SECURITY CHALLENGES IN DEPLOYING A CLOUD-BASED DJANGO APPLICATION USING AMAZON WEB SERVICES AND ELASTIC BEANSTALK

Capstone Project Presentation

March 29, 2024

Napoleon Davis II

Dr. Felicia Doswell (Advisor)

Dr. Thorna Humphries (Reviewer)

- Section 1. Introduction
- Section 2. Literature Review
- Section 3. Methodology
- Section 4. Results and Findings
- Section 5. Conclusion

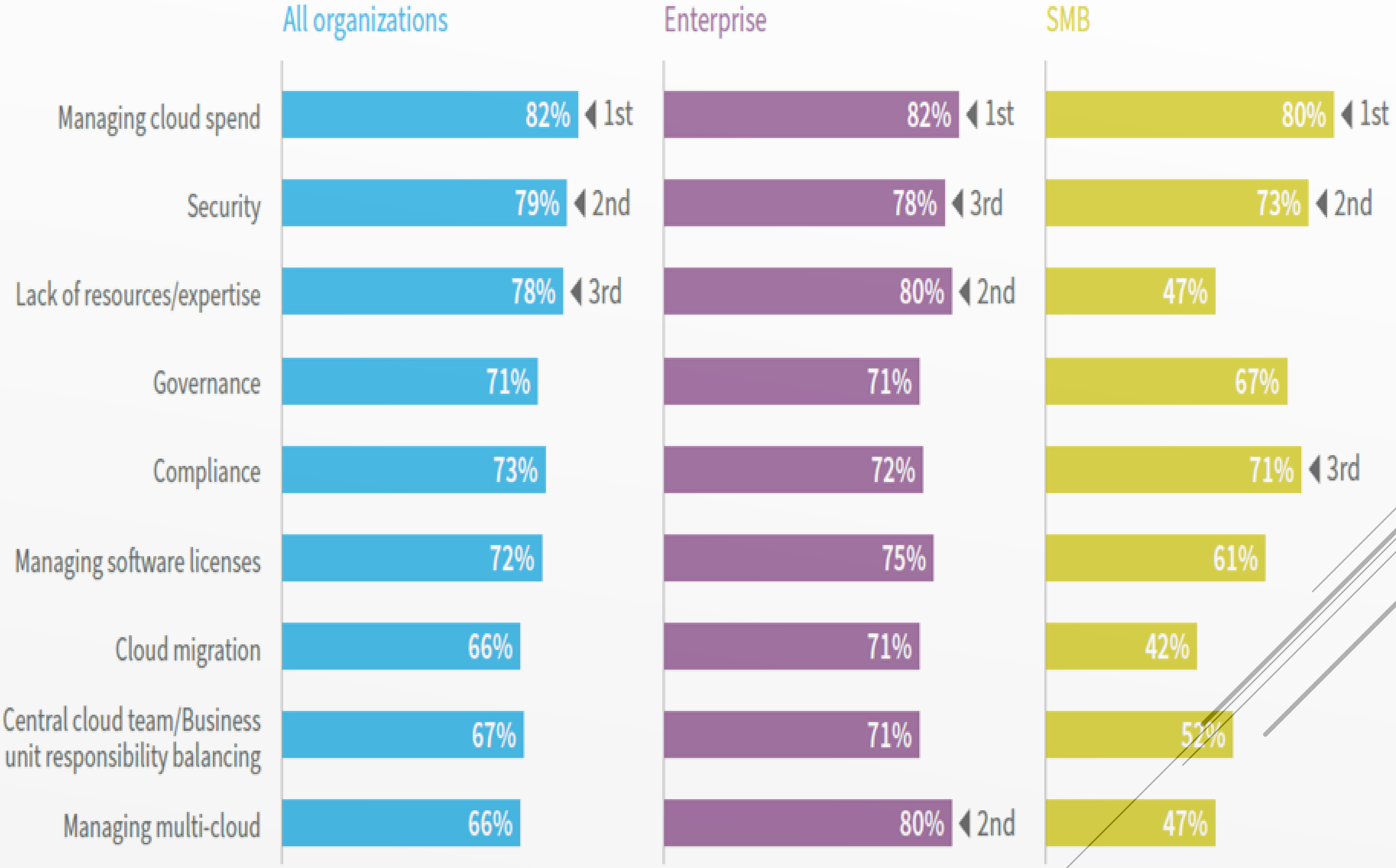
- Research Objectives
- Background on Cloud Computing
- Importance of Security in Cloud-Based Applications
- Overview of Django and Its Use in Web Development
- Significance of AWS and EBS
- Example Django Web Application ran on Cloud Model

INTRODUCTION OVERVIEW

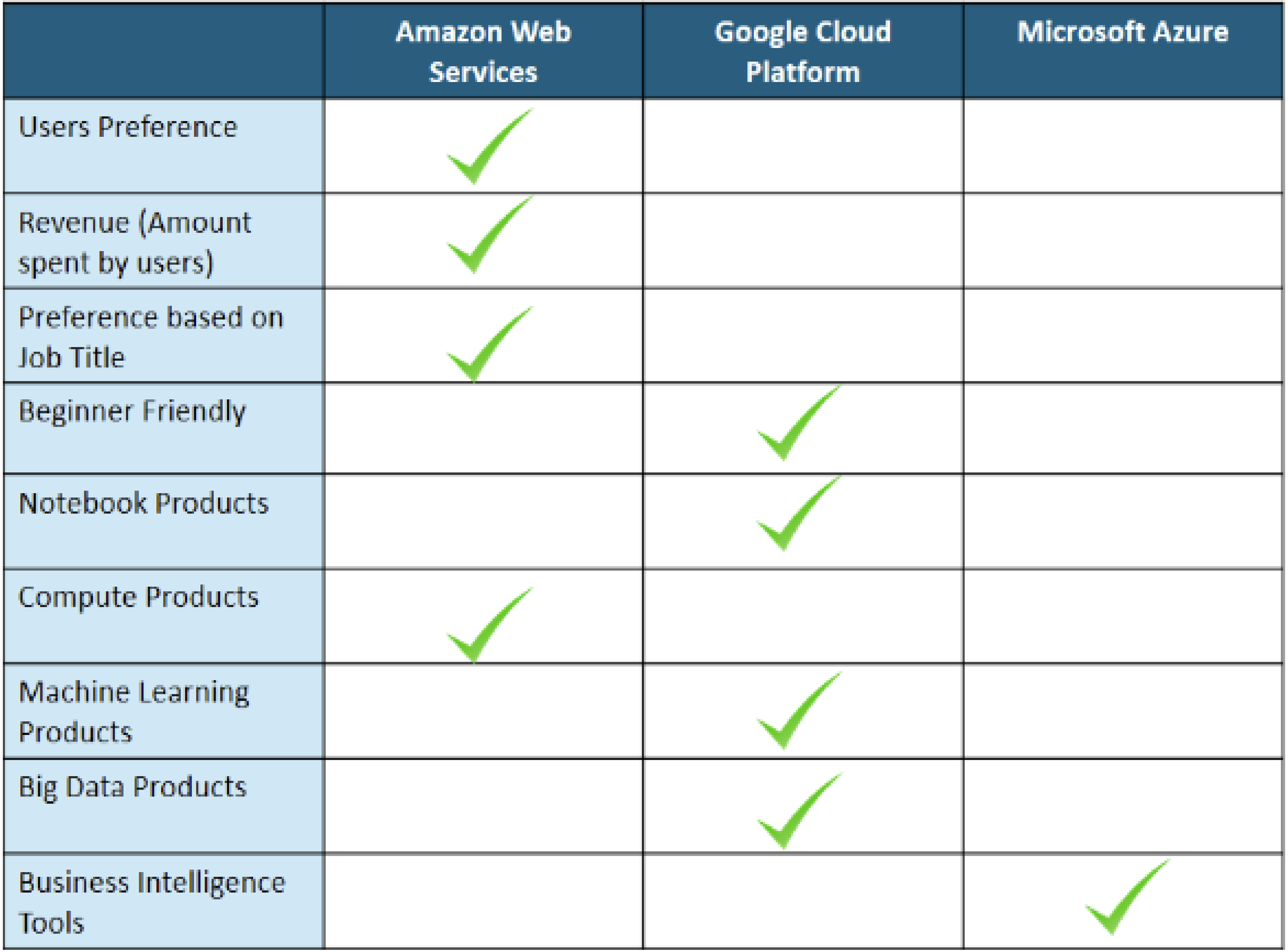
- Review the security landscape within AWS cloud computing environments
- Identifies users and usage scenarios of AWS Console
- Discusses architectural components of a Django Web Application deployed via AWS Elastic Beanstalk
- Emphasize understanding and mitigating security challenges involved in deploying a Django Web Application via AWS Elastic Beanstalk

INTRODUCTION
RESEARCH OBJECTIVES

TOP CLOUD CHALLENGES



Flexera, "Flexera State of the Cloud Report 2023," 2023. [Online]. Available: https://resources.flexera.com/web/pdf/Flexera-State-of-the-Cloud-Report-2023.pdf. [Accessed 21 11 2023].



	Amazon Web Services	Google Cloud Platform	Microsoft Azure
Users Preference	✓		
Revenue (Amount spent by users)	✓		
Preference based on Job Title	✓		
Beginner Friendly		✓	
Notebook Products		✓	
Compute Products	✓		
Machine Learning Products		✓	
Big Data Products		✓	
Business Intelligence Tools			✓

https://www.kaggle.com/code/nitishabharathi/data-science-in-the-cloud-who-wins-the-cloud-war

- Cloud computing allows users to access servers, software, and databases over the Internet, housed in data centers worldwide.
- Offers flexibility, scalability, and cost-efficiency, moving away from managing physical servers and software applications on personal devices.
- Significant milestones include the launch of AWS in 2006 and Google App Engine in 2008, marking the beginning of cloud computing's major impact on IT and business.
- The evolution of cloud services into IaaS, PaaS, and SaaS models has significantly reduced capital expenses and improved operational efficiencies for businesses.

INTRODUCTION
BACKGROUND ON CLOUD COMPUTING

- Security in cloud computing is a critical concern, focusing on data integrity, confidentiality, and availability due to the shared responsibility model.
- Early concerns included loss of data control and reliance on third-party security measures, evolving to address vulnerabilities unique to the cloud environment.
- Developments in encryption, access control, and regular security audits have become standard to protect against threats like data breaches and DoS attacks.
- Despite advancements, continuous vigilance and innovation in security practices are required to combat the dynamic nature of cloud computing and cyber threats.

INTRODUCTION

IMPORTANCE OF SECURITY IN CLOUD-BASED APPLICATIONS

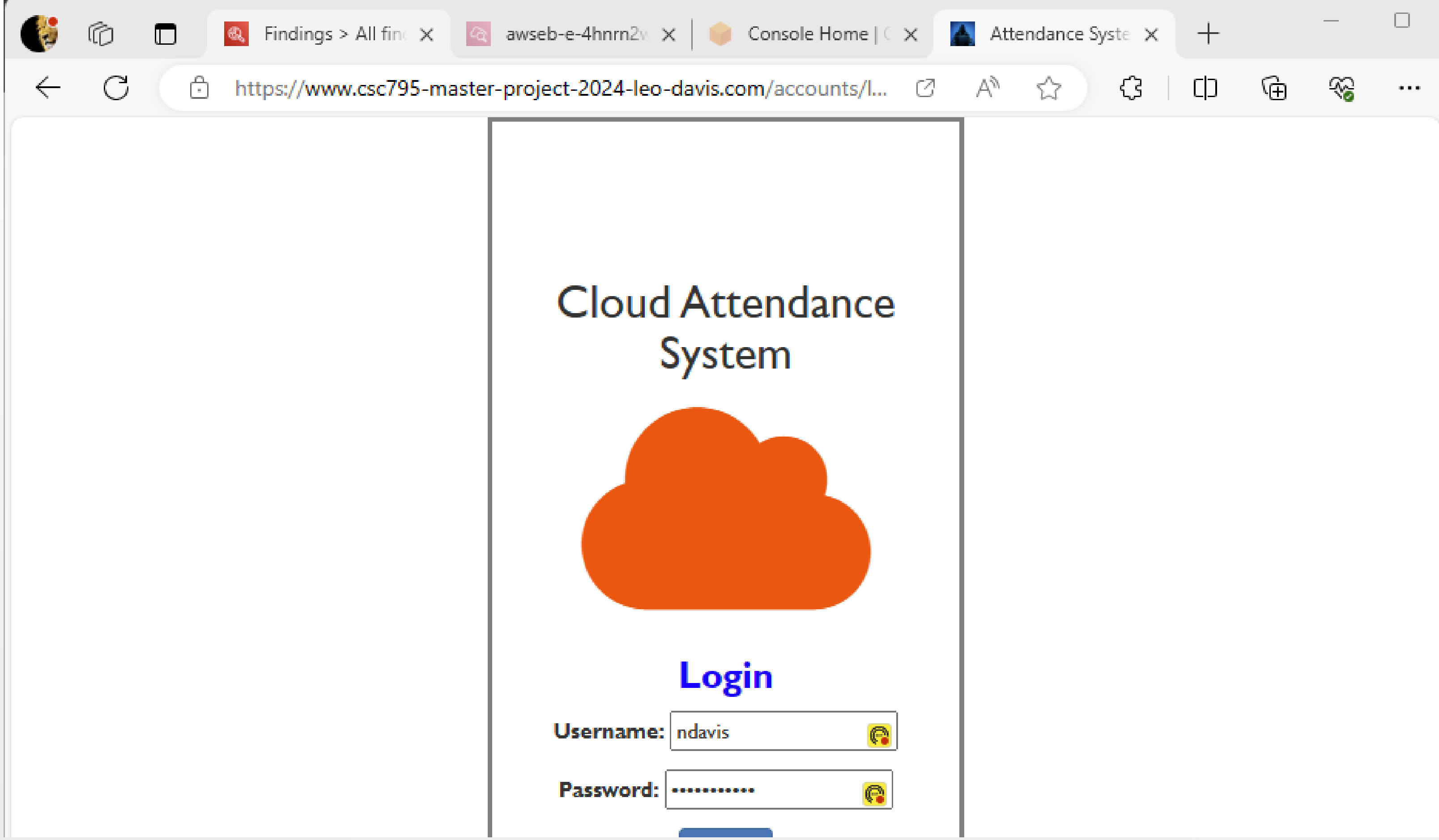
- Django, a high-level Python web framework, focuses on rapid development and DRY (Don't Repeat Yourself) principles to minimize code redundancy.
- Praised for its ORM system for database interactions and built-in protections against common vulnerabilities, Django is a choice for secure and scalable web development.
- Django supports horizontal scaling and integrates with caching mechanisms, with a community that provides reusable apps, plugins, and libraries to extend functionality.

