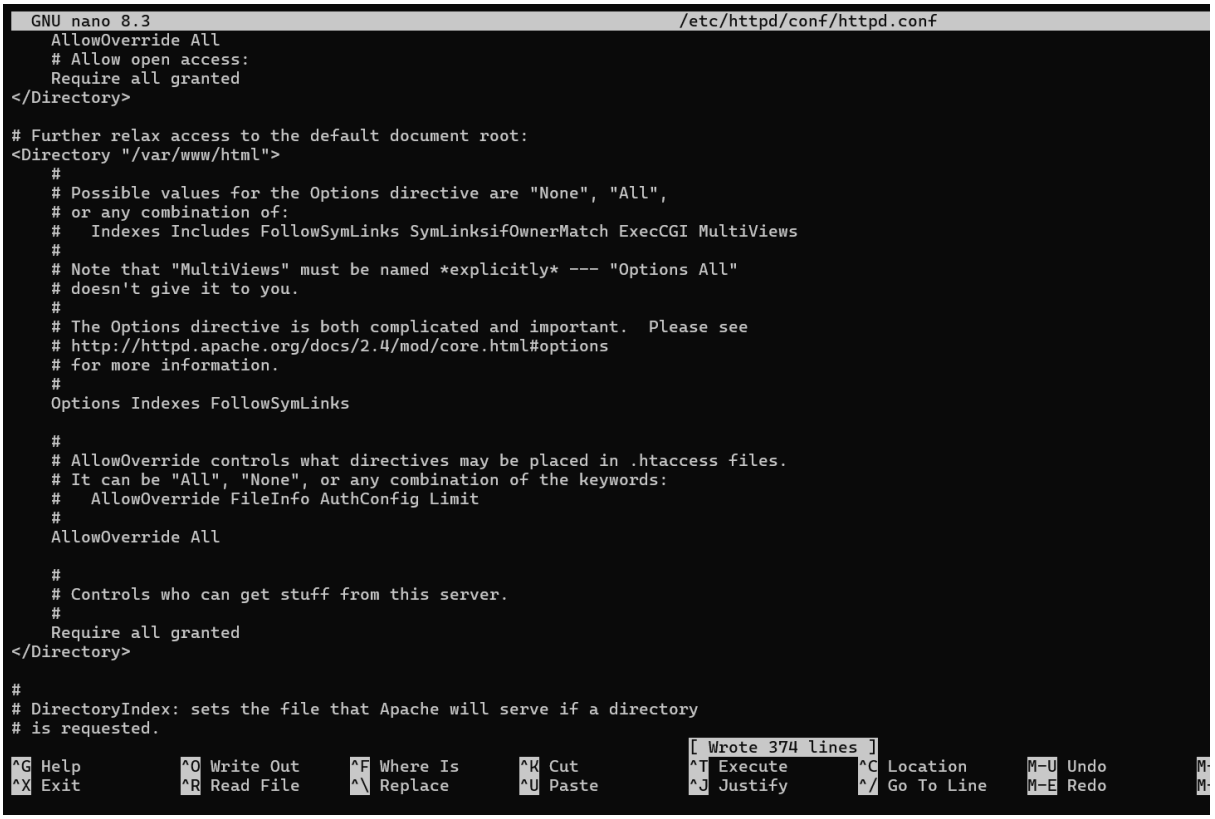
📝 10. Modify .htaccess

In `/var/www/html/.htaccess`, configure URLs to load images via CloudFront:

```
# Example: Redirect image URLs to CloudFront
RewriteEngine On
```

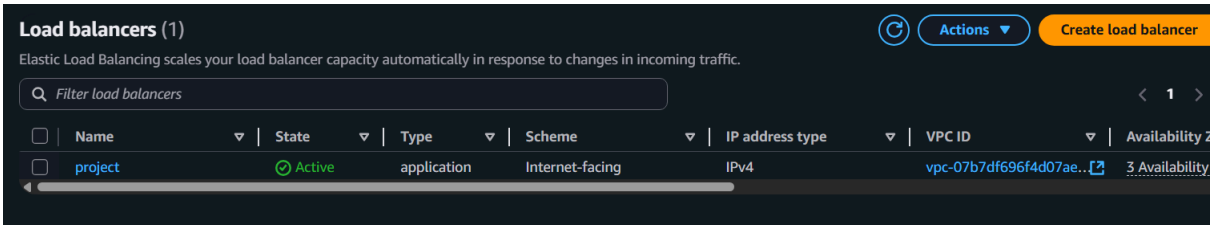
```
RewriteCond %{REQUEST_URI} ^/wp-content/uploads/
RewriteRule ^wp-content/uploads/(.*)$ https://<CLOUDFRONT-DOMAIN>.cloudfront.net/$1 [R=301,L]
```

Replace `<CLOUDFRONT-DOMAIN>` with your actual distribution domain.



