Table of Contents

Table of Figures

Tables

Yogesh Anandhakumar
MSc Cyber Security
National College of Ireland
Dublin, Ireland
x23167998@student.ncirl.ie

CA1

Introduction

Cloud computing refers to the on-demand provision of IT resources, whereby users receive metered services via a network from an IT infrastructure and applications. Salesforce, Dropbox, Facebook, Gmail, and others are a few examples of cloud systems. Cloud computing features include distributed storage, rapid elasticity, automated management, resource pooling, wide network access, measured service, and virtualization technologies.

Here I have deployed a WordPress web application in AWS Academy cloud platform as per our project description [1], [2], [3], [4]. I have used the IAAS & private cloud deployment model, where I have managed the data, interfaces, applications, middleware, OS, VM's & Virtual network. Also used CloudWatch & Net data for monitoring the EC2 Instance. Then a custom theme and many plugins related to security has been installed. Then various web security scans and penetration tests has been done and mitigations for vulnerabilities which are present in the application. Finally recorded those in this report. This project ensures high availability and scalability of applications.

Approach & Project Planning

The approach I have taken to implement security across the system in this project is ZTA (Zero Trust Architecture) & DID (Defense-in-Depth) and Agile methodology as my project plan for specifying the tasks and dependencies, associated with the implementation of systems & services across the selected cloud assets.

Here in this project, a 3-tier architecture in two availability zones (us-east 1a & us-east 1b) was used as architecture for running a WordPress web application in AWS Academy Learner's Lab, namely, Web Tier, App Tier & Database Tier. This website was created using WordPress in AL2023 instance.

Initially, a VPC has been created. Then an Internet Gateway has been created and attached to the VPC. Then 6 Subnets has been created in the two availability zones, where 2 are public subnets (web tier) & 4 are private subnets (app tier & database tier). Then 2 NAT Gateways has been created and attached with Elastic IP's, on two available zones in the public subnet. Then one Public Route table & two Private Route Tables has been created. Then 5 VPC Security groups has been created, where each security group was allocated for each service. The security groups are, ALBSG accepts Http & Https protocol traffics alone from anywhere. WEBSG accepts Http & Https protocols traffics alone but only from the ALBSG. DBSG accepts MySQL/Aurora traffic alone from WEBSG only. ELBSG (EFS-SG) accepts NFS traffic alone from WEBSG. SSHSG allows SSH only from my IP Address. In RDS, a database subnet group has been created by selecting the private database subnets in the two availability zones. Then an main and standby RDS MySQL database has been created under RDS DB Subnet group and using DBSG & 2 private subnets (DB Tier). Then an Elastic File System has been created with ELBSG(EFSSG). Then 3 EC2 instances have been created where 1 instance launched on public subnet (Web Tier) in availability zone 1with an Elastic IP, which is the jump server and 2 instances launched on private subnet (App Tier) in two availability zones each with an Elastic IP, used as load balancing servers. Instance in web tier has been launched with ALBSG, SSHSG & WEBSG. Instances in app tier has been launched with WEBSG alone. Then two target groups (80 & 443) have been created in EC2 for creating a load balancer. Then an Application Load Balancer has been launched with ALBSG. Below diagram is my 3-Tier Architecture.

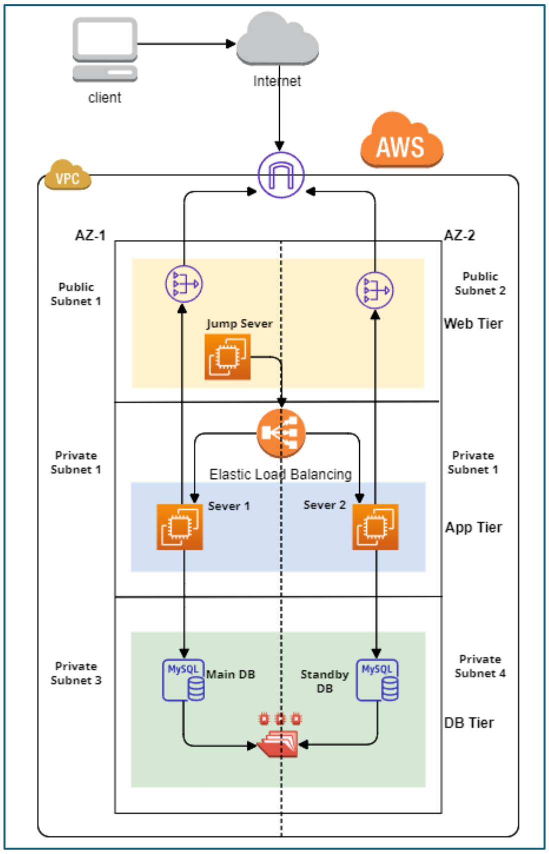
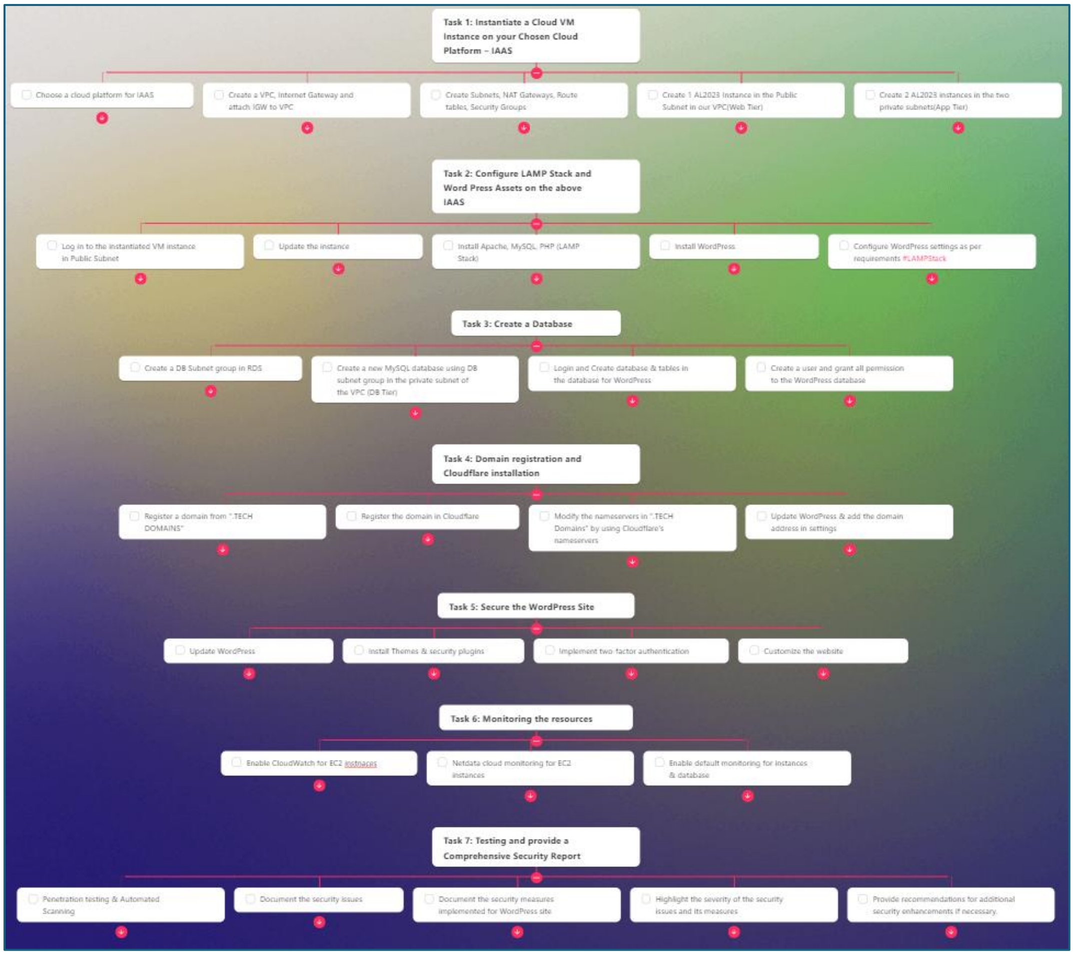


Figure 1 AWS 3 Tier Architecture

The website has been created mainly focused on helping peoples to overcome from poverty. The website has 9 pages which are About us, Registration, My Account, Donor Dashboard, Donation Confirmation, Donation Failed, Terms & Conditions, Disclaimer and Privacy Policy.

Below diagram represents the project planning approach which have been chosen and implemented successfully.



Task 1: Instantiate a Cloud VM Instance on your Chosen Cloud Platform – IAAS

- □ Choose a cloud platform for IAAS
- □ Create a VPC, Internet Gateway and attach IGW to VPC
- □ Create Subnets, NAT Gateways, Route tables, Security Groups
- □ Create 1 AL2023 Instance in the Public Subnet in our VPC(Web Tier)
- □ Create 2 AL2023 instances in the two private subnets(App Tier)

Task 2: Configure LAMP Stack and Word Press Assets on the above IAAS

- □ Log in to the instantiated VM instance in Public Subnet
- □ Update the instance
- □ Install Apache, MySQL, PHP (LAMP Stack)
- □ Install WordPress
- □ Configure WordPress settings as per requirements #LAMPStack

Task 3: Create a Database

- □ Create a DB Subnet group in RDS
- □ Create a new MySQL database using DB subnet group in the private subnet of the VPC (DB Tier)
- □ Login and Create database & tables in the database for WordPress
- □ Create a user and grant all permission to the WordPress database

Task 4: Domain registration and Cloudflare installation

- □ Register a domain from ".TECH DOMAINS"
- □ Register the domain in Cloudflare
- □ Modify the nameservers in ".TECH Domains" by using Cloudflare's nameservers
- □ Update WordPress & add the domain address in settings

Task 5: Secure the WordPress Site

- □ Update WordPress
- □ Install Themes & security plugins
- □ Implement two factor authentication
- □ Customize the website

Task 6: Monitoring the resources

- □ Enable CloudWatch for EC2 instnaces
- □ Netdata cloud monitoring for EC2 instances
- □ Enable default monitoring for instances & database

Task 7: Testing and provide a Comprehensive Security Report

- □ Penetration testing & Automated Scanning
- □ Document the security issues
- □ Document the security measures implemented for WordPress site
- □ Highlight the severity of the security issues and its measures
- □ Provide recommendations for additional security enhancements if necessary.

Figure 2 Planning

Selection of Tools Methodologies, Frameworks & Benchmarking

AWS Cloud platform has been chosen in this project. It has been chosen because of having previous experience with AWS Cloud services. In AWS Cloud, the services which are used in this project are VPC, EC2, RDS, CloudWatch & EFS. VPC has been chosen to create a private cloud infrastructure in AWS. EC2 has been chosen to create instances to act as a server and an elastic load balancer also created. RDS has been chosen to run a MySQL Database, where WordPress data like configurations, users, passwords, etc, are stored. EFS has been chosen, so that the webservers can pull application data from EFS. CloudWatch has been chosen to monitor the EC2 instances. Netdata, an online cloud monitoring tool, also used as a monitoring tool. STRIDE tool used for threat modelling. Nmap is used for identifying open ports and running services & its version. Wireshark is used for packet capturing and analysing the web traffic from client to server. Burp suite is used for penetration testing the application. Automated scanning tools are used to scan the web application, namely Acunetix, Burp Scan, Nikto, whatweb, Vooki & wpscan-cli.

The approach I have taken to develop and implement security across the system in this project is ZTA (Zero Trust Architecture) & DID (Defense-in-Depth) and Agile methodology as my project plan for specifying the tasks and dependencies, associated with the implementation of systems &services across the selected cloud assets.

Agile methodology prioritizes tasks and adjusts to changing requirements throughout the project. It focuses on iterative development and continuous improvement and calls for close monitoring for useful feedback and course correction. The project is divided into smaller, more manageable tasks within brief development cycles. Its advantages include flexibility in the face of change, ongoing development, and improved communication. Its disadvantages include the need for more preparation and work up front, which can be problematic for big projects [5].

Although ZTA (Zero Trust Architecture) and Defense-in-Depth are security techniques, they take distinct approaches to security. Below is a summary of their main distinctions. ZTA stands for "Verify first, trust later." This entails constantly confirming, whether on-site or off-site, the legitimacy and authorization of any person or device attempting to access a resource. focuses entirely on defending systems and data against internal and external attacks. Uses least privilege access constraints, micro-segmentation, and multi-factor authentication (MFA). DID refers to building several tiers of security measures to impede and even halt intruders. primarily concerned with protecting the network perimeter from outside attacks. putting it into practice by making use of network segmentation, firewalls, intrusion detection/prevention systems (IDS/IPS), and access control lists (ACLs) [6], [7].

Here, I've used the high-level Cyber Security Framework (NIST CSF) from the National Institute of Standards & Technology, which offers a procedure for recognizing, safeguarding against, identifying, responding to, and recovering from cyberattacks. In order to strengthen the configuration, I have also implemented Center of Internet Security Controls to the AWS infrastructure (EC2 instances & RDS Databases). The web application has been hardened to protect it from security flaws and attacks based on OWASP Top 10 2023.

Technical Testing approach

Initially I have made many security implementations in AWS IAAS environment as well as in the Web Application. After these security Implementations, I conducted manual penetration testing as well as automated scans for finding vulnerability in my application.

Below table represents the security implementation done in IAAS environment,

Table 1 Security Implementations made in IAAS environment

Services	Purpose
VPC	It offers our cloud resources a private network environment that is isolated from other users' resources in the public cloud. This isolation limits illegal access to our data and applications, which contributes to increased security.
Subnets	An IP address range is divided into VPC subnets inside of bigger Virtual Private

	Clouds (VPCs). It facilitates the logical grouping of our AWS resources into VPCs according to their purposes or security needs. Within a VPC, we can build numerous subnets, each with a unique range of IP addresses.
Internet Gateway	It serves as a controlled entry point or exit point for internet traffic. It permits connections between our VPC's resources and the outside internet, and the other way around.
NAT Gateway	It gives our resources inside private subnets in our VPC to access the outside world. In our project, it provides the two load-balancing servers in the public subnet of the two availability zones (App Tier) with outgoing internet connectivity.
Route Table	It functions as a route map for our VPC, which needs to be set up with IGW or NATGW depending on what we require. This will send traffic to the routes that we have set up.
Security Groups	It controls incoming and outgoing traffic to protect your resources, functioning as virtual firewalls.
RDS Database Subnets	It's a group of subnets in our VPC that we use especially for our RDS database instances. It guarantees dependable and safe database connectivity within your AWS setup.
RDS MySQL Database	AWS provides a managed database that we can construct, utilize, and scale up or down based on our needs.
Elastic File System	Our web application data is kept in this scalable and centralized storage facility, which is accessible by numerous web servers.
Load Balancing Target Groups	It serves as a reservoir of possible locations for incoming traffic that is dispersed by an ELB.
Load balancer	To guarantee high availability and scalability, it serves as a traffic cop, automatically distributing incoming web traffic among our ELB target groups.
EC2 Instances	It functions as a virtual server and uses the necessary system resources in accordance with our configuration. Three t2medium instances were employed in this project to provide high availability and scalability in

	both public and private subnet (Stage). One of the instances served as a jump server in the public subnet on availability zone one (Web Tier), while the other two served as load balancers in the private subnet (App Tier).
Elastic IP	An internet connection is made possible for us by a static public IPV4 address that is assigned to us in a particular region.
Snapshots	This is used to capture the entire state of volumes attached to instances. Here we have taken one snapshots of each instance for backup as well as safety purpose.
CloudWatch	This is how the complete state of volumes connected to instances is captured. Here, we have a snapshot of every instance for safety and backup purposes.
Netdata	An online tool for cloud monitoring that assists us in gathering data, logs, and events related to our AWS resources and notifies us via email when certain criteria are met [8].
MobaXterm_Personal_24.0	A SSH Client tool, which is used in this project to securely ssh into the EC2 Instances.

Below are the Security Implementations done in WordPress Web Application,

Table 2 Security Implementations made in WordPress site

Services/Plugins	Purpose
. TECH DOMAINS	A platform built on the GitHub student developer bundle that offers a free domain for a year.
Cloudflare	Content Delivery Network (CDN), DDoS prevention, Internet Security, SSL Certificates, DNS security, website optimization tools, analytics, and other services are among the many services it offers connected to internet security and performance. Since we have linked Cloudflare's name servers to .Tech domains, all traffic will go via Cloudflare, which is a safe and difficult to evade system.
SSL Certificates	This is supplied by Cloudflare, which is used to give privacy and data integrity to visitors of our website.