INTRODUCTION

OVERVIEW OF DJANGO AND ITS USE IN WEB DEVELOPMENT

- AWS has been a pivotal force in cloud computing since 2006, offering a wide array of services that revolutionized IT infrastructure management.
- Elastic Beanstalk, introduced in 2011, simplifies deploying and managing applications, automating key tasks like provisioning, load balancing, and application health monitoring.
- The service has democratized cloud computing, making it accessible to developers without deep expertise in cloud environments, and contributed to trends like microservices and DevOps.

INTRODUCTION
SIGNIFICANCE OF AMAZON WEB SERVICES AND ELASTIC BEANSTALK IN CLOUD COMPUTING


Findings > All fin
awseb-e-4hnrn2v
Console Home | C
Attendance Syste
https://www.csc795-master-project-2024-leo-davis.com/accounts/l...

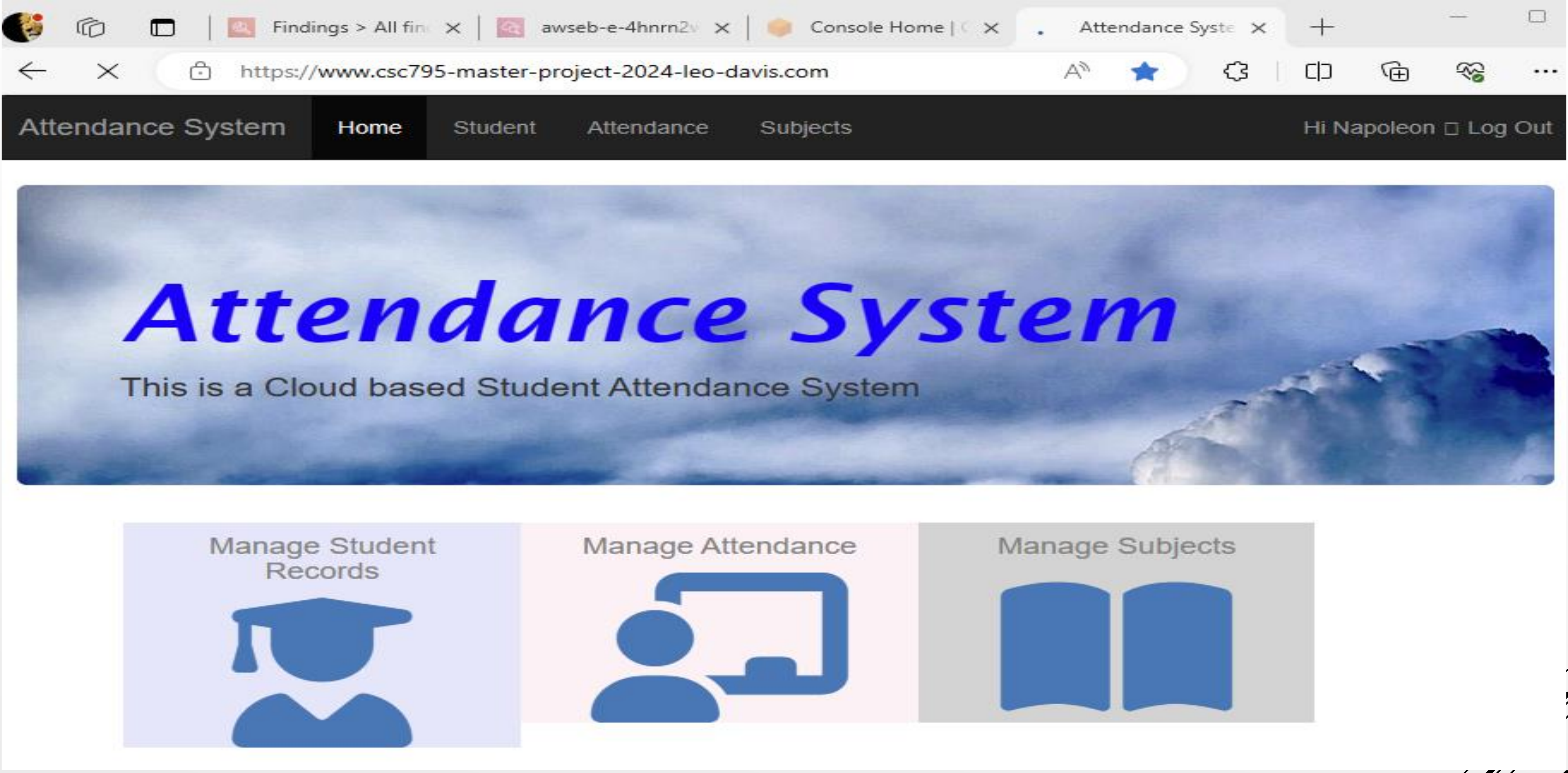
Cloud Attendance System

Login

Username: ndavis

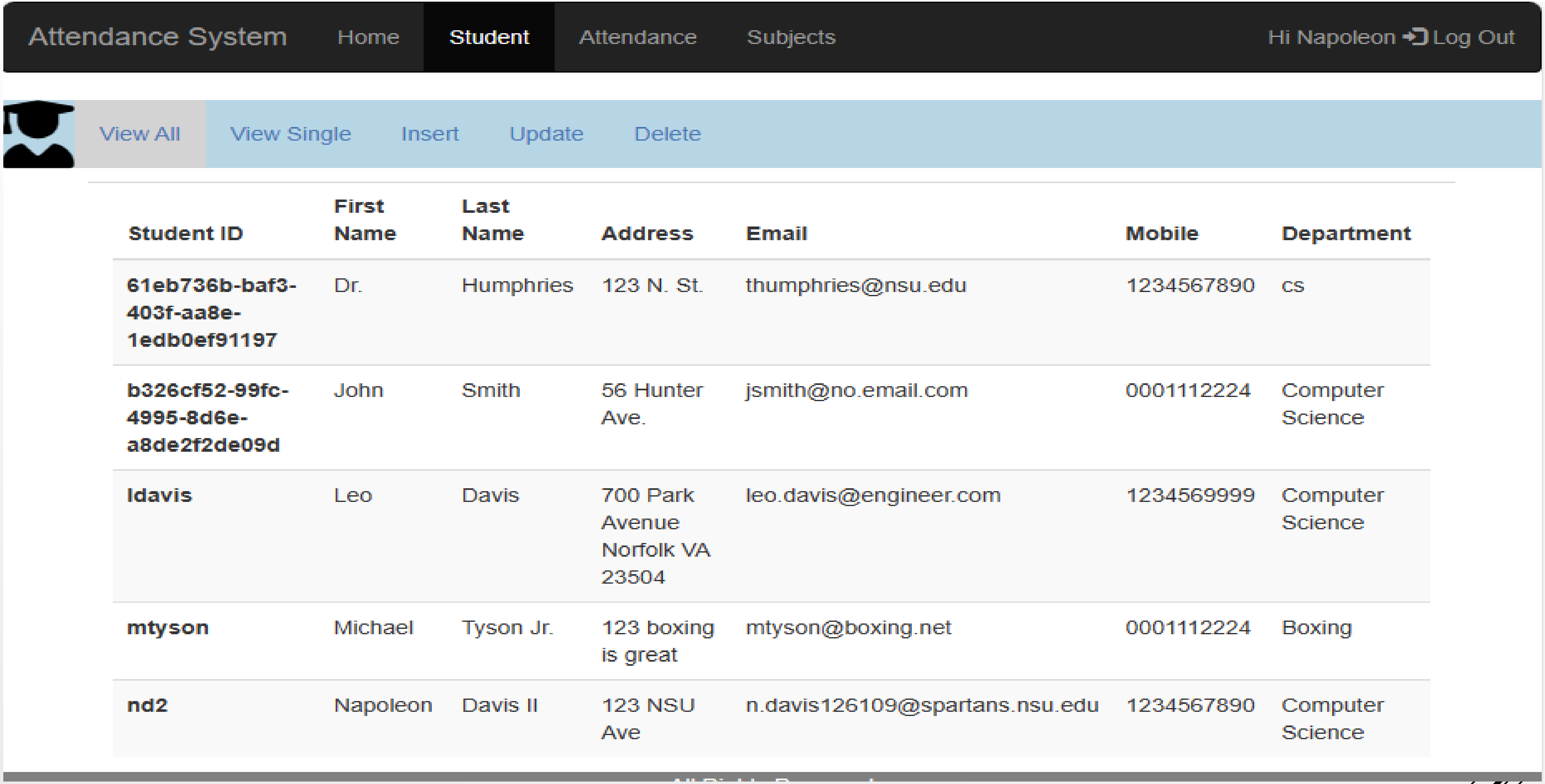
Password: ••••••••••••

INTRODUCTION
EXAMPLE DJANGO WEB APPLICATION



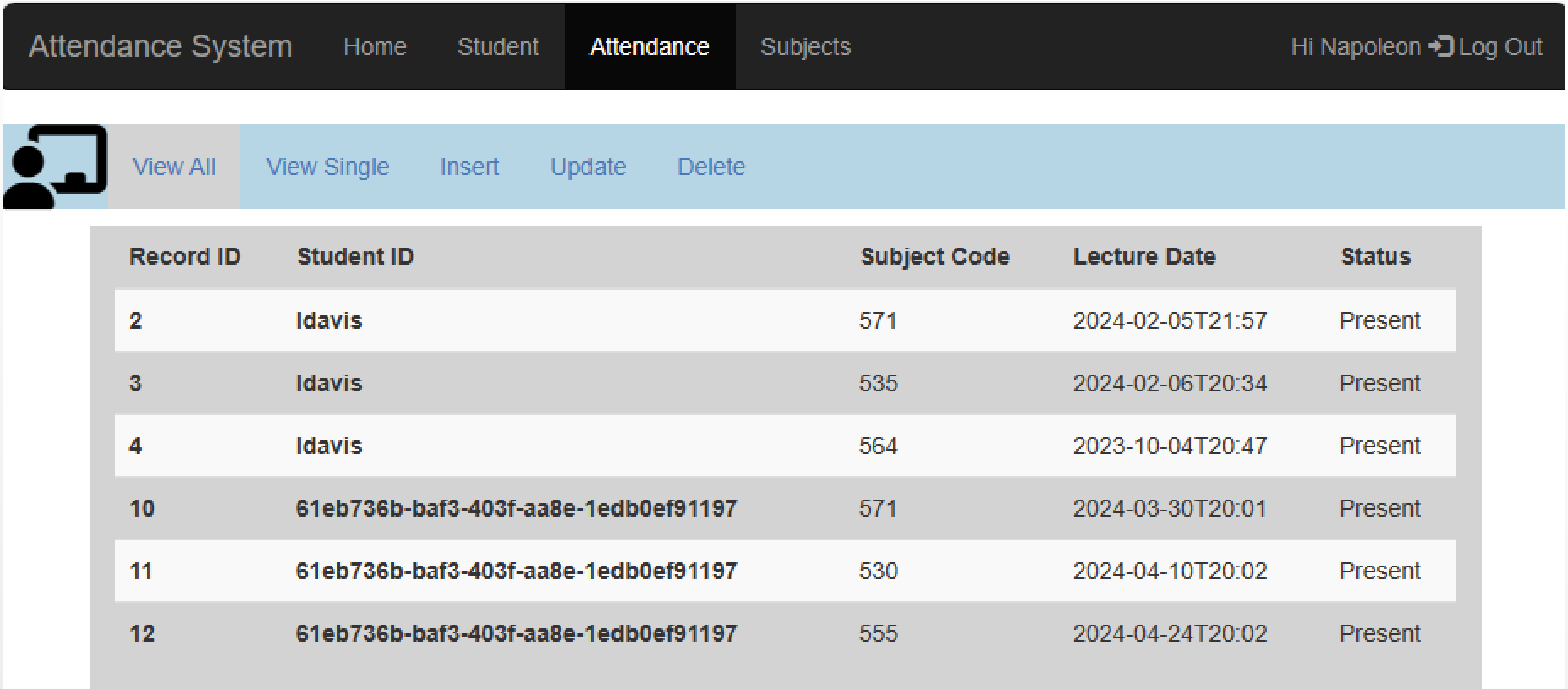
INTRODUCTION

EXAMPLE DJANGO WEB APPLICATION



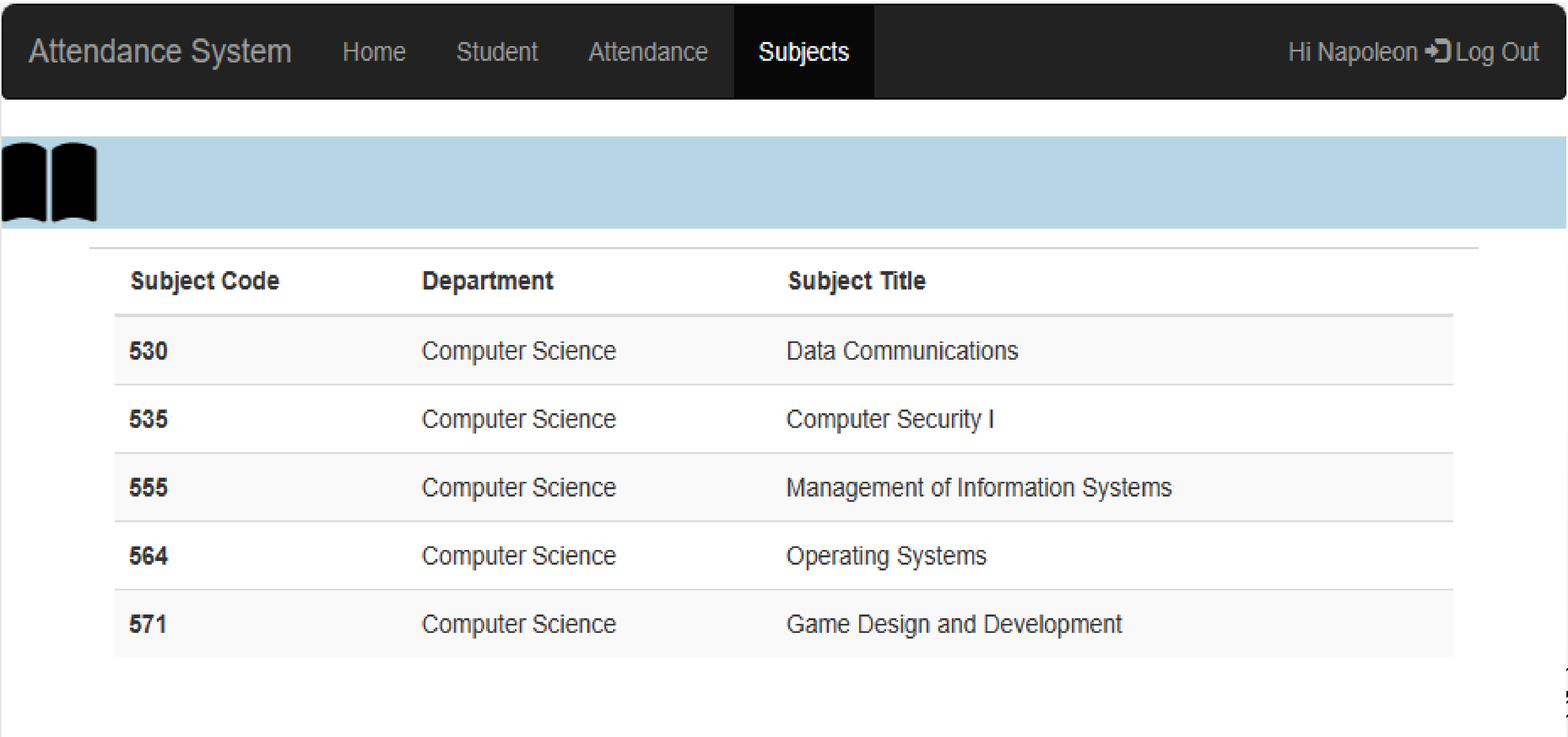
Student ID	First Name	Last Name	Address	Email	Mobile	Department
61eb736b-baf3-403f-aa8e-1edb0ef91197	Dr.	Humphries	123 N. St.	thumphries@nsu.edu	1234567890	cs
b326cf52-99fc-4995-8d6e-a8de2f2de09d	John	Smith	56 Hunter Ave.	jsmith@no.email.com	0001112224	Computer Science
ldavis	Leo	Davis	700 Park Avenue Norfolk VA 23504	leo.davis@engineer.com	1234569999	Computer Science
mtyson	Michael	Tyson Jr.	123 boxing is great	mtyson@boxing.net	0001112224	Boxing
nd2	Napoleon	Davis II	123 NSU Ave	n.davis126109@spartans.nsu.edu	1234567890	Computer Science