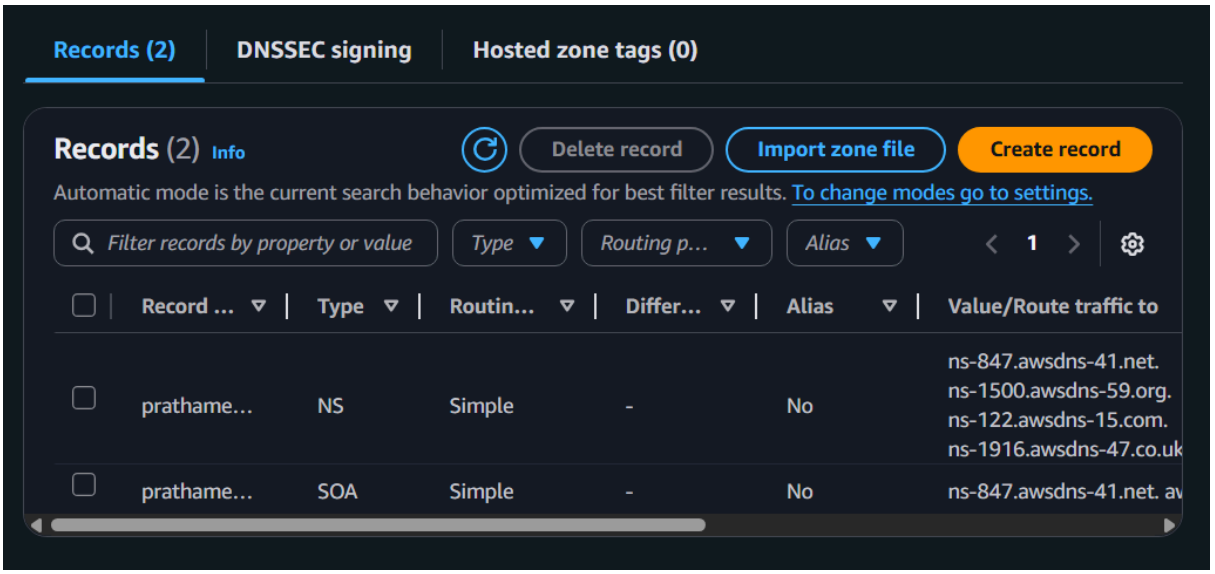
⚖️ 11. Setup Application Load Balancer

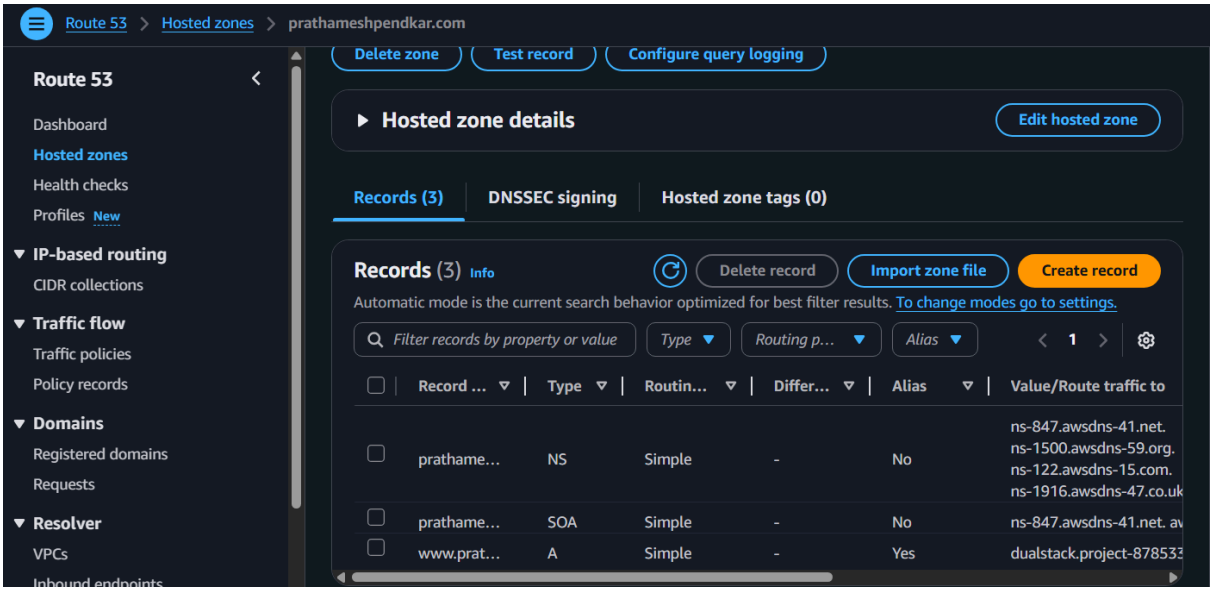
- Create ALB, select:
  - Scheme: internet-facing
  - Listeners: HTTP (80)
- Target group: your EC2 instance
- Route through Route 53