PhpMyAdmin	An open-source administration tool specifically designed to manage MySQL and MariaDB databases.
Akismet Anti-spam: Spam Protection	To protect my website from spam.
All In One WP Security	Provides MFA, file backup options, Import/Export functionalities.
GuardGiant Brute Force Protection	Prevents brute force attacks, provides Captcha, reverse proxy, whitelists IP addresses.
HTTP Headers	Provides every HTTP Headers, where we can customize as our security need.
LoginWP (Formerly Peter's Login Redirect)	Provides a secure Login as well as New User Registration page for WordPress website.
Members	Provides flexibility for admin to restrict the permissions of users, more than default permissions given by WordPress.
Security Optimizer	All-in-one security solution for WordPress website, which secure website and prevents several threats such as brute-force attacks, compromised login, data leaks and more.
Stop User Enumeration	Helps securing WordPress site against hacking attacks through detecting User Enumeration
Super Page Cache for Cloudflare	Speed up your website by enabling page caching on a Cloudflare free plans.
User Registration	Drag and Drop user registration form and login form builder. Used to create a secure login and registration page for donors.
w3v-xml-rpc-security	This disables XML-RPC, by removing some methods and make more secure your WordPress site.
WP 2FA - Two-factor authentication for WordPress	Provides an additional layer of security to WordPress login pages. Enables Two-Factor Authentication for all users in my WordPress website.
WP Anti-Clickjack	This prevents website from being clickjacked, by adding OWASP's legacy browser frame breaking script & X-Frame-Options.

Also, I have done manual penetration testing and many automated scans over this website. Before starting the testing process, I have taken backups of files & snapshots of all the three instances for safety purposes. So, even if I lose any data’s while testing, I can recover those from the snapshot and backups. Manual testing has been done like XSS, URL redirection, parameter tampering, etc, by using Burp suite, which acted as a proxy, where I have intercepted the requests & modified the requests. Also used Intruder tool in burp suite, which helped in performing automated attacks like password brute force attacks. Also used repeater tool in burp suite, which helped me to resend any captured packets and analyse the response of modified requests. Also used the burp scanner, for running automated scans. I have used Acunetix, Vooki, Nikto & WP-Scan CLI for automated scans. I have used Nmap for identifying open ports and its services, also used Wireshark to capture packets and check if the traffic is encrypted or not [9], [10], [11], [12], [13], [14], [15], [16].

Findings & Risk Ratings

Table 3 Findings, Risk Ratings & Mitigations

Vulnerability	Risk	Mitigations
Directory Listing	Medium	Mitigated by removing "-Indexes" in Apache server config file.
Admin login page detection	Medium	I have enforced MFA, so this is not applicable.
XML_RPC Authentication brute force	Medium	Mitigated by disabling XML-RPC Authentication by "w3v-xml-rpc-security" plugin.
Missing Security Headers – Cache-Control	Low	All the traffics are secured and encrypted as I used Cloudflare, so this is not applicable.
Missing Security Headers – X-Frame Options	Low	All the traffics are secured and encrypted as I used Cloudflare, so this is not applicable.
Missing Security Headers – Referrer-Policy	Low	All the traffics are secured and encrypted as I used Cloudflare, so this is not applicable.
Missing Security Headers – Content Security Policy	Low	All the traffics are secured and encrypted as I used Cloudflare, so this is not applicable.
Missing Security Headers – X-XSS Protection	Low	All the traffics are secured and encrypted as I used Cloudflare, so this is not applicable.
Missing Security Headers – Permissions Policy	Low	All the traffics are secured and encrypted as I used Cloudflare, so this is not applicable.
HSTS not implemented	Low	All the traffics are secured and encrypted as I used

		Cloudflare, so this is not applicable.
User registration page detection	Info	This page helps donors to register & donate funds to overcome poverty.

As per the scan results and my manual testing, my AWS environment is completely safe, which also ensures high availability and scalability of applications. The Web Application has some vulnerabilities, which are mitigated later. Now my website is completely safe after implementing Two Factor Authentication, Security Plugins, making few changes in server configurations, restricting file permissions, etc.

Challenges & Limitations

As I have used AWS Academy Learner's lab for this project, I faced many restrictions. My project plan is to create the setup which I have done in AWS Academy learners lab as mentioned previously and create a DR in Microsoft Azure environment. After creating the setup in two different cloud environments, I would have connected these two environments by using AWS Direct Connect and Azure Express Route or I would have connected these two environments by using VPN Connections, AWS Transit Gateway in AWS environment and Azure VPN Gateway in Azure environment. Also, I wanted to use AWS WAF as firewall, AWS Certificate Manager for SSL Certificate management, AWS Route 53 for domain registration, IAM permissions for creating users, roles, groups, custom policies as per plan. As I have restrictions in AWS Academy Learner's lab, I was not able to use many resources. Below is my actual project plan,

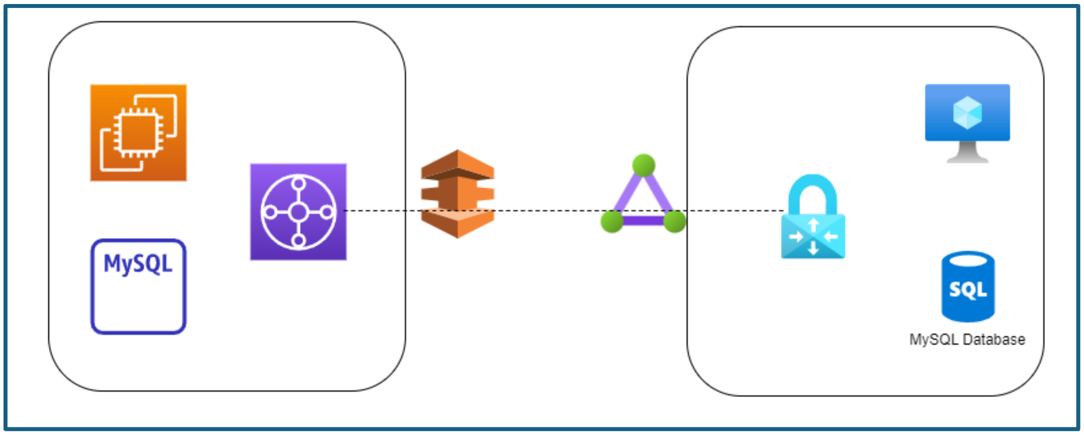


Figure 3 Actual Architecture Plan

Conclusion & Findings

This project's main goal is to setup a secure cloud environment on AWS, instantiate a cloud VM instance, configure LAMP Stack & WordPress assets on the IAAS. Then secure both VM instance & WordPress web application and provide a comprehensive security report which shows our efforts in securing the Cloud environment as well as WordPress web application.

As per the project requirements, I have secured the cloud VM instance by following steps.

- Designed a 3-Tier architecture (Web-Tier, App-Tier & Database-Tier).
- Created a VPC
- Created an Internet Gateway and attached it to VPC
- Created 3 subnets in Availability zone 1 (us-east 1a) and 3 subnets in Availability zone 2 (us-east 1b). (1 Public subnet & 2 Private Subnet)
- Launched a t2medium AL2023 instance in Public Subnet (Web Tier) with an Elastic IP, configured LAMP Stack, MySQL, PhpMyAdmin, WordPress & mounted EFS on /var/www/html folder.
- Created 2 NAT gateways with one Elastic IP for each in two availability zones in public subnet (Web-Tier).
- Created 4 private subnets, 2 in App-Tier, 2 in Database-Tier.
- Created 2 t2medium instances in public subnet of 2 availability zones in App-Tier, with some user data, to install PHP and MySQL, mounted EFS on /var/www/html folder and start those two services by default upon every time when instance starts.
- Created a RDS Subnet group and then created one RDS MySQL Instance in Availability zone 1 and another one standby database in Availability zone 2 in the Database Tier.
- Then connected the server and DB with WordPress.
- Made customizations as well as security implementations in WordPress.
- Undergone manual as well as automated penetration testing on the WordPress website.
- Finally mitigated all vulnerabilities and documented.

Critical insights on UN Sustainability Goals

This website has been created based on the first goal of UN Sustainability goals, **"POVERTY".** This website has been created to mainly focus on helping peoples to overcome from poverty, by the donations which are provided by the donors. This website acts as a helping hand for peoples who need education, food, dresses, etc. This website has a registration page, where you can register yourself and donate the funds as much as possible for their welfare.

Individual Grading Score / Team Member Score

This entire project has been done and documented by me alone.

References:

[1] AWS, "Tutorial: Host a WordPress blog on AL2023 - Amazon Linux 2023," AWS. Accessed: Apr. 08, 2024. [Online]. Available: https://docs.aws.amazon.com/linux/al2023/ug/hosting-wordpress-aml-2023.html

[2] AWS, "Tutorial: Configure SSL/TLS on AL2023 - Amazon Linux 2023," AWS. Accessed: Apr. 08, 2024. [Online]. Available: https://docs.aws.amazon.com/linux/al2023/ug/SSL-on-amazon-linux-2023.html

[3] AWS, “Tutorial: Install a LAMP server on AL2023 - Amazon Linux 2023,” AWS. Accessed: Apr. 08, 2024. [Online]. Available: https://docs.aws.amazon.com/linux/al2023/ug/ec2-lamp-amazon-linux-2023.html

[4] WordPress, “WordPress.com: Build a Site, Sell Your Stuff, Start a Blog & More,” WordPress.com. Accessed: Apr. 08, 2024. [Online]. Available: https://wordpress.com/

[5] Sunil Chahal, “Agile and Project Management in Cybersecurity Optimisation | Institute of Project Management,” Institute Project Management. Accessed: Apr. 08, 2024. [Online]. Available: https://projectmanagement.ie/blog/agile-and-project-management-in-cybersecurity-optimisation/

[6] CrowdStrike, “What is Zero Trust Architecture (ZTA)? - CrowdStrike,” CrowdStrike. Accessed: Apr. 08, 2024. [Online]. Available: https://www.crowdstrike.com/cybersecurity-101/zero-trust-security/zero-trust-architecture/

[7] Fortinet, “What is Defense in Depth? Defined and Explained | Fortinet,” Fortinet. Accessed: Apr. 08, 2024. [Online]. Available: https://www.fortinet.com/resources/cyberglossary/defense-in-depth

[8] Netdata, “Netdata: Monitoring and troubleshooting transformed,” Netdata. Accessed: Apr. 08, 2024. [Online]. Available: https://www.netdata.cloud/

[9] WPScan, “WPScan: WordPress Security Scanner,” WPScan. Accessed: Apr. 08, 2024. [Online]. Available: https://wpscan.com/

[10] Wireshark, “Wireshark · Go Deep,” Wireshark. Accessed: Apr. 08, 2024. [Online]. Available: https://www.wireshark.org/

[11] Nmap, “Nmap: the Network Mapper - Free Security Scanner,” Nmap. Accessed: Apr. 08, 2024. [Online]. Available: https://nmap.org/

[12] Acunetix, “Vulnerability Scanner - Web Application Security | Acunetix,” Acunetix. Accessed: Apr. 08, 2024. [Online]. Available: https://www.acunetix.com/vulnerability-scanner/

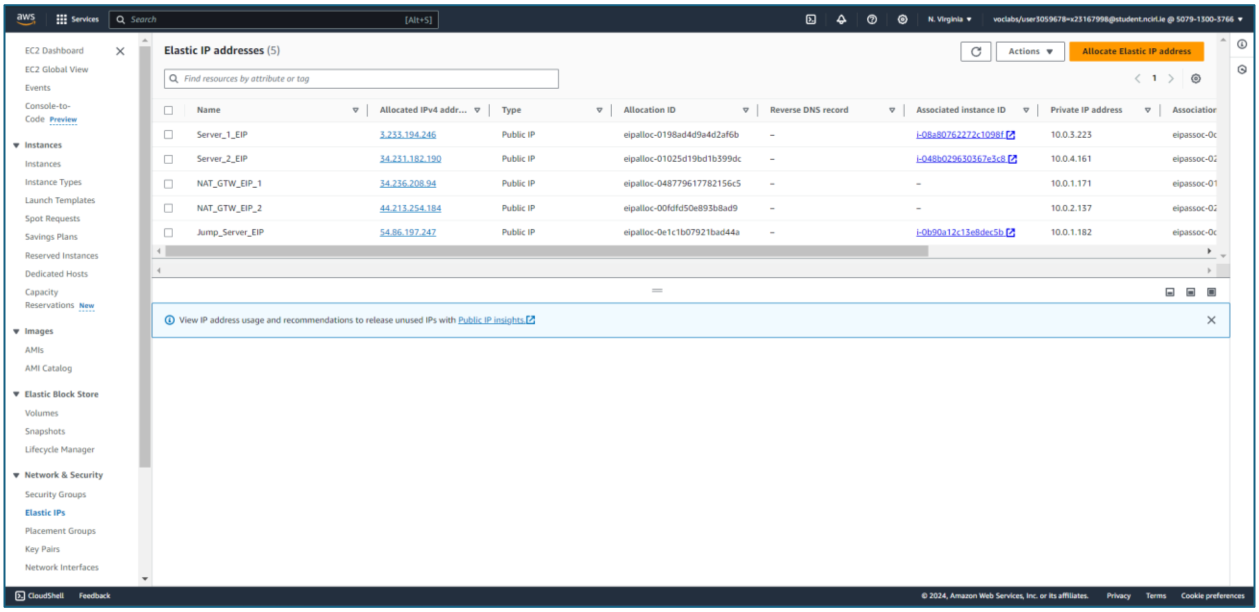
[13] Kali, “whatweb | Kali Linux Tools,” Kali. Accessed: Apr. 08, 2024. [Online]. Available: https://www.kali.org/tools/whatweb/

[14] Nikto, “Nikto Web Vulnerability Scanner | HackerTarget.com,” Nikto. Accessed: Apr. 08, 2024. [Online]. Available: https://hackertarget.com/nikto-website-scanner/

[15] Vooki, “VOOKI - Web Application and API Vulnerability Scanner | Vooki Infosec,” Vooki. Accessed: Apr. 08, 2024. [Online]. Available: https://www.vegabird.com/vooki/

[16] Burp Suite, “Burp Suite - Application Security Testing Software - PortSwigger,” Burp Suite. Accessed: Apr. 08, 2024. [Online]. Available: https://portswigger.net/burp

Appendix

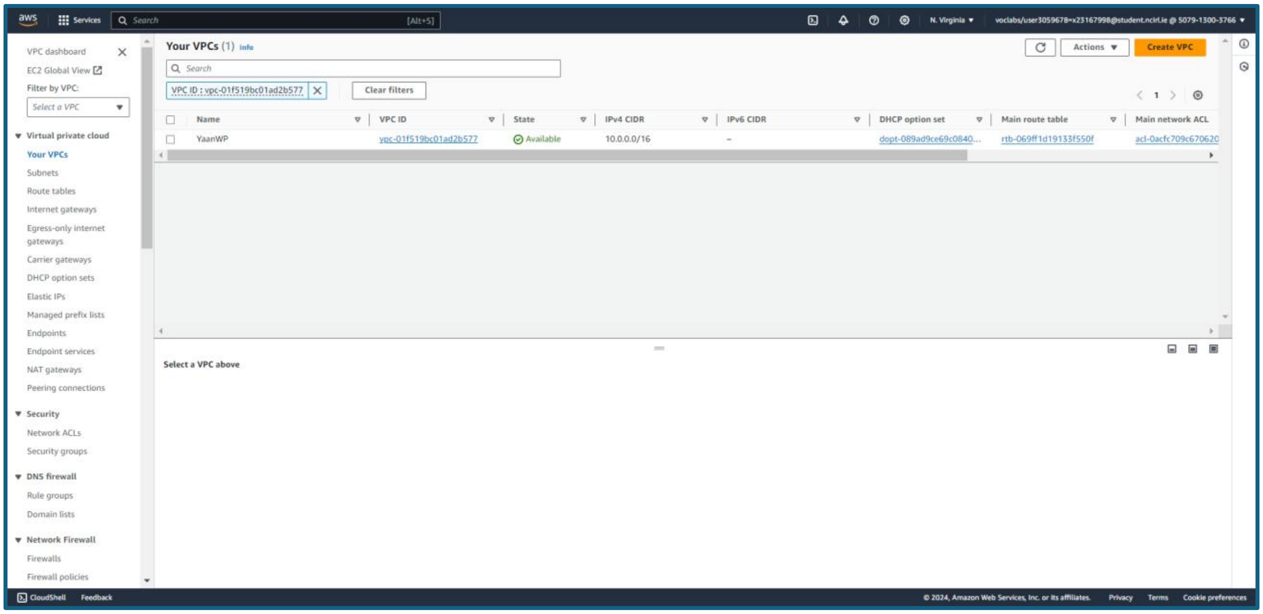


Elastic IP addresses (5)