INTRODUCTION
EXAMPLE DJANGO WEB APPLICATION



Record ID	Student ID	Subject Code	Lecture Date	Status
2	ldavis	571	2024-02-05T21:57	Present
3	ldavis	535	2024-02-06T20:34	Present
4	ldavis	564	2023-10-04T20:47	Present
10	61eb736b-baf3-403f-aa8e-1edb0ef91197	571	2024-03-30T20:01	Present
11	61eb736b-baf3-403f-aa8e-1edb0ef91197	530	2024-04-10T20:02	Present
12	61eb736b-baf3-403f-aa8e-1edb0ef91197	555	2024-04-24T20:02	Present

INTRODUCTION
EXAMPLE DJANGO WEB APPLICATION



Subject Code	Department	Subject Title
530	Computer Science	Data Communications
535	Computer Science	Computer Security I
555	Computer Science	Management of Information Systems
564	Computer Science	Operating Systems
571	Computer Science	Game Design and Development

INTRODUCTION

EXAMPLE DJANGO WEB APPLICATION

- Section 1. Introduction
- Section 2. Literature Review
- Section 3. Methodology
- Section 4. Results and Findings
- Section 5. Conclusion

- Fundamentals of Cloud Computing
- Evolution of Cloud Computing
- Overview of Secure Cloud Computing
- Reliance on Automated Tools
- Previous Works concerning Cloud Security Challenges
- Security Challenges in Deploying Django Applications on AWS
- AWS Specific Security Challenges
- AWS Infrastructure and Elastic Beanstalk Overview
- Related Work on Cloud Computing
- Gaps in Existing Research

LITERATURE REVIEW
OVERVIEW

- Detailed explanation of cloud computing characteristics, service models (IaaS, PaaS, SaaS), and deployment models (public, private, hybrid).
- Benefits and challenges of cloud computing discussed.

LITERATURE REVIEW

FUNDAMENTALS OF CLOUD COMPUTING

- Shift from on-premises data centers to cloud-based infrastructure for scalability, performance, and cost-effectiveness.
- Initial cloud services categorized into IaaS, PaaS, and SaaS.
- Security as a paramount concern with solutions like enhanced encryption and IAM frameworks.
- Future of cloud computing looks towards edge computing, quantum computing, and AI-driven services.

LITERATURE REVIEW

EVOLUTION OF CLOUD COMPUTING

- Evolution of cloud security measures from early concerns to advanced security architectures and technologies.
- Emphasis on encryption, IAM, and best practices for secure cloud computing.

LITERATURE REVIEW

OVERVIEW OF SECURE CLOUD COMPUTING

- Shift towards using automated tools and frameworks enhancing productivity but introducing dependencies.
- Trust issues in automated processes discussed with examples of vulnerabilities and ethical concerns.

LITERATURE REVIEW

RELIANCE ON AUTOMATED TOOLS

- Multi-Tenancy and Data Location:
  - Jajodia, addresses multi-tenancy and data location's complexities within cloud environments.
  - Safhi, Al-Zahrani, and Mubaraki’s research brings our focus to encryption and secure configurations to safeguard data.

- Vulnerabilities and Compliance
  - The “Taxonomy of Cloud Computing Vulnerabilities” presented by Mishra, Kumar, Singh, and Dwivedi laid the groundwork for our emphasis on identifying and mitigating specific threats.
  - The shared responsibility model and integration of security measures across the cloud stack, as advocated by "Cloud Security & Compliance For Dummies”, by Miller have been pivotal in breaking up the design model into phases.

LITERATURE REVIEW

PREVIOUS WORK ON CLOUD SECURITY CHALLENGES

- Discussion on Django's security features including CSRF protection, SQL injection prevention, and secure password handling.
- Challenges such as security misconfigurations and the balance between security measures and performance.

LITERATURE REVIEW

DJANGO SECURITY FEATURES AND LIMITATIONS

- Challenges like misconfigured S3 buckets, inadequate IAM policies, and insufficient network access control highlighted.
- Solutions include automated security scanning, encryption, and enhanced monitoring and logging.

LITERATURE REVIEW

AWS-SPECIFIC SECURITY CHALLENGES

- Evolution of AWS and Elastic Beanstalk security features to address cybersecurity threats.
- Introduction of services like AWS Shield, AWS WAF, and Amazon Inspector for improved security.

LITERATURE REVIEW

AWS AND ELASTIC BEANSTALK'S SECURITY MECHANISMS

- Application Modernization and Cloud Deployment Strategies
  - Our methodology is informed by the insights of Pushpaleela et al., who advocate for a structured approach to cloud deployment, emphasizing analysis, planning, and the leverage of AWS cloud automation and DevOps tools.
- Comparative Analysis of Cloud Computing Services
  - The comparative analysis provided by Kaushik et al., highlighting AWS's superior disk performance and RAM speed, has directly influenced our choice of AWS RDS for backend storage. This selection is pivotal for supporting database-intensive applications such as the attendance system, ensuring optimal performance and cost-effectiveness.

LITERATURE REVIEW

RELATED WORK ON CLOUD-BASED ATTENDANCE SYSTEMS

- Security Mechanisms on Cloud Platforms
  - Our methodology also integrates the findings of Kaur et al., who evaluated AWS and IBM Cloud's performance and security mechanisms. This comparison is vital for our deployment strategy, particularly for utilizing AWS RDS's security features to ensure the secure storage of sensitive attendance data, thus aligning our security measures with the specific requirements of our Django-based attendance system.
- AWS Cloud Computing Security Challenges and Solutions
  - The work of Mishra et al. on AWS Cloud Computing's security challenges offers insights into security measures, best practices, and AWS's efforts in ensuring data privacy and infrastructure security. This research is particularly relevant to our deployment, highlighting the necessity of robust security configurations in Elastic Beanstalk and RDS to safeguard against vulnerabilities.

LITERATURE REVIEW

RELATED WORK ON CLOUD-BASED ATTENDANCE SYSTEMS CONT…

- GAPS
  - Lack of in-depth analysis on specific security challenges for Django applications on AWS Elastic Beanstalk.
- BRIDGING THE GAP
  - My research, "Security Challenges in Deploying a Cloud-Based Django Application Using Amazon Web Services and Elastic Beanstalk," aims to provide comprehensive insights into deploying Django applications securely on AWS.

LITERATURE REVIEW

GAPS IN EXISTING RESEARCH

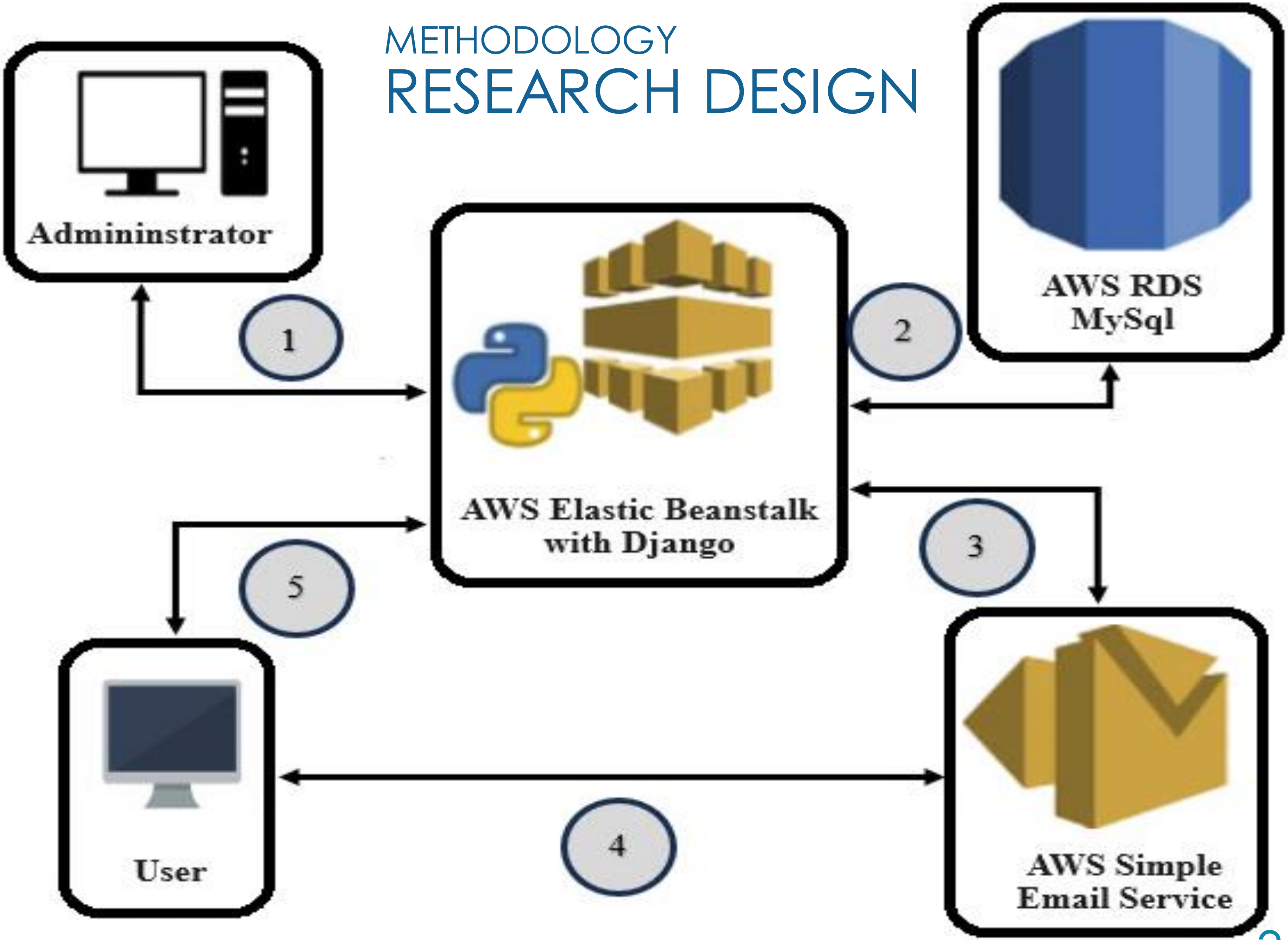
- Section 1. Introduction
- Section 2. Literature Review
- Section 3. Methodology
- Section 4. Results and Findings
- Section 5. Conclusion

- Research Design
- Implementation
- Data Collection
- Analysis

METHODOLOGY OVERVIEW

METHODOLOGY

RESEARCH DESIGN



GitHub - kujalk/Cloud_Attendance_System: Cloud based student attendance system

METHODOLOGY
PHASES

- Phase I: Preparation and Security Setup
- Phase 2: Database and Email Service Configuration
- Phase 3. Application Preparation and Deployment
- Phase 4: Post-Deployment Security

METHODOLOGY

PHASE 1: PREPARATION AND SECURITY SETUP

Task	Objective	Procedure
Install Python 3.8.0:	Install Python 3.8.0 for compatibility with Django and AWS services.	Download Python from the official website, verify the checksum, and set up a virtual environment for dependency management.
Install MySQL Workbench	Facilitate database schema design and management.	MySQL Workbench configures SSL connections to AWS RDS instances for secure data management.
Create an AWS Free Tier Account	Utilize AWS services without initial costs.	Sign up, provide payment details, verify identity, and select a support plan.
Secure the AWS Account		▪ Setup MFA for Root User: Enhance security by adding a layer beyond passwords. ▪ Create Security Group for Power User: Define IAM policies for necessary permissions without full administrative access. ▪ Create IAM User and Setup MFA: Minimize root account usage and secure IAM user access. ▪ Assign IAM User to Power User Group: Streamline permission management. ▪ Create Security Access Key for IAM User: Enable programmatic access to AWS services, ensuring critical security.
Install and Configure Amazon CLI	Automate interactions with AWS services.	Install AWS CLI, configure it with the IAM user's security access key, and set up the default region and output format.

Task	Objective	Procedure
Create RDS MySQL Instance	Set up a scalable and secure managed database service.	Configure instances with security groups, appropriate sizes, automatic backups, and encryption.
Create an AWS SES Instance	Enable the application to send emails reliably and securely.	Verify a domain/email, set up DKIM, and create SMTP credentials.

METHODOLOGY

PHASE 2: DATABASE AND EMAIL SERVICE CONFIGURATION

Task	Objective	Procedure
Prepare Cloud Attendance System Project on Local Host	Ensure the application functions correctly before deployment.	Set up the development environment, install dependencies, and test the application locally.
Secure Secret Keys and Update settings.py	Enhance security by removing sensitive data from the source code.	Use environment variables for secret keys and database configurations.
Deploy Django Application to AWS via Elastic Beanstalk	Deploy the application in a secure and scalable manner.	Configure Elastic Beanstalk environment correctly, specifying Python version.