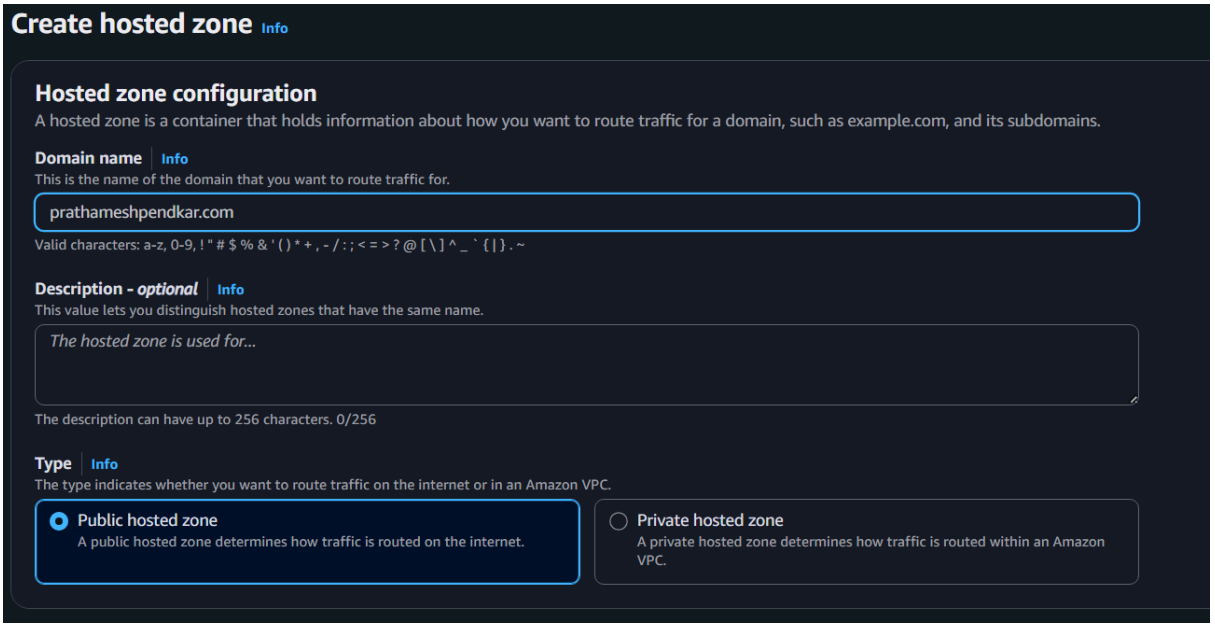


🌐 12. Configure Route 53

- Add a hosted zone with your domain.
- Add A Record (alias) to point to your ALB.
- Update your domain registrar with the provided NS (Name Servers).

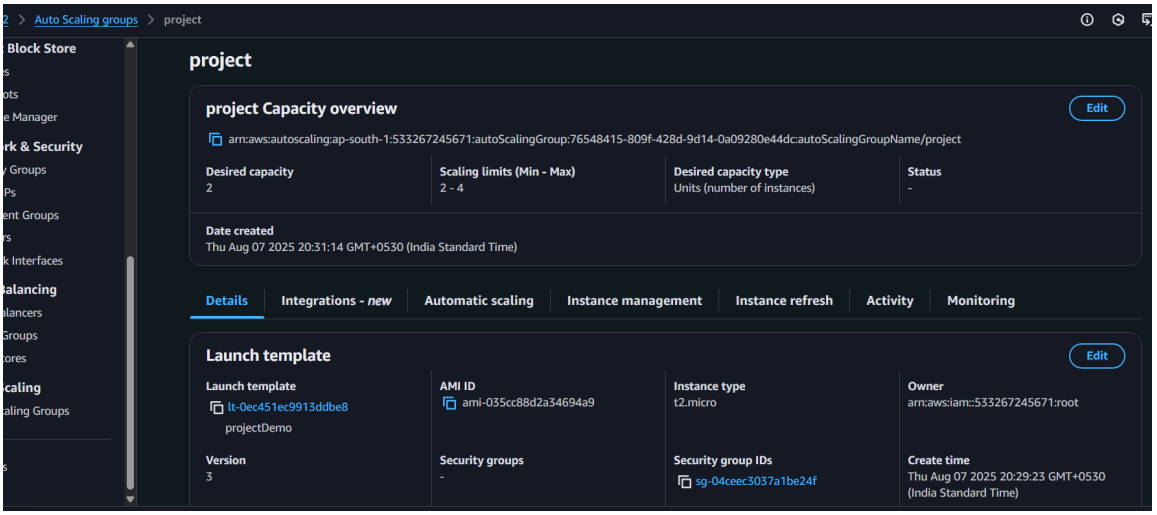






🧬 13. Create AMI and Auto Scaling Group

- From EC2 instance:
  - Create an AMI
- Launch template from AMI
- Create Auto Scaling Group:
  - Use template
  - Attach to target group of ALB
  - Define desired min/max capacity



🧽 Cleanup Checklist (for Notion)

- [x] ~~EC2 instance~~
- [x] ~~Elastic IP~~
- [x] ~~S3 Buckets (code-2005, media-2005)~~
- [ ] CloudFront Distribution
- [x] ~~RDS Instance (project-db)~~
- [x] ~~Security Groups (website-sg, db-sg)~~
- [x] ~~IAM Role (s3-forproject)~~
- [x] ~~Load Balancer (ALB)~~
- [x] ~~Auto Scaling Group~~
- [ ] Launch Template / AMI
- [x] ~~Route 53 Hosted Zone~~
- [ ] Crontab Entries

🔍 Website Overview

- **Platform:** WordPress 6.8.2
- **Theme:** Adas Personal Portfolio (v1.7)
- **Theme Developer:** PencilWp
- **Page Builder Used:** Elementor
- **Purpose:** Personal portfolio website

🎯 Intended Use Cases of Adas Theme

The **Adas Personal Portfolio** theme is designed specifically for:

- **Freelancers** and **job seekers** building their online resume
- **Developers** and **designers** showcasing coding or UI work
- **Photographers** and **artists** creating digital galleries
- **Lawyers, consultants, educators, doctors**, and **speakers** presenting professional credentials

- **Entrepreneurs** promoting a personal brand or service offering

---

✨ Key Features of the Website Theme

- **Elementor Integration** for no-code customization
- **Responsive design** (mobile/tablet friendly)
- **SEO-optimized** structure for better visibility
- **Fast loading performance**
- **Customizable sections:**
  - Resume/CV
  - Skills and achievements
  - Portfolio gallery
  - Blog or news updates
  - Contact forms
- **Supports:** Featured images, custom logos, sticky posts, threaded comments, and translations

---

🧩 Design and Layout Tags

- Blog
- Portfolio
- News
- Grid Layout
- One to Four Column Support
- Custom Background and Logo
- Footer Widgets
- Post Formats
- Sticky Posts
- Theme Options

Prathamesh Pendkar
Cybersecurity Student | IAM & Cloud Security Enthusiast

Skills Project Contact CTF Participation Blog & Write-Ups

HOME

👋 About Me

I'm an aspiring **cybersecurity professional** from 🌆 **Pune** with a strong focus on **Identity and Access Management (IAM)**, ☁️ **cloud security**, and 🔍 **vulnerability assessment**.