Name	Allocated IPv4 addr...	Type	Allocation ID	Reverse DNS record	Associated instance ID	Private IP address	Association
Server_1_EIP	3.233.194.246	Public IP	eipalloc-0198ad4d9a4d2af6b	–	i-08a80762272c1098f	10.0.3.223	eipassoc-0c
Server_2_EIP	34.231.182.190	Public IP	eipalloc-01025d19bd1b399dc	–	i-048b029630367e3c8	10.0.4.161	eipassoc-02
NAT_GTW_EIP_1	34.236.208.94	Public IP	eipalloc-048779617782156c5	–	–	10.0.1.171	eipassoc-01
NAT_GTW_EIP_2	44.213.254.184	Public IP	eipalloc-00fdfd50e893b8ad9	–	–	10.0.2.137	eipassoc-02
Jump_Server_EIP	54.86.197.247	Public IP	eipalloc-0e1c1b07921bad44a	–	i-0b90a12c13e8dec5b	10.0.1.182	eipassoc-0c

View IP address usage and recommendations to release unused IPs with Public IP insights

Figure 4 Elastic IP's



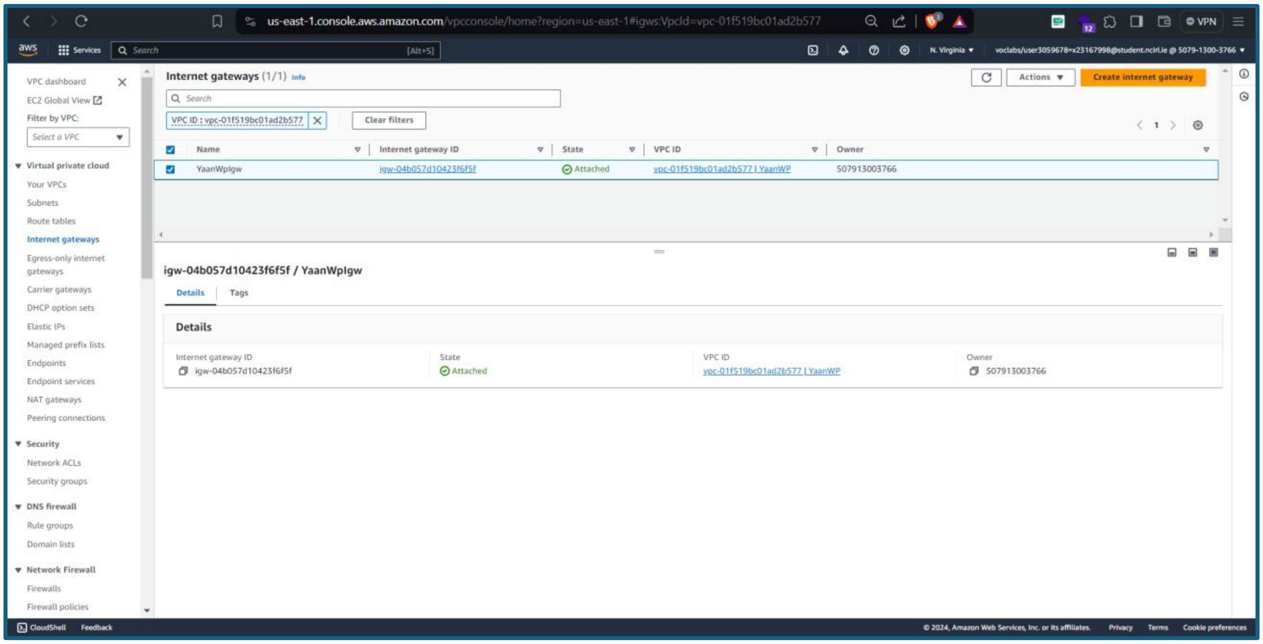
Your VPCs (1) Info

VPC ID : vpc-01f519bc01ad2b577

Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR	DHCP option set	Main route table	Main network ACL
YaanWP	vpc-01f519bc01ad2b577	Available	10.0.0.0/16	–	dopt-089ad9ce69c0840...	rtb-069ff1d19133f550f	acl-0acfc709c670620

Select a VPC above

Figure 5 VPC:



Internet gateways (1/1) Info

VPC ID : vpc-01f519bc01ad2b577

☑	Name	Internet gateway ID	State	VPC ID	Owner
☑	YaanWplgw	igw-04b057d10423f6f5f	✓ Attached	vpc-01f519bc01ad2b577 | YaanWP	507913003766

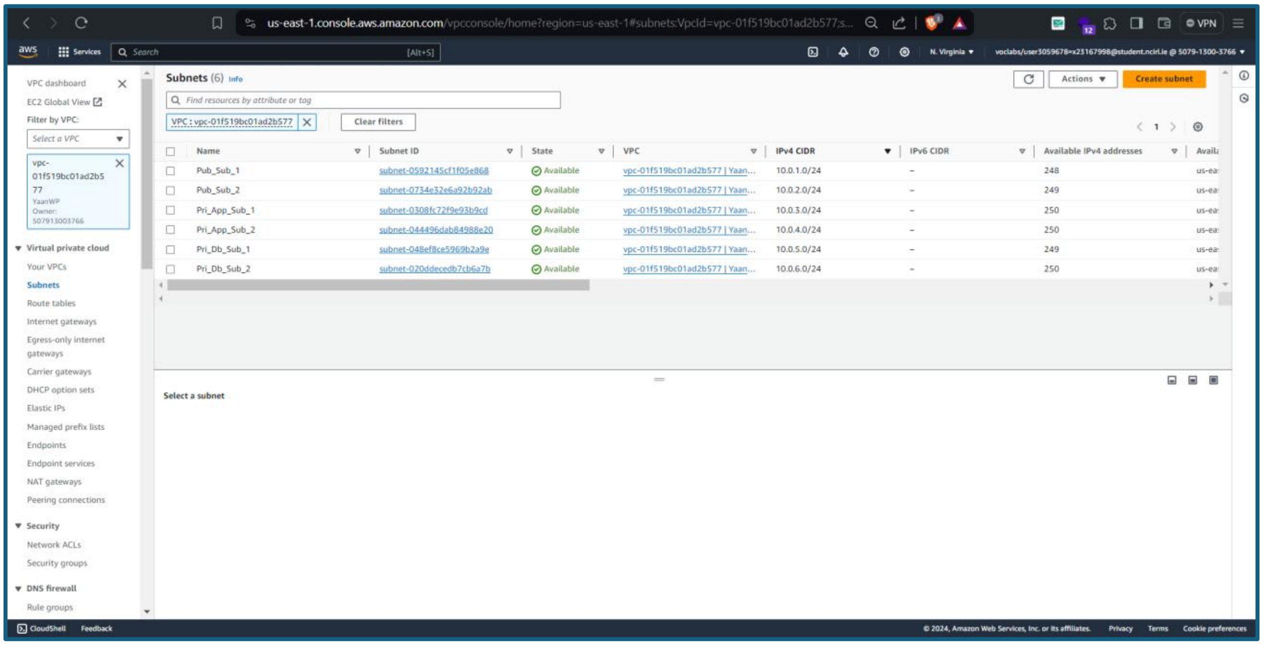
igw-04b057d10423f6f5f / YaanWplgw

Details | Tags

Details

Internet gateway ID	State	VPC ID	Owner
igw-04b057d10423f6f5f	✓ Attached	vpc-01f519bc01ad2b577 | YaanWP	507913003766

Figure 6 VPC Internet Gateway:



Subnets (6) Info

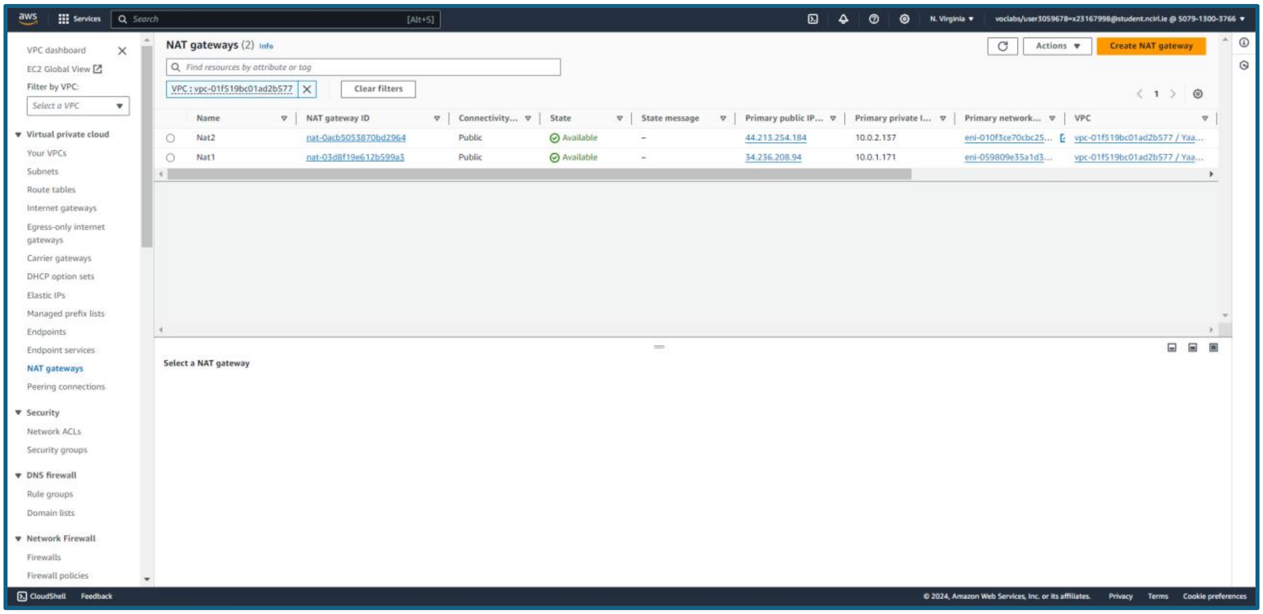
Find resources by attribute or tag

VPC : vpc-01f519bc01ad2b577

□	Name	Subnet ID	State	VPC	IPv4 CIDR	IPv6 CIDR	Available IPv4 addresses	Avail
□	Pub_Sub_1	subnet-0592145cf1f05e868	✓ Available	vpc-01f519bc01ad2b577 | Yaan...	10.0.1.0/24	–	248	us-ea
□	Pub_Sub_2	subnet-0734e32e6a92b92ab	✓ Available	vpc-01f519bc01ad2b577 | Yaan...	10.0.2.0/24	–	249	us-ea
□	Pri_App_Sub_1	subnet-0308fc72f9e93b9cd	✓ Available	vpc-01f519bc01ad2b577 | Yaan...	10.0.3.0/24	–	250	us-ea
□	Pri_App_Sub_2	subnet-044496dab84988e20	✓ Available	vpc-01f519bc01ad2b577 | Yaan...	10.0.4.0/24	–	250	us-ea
□	Pri_Db_Sub_1	subnet-048ef8ce5969b2a9e	✓ Available	vpc-01f519bc01ad2b577 | Yaan...	10.0.5.0/24	–	249	us-ea
□	Pri_Db_Sub_2	subnet-020ddecedb7cb6a7b	✓ Available	vpc-01f519bc01ad2b577 | Yaan...	10.0.6.0/24	–	250	us-ea

Select a subnet

Figure 7 VPC Subnets:



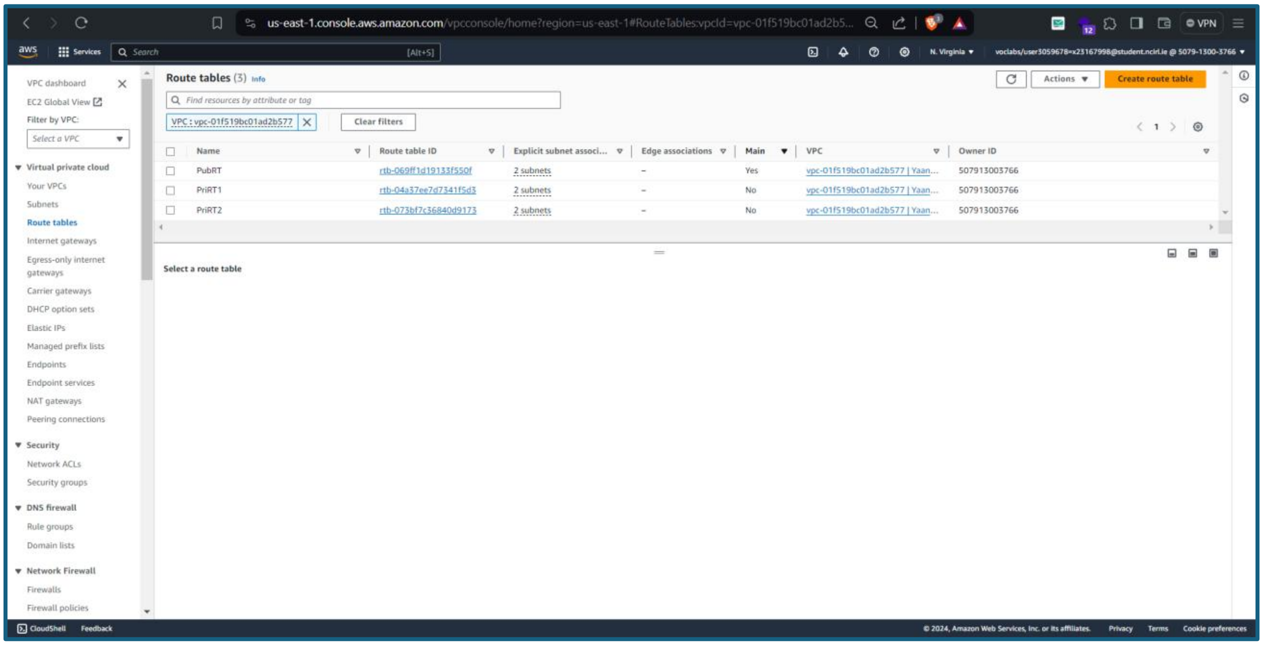
NAT gateways (2)

VPC : vpc-01f519bc01ad2b577

Name	NAT gateway ID	Connectivity...	State	State message	Primary public IP...	Primary private I...	Primary network...	VPC
Nat2	nat-0acb5053870bd2964	Public	Available	-	44.213.254.184	10.0.2.137	eni-010f3ce70cbc25...	vpc-01f519bc01ad2b577 / Yaa...
Nat1	nat-03d8f19e612b599a3	Public	Available	-	34.236.208.94	10.0.1.171	eni-059809e35a1d3...	vpc-01f519bc01ad2b577 / Yaa...

Select a NAT gateway

Figure 8 VPC NAT Gateway:



us-east-1.console.aws.amazon.com/vpcconsole/home?region=us-east-1#RouteTables:vpcId=vpc-01f519bc01ad2b5...