METHODOLOGY

PHASE 3: APPLICATION PREPARATION AND DEPLOYMENT

Task	Objective	Procedure
Monitor Application Health with Elastic Beanstalk	Ensure application reliability and performance.	Utilize monitoring tools and set up health checks and alarms.
Configure HTTPS and Domain Name	Establish a secure and professional online presence.	▪ Obtain and configure SSL certificate. ▪ Set up a domain name with Route 53. ▪ Implement HTTP to HTTPS redirection.
Setup Amazon Inspector	Assess the security and compliance of AWS resources.	▪ Enable Amazon Inspector ▪ Define assessment targets and templates. ▪ Run assessments ▪ Mitigate vulnerabilities

METHODOLOGY

PHASE 4: POST-DEPLOYMENT SECURITY

- Research design can be implemented using AWS Free Tier Services.
- The purchase of a custom domain name was involved but not necessary.

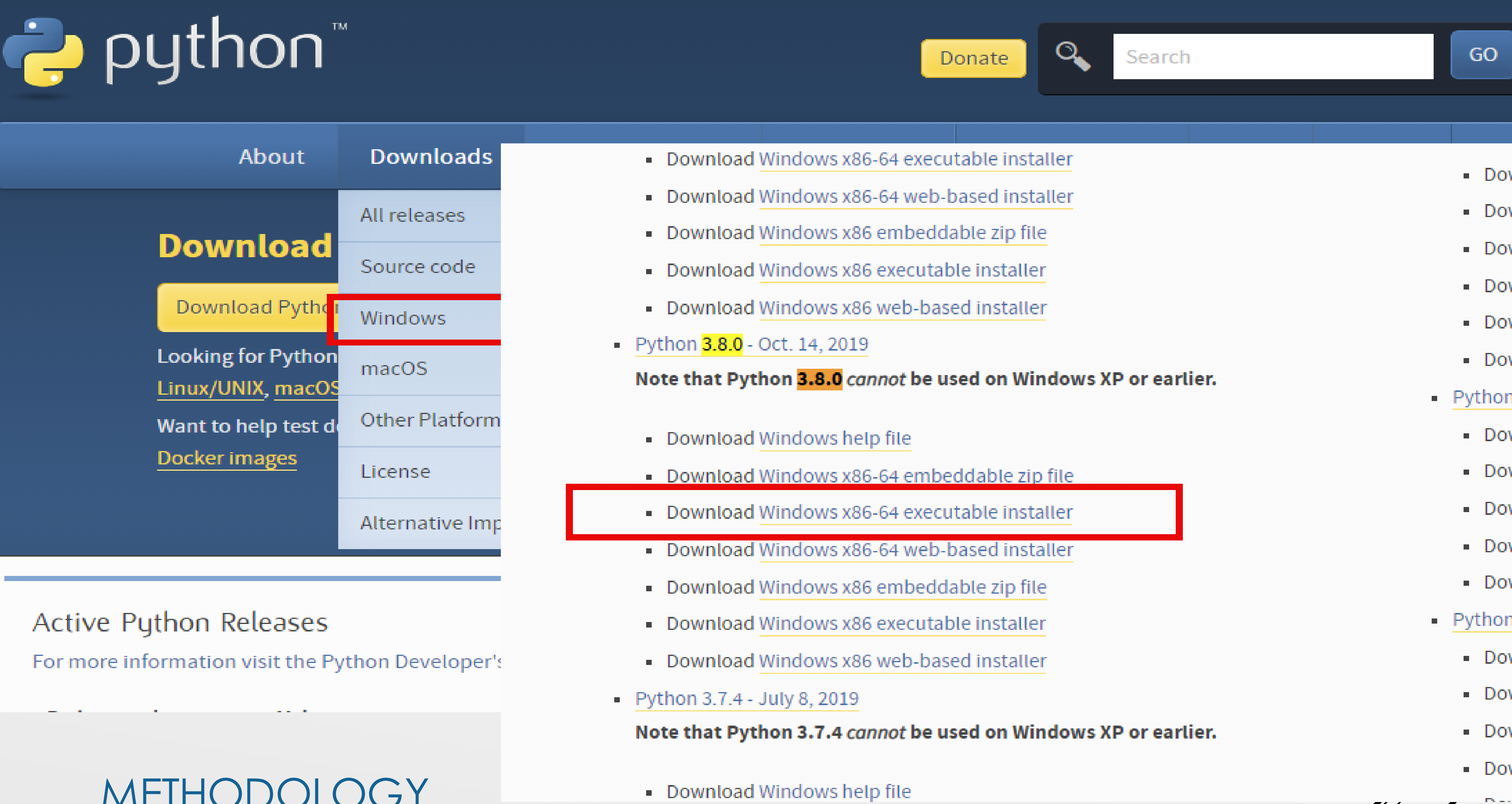
METHODOLOGY

DESIGN INITIAL STARTUP COSTS

Python 3.8.0 Installation	Python 3.8.0	$	Open Source
MySQL Workbench Installation	MySql Workbench Community Edition	$0	Open Source
AWS Free Tier Account Creation	AWS Free Tier	$0	Free for the first 12 months, certain limits apply.
AWS Account Security Setup	AWS Identity and Access Management	$0	Estimated Time to complete setup depends on experience.
Amazon CLI Installation and Configuration	AWS CLI	$0	Estimated Time to complete setup depends on experience.
RDS MySQL Instance Creation	AWS RDS	$0	Free Tier eligible; costs may apply for higher specifications
AWS SES Instance Creation	AWS SES	$0	Free Tier eligible; costs may apply for higher specifications. Time varies depending on the sandbox or production. Production requires some additional verifications that can take up to 72 hours.
Django Application Preparation	Cloud Attendance System Example	$0	
Elastic Beanstalk Deployment	AWS Elastic Beanstalk	$0	Free Tier eligible, costs may apply based on resources.
HTTPS and Domain Configuration	Domain Name	$ 13.00	Domain Name purchase varies depending on the domain name's current existence, whether someone already owns it, and the demand/number of requests for the same name.
Application Health Monitoring	AWS Elastic Beanstalk, CloudWatch	$0	Costs based on assessment runs and instances

- Stresses the importance of installing Python 3.8.0 for compatibility and securing interactions through MySQL Workbench with AWS RDS.
- Highlights the significance of AWS Free Tier for cost-effective exploration of AWS services.
- Emphasizes securing the AWS account through MFA and the creation of IAM users and groups for minimized root account usage and streamlined permission management.
- Discusses automating interactions with AWS services through the Amazon CLI and securing programmatic access with security access keys.
- Details the creation of a scalable and secure RDS MySQL instance and SES instance for reliable email sending.
- Preparing the application locally and securing it before deploying to AWS Elastic Beanstalk for a secure, scalable presence.

METHODOLOGY
IMPLEMENTATION



- Download Windows x86-64 executable installer
- Download Windows x86-64 web-based installer
- Download Windows x86 embeddable zip file
- Download Windows x86 executable installer
- Download Windows x86 web-based installer

- Python 3.8.0 - Oct. 14, 2019

  Note that Python 3.8.0 *cannot* be used on Windows XP or earlier.

  - Download Windows help file
  - Download Windows x86-64 embeddable zip file
  - Download Windows x86-64 executable installer
  - Download Windows x86-64 web-based installer
  - Download Windows x86 embeddable zip file
  - Download Windows x86 executable installer
  - Download Windows x86 web-based installer

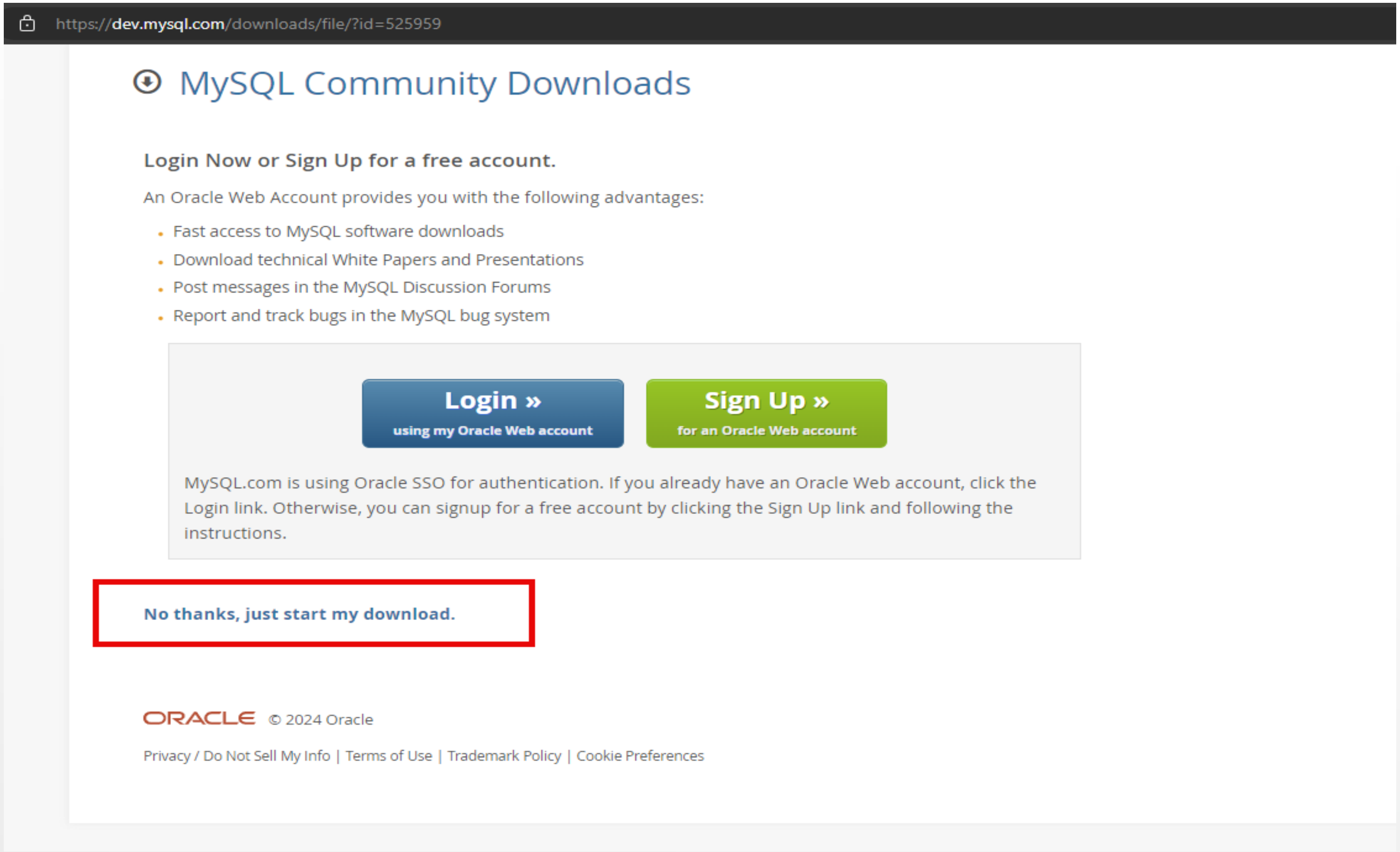
- Python 3.7.4 - July 8, 2019

  Note that Python 3.7.4 *cannot* be used on Windows XP or earlier.

  - Download Windows help file

METHODOLOGY

IMPLEMENTATION - PYTHON INSTALL



https://dev.mysql.com/downloads/file/?id=525959

MySQL Community Downloads

Login Now or Sign Up for a free account.

An Oracle Web Account provides you with the following advantages:

- Fast access to MySQL software downloads
- Download technical White Papers and Presentations
- Post messages in the MySQL Discussion Forums
- Report and track bugs in the MySQL bug system

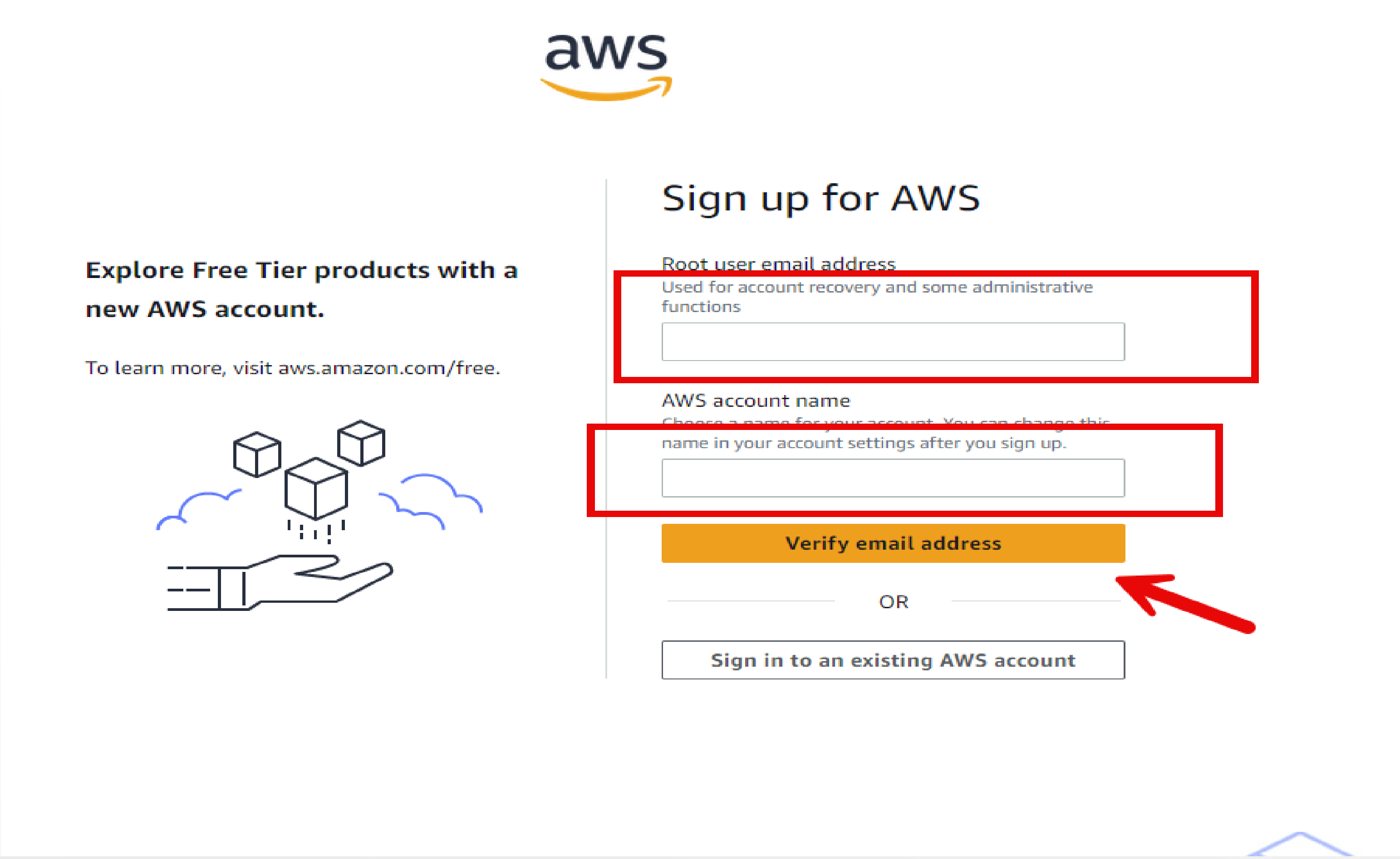
MySQL.com is using Oracle SSO for authentication. If you already have an Oracle Web account, click the Login link. Otherwise, you can signup for a free account by clicking the Sign Up link and following the instructions.