🛠️ Skilled in industry-standard tools like **OWASP ZAP**, **Nmap**, **Wireshark**, and **Metasploit** — I've contributed to **real-world bug bounty programs**, performed **cloud infrastructure hardening**, and conducted **digital forensic investigations**.

🔐 My passion lies in building secure systems through **Zero Trust architecture** and implementing effective **access control policies** that protect against modern threats.

🤝 Let's collaborate to build a **secure digital future** together.

View My Projects

Prathamesh Pendkar
Cybersecurity Student | IAM & Cloud Security Enthusiast

Skills Project Contact CTF Participation Blog & Write-Ups

project

Featured Projects

🔐 Secure Web Hosting on AWS

Deployed a secure web application using AWS EC2 and S3. Implemented custom IAM policies to enforce least-privilege access, segregate roles, and secure cloud resources. Used security groups and logging to enhance visibility and prevent unauthorized access.

🛠️ Recon Automation Bash Script

Developed an automated reconnaissance script using Bash to perform subdomain enumeration, port scanning, HTTP probing, and wayback data extraction. Integrated Nmap and FFUF for vulnerability enumeration and generated simplified HTML reports for findings.

🕵️ TSCM Product Design (Surveillance Detection)

Co-designed a hardware-assisted solution to detect hidden surveillance devices. Integrated IAM policy controls to restrict access to logs and sensor data, ensuring secure handling of sensitive environments.

🧪 Web Vulnerability Testing Lab

Built a controlled test environment to simulate OWASP Top 10 vulnerabilities. Used tools like OWASP ZAP, Burp Suite, and Metasploit to test, document, and patch issues. The lab served as a training ground for VAPT practices.

contact

Feel free to reach out to me for cybersecurity projects, internship opportunities, collaborations, or professional inquiries. I'm always open to connecting with like-minded professionals and organizations.

Email: prathameshpendkar@gmail.com
Phone: +91-8390088075
Location: Pune, Maharashtra, India

LinkedIn

GitHub

CTF Participation

CTF

- **Hack IITK – Capture the Flag**
  Participated in IIT Kanpur's prestigious CTF event, focusing on real-world exploitation and binary challenges.
- **Hicathon CTF**
  Competed in a practical CTF challenge simulating real web application vulnerabilities and attack chains.
- **Hacktify CTF Challenge**
  Hands-on bug bounty-style CTF organized by Hacktify, targeting OWASP Top 10 and authentication flaws.

CERTIFICATION

- **AWS Cloud Certification** – SevenMentor, 2025
- **AWS Educate** – IAM, Networking, Security, Cloud 101 (April 2024)
- **CompTIA PenTest+** – Udemy (Self-paced learning)
- **Digital Forensics Essentials (DFE)** – EC-Council (March 2023)

1 Comment
Posted on August 7, 2025

5 Key Lessons from My First Bug Bounty and CTF Experience

Introduction Participating in Capture the Flag (CTF) challenges and bug bounty programs has been a game-changer in my journey as a […]

View Article

changer in my journey as a […]

View Article

Search

Search

Recent Posts

5 Key Lessons from My First Bug Bounty and CTF Experience

Recent Comments

A WordPress Commenter on 5 Key Lessons from My First Bug Bounty and CTF Experience

Your name

Your email

Subject

Recent Comments

A WordPress Commenter on 5 Key Lessons from My First Bug Bounty and CTF Experience