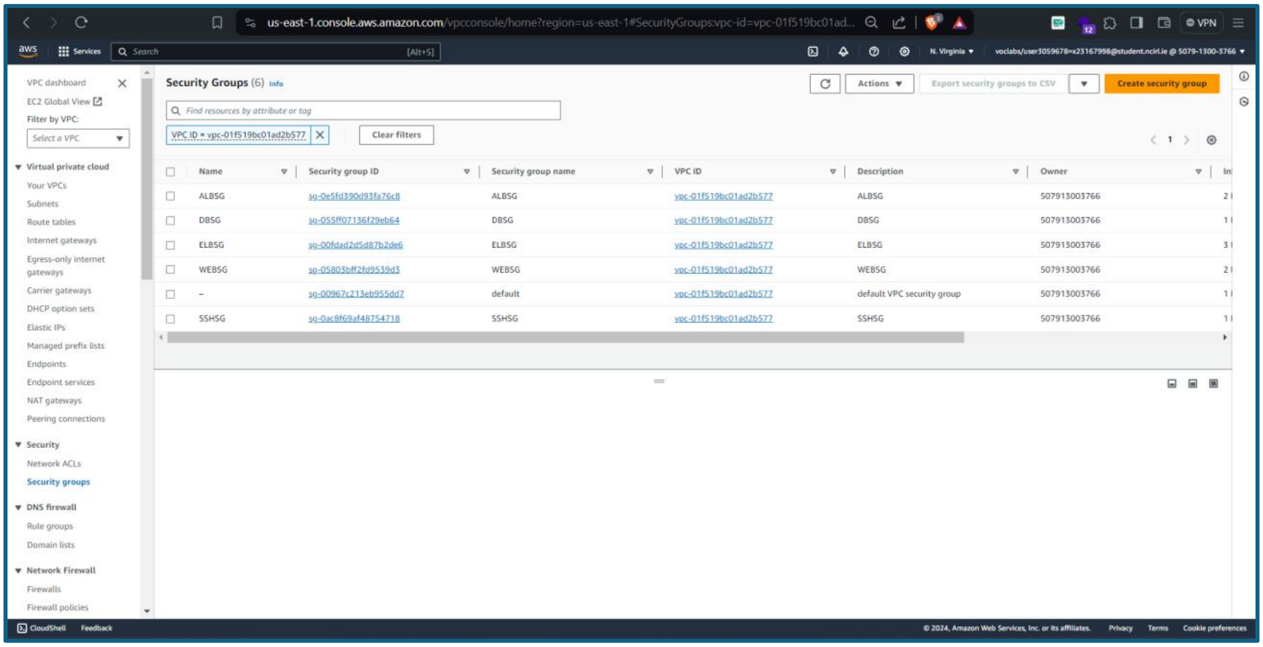
Route tables (3)

VPC : vpc-01f519bc01ad2b577

Name	Route table ID	Explicit subnet associ...	Edge associations	Main	VPC	Owner ID
PubRT	rtb-069ff1d19133f550f	2 subnets	-	Yes	vpc-01f519bc01ad2b577 | Yaan...	507913003766
PriRT1	rtb-04a37ee7d7341f5d3	2 subnets	-	No	vpc-01f519bc01ad2b577 | Yaan...	507913003766
PriRT2	rtb-073bf7c36840d9173	2 subnets	-	No	vpc-01f519bc01ad2b577 | Yaan...	507913003766

Select a route table

Figure 9 VPC Route Tables:



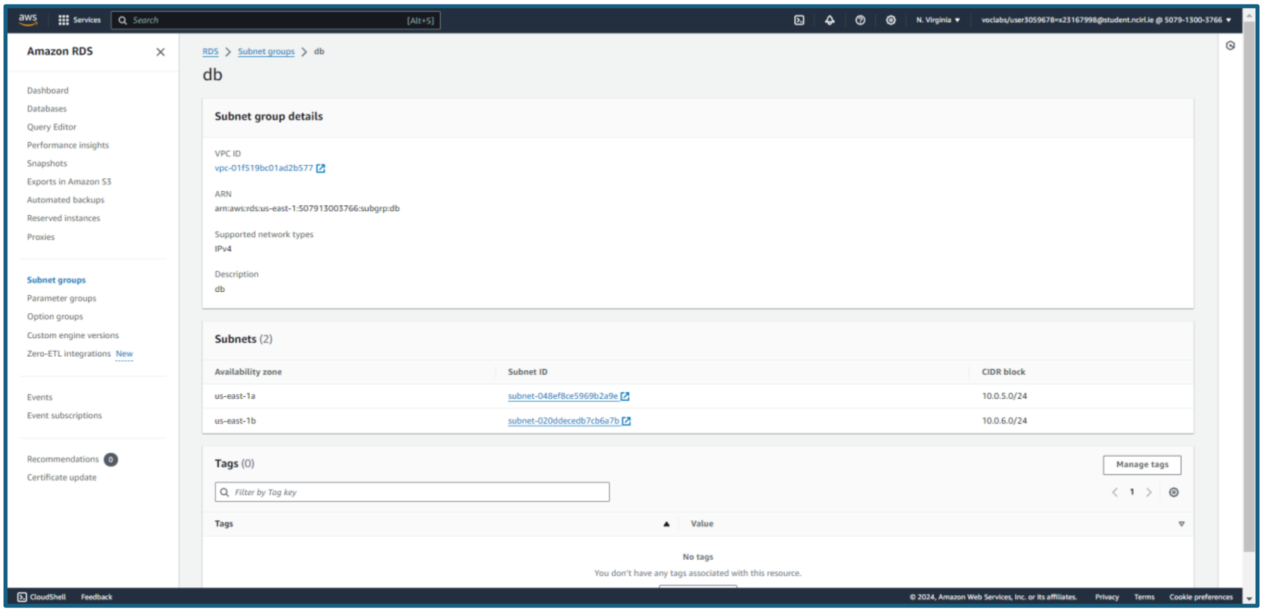
us-east-1.console.aws.amazon.com/vpcconsole/home?region=us-east-1#SecurityGroups:vpc-id=vpc-01f519bc01ad...

VPC ID = vpc-01f519bc01ad2b577

Security Groups (6)

Name	Security group ID	Security group name	VPC ID	Description	Owner	In
ALBSG	sg-0e5fd390d93fa76c8	ALBSG	vpc-01f519bc01ad2b577	ALBSG	507913003766	2
DBSG	sg-055ff07136f29eb64	DBSG	vpc-01f519bc01ad2b577	DBSG	507913003766	1
ELBSG	sg-00fdad2d5d87b2de6	ELBSG	vpc-01f519bc01ad2b577	ELBSG	507913003766	3
WEBSG	sg-05803bff2fd9539d3	WEBSG	vpc-01f519bc01ad2b577	WEBSG	507913003766	2
–	sg-00967c213eb955dd7	default	vpc-01f519bc01ad2b577	default VPC security group	507913003766	1
SSHSG	sg-0ac8f69af48754718	SSHSG	vpc-01f519bc01ad2b577	SSHSG	507913003766	1

Figure 10 VPC Security Groups:



RDS > Subnet groups > db

db

Subnet group details

VPC ID
vpc-01f519bc01ad2b577

ARN
arn:aws:rds:us-east-1:507913003766:subgrp:db

Supported network types
IPv4

Description
db

Subnets (2)

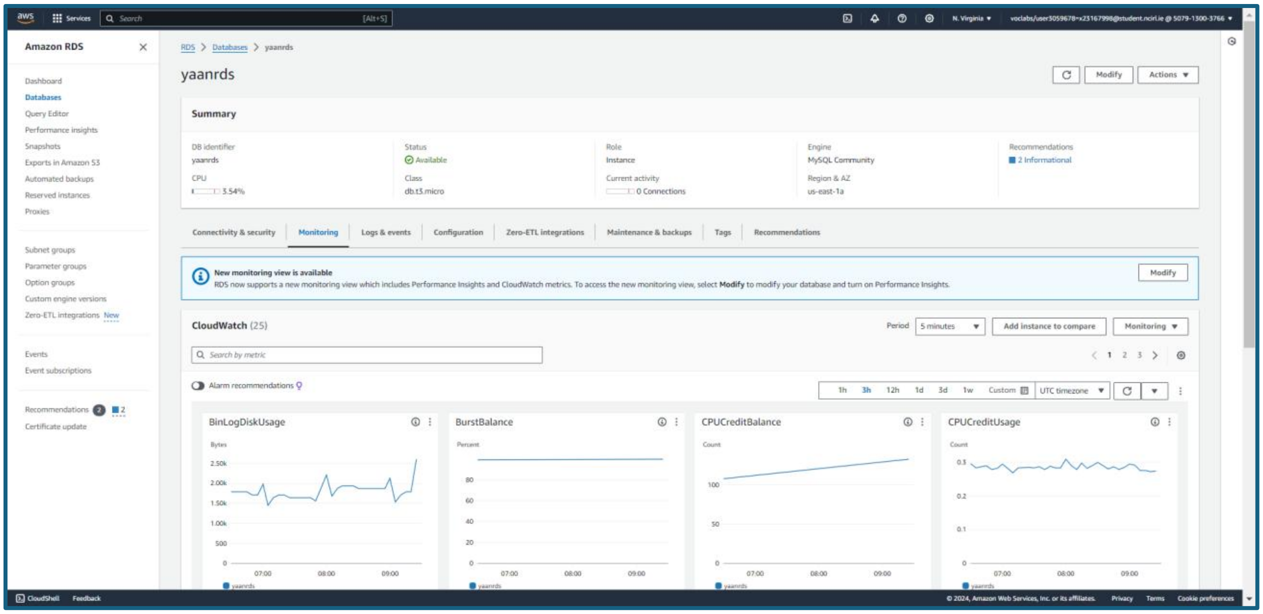
Availability zone	Subnet ID	CIDR block
us-east-1a	subnet-048ef8ce5969b2a9e	10.0.5.0/24
us-east-1b	subnet-020ddecedb7cb6a7b	10.0.6.0/24

Tags (0)

Tags	Value

No tags
You don't have any tags associated with this resource.

Figure 11 Database Security Groups:



yaanrds

Summary

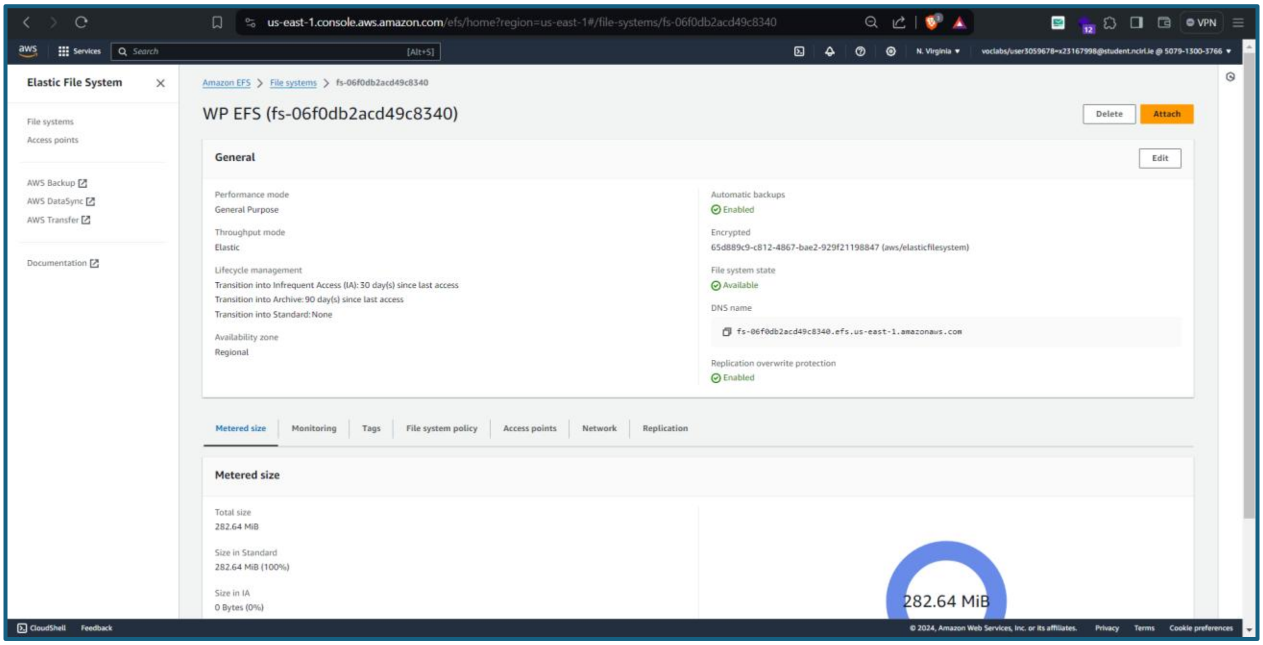
DB identifier: yaanrds
CPU: 3.54%
Status: Available
Class: db.t3.micro
Role: Instance
Current activity: 0 Connections
Engine: MySQL Community
Region & AZ: us-east-1a
Recommendations: 2 Informational

New monitoring view is available
RDS now supports a new monitoring view which includes Performance Insights and CloudWatch metrics. To access the new monitoring view, select **Modify** to modify your database and turn on Performance Insights.

CloudWatch (25)

Period: 5 minutes

Figure 12 RDS Database:



us-east-1.console.aws.amazon.com/efs/home?region=us-east-1#/file-systems/fs-06f0db2acd49c8340

WP EFS (fs-06f0db2acd49c8340)

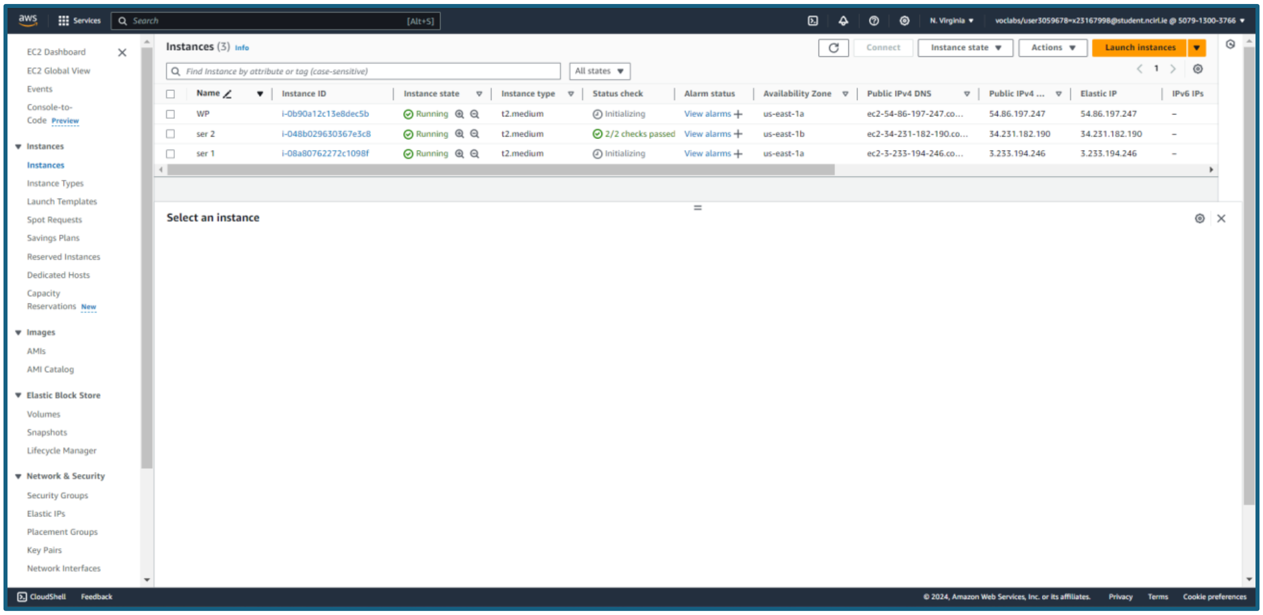
General

Performance mode: General Purpose
Throughput mode: Elastic
Lifecycle management:
Transition into Infrequent Access (IA): 30 day(s) since last access
Transition into Archive: 90 day(s) since last access
Transition into Standard: None
Availability zone: Regional
Automatic backups: Enabled
Encrypted: 65d889c9-c812-4867-bae2-929f21198847 (aws/elasticfilesystem)
File system state: Available
DNS name: fs-06f0db2acd49c8340.efs.us-east-1.amazonaws.com
Replication overwrite protection: Enabled

Metered size

Total size: 282.64 MiB
Size in Standard: 282.64 MiB (100%)
Size in IA: 0 Bytes (0%)

Figure 13 Elastic File System:



Instances (3) Info

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...	Elastic IP	IPv6 IPs
WP	i-0b90a12c13e8dec5b	Running	t2.medium	Initializing	View alarms +	us-east-1a	ec2-54-86-197-247.co...	54.86.197.247	54.86.197.247	–
ser 2	i-048b029630367e3c8	Running	t2.medium	2/2 checks passed	View alarms +	us-east-1b	ec2-34-231-182-190.co...	34.231.182.190	34.231.182.190	–
ser 1	i-08a80762272c1098f	Running	t2.medium	Initializing	View alarms +	us-east-1a	ec2-3-233-194-246.co...	3.233.194.246	3.233.194.246	–

Select an instance

Figure 14 EC2 Instances:

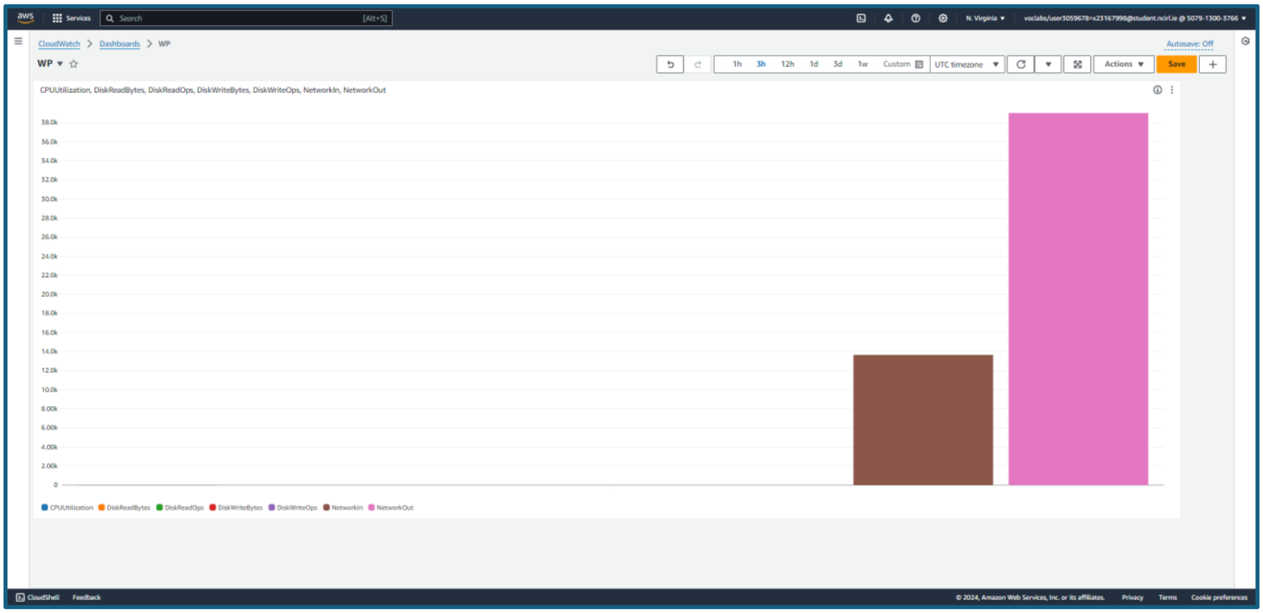
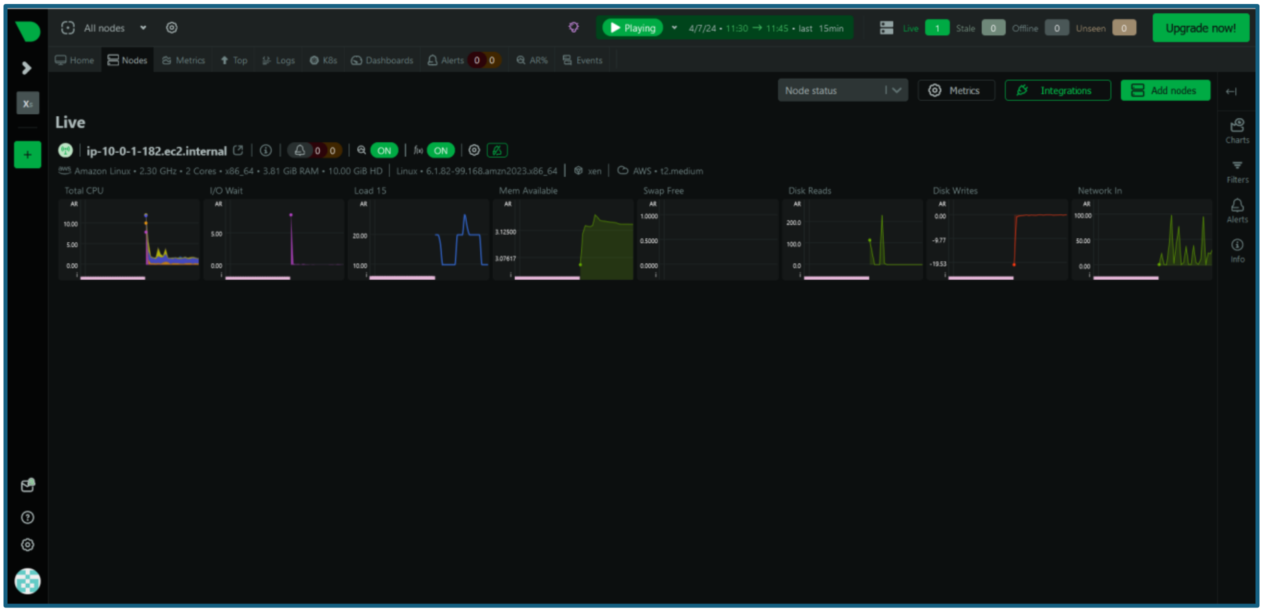


Figure 15 CloudWSatch Monitoring for AWS EC2:

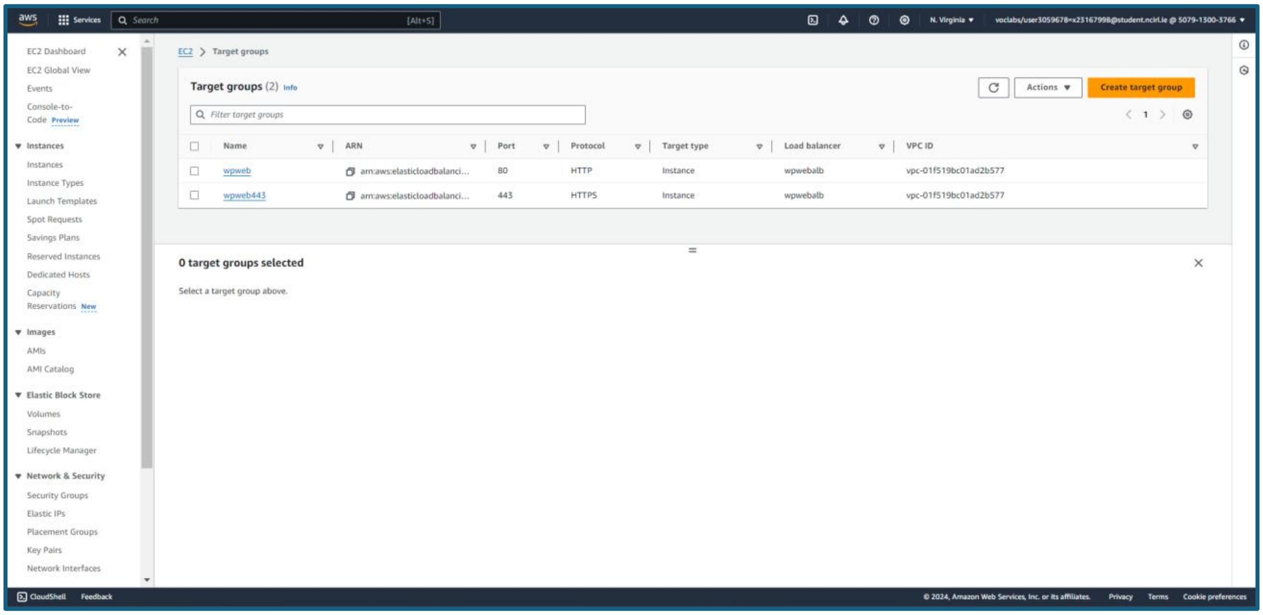


Live

ip-10-0-1-182.ec2.internal | 0 0 | ON | ON

Amazon Linux • 2.30 GHz • 2 Cores • x86_64 • 3.81 GiB RAM • 10.00 GiB HD | Linux • 6.1.82-99.168.amzn2023.x86_64 | xen | AWS • t2.medium

Figure 16 Netdata Monitoring



EC2 > Target groups

Target groups (2) Info

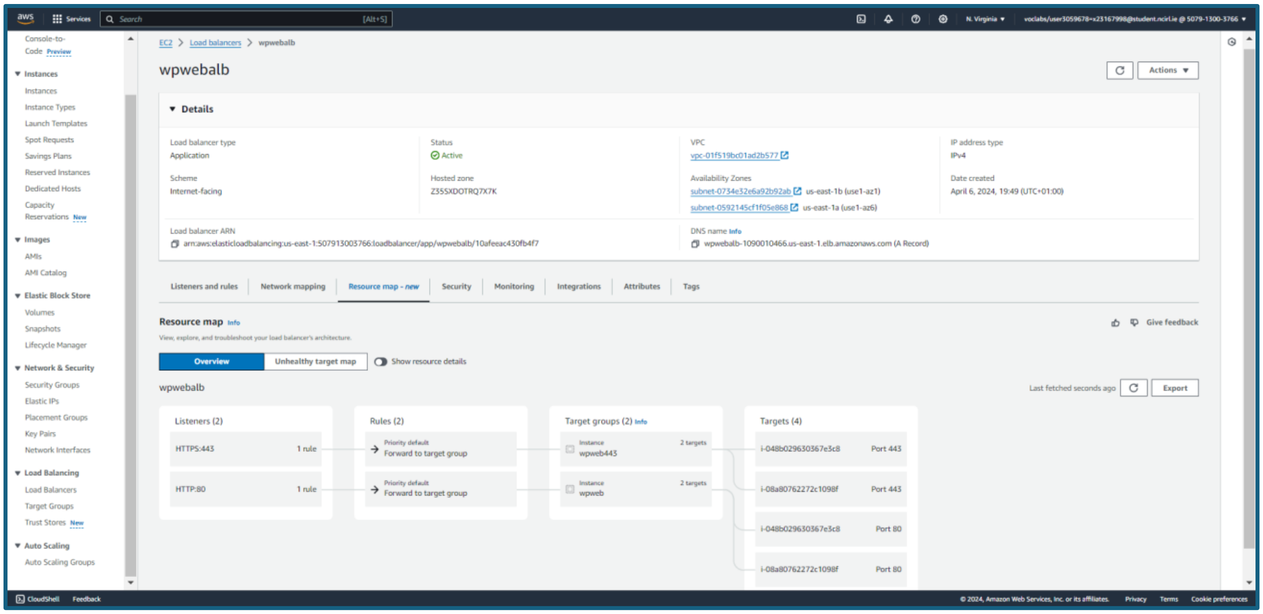
Filter target groups

	Name	ARN	Port	Protocol	Target type	Load balancer	VPC ID
□	wpweb	arn:aws:elasticloadbalanci...	80	HTTP	Instance	wpwebalb	vpc-01f519bc01ad2b577
□	wpweb443	arn:aws:elasticloadbalanci...	443	HTTPS	Instance	wpwebalb	vpc-01f519bc01ad2b577

0 target groups selected

Select a target group above.

Figure 17 Application Load Balancer Target Groups:



wpwebalb

Details

Load balancer type: Application

Status: Active

VPC: vpc-01f519bc01ad2b577

IP address type: IPv4

Scheme: Internet-facing

Hosted zone: Z35SXDOTRQ7X7K

Availability Zones:
subnet-0734e32e6a92b92ab us-east-1b (use1-az1)
subnet-0592145cf1f05e868 us-east-1a (use1-az6)

Date created: April 6, 2024, 19:49 (UTC+01:00)

Load balancer ARN: arn:aws:elasticloadbalancing:us-east-1:507913003766:loadbalancer/app/wpwebalb/10afeeac430fb4f7

DNS name: wpwebalb-1090010466.us-east-1.elb.amazonaws.com (A Record)

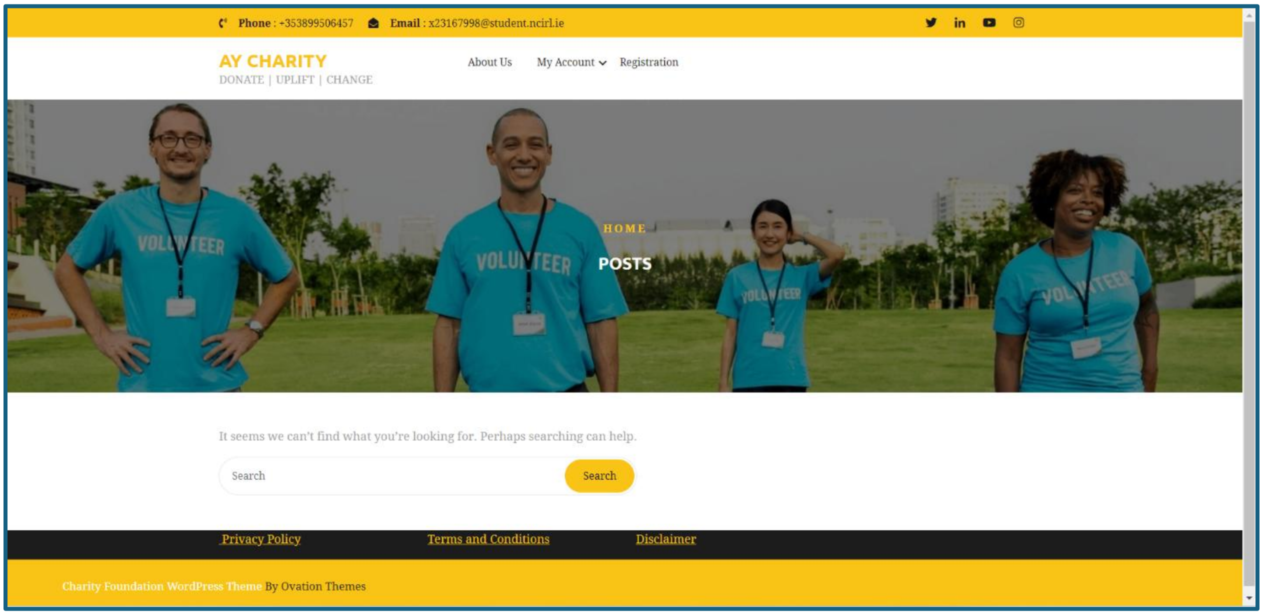
Resource map

View, explore, and troubleshoot your load balancer's architecture.

wpwebalb

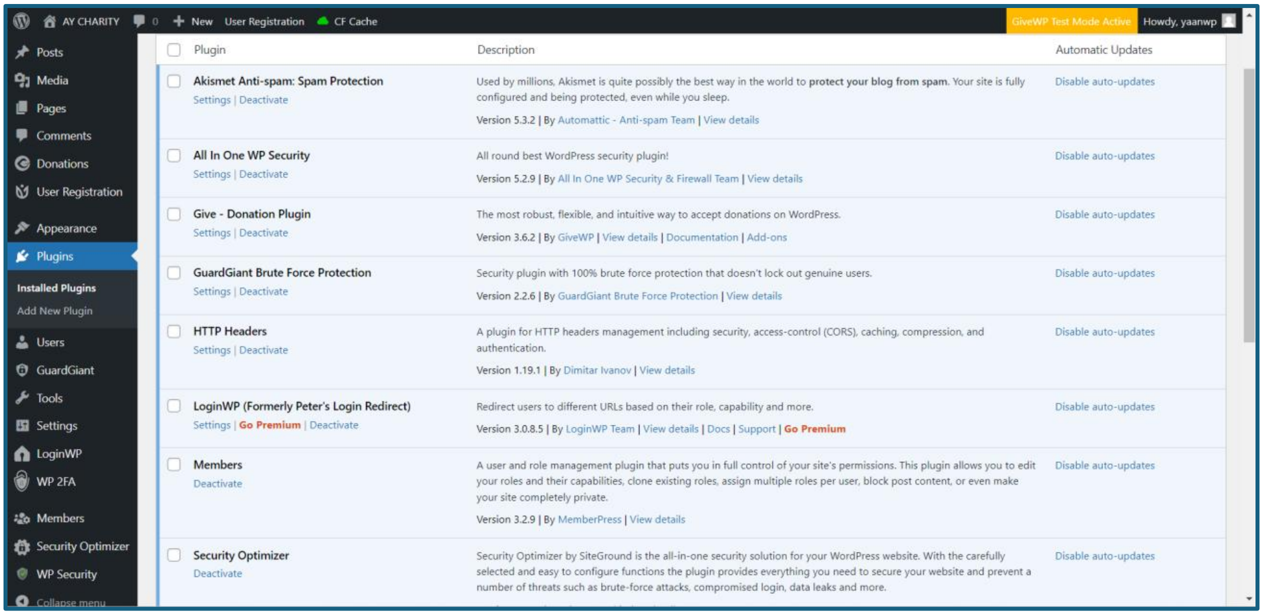
Listeners (2)	Rules (2)	Target groups (2)	Targets (4)
HTTPS:443 1 rule	Priority default Forward to target group	Instance wpweb443 2 targets	i-048b029630367e3c8 Port 443
HTTP:80 1 rule	Priority default Forward to target group	Instance wpweb 2 targets	i-08a80762272c1098f Port 443
			i-048b029630367e3c8 Port 80
			i-08a80762272c1098f Port 80