No thanks, just start my download.

ORACLE © 2024 Oracle

Privacy / Do Not Sell My Info | Terms of Use | Trademark Policy | Cookie Preferences

METHODOLOGY
IMPLEMENTATION - MYSQL WORKBENCH INSTALL



Explore Free Tier products with a new AWS account.

To learn more, visit aws.amazon.com/free.

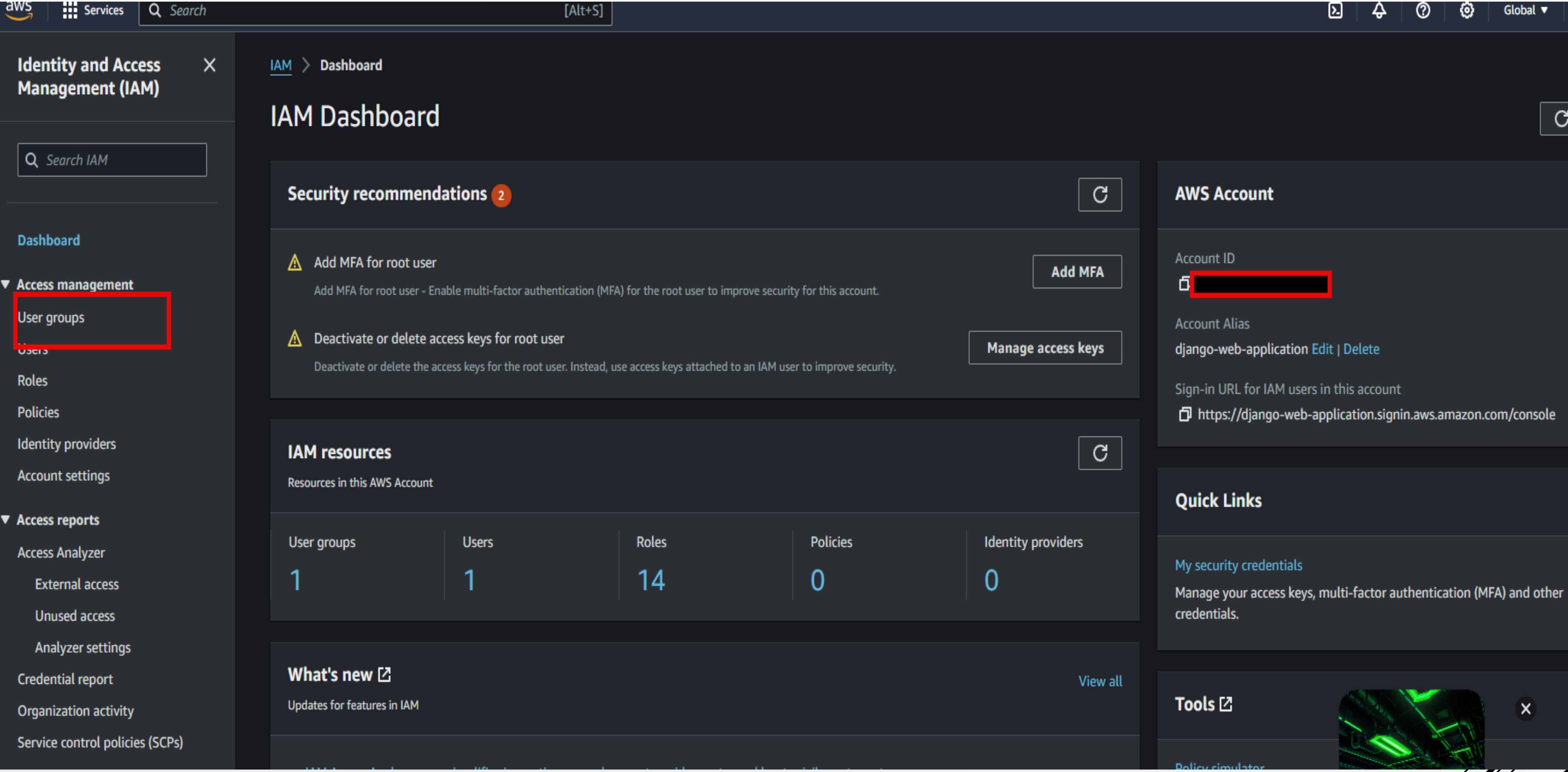
Sign up for AWS

Root user email address
Used for account recovery and some administrative functions

AWS account name
Choose a name for your account. You can change this name in your account settings after you sign up.

METHODOLOGY

IMPLEMENTATION - AWS FREE TIER ACCOUNT SETUP



IAM Dashboard

Security recommendations 2

⚠ Add MFA for root user

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

⚠ Deactivate or delete access keys for root user

Deactivate or delete the access keys for the root user. Instead, use access keys attached to an IAM user to improve security.

IAM resources

Resources in this AWS Account

User groups	Users	Roles	Policies	Identity providers
1	1	14	0	0

What's new

Updates for features in IAM

AWS Account

Account ID
[redacted]

Account Alias
django-web-application Edit | Delete

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

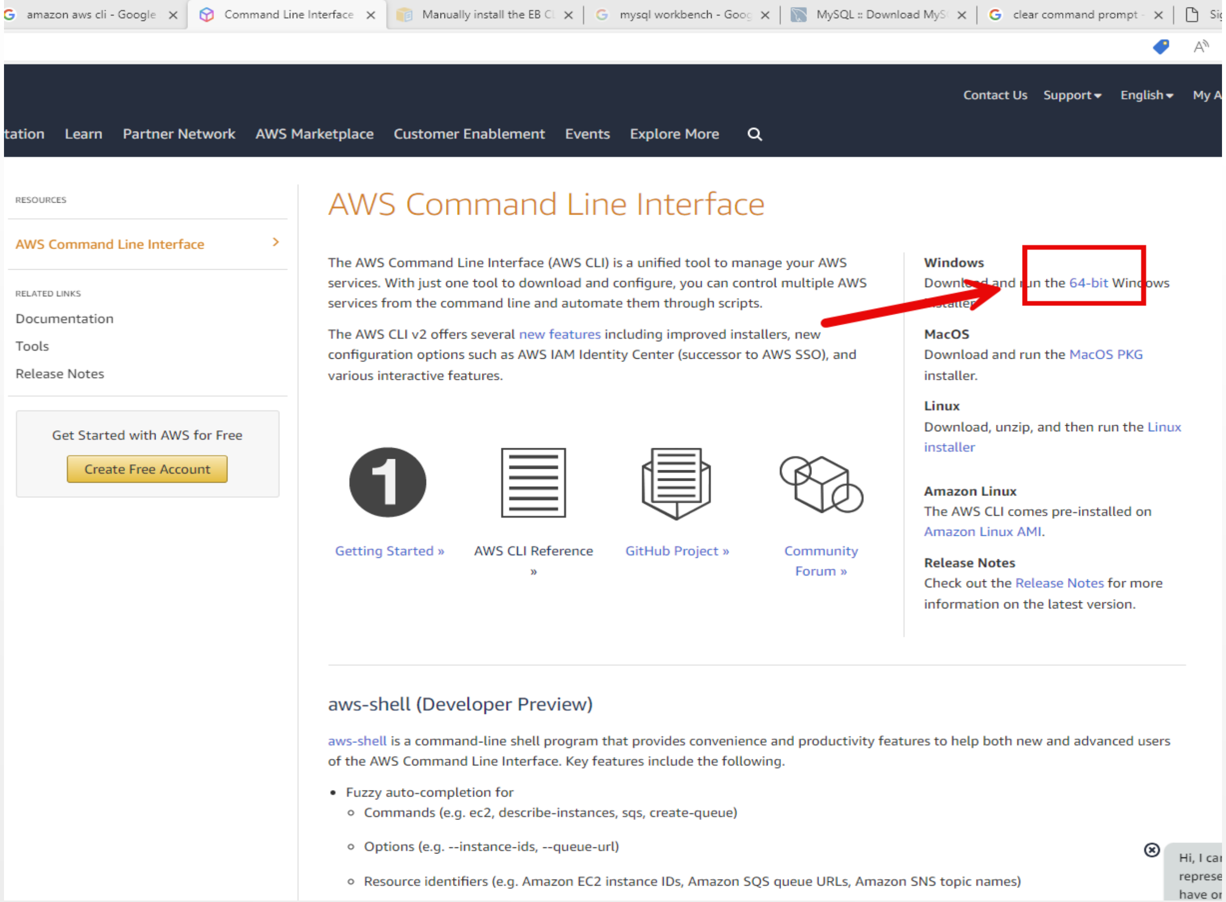
Quick Links

My security credentials

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

METHODOLOGY

IMPLEMENTATION – IAM USERS, GROUPS, PERMISSIONS, AND POLICIES



AWS Command Line Interface

The AWS Command Line Interface (AWS CLI) is a unified tool to manage your AWS services. With just one tool to download and configure, you can control multiple AWS services from the command line and automate them through scripts.

The AWS CLI v2 offers several new features including improved installers, new configuration options such as AWS IAM Identity Center (successor to AWS SSO), and various interactive features.

Windows
Download and run the 64-bit Windows installer.

MacOS
Download and run the MacOS PKG installer.

Linux
Download, unzip, and then run the Linux installer

Amazon Linux
The AWS CLI comes pre-installed on Amazon Linux AMI.

Release Notes
Check out the Release Notes for more information on the latest version.

aws-shell (Developer Preview)

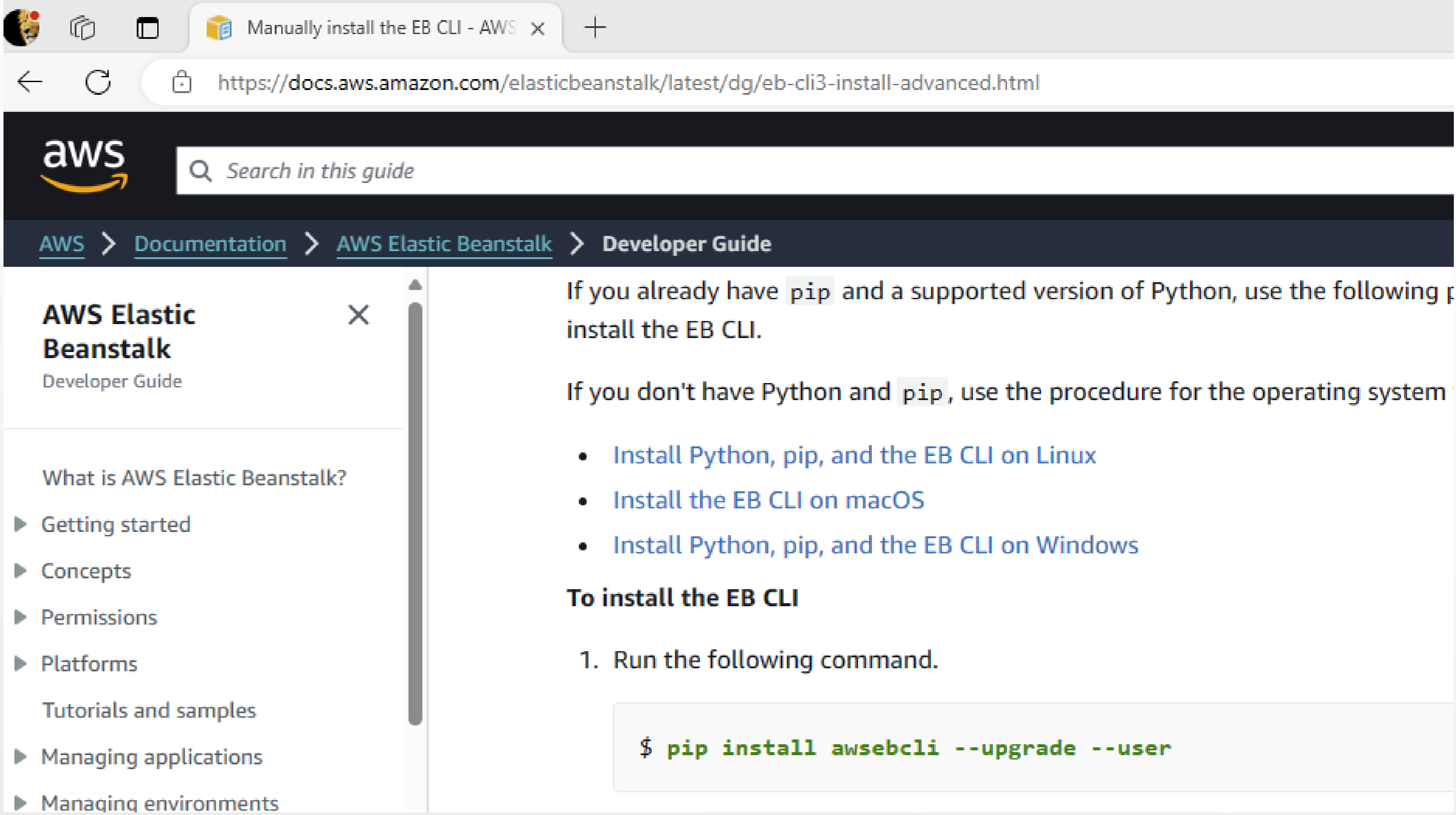
aws-shell is a command-line shell program that provides convenience and productivity features to help both new and advanced users of the AWS Command Line Interface. Key features include the following.

- Fuzzy auto-completion for
  - Commands (e.g. ec2, describe-instances, sqs, create-queue)
  - Options (e.g. --instance-ids, --queue-url)
  - Resource identifiers (e.g. Amazon EC2 instance IDs, Amazon SQS queue URLs, Amazon SNS topic names)

Hi, I car
represe
have or

METHODOLOGY

IMPLEMENTATION – AWS CLI CONFIGURATION



Manually install the EB CLI - AWS
https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/eb-cli3-install-advanced.html
aws
Search in this guide
AWS > Documentation > AWS Elastic Beanstalk > Developer Guide
AWS Elastic Beanstalk
Developer Guide
What is AWS Elastic Beanstalk?
Getting started
Concepts
Permissions
Platforms
Tutorials and samples
Managing applications
Managing environments

If you already have pip and a supported version of Python, use the following p install the EB CLI.