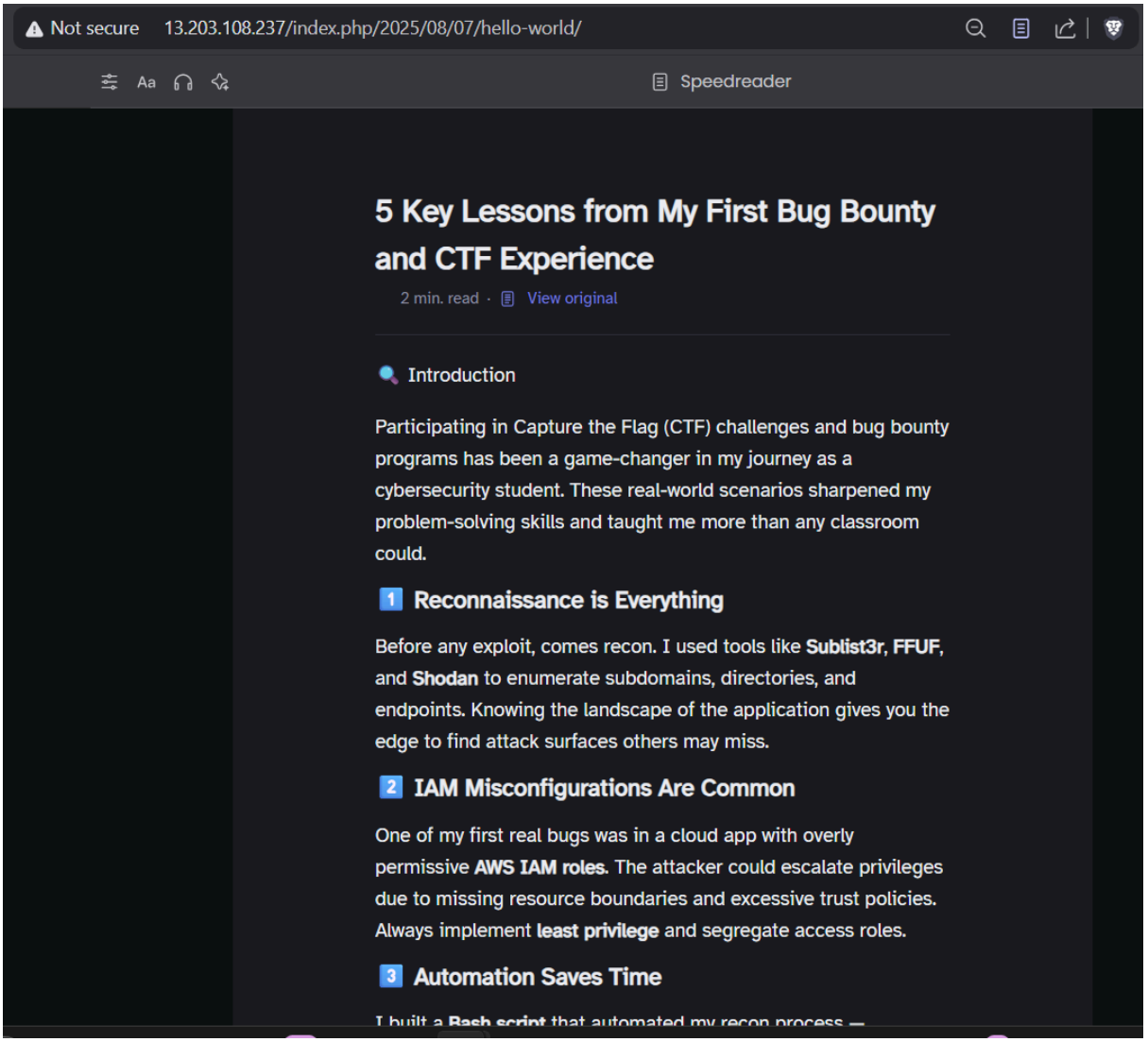
Your name

Your email

Subject

Your message (optional)

Submit



🎓 Learning Outcomes & Core Skills Gained

🛠️ Technical Skills Gained (LOUD AND CLEAR)

🌐 1. Cloud Infrastructure Mastery (AWS)

- Proficient in setting up **S3 Buckets** with appropriate access policies.
- Integrated **CloudFront CDN** with S3 for high-speed global content delivery.
- Deployed **EC2 instances** with Elastic IP, custom bootstrapping, and Apache configuration.

- Managed **IAM roles and permissions** for secure EC2-S3 communication.
- Created and managed **RDS MySQL databases**, understanding subnetting and security groups.
- Configured **Auto Scaling Groups** and **AMI snapshots** for high availability and disaster recovery.
- Utilized **Route 53** for DNS and domain mapping to Application Load Balancer.

⚙️ 2. Web Server & WordPress Configuration

- Installed and configured **Apache**, **PHP**, **MySQL**, and **WordPress** on Amazon Linux 2.
- Automated deployments using **bash bootstrap scripts** and `crontab` for scheduled syncing.
- Integrated and modified the `.htaccess` file for **URL rewriting** and **CloudFront offloading**.
- Enabled **media redundancy** by syncing `/var/www/html` with **S3 buckets**.
- Applied **custom WordPress themes** (Adas) and ensured **Elementor compatibility**.

🧱 3. Security & Networking

- Designed and applied **VPC Security Groups** for safe access (HTTP, SSH, MySQL).
- Enforced **least privilege access** using custom IAM roles and policies.
- Hardened bucket access with **explicit S3 bucket policies**.
- Bound EC2 ↔ RDS securely using internal traffic rules.

🗃️ 4. Content Delivery & Performance Optimization

- Offloaded static content (images, assets) to S3 and served via **CloudFront CDN**.
- Achieved **fast-loading WordPress performance** by minimizing EC2 load and maximizing cache delivery.

- Created scalable infrastructure for **WordPress-based applications** using AWS-native services.

🔧 Other Technical Tools Mastered

- `awscli` commands (`s3 sync`, `configure`, `ec2`, `rds`)
- Bash scripting for automation
- `crontab` for scheduled tasks
- `nano`, `yum`, `wget`, `tar`, `chkconfig`, `service` commands in Linux

💡 Soft Skills & Professional Development

🧠 1. Problem-Solving & Troubleshooting

- Diagnosed EC2 package issues, permission problems, and RDS connectivity in real time.
- Adapted `.htaccess` rules for seamless CDN redirection without breaking image paths.
- Resolved permission conflicts between Apache, S3, and WordPress.

🎯 2. Project Management & System Design

- Designed a **modular, scalable architecture** from scratch.
- Created detailed implementation steps and infrastructure documentation (Notion-compatible).
- Implemented redundancy, performance optimization, and auto-healing via autoscaling.

🤝 3. Communication & Documentation

- Maintained structured documentation for deployment, security, and operations.
- Clearly explained the architecture flow and components involved (for clients, team, or stakeholders).