Figure 18 Application Load Balancer:



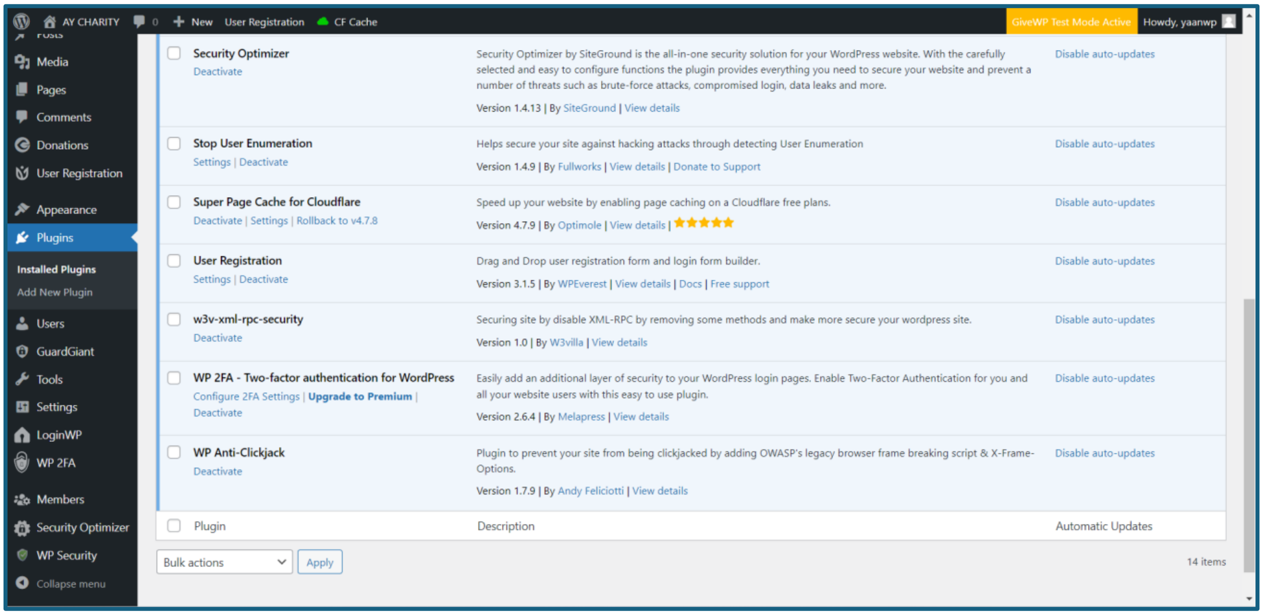
It seems we can't find what you're looking for. Perhaps searching can help.

Figure 19 Website Home Page



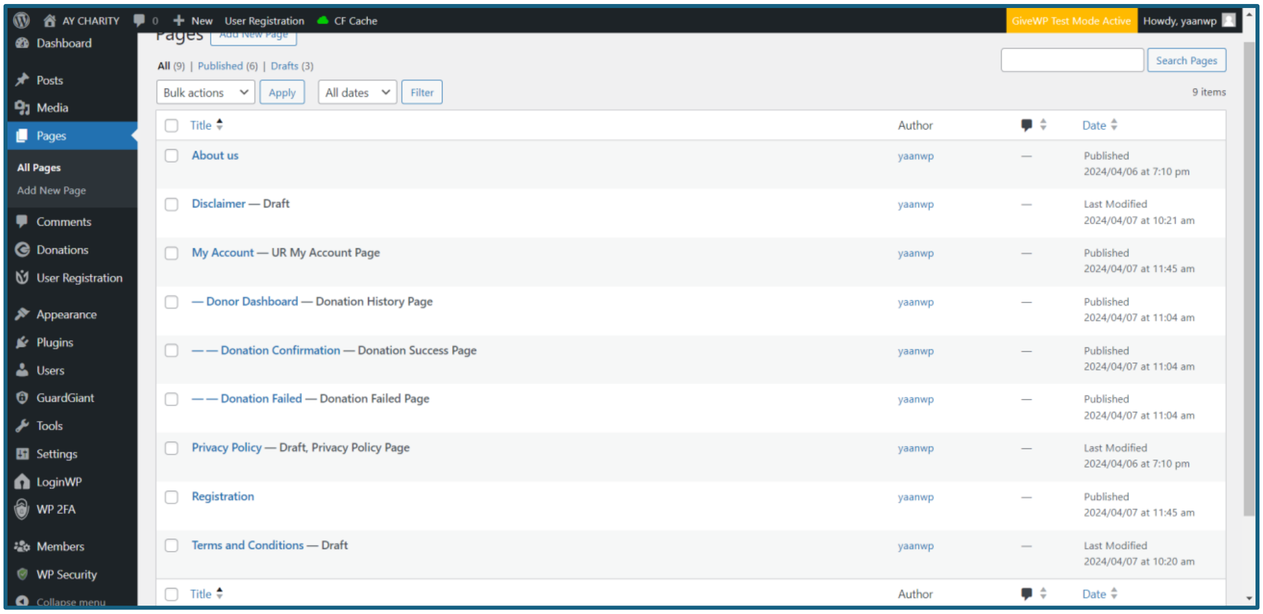
Plugin	Description	Automatic Updates
Akismet Anti-spam: Spam Protection Settings | Deactivate	Used by millions, Akismet is quite possibly the best way in the world to **protect your blog from spam**. Your site is fully configured and being protected, even while you sleep. Version 5.3.2 | By Automattic - Anti-spam Team | View details	Disable auto-updates
All In One WP Security Settings | Deactivate	All round best WordPress security plugin! Version 5.2.9 | By All In One WP Security & Firewall Team | View details	Disable auto-updates
Give - Donation Plugin Settings | Deactivate	The most robust, flexible, and intuitive way to accept donations on WordPress. Version 3.6.2 | By GiveWP | View details | Documentation | Add-ons	Disable auto-updates
GuardGiant Brute Force Protection Settings | Deactivate	Security plugin with 100% brute force protection that doesn't lock out genuine users. Version 2.2.6 | By GuardGiant Brute Force Protection | View details	Disable auto-updates
HTTP Headers Settings | Deactivate	A plugin for HTTP headers management including security, access-control (CORS), caching, compression, and authentication. Version 1.19.1 | By Dimitar Ivanov | View details	Disable auto-updates
LoginWP (Formerly Peter's Login Redirect) Settings | **Go Premium** | Deactivate	Redirect users to different URLs based on their role, capability and more. Version 3.0.8.5 | By LoginWP Team | View details | Docs | Support | **Go Premium**	Disable auto-updates
Members Deactivate	A user and role management plugin that puts you in full control of your site's permissions. This plugin allows you to edit your roles and their capabilities, clone existing roles, assign multiple roles per user, block post content, or even make your site completely private. Version 3.2.9 | By MemberPress | View details	Disable auto-updates
Security Optimizer Deactivate	Security Optimizer by SiteGround is the all-in-one security solution for your WordPress website. With the carefully selected and easy to configure functions the plugin provides everything you need to secure your website and prevent a number of threats such as brute-force attacks, compromised login, data leaks and more.	Disable auto-updates

Figure 20 Website Plugins - 1



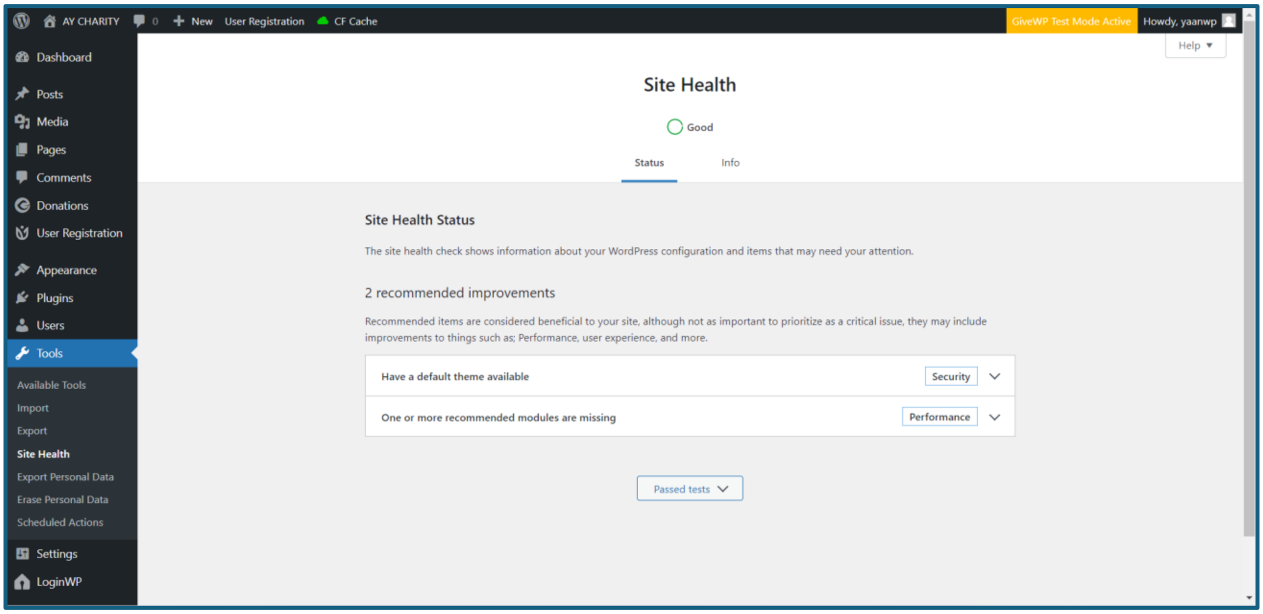
Plugin	Description	Automatic Updates
Security Optimizer Deactivate	Security Optimizer by SiteGround is the all-in-one security solution for your WordPress website. With the carefully selected and easy to configure functions the plugin provides everything you need to secure your website and prevent a number of threats such as brute-force attacks, compromised login, data leaks and more. Version 1.4.13 | By SiteGround | View details	Disable auto-updates
Stop User Enumeration Settings | Deactivate	Helps secure your site against hacking attacks through detecting User Enumeration Version 1.4.9 | By Fullworks | View details | Donate to Support	Disable auto-updates
Super Page Cache for Cloudflare Deactivate | Settings | Rollback to v4.7.8	Speed up your website by enabling page caching on a Cloudflare free plans. Version 4.7.9 | By Optimole | View details | ★★★★★	Disable auto-updates
User Registration Settings | Deactivate	Drag and Drop user registration form and login form builder. Version 3.1.5 | By WPEverest | View details | Docs | Free support	Disable auto-updates
w3v-xml-rpc-security Deactivate	Securing site by disable XML-RPC by removing some methods and make more secure your wordpress site. Version 1.0 | By W3villa | View details	Disable auto-updates
WP 2FA - Two-factor authentication for WordPress Configure 2FA Settings | **Upgrade to Premium** | Deactivate	Easily add an additional layer of security to your WordPress login pages. Enable Two-Factor Authentication for you and all your website users with this easy to use plugin. Version 2.6.4 | By Melapress | View details	Disable auto-updates
WP Anti-Clickjack Deactivate	Plugin to prevent your site from being clickjacked by adding OWASP's legacy browser frame breaking script & X-Frame-Options. Version 1.7.9 | By Andy Feliciotti | View details	Disable auto-updates
Plugin	Description	Automatic Updates

Figure 21Website Plugins -2



□ Title	Author		Date
□ About us	yaanwp	—	Published 2024/04/06 at 7:10 pm
□ Disclaimer — Draft	yaanwp	—	Last Modified 2024/04/07 at 10:21 am
□ My Account — UR My Account Page	yaanwp	—	Published 2024/04/07 at 11:45 am
□ — Donor Dashboard — Donation History Page	yaanwp	—	Published 2024/04/07 at 11:04 am
□ — — Donation Confirmation — Donation Success Page	yaanwp	—	Published 2024/04/07 at 11:04 am
□ — — Donation Failed — Donation Failed Page	yaanwp	—	Published 2024/04/07 at 11:04 am
□ Privacy Policy — Draft, Privacy Policy Page	yaanwp	—	Last Modified 2024/04/06 at 7:10 pm
□ Registration	yaanwp	—	Published 2024/04/07 at 11:45 am
□ Terms and Conditions — Draft	yaanwp	—	Last Modified 2024/04/07 at 10:20 am
□ Title	Author		Date

Figure 22 Website Pages



Site Health

○ Good

Site Health Status

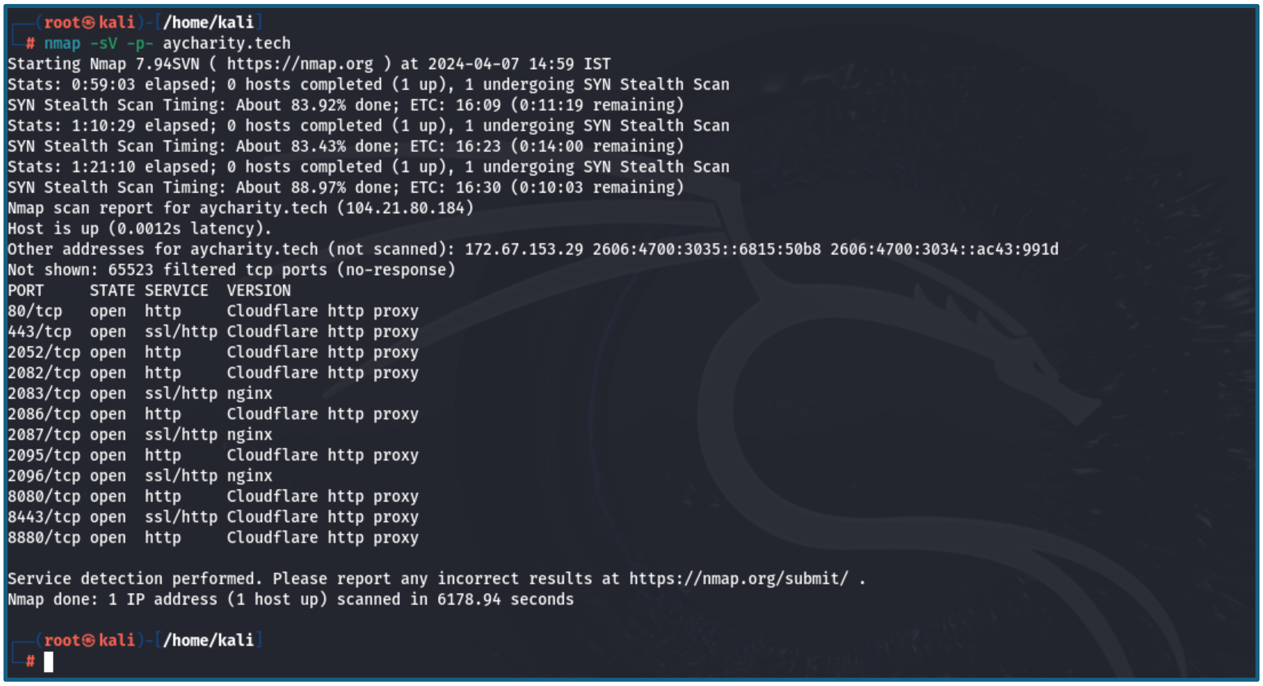
The site health check shows information about your WordPress configuration and items that may need your attention.

2 recommended improvements

Recommended items are considered beneficial to your site, although not as important to prioritize as a critical issue, they may include improvements to things such as; Performance, user experience, and more.