If you don't have Python and pip, use the procedure for the operating system

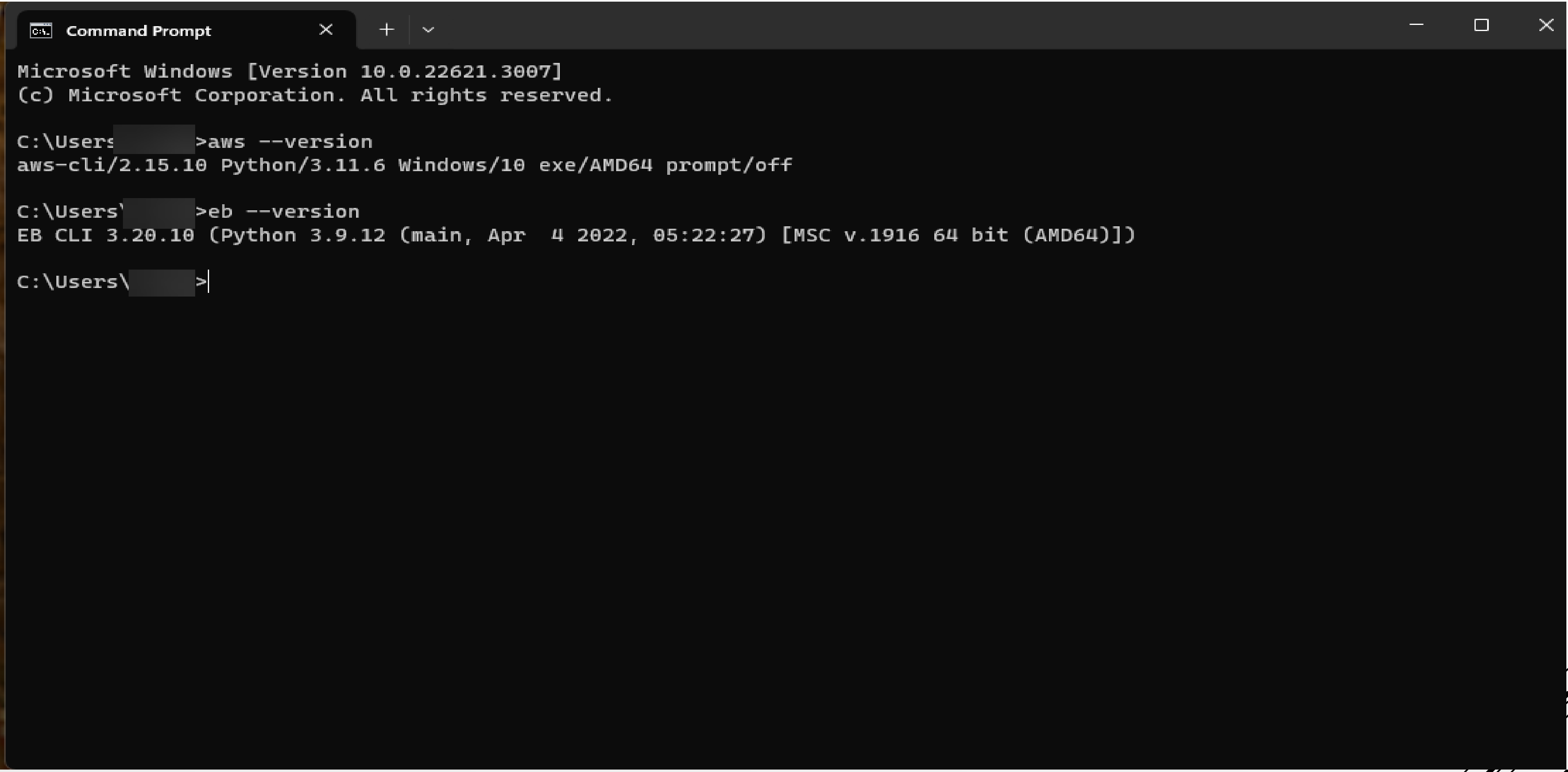
- Install Python, pip, and the EB CLI on Linux
- Install the EB CLI on macOS
- Install Python, pip, and the EB CLI on Windows

To install the EB CLI

1. Run the following command.

```
$ pip install awsebcli --upgrade --user
```

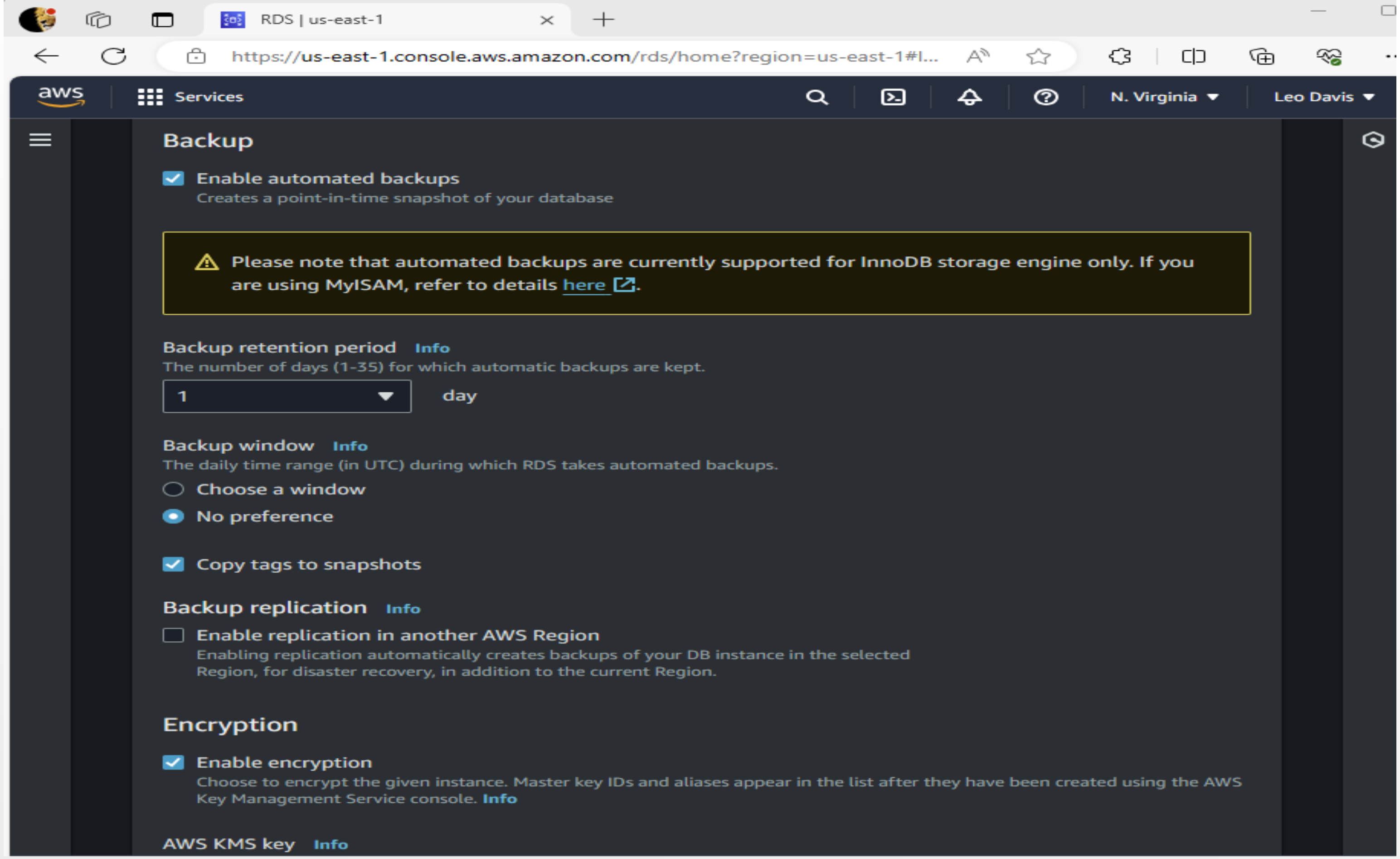
METHODOLOGY
IMPLEMENTATION – EBS CLI CONFIGURATION



```
Microsoft Windows [Version 10.0.22621.3007]
(c) Microsoft Corporation. All rights reserved.

C:\Users[redacted]>aws --version
aws-cli/2.15.10 Python/3.11.6 Windows/10 exe/AMD64 prompt/off

C:\Users[redacted]>eb --version
EB CLI 3.20.10 (Python 3.9.12 (main, Apr  4 2022, 05:22:27) [MSC v.1916 64 bit (AMD64)])

C:\Users\[redacted]>
```

METHODOLOGY

IMPLEMENTATION – AWS AND EBS CLI INTERFACE VERSION


RDS | us-east-1
https://us-east-1.console.aws.amazon.com/rds/home?region=us-east-1#l...
aws
Services
N. Virginia
Leo Davis

Backup

☑ Enable automated backups
Creates a point-in-time snapshot of your database

⚠ Please note that automated backups are currently supported for InnoDB storage engine only. If you are using MyISAM, refer to details here.

Backup retention period Info
The number of days (1-35) for which automatic backups are kept.
1 day

Backup window Info
The daily time range (in UTC) during which RDS takes automated backups.
○ Choose a window
● No preference

☑ Copy tags to snapshots

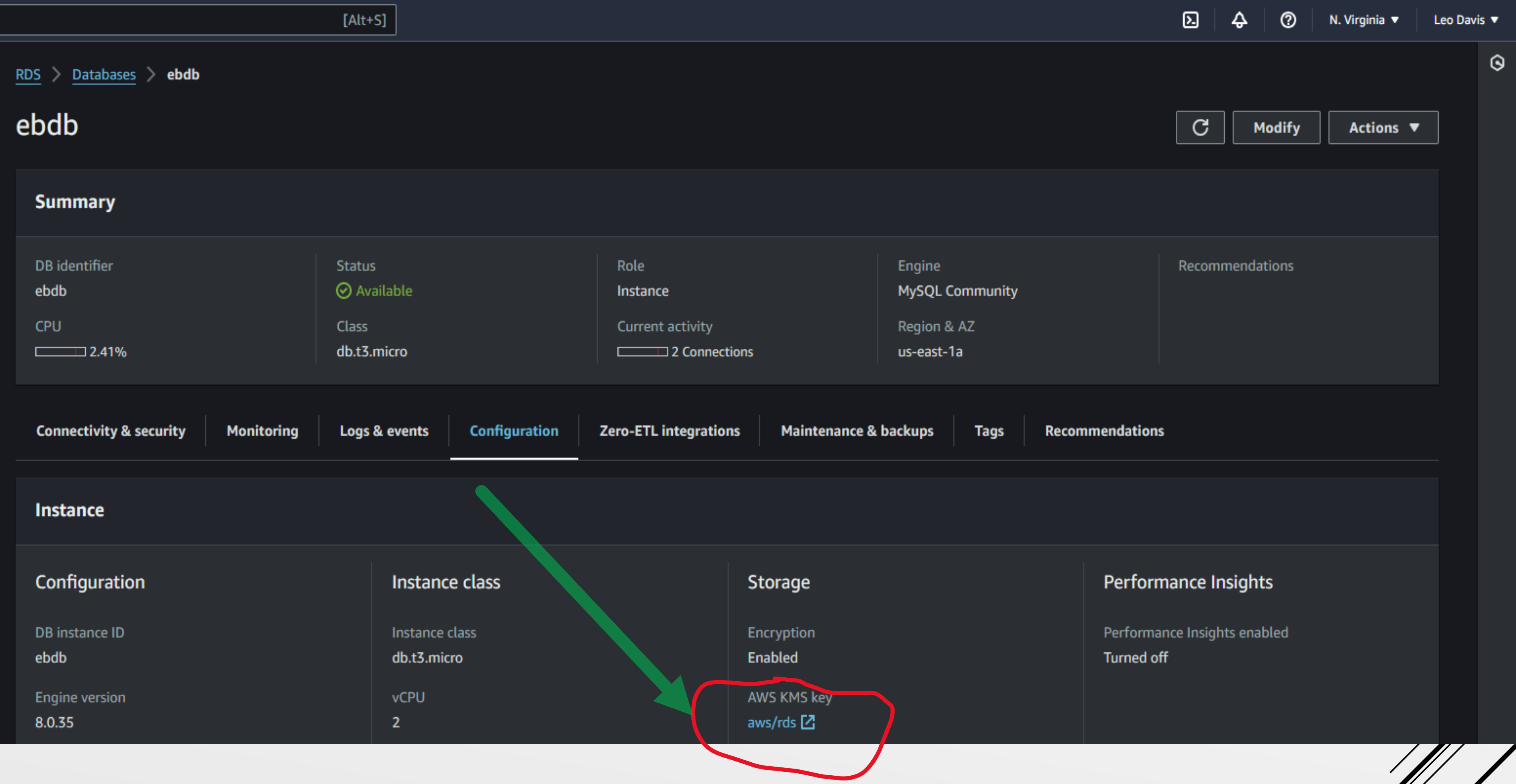
Backup replication Info
□ Enable replication in another AWS Region
Enabling replication automatically creates backups of your DB instance in the selected Region, for disaster recovery, in addition to the current Region.