👨‍💻 4. DevOps & Automation Mindset

- Automated WordPress installation and S3 syncing.
- Used `crontab`, AMI templates, and bootstrapping to reduce manual efforts and human errors.

🚀 Highlight Achievement

> ✅ Successfully deployed a scalable, cloud-native WordPress website using modern AWS services and served media via CloudFront for high-performance delivery — demonstrating real-world DevOps and cloud engineering expertise.

🔗 LinkedIn Post

🚀 **Project Launch Alert!**

I'm thrilled to share that I've successfully **designed, deployed, and scaled** a complete **WordPress-based personal portfolio website** on **Amazon Web Services (AWS)**! 🌐⚙️

Hosted here 👉 http://13.203.108.237/

Built using: **WordPress 6.8.2**, **Adas Personal Portfolio Theme**, and the powerful **Elementor** builder.

💡 **What I Did:**

- Deployed EC2 with Apache, PHP, and WordPress
- Configured RDS (MySQL) and bound securely with EC2
- Set up S3 buckets for static assets + CloudFront CDN
- Automated syncing via crontab
- Enabled Route 53 DNS + Application Load Balancer
- Scaled the setup using AMIs and Auto Scaling Groups

🔐 Also integrated secure access using IAM roles and policies, along with well-defined security groups and VPC setup.

📈 **Core Skills Gained:**

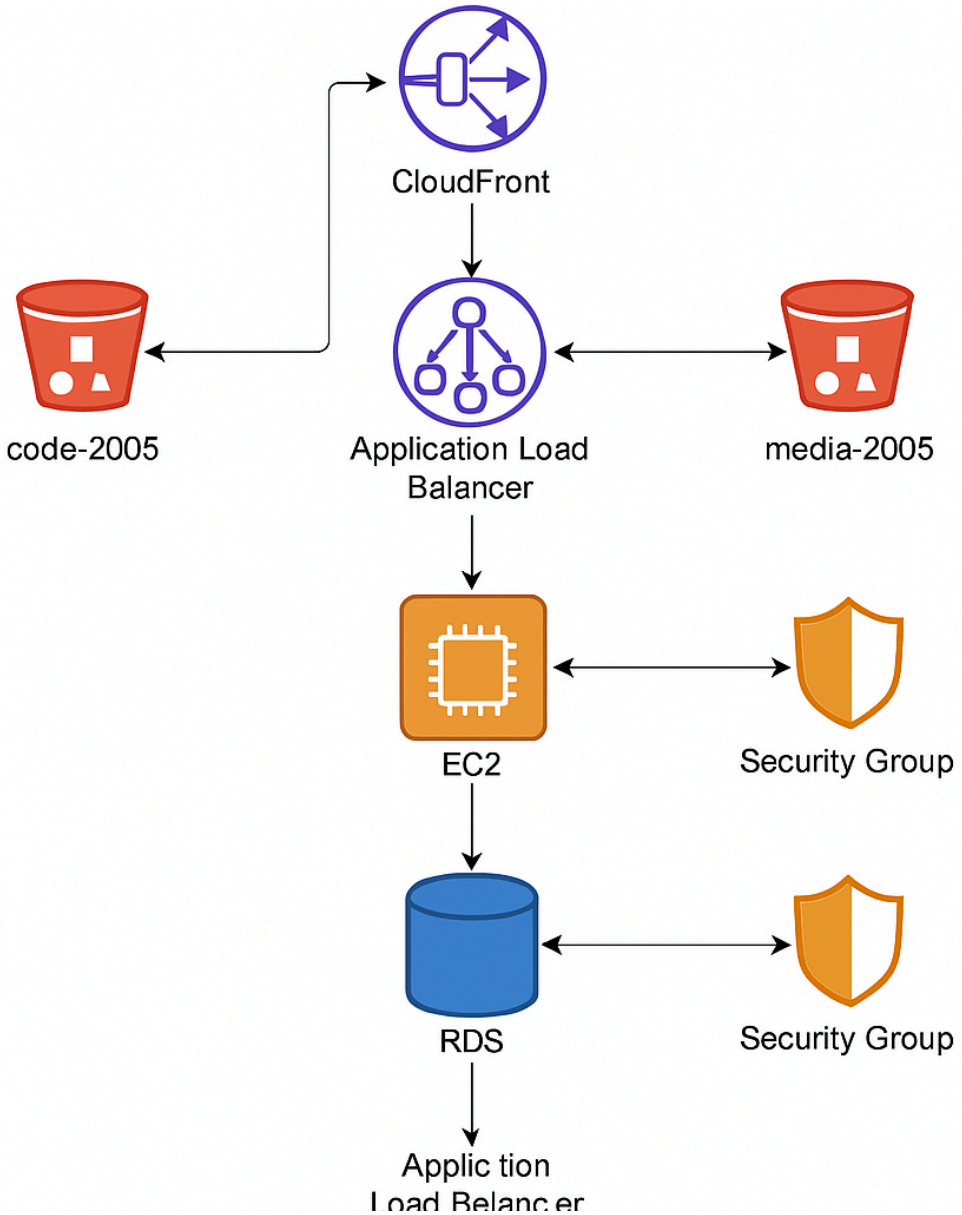
- Cloud Infrastructure Design
- Web Server & WordPress Management
- Automation with Bash & Crontab
- Performance Optimization via S3 & CDN
- Hands-on DevOps Mindset