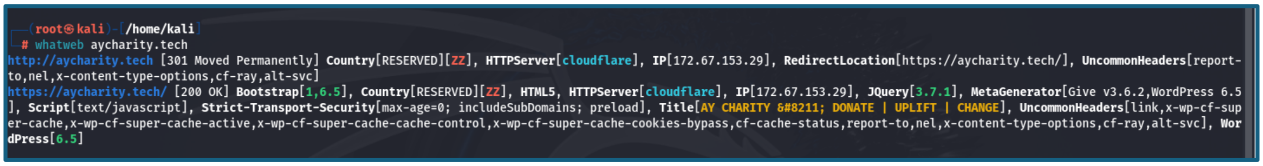
Have a default theme available	Security
One or more recommended modules are missing	Performance

Figure 23 WP Site Health



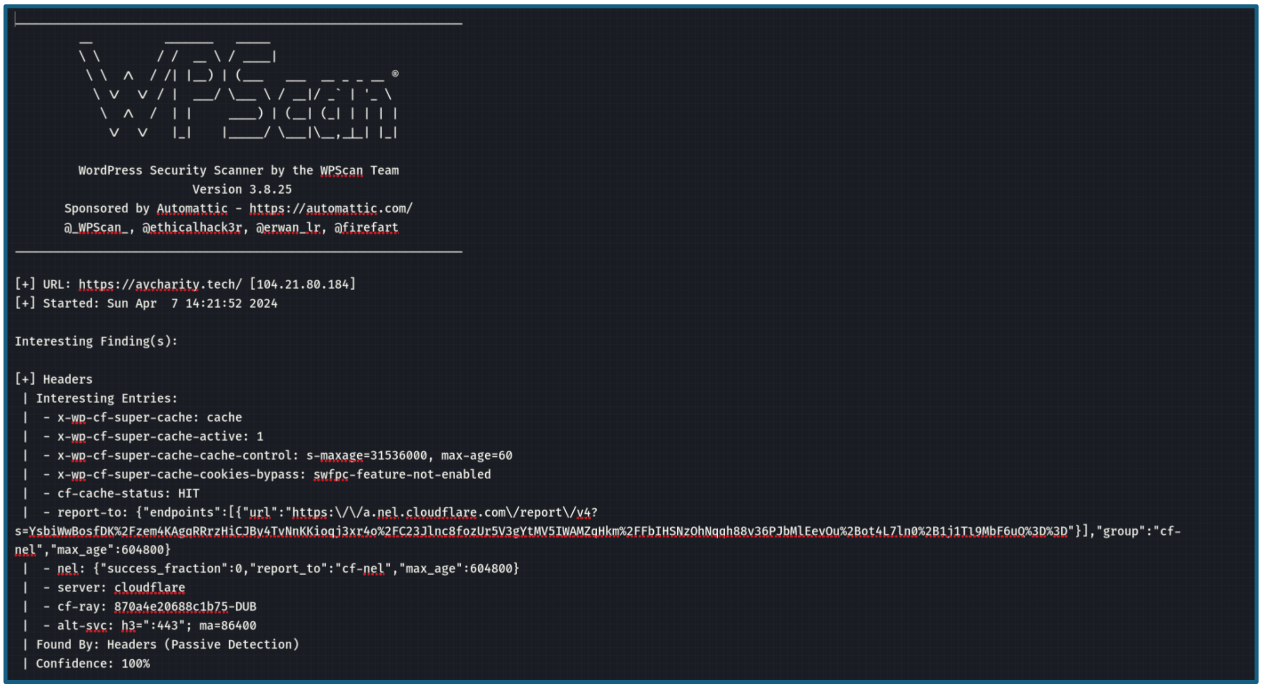
```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV -p- aycharity.tech
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-07 14:59 IST
Stats: 0:59:03 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 83.92% done; ETC: 16:09 (0:11:19 remaining)
Stats: 1:10:29 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 83.43% done; ETC: 16:23 (0:14:00 remaining)
Stats: 1:21:10 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 88.97% done; ETC: 16:30 (0:10:03 remaining)
Nmap scan report for aycharity.tech (104.21.80.184)
Host is up (0.0012s latency).
Other addresses for aycharity.tech (not scanned): 172.67.153.29 2606:4700:3035::6815:50b8 2606:4700:3034::ac43:991d
Not shown: 65523 filtered tcp ports (no-response)
PORT     STATE SERVICE  VERSION
80/tcp   open  http     Cloudflare http proxy
443/tcp  open  ssl/http Cloudflare http proxy
2052/tcp open  http     Cloudflare http proxy
2082/tcp open  http     Cloudflare http proxy
2083/tcp open  ssl/http nginx
2086/tcp open  http     Cloudflare http proxy
2087/tcp open  ssl/http nginx
2095/tcp open  http     Cloudflare http proxy
2096/tcp open  ssl/http nginx
8080/tcp open  http     Cloudflare http proxy
8443/tcp open  ssl/http Cloudflare http proxy
8880/tcp open  http     Cloudflare http proxy

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6178.94 seconds

┌──(root㉿kali)-[/home/kali]
└─# 
```

Figure 24 Nmap scan



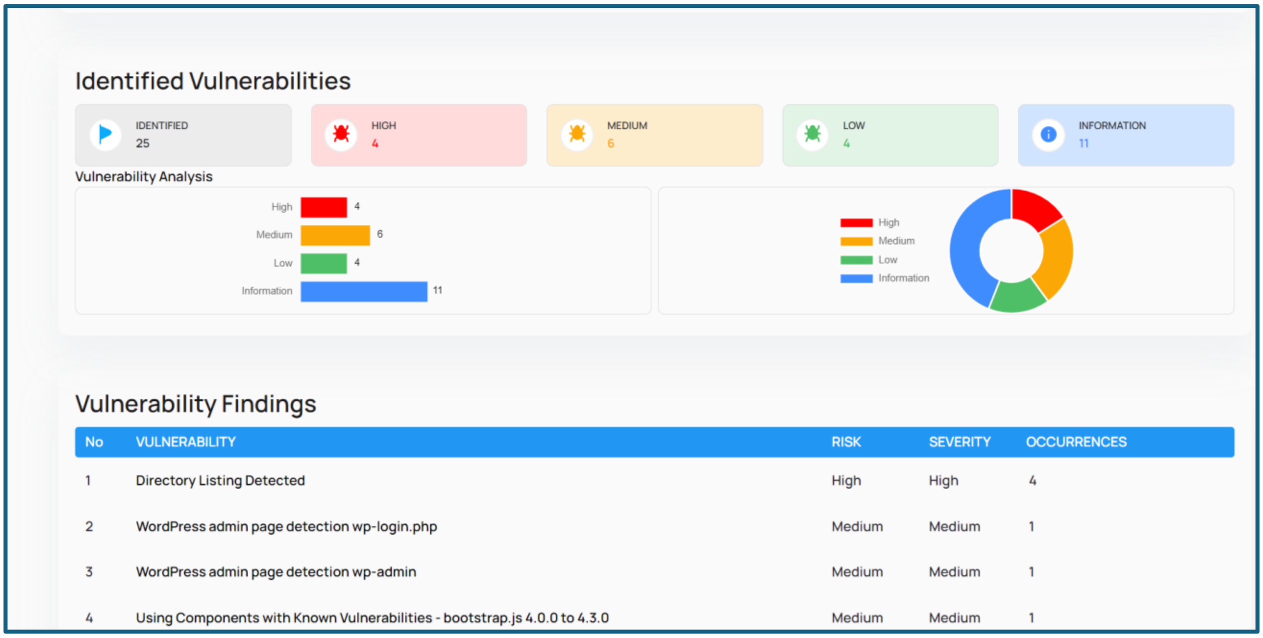
```
┌──(root㉿kali)-[/home/kali]
└─# whatweb aycharity.tech
http://aycharity.tech [301 Moved Permanently] Country[RESERVED][ZZ], HTTPServer[cloudflare], IP[172.67.153.29], RedirectLocation[https://aycharity.tech/], UncommonHeaders[report-
to,nel,x-content-type-options,cf-ray,alt-svc]
https://aycharity.tech/ [200 OK] Bootstrap[1,6.5], Country[RESERVED][ZZ], HTML5, HTTPServer[cloudflare], IP[172.67.153.29], JQuery[3.7.1], MetaGenerator[Give v3.6.2,WordPress 6.5
], Script[text/javascript], Strict-Transport-Security[max-age=0; includeSubDomains; preload], Title[AY CHARITY &#8211; DONATE | UPLIFT | CHANGE], UncommonHeaders[link,x-wp-cf-sup
er-cache,x-wp-cf-super-cache-active,x-wp-cf-super-cache-cache-control,x-wp-cf-super-cache-cookies-bypass,cf-cache-status,report-to,nel,x-content-type-options,cf-ray,alt-svc], Wor
dPress[6.5]
```

Figure 25 Whatweb scan



```
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.25
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: https://aycharity.tech/ [104.21.80.184]
[+] Started: Sun Apr  7 14:21:52 2024

Interesting Finding(s):

[+] Headers
 | Interesting Entries:
 |  - x-wp-cf-super-cache: cache
 |  - x-wp-cf-super-cache-active: 1
 |  - x-wp-cf-super-cache-cache-control: s-maxage=31536000, max-age=60
 |  - x-wp-cf-super-cache-cookies-bypass: swfpc-feature-not-enabled
 |  - cf-cache-status: HIT
 |  - report-to: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v4?
s=YsbiWwBosfDK%2Fzem4KAgqRRrzHiCJBy4TvNnKKioqj3xr4o%2FC23Jlnc8fozUr5V3gYtMV5IWAMZqHkm%2FFbIHSNzOhNqqh88v36PJbMlEevOu%2Bot4L7ln0%2B1j1Tl9MbF6uQ%3D%3D"}],"group":"cf-
nel","max_age":604800}
 |  - nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
 |  - server: cloudflare
 |  - cf-ray: 870a4e20688c1b75-DUB
 |  - alt-svc: h3=":443"; ma=86400
 | Found By: Headers (Passive Detection)
 | Confidence: 100%
```

Figure 26 WPScan result



Identified Vulnerabilities

IDENTIFIED 25

HIGH 4

MEDIUM 6

LOW 4

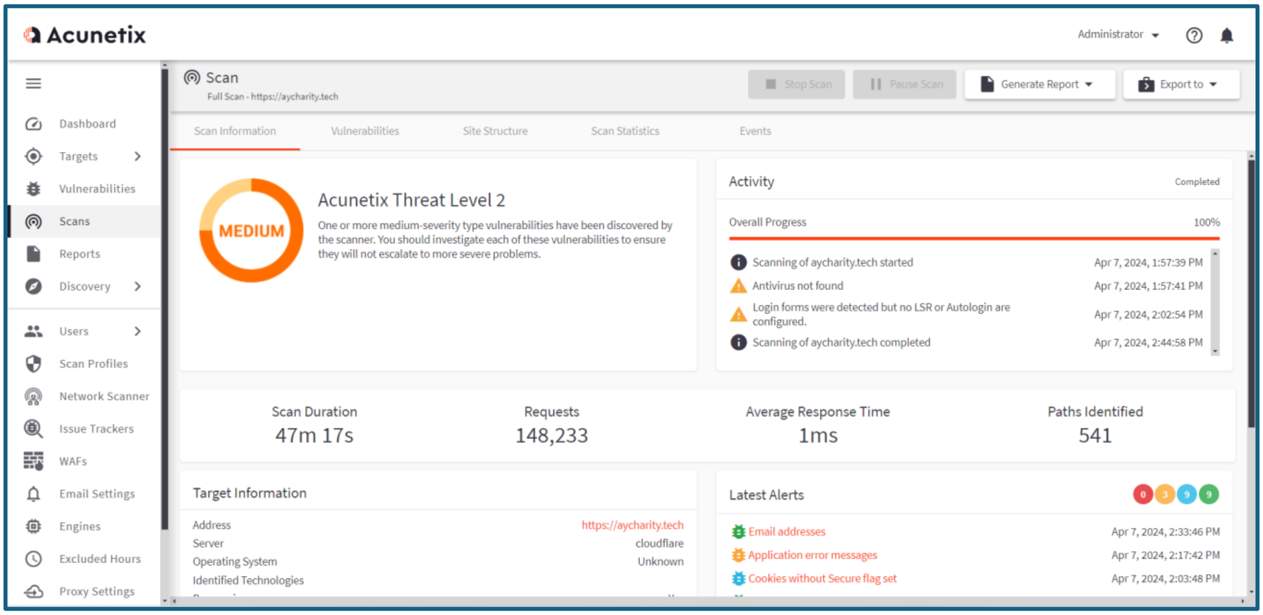
INFORMATION 11

Vulnerability Analysis

Vulnerability Findings

No	VULNERABILITY	RISK	SEVERITY	OCCURRENCES
1	Directory Listing Detected	High	High	4
2	WordPress admin page detection wp-login.php	Medium	Medium	1
3	WordPress admin page detection wp-admin	Medium	Medium	1
4	Using Components with Known Vulnerabilities - bootstrap.js 4.0.0 to 4.3.0	Medium	Medium	1

Figure 27 Vooki Web Application Scanner Results



Scan

Full Scan - https://aycharity.tech

Acunetix Threat Level 2

One or more medium-severity type vulnerabilities have been discovered by the scanner. You should investigate each of these vulnerabilities to ensure they will not escalate to more severe problems.

Activity — Completed

Overall Progress 100%

Scanning of aycharity.tech started	Apr 7, 2024, 1:57:39 PM
Antivirus not found	Apr 7, 2024, 1:57:41 PM
Login forms were detected but no LSR or Autologin are configured.	Apr 7, 2024, 2:02:54 PM
Scanning of aycharity.tech completed	Apr 7, 2024, 2:44:58 PM

Scan Duration	Requests	Average Response Time	Paths Identified
47m 17s	148,233	1ms	541

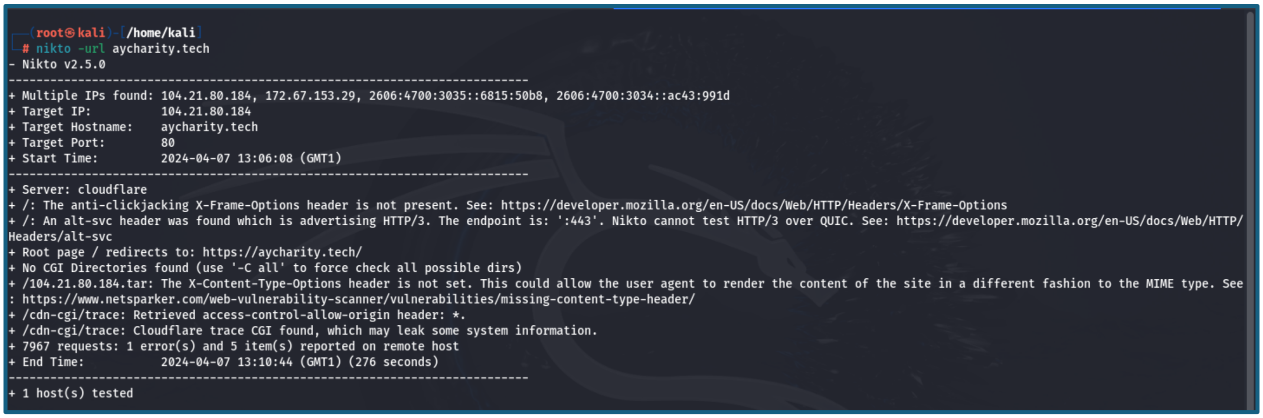
Target Information

Address	https://aycharity.tech
Server	cloudflare
Operating System	Unknown
Identified Technologies	

Latest Alerts

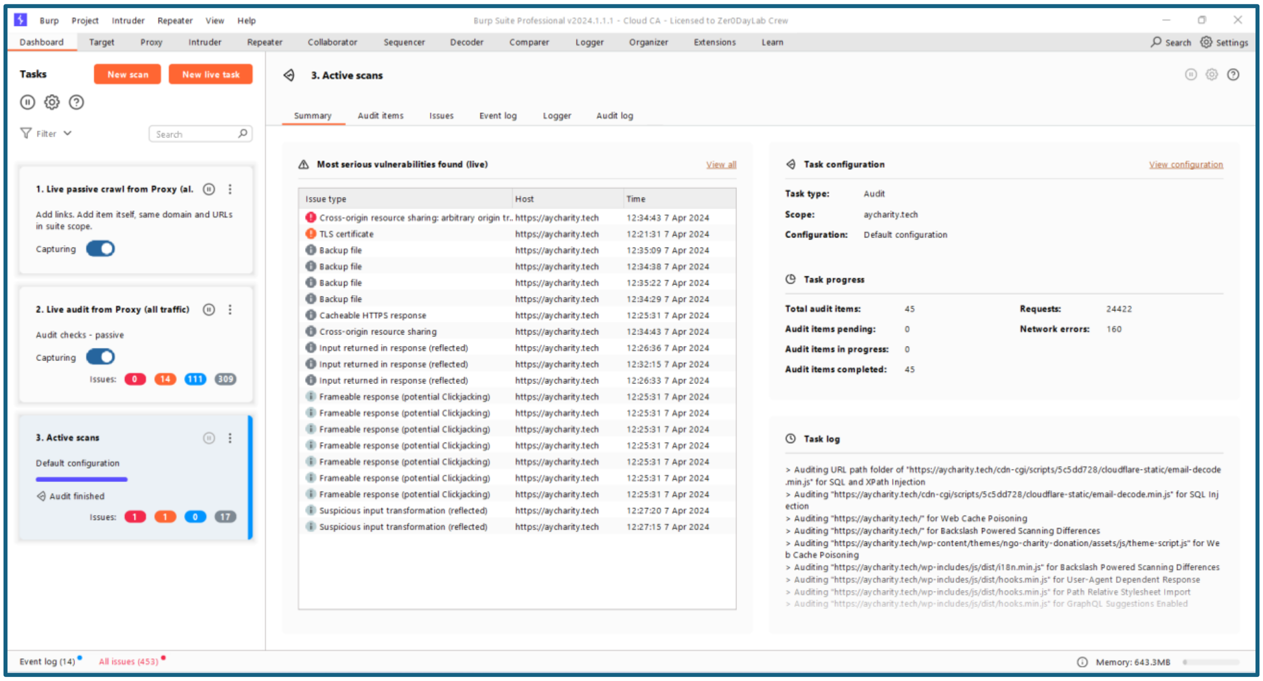
Email addresses	Apr 7, 2024, 2:33:46 PM
Application error messages	Apr 7, 2024, 2:17:42 PM
Cookies without Secure flag set	Apr 7, 2024, 2:03:48 PM