Encryption

☑ Enable encryption
Choose to encrypt the given instance. Master key IDs and aliases appear in the list after they have been created using the AWS Key Management Service console. Info

AWS KMS key Info

METHODOLOGY
IMPLEMENTATION – RDS SETUP



[Alt+S]

N. Virginia ▼ Leo Davis ▼

RDS > Databases > ebdb

ebdb

Modify Actions ▼

Summary

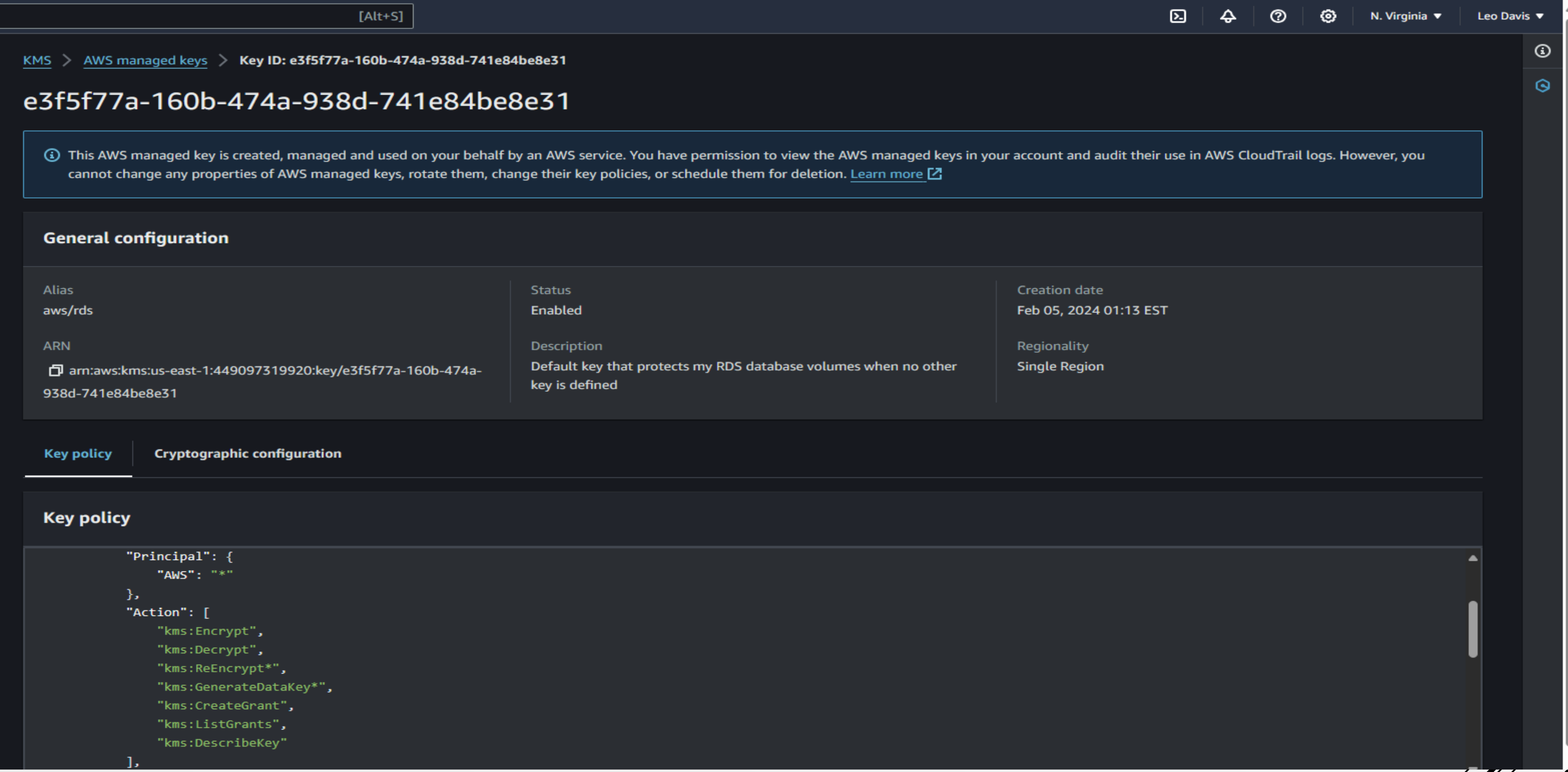
DB identifier	Status	Role	Engine	Recommendations
ebdb	Available	Instance	MySQL Community	
CPU	Class	Current activity	Region & AZ	
2.41%	db.t3.micro	2 Connections	us-east-1a	

Connectivity & security | Monitoring | Logs & events | Configuration | Zero-ETL integrations | Maintenance & backups | Tags | Recommendations

Instance

Configuration	Instance class	Storage	Performance Insights
DB instance ID ebdb	Instance class db.t3.micro	Encryption Enabled	Performance Insights enabled Turned off
Engine version 8.0.35	vCPU 2	AWS KMS key aws/rds	

METHODOLOGY
IMPLEMENTATION – RDS SETUP



KMS > AWS managed keys > Key ID: e3f5f77a-160b-474a-938d-741e84be8e31

e3f5f77a-160b-474a-938d-741e84be8e31

This AWS managed key is created, managed and used on your behalf by an AWS service. You have permission to view the AWS managed keys in your account and audit their use in AWS CloudTrail logs. However, you cannot change any properties of AWS managed keys, rotate them, change their key policies, or schedule them for deletion. Learn more

General configuration

Alias
aws/rds

ARN
arn:aws:kms:us-east-1:449097319920:key/e3f5f77a-160b-474a-938d-741e84be8e31

Status
Enabled

Description
Default key that protects my RDS database volumes when no other key is defined

Creation date
Feb 05, 2024 01:13 EST

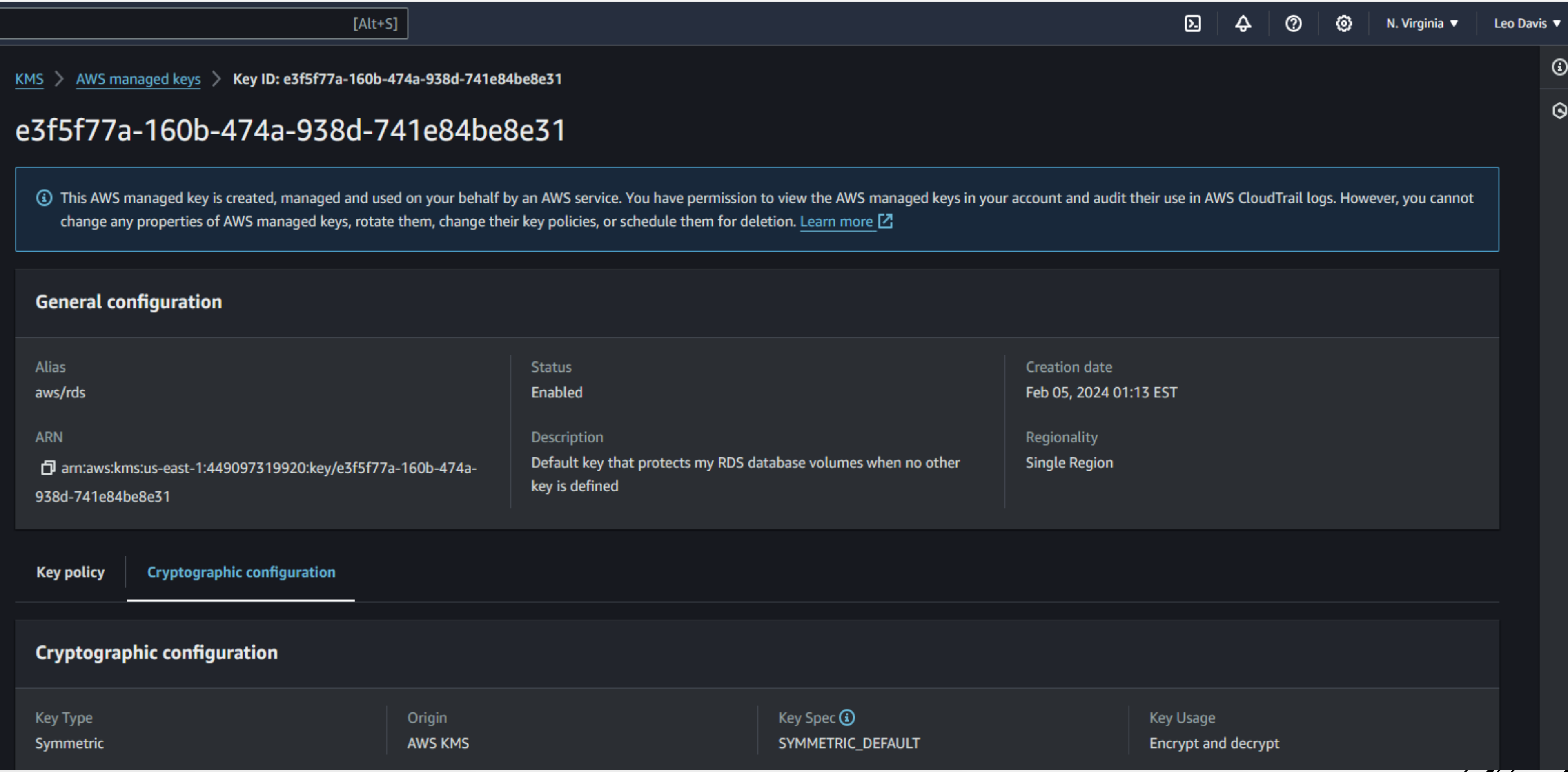
Regionality
Single Region

Key policy | Cryptographic configuration

Key policy

```
            "Principal": {
                "AWS": "*"
            },
            "Action": [
                "kms:Encrypt",
                "kms:Decrypt",
                "kms:ReEncrypt*",
                "kms:GenerateDataKey*",
                "kms:CreateGrant",
                "kms:ListGrants",
                "kms:DescribeKey"
            ],
```

METHODOLOGY
IMPLEMENTATION – RDS SETUP



KMS > AWS managed keys > Key ID: e3f5f77a-160b-474a-938d-741e84be8e31

e3f5f77a-160b-474a-938d-741e84be8e31

ⓘ This AWS managed key is created, managed and used on your behalf by an AWS service. You have permission to view the AWS managed keys in your account and audit their use in AWS CloudTrail logs. However, you cannot change any properties of AWS managed keys, rotate them, change their key policies, or schedule them for deletion. Learn more

General configuration

Alias
aws/rds

ARN
arn:aws:kms:us-east-1:449097319920:key/e3f5f77a-160b-474a-938d-741e84be8e31

Status
Enabled

Description
Default key that protects my RDS database volumes when no other key is defined

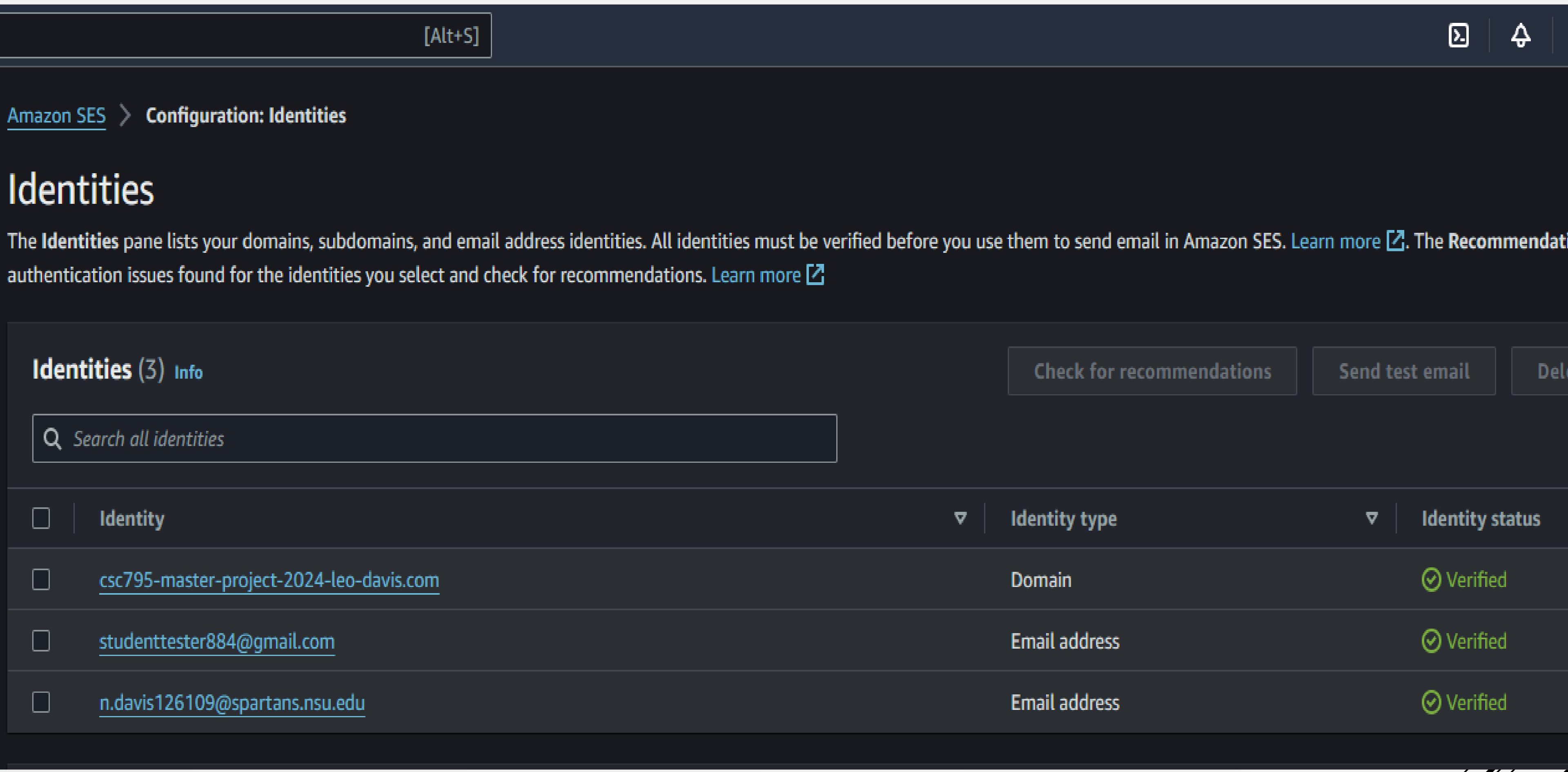
Creation date
Feb 05, 2024 01:13 EST

Regionality
Single Region

Cryptographic configuration

Key Type	Origin	Key Spec	Key Usage
Symmetric	AWS KMS	SYMMETRIC_DEFAULT	Encrypt and decrypt