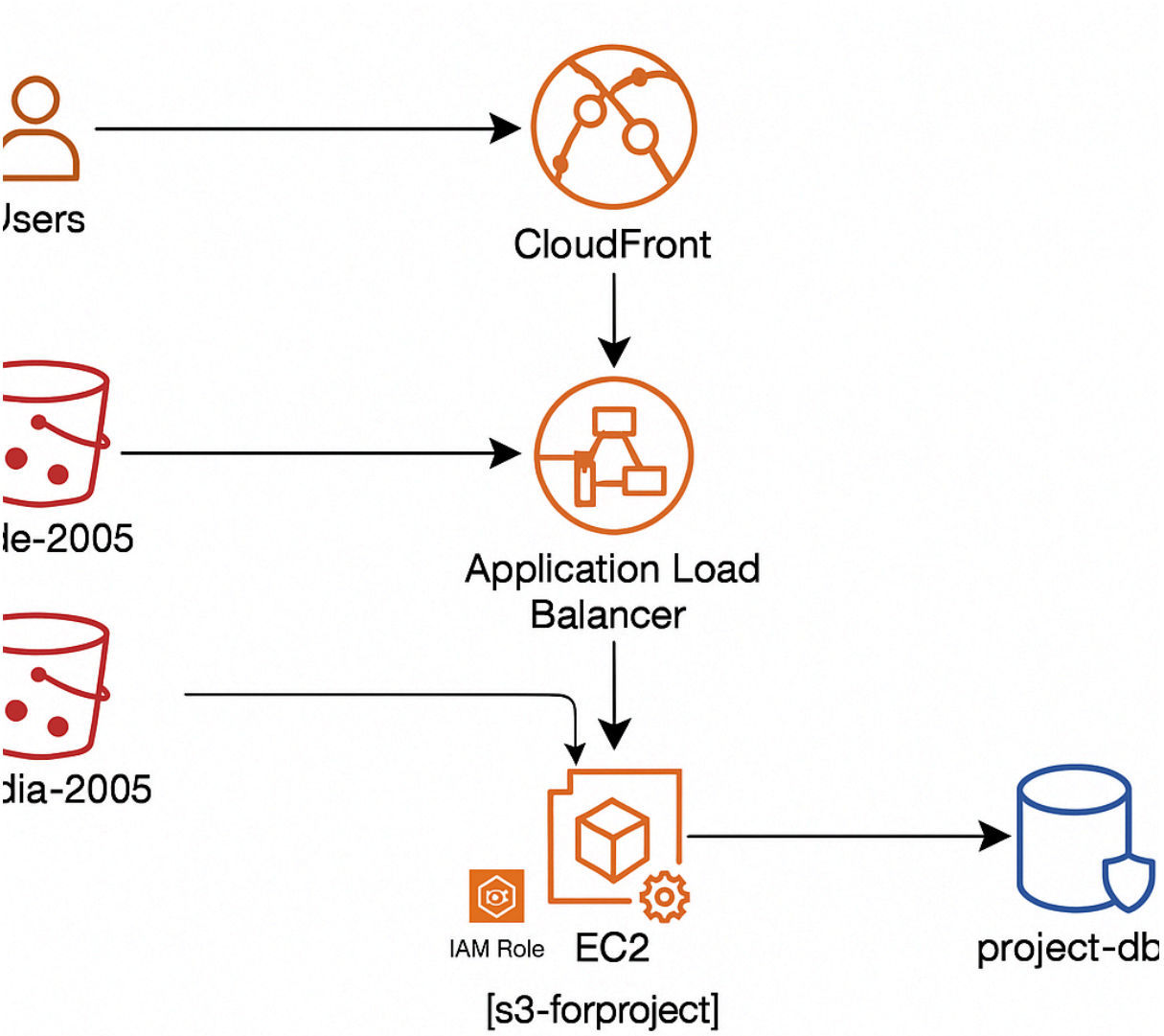
🙏 Special thanks to **@SevenMentor Pvt. Ltd.** and our amazing mentor **@Nilesh Lipane** for constant guidance, inspiration, and knowledge-sharing throughout the journey. Your support truly elevated this project! 💯