Figure 28 Acunetix Web Application Scanner Results



```
┌──(root㉿kali)-[/home/kali]
└─# nikto -url aycharity.tech
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Multiple IPs found: 104.21.80.184, 172.67.153.29, 2606:4700:3035::6815:50b8, 2606:4700:3034::ac43:991d
+ Target IP:          104.21.80.184
+ Target Hostname:    aycharity.tech
+ Target Port:        80
+ Start Time:         2024-04-07 13:06:08 (GMT1)
---------------------------------------------------------------------------
+ Server: cloudflare
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: An alt-svc header was found which is advertising HTTP/3. The endpoint is: ':443'. Nikto cannot test HTTP/3 over QUIC. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/
Headers/alt-svc
+ Root page / redirects to: https://aycharity.tech/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /104.21.80.184.tar: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See
: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ /cdn-cgi/trace: Retrieved access-control-allow-origin header: *.
+ /cdn-cgi/trace: Cloudflare trace CGI found, which may leak some system information.
+ 7967 requests: 1 error(s) and 5 item(s) reported on remote host
+ End Time:           2024-04-07 13:10:44 (GMT1) (276 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Figure 29 Nikto scan results



1. Live passive crawl from Proxy (al.

Add links. Add item itself, same domain and URLs in suite scope.

Capturing

2. Live audit from Proxy (all traffic)

Audit checks - passive

Capturing

Issues: 0 14 111 309

3. Active scans

Default configuration

Audit finished

Issues: 1 1 0 17

Most serious vulnerabilities found (live)

Issue type	Host	Time
Cross-origin resource sharing: arbitrary origin tr..	https://aycharity.tech	12:34:43 7 Apr 2024
TLS certificate	https://aycharity.tech	12:21:31 7 Apr 2024
Backup file	https://aycharity.tech	12:35:09 7 Apr 2024
Backup file	https://aycharity.tech	12:34:38 7 Apr 2024
Backup file	https://aycharity.tech	12:35:22 7 Apr 2024
Backup file	https://aycharity.tech	12:34:29 7 Apr 2024
Cacheable HTTPS response	https://aycharity.tech	12:25:31 7 Apr 2024
Cross-origin resource sharing	https://aycharity.tech	12:34:43 7 Apr 2024
Input returned in response (reflected)	https://aycharity.tech	12:26:36 7 Apr 2024
Input returned in response (reflected)	https://aycharity.tech	12:32:15 7 Apr 2024
Input returned in response (reflected)	https://aycharity.tech	12:26:33 7 Apr 2024
Frameable response (potential Clickjacking)	https://aycharity.tech	12:25:31 7 Apr 2024
Frameable response (potential Clickjacking)	https://aycharity.tech	12:25:31 7 Apr 2024
Frameable response (potential Clickjacking)	https://aycharity.tech	12:25:31 7 Apr 2024
Frameable response (potential Clickjacking)	https://aycharity.tech	12:25:31 7 Apr 2024
Frameable response (potential Clickjacking)	https://aycharity.tech	12:25:31 7 Apr 2024
Frameable response (potential Clickjacking)	https://aycharity.tech	12:25:31 7 Apr 2024
Frameable response (potential Clickjacking)	https://aycharity.tech	12:25:31 7 Apr 2024
Suspicious input transformation (reflected)	https://aycharity.tech	12:27:20 7 Apr 2024
Suspicious input transformation (reflected)	https://aycharity.tech	12:27:15 7 Apr 2024

Task configuration

Task type: Audit
Scope: aycharity.tech
Configuration: Default configuration

Task progress

Total audit items:	45	Requests:	24422
Audit items pending:	0	Network errors:	160
Audit items in progress:	0		
Audit items completed:	45		

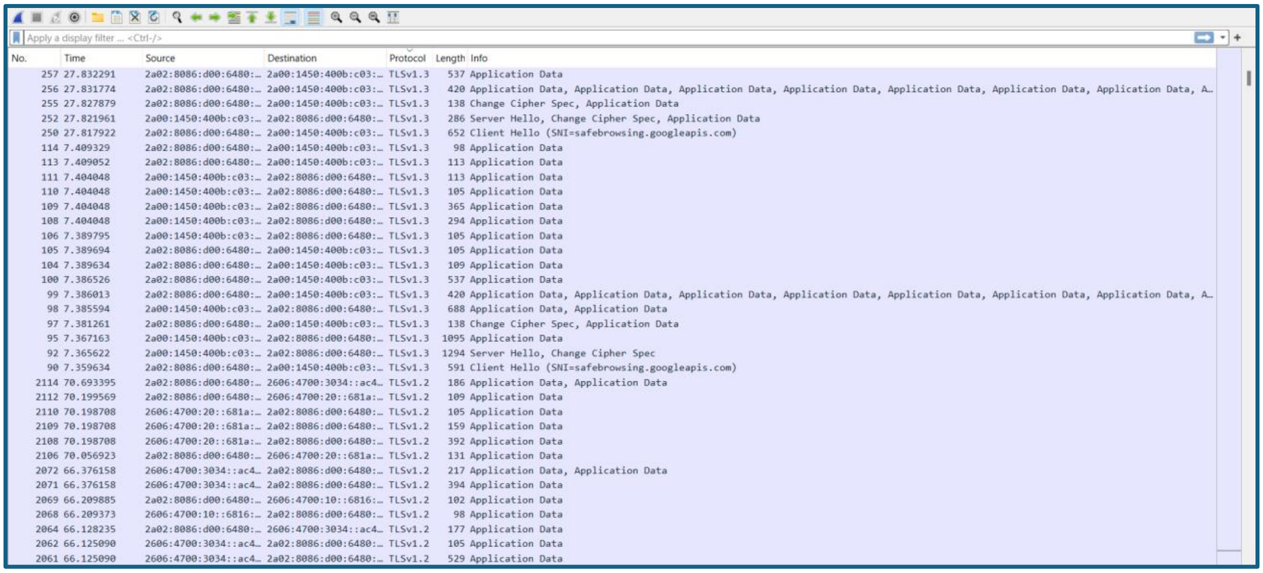
Task log

```
> Auditing URL path folder of "https://aycharity.tech/cdn-cgi/scripts/5c5dd728/cloudflare-static/email-decode
.min.js" for SQL and XPath Injection
> Auditing "https://aycharity.tech/cdn-cgi/scripts/5c5dd728/cloudflare-static/email-decode.min.js" for SQL Inj
ection
> Auditing "https://aycharity.tech/" for Web Cache Poisoning
> Auditing "https://aycharity.tech/" for Backslash Powered Scanning Differences
> Auditing "https://aycharity.tech/wp-content/themes/ngo-charity-donation/assets/js/theme-script.js" for We
b Cache Poisoning
> Auditing "https://aycharity.tech/wp-includes/js/dist/i18n.min.js" for Backslash Powered Scanning Differences
> Auditing "https://aycharity.tech/wp-includes/js/dist/hooks.min.js" for User-Agent Dependent Response
> Auditing "https://aycharity.tech/wp-includes/js/dist/hooks.min.js" for Path Relative Stylesheet Import
> Auditing "https://aycharity.tech/wp-includes/js/dist/hooks.min.js" for GraphQL Suggestions Enabled
```

Event log (14) All issues (453)

Memory: 643.3MB

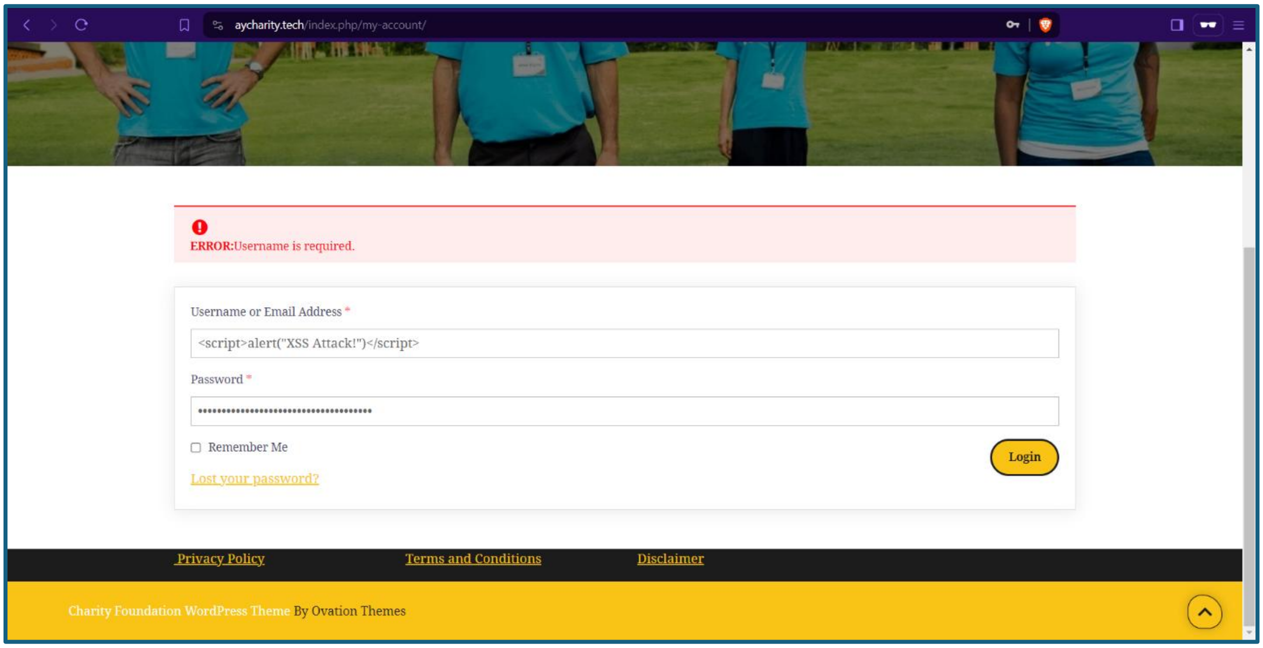
Figure 30 Burp Scan results



Apply a display filter ... <Ctrl-/>

```
No.   Time       Source               Destination          Protocol Length Info
  257 27.832291  2a02:8086:d00:6480:… 2a00:1450:400b:c03:… TLSv1.3   537 Application Data
  256 27.831774  2a02:8086:d00:6480:… 2a00:1450:400b:c03:… TLSv1.3   420 Application Data, Application Data, Application Data, Application Data, Application Data, Application Data, Application Data, A…
  255 27.827879  2a02:8086:d00:6480:… 2a00:1450:400b:c03:… TLSv1.3   138 Change Cipher Spec, Application Data
  252 27.821961  2a00:1450:400b:c03:… 2a02:8086:d00:6480:… TLSv1.3   286 Server Hello, Change Cipher Spec, Application Data
  250 27.817922  2a02:8086:d00:6480:… 2a00:1450:400b:c03:… TLSv1.3   652 Client Hello (SNI=safebrowsing.googleapis.com)
  114 7.409329   2a02:8086:d00:6480:… 2a00:1450:400b:c03:… TLSv1.3    98 Application Data
  113 7.409052   2a02:8086:d00:6480:… 2a00:1450:400b:c03:… TLSv1.3   113 Application Data
  111 7.404048   2a00:1450:400b:c03:… 2a02:8086:d00:6480:… TLSv1.3   113 Application Data
  110 7.404048   2a00:1450:400b:c03:… 2a02:8086:d00:6480:… TLSv1.3   105 Application Data
  109 7.404048   2a00:1450:400b:c03:… 2a02:8086:d00:6480:… TLSv1.3   365 Application Data
  108 7.404048   2a00:1450:400b:c03:… 2a02:8086:d00:6480:… TLSv1.3   294 Application Data
  106 7.389795   2a00:1450:400b:c03:… 2a02:8086:d00:6480:… TLSv1.3   105 Application Data
  105 7.389694   2a02:8086:d00:6480:… 2a00:1450:400b:c03:… TLSv1.3   105 Application Data
  104 7.389634   2a02:8086:d00:6480:… 2a00:1450:400b:c03:… TLSv1.3   109 Application Data
  100 7.386526   2a02:8086:d00:6480:… 2a00:1450:400b:c03:… TLSv1.3   537 Application Data
   99 7.386013   2a02:8086:d00:6480:… 2a00:1450:400b:c03:… TLSv1.3   420 Application Data, Application Data, Application Data, Application Data, Application Data, Application Data, Application Data, A…
   98 7.385594   2a00:1450:400b:c03:… 2a02:8086:d00:6480:… TLSv1.3   688 Application Data, Application Data
   97 7.381261   2a02:8086:d00:6480:… 2a00:1450:400b:c03:… TLSv1.3   138 Change Cipher Spec, Application Data
   95 7.367163   2a00:1450:400b:c03:… 2a02:8086:d00:6480:… TLSv1.3  1095 Application Data
   92 7.365622   2a00:1450:400b:c03:… 2a02:8086:d00:6480:… TLSv1.3  1294 Server Hello, Change Cipher Spec
   90 7.359634   2a02:8086:d00:6480:… 2a00:1450:400b:c03:… TLSv1.3   591 Client Hello (SNI=safebrowsing.googleapis.com)
 2114 70.693395  2a02:8086:d00:6480:… 2606:4700:3034::ac4… TLSv1.2   186 Application Data, Application Data
 2112 70.199569  2a02:8086:d00:6480:… 2606:4700:20::681a:… TLSv1.2   109 Application Data
 2110 70.198708  2606:4700:20::681a:… 2a02:8086:d00:6480:… TLSv1.2   105 Application Data
 2109 70.198708  2606:4700:20::681a:… 2a02:8086:d00:6480:… TLSv1.2   159 Application Data
 2108 70.198708  2606:4700:20::681a:… 2a02:8086:d00:6480:… TLSv1.2   392 Application Data
 2106 70.056923  2a02:8086:d00:6480:… 2606:4700:20::681a:… TLSv1.2   131 Application Data
 2072 66.376158  2606:4700:3034::ac4… 2a02:8086:d00:6480:… TLSv1.2   217 Application Data, Application Data
 2071 66.376158  2606:4700:3034::ac4… 2a02:8086:d00:6480:… TLSv1.2   394 Application Data
 2069 66.209885  2a02:8086:d00:6480:… 2606:4700:10::6816:… TLSv1.2   102 Application Data
 2068 66.209373  2606:4700:10::6816:… 2a02:8086:d00:6480:… TLSv1.2    98 Application Data
 2064 66.128235  2a02:8086:d00:6480:… 2606:4700:3034::ac4… TLSv1.2   177 Application Data
 2062 66.125090  2606:4700:3034::ac4… 2a02:8086:d00:6480:… TLSv1.2   105 Application Data
 2061 66.125090  2606:4700:3034::ac4… 2a02:8086:d00:6480:… TLSv1.2   529 Application Data
```

Figure 31 Wireshark Packet Captured - Encrypted traffic



aycharity.tech/index.php/my-account/

ERROR: Username is required.

Username or Email Address *

<script>alert("XSS Attack!")</script>

Password *

••••••••••••••••••••••••••••••••••••

□ Remember Me

Figure 32Cross Site Scripting Failed