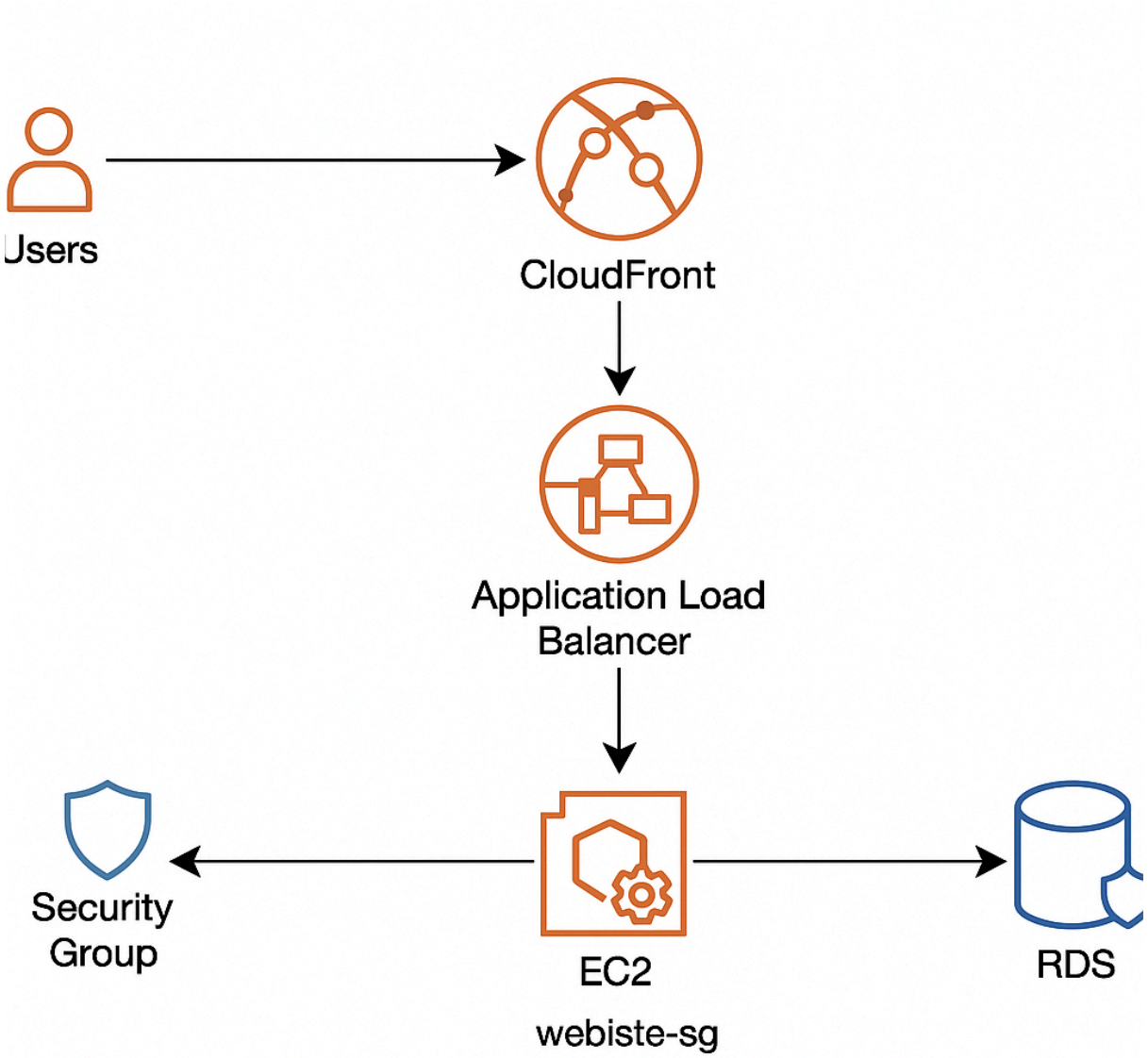
🔧 This wasn't just a website — it was a full **cloud-native deployment experience** and an opportunity to master end-to-end AWS hosting for dynamic applications.

#WordPress #AWS #DevOps #CloudComputing #PortfolioWebsite #Automation #S3 #CloudFront #EC2 #Route53 #AutoScaling #Linux #MySQL #WebHosting #Elementor #AdasTheme #SevenMentor #NileshLipane #LearningByDoing

---


CloudFront
code-2005
Application Load Balancer
media-2005
EC2
Security Group
RDS
Security Group
Applic tion
Load Belanc er


Users
CloudFront
le-2005
Application Load Balancer
dia-2005
IAM Role
EC2
[s3-forproject]
project-db



🔐 Security Report: Cloud-Based Printer Management System

✅ 1. Current Security Architecture Overview

- **Authentication**: Implemented via Cognito or IAM-based access control.
- **Network Security**: VPC with Public/Private subnets, Security Groups, and NACLs.
- **Storage Security**: S3 buckets with restricted IAM roles; versioning enabled.
- **Database Security**: RDS encrypted at rest; access controlled via SG & IAM.

- **Logging & Monitoring**: CloudTrail, GuardDuty, and AWS Config are active.
- **Data in Transit**: Enforced HTTPS via ACM + ALB/CloudFront TLS 1.2+.
- **WAF**: AWS WAF configured to block common threats (SQLi, XSS).
- **Endpoint Protection**: EC2 instances use Systems Manager & EDR tools.

🚨 2. Identified Risks

Risk ID	Description	Severity	Affected Component
R-01	Overly permissive IAM policies	High	IAM Roles/Users
R-02	S3 bucket public access not fully disabled	High	Media Storage
R-03	No MFA enforcement for admin accounts	Medium	IAM
R-04	No automated backup validation	Medium	RDS
R-05	Lack of rate-limiting on API endpoints	Medium	API Gateway
R-06	Logs retention not clearly defined	Low	CloudWatch Logs

🛠️ 3. Recommendations for Improvement

Area	Recommendation	Benefit
IAM	Enforce least privilege & use IAM Access Analyzer	Reduces blast radius
S3	Block public access at account level, enable object lock	Prevents data leaks
MFA	Enforce MFA for all IAM users and root	Stops unauthorized access
API	Enable throttling & AWS Shield Standard	Mitigates API abuse
RDS	Add automated backups + test recovery scripts	Ensures data availability
WAF	Create custom rules for printer abuse detection	Increases app resilience

Area	Recommendation	Benefit
Monitoring	Enable Amazon Detective & GuardDuty alerts	Speeds up incident response
CI/CD	Add static code scanning (e.g., CodeGuru/Snyk)	Prevents insecure code

🧩 4. Suggested Security Tools/Services

Tool	Use Case
AWS Config	Continuous compliance checks
AWS Inspector	Automated vulnerability scans
AWS Secrets Manager	Secure credential storage
Amazon Macie	Sensitive data discovery in S3
AWS Shield Advanced	DDoS protection for critical services