METHODOLOGY
IMPLEMENTATION – RDS SETUP



Amazon SES > Configuration: Identities

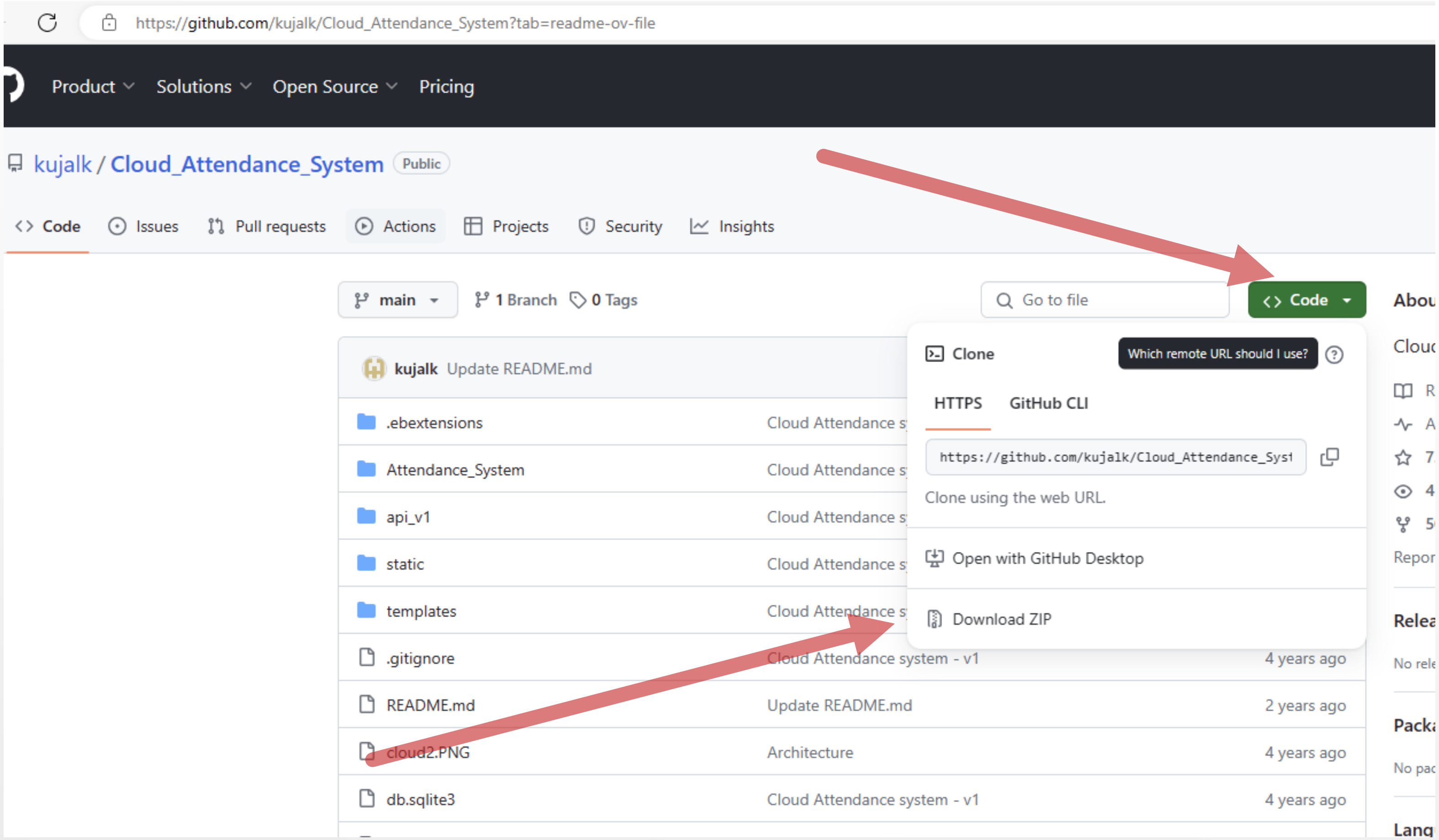
Identities

The **Identities** pane lists your domains, subdomains, and email address identities. All identities must be verified before you use them to send email in Amazon SES. Learn more. The **Recommendat**
authentication issues found for the identities you select and check for recommendations. Learn more

Identities (3) Info

□	Identity	Identity type	Identity status
□	csc795-master-project-2024-leo-davis.com	Domain	✓ Verified
□	studenttester884@gmail.com	Email address	✓ Verified
□	n.davis126109@spartans.nsu.edu	Email address	✓ Verified

METHODOLOGY
IMPLEMENTATION – SES SETUP



https://github.com/kujalk/Cloud_Attendance_System?tab=readme-ov-file

```
https://github.com/kujalk/Cloud_Attendance_Syst
```

Clone using the web URL.

kujalk Update README.md

.ebextensions	Cloud Attendance s	
Attendance_System	Cloud Attendance s	
api_v1	Cloud Attendance s	
static	Cloud Attendance s	
templates	Cloud Attendance s	
.gitignore	Cloud Attendance system - v1	4 years ago
README.md	Update README.md	2 years ago
cloud2.PNG	Architecture	4 years ago
db.sqlite3	Cloud Attendance system - v1	4 years ago

METHODOLOGY

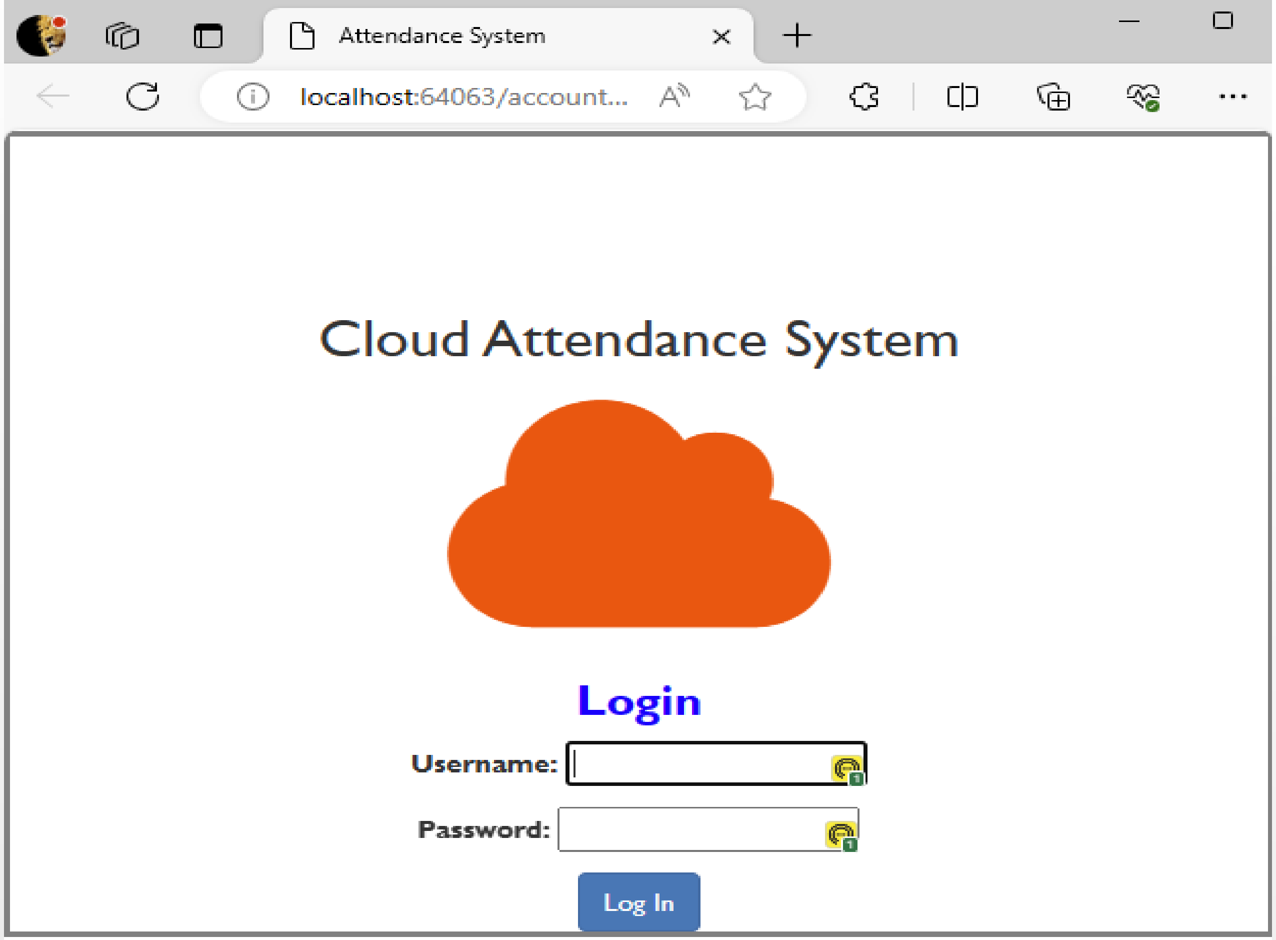
IMPLEMENTATION – DJANGO APPLICATION DEPLOYMENT

https://github.com/kujalk/Cloud_Attendance_System?tab=readme-ov-file

- Create Virtual Environment
- Activate virtual environment
- Install the packages using requirements.txt
- Launch web application locally to test
  - python .\manage.py runserver

METHODOLOGY

IMPLEMENTATION – DJANGO APPLICATION DEPLOYMENT



Cloud Attendance System

Login

Username:

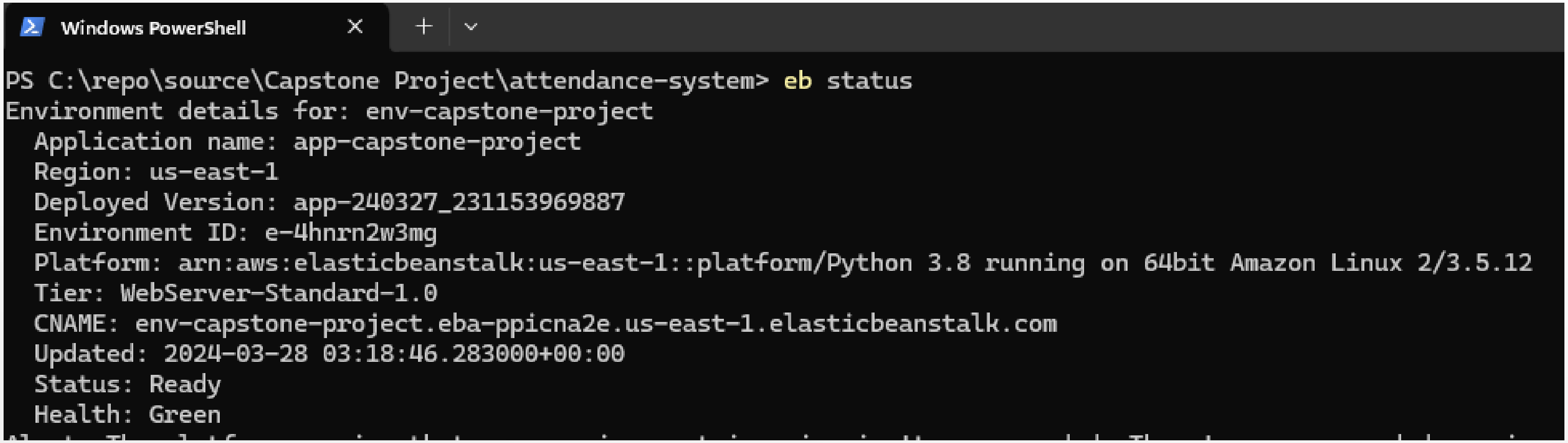
Password:

METHODOLOGY
IMPLEMENTATION – DJANGO APPLICATION DEPLOYMENT

- Create Application on Elastic Beanstalk
  - eb init – p python-3.8 app-name
- Create Environment on Elastic Beanstalk
  - eb create env-name
- Deploy Application
  - eb deploy
- Verify Status
  - eb status

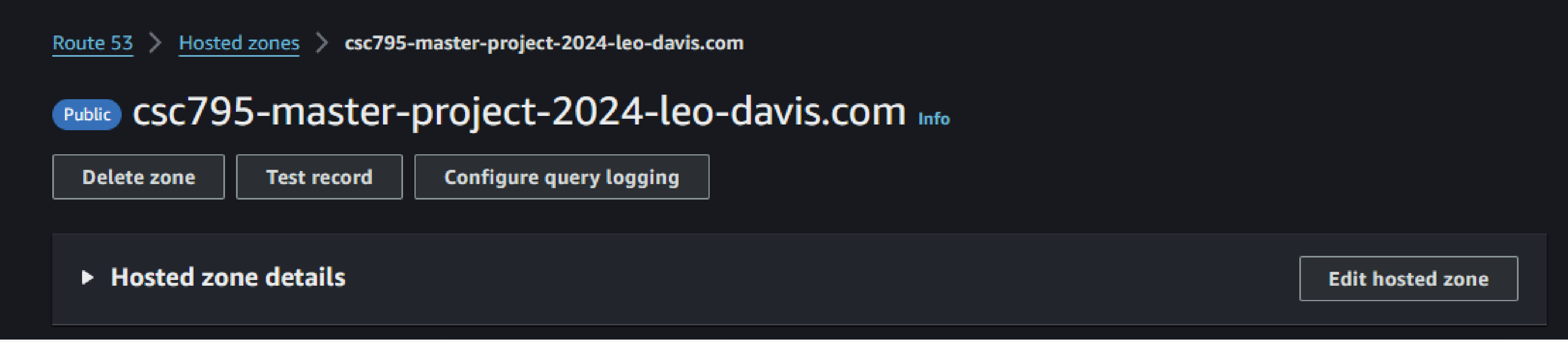
METHODOLOGY

IMPLEMENTATION – DJANGO APPLICATION DEPLOYMENT

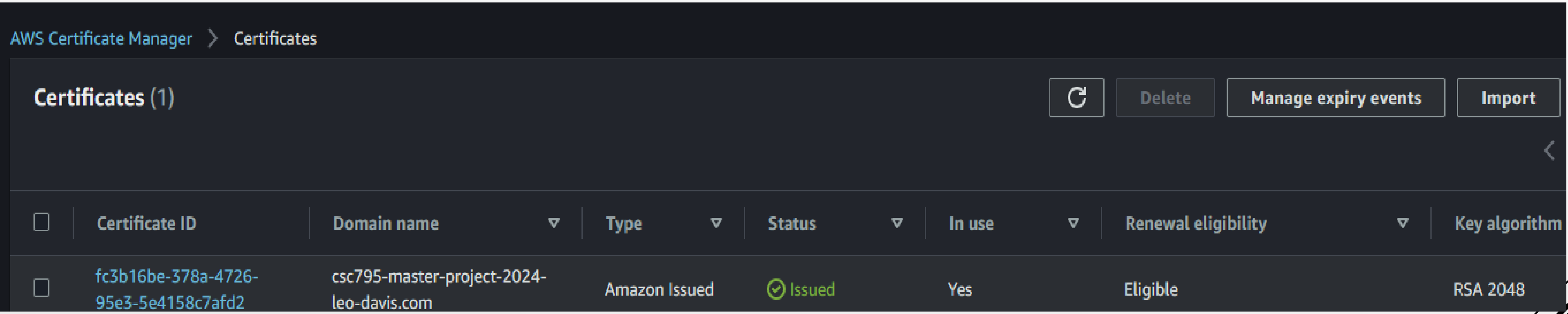


```
PS C:\repo\source\Capstone Project\attendance-system> eb status
Environment details for: env-capstone-project
  Application name: app-capstone-project
  Region: us-east-1
  Deployed Version: app-240327_231153969887
  Environment ID: e-4hnrn2w3mg
  Platform: arn:aws:elasticbeanstalk:us-east-1::platform/Python 3.8 running on 64bit Amazon Linux 2/3.5.12
  Tier: WebServer-Standard-1.0
  CNAME: env-capstone-project.eba-ppicna2e.us-east-1.elasticbeanstalk.com
  Updated: 2024-03-28 03:18:46.283000+00:00
  Status: Ready
  Health: Green
```

METHODOLOGY
IMPLEMENTATION – DJANGO APPLICATION DEPLOYMENT



csc795-master-project-2024-leo-davis.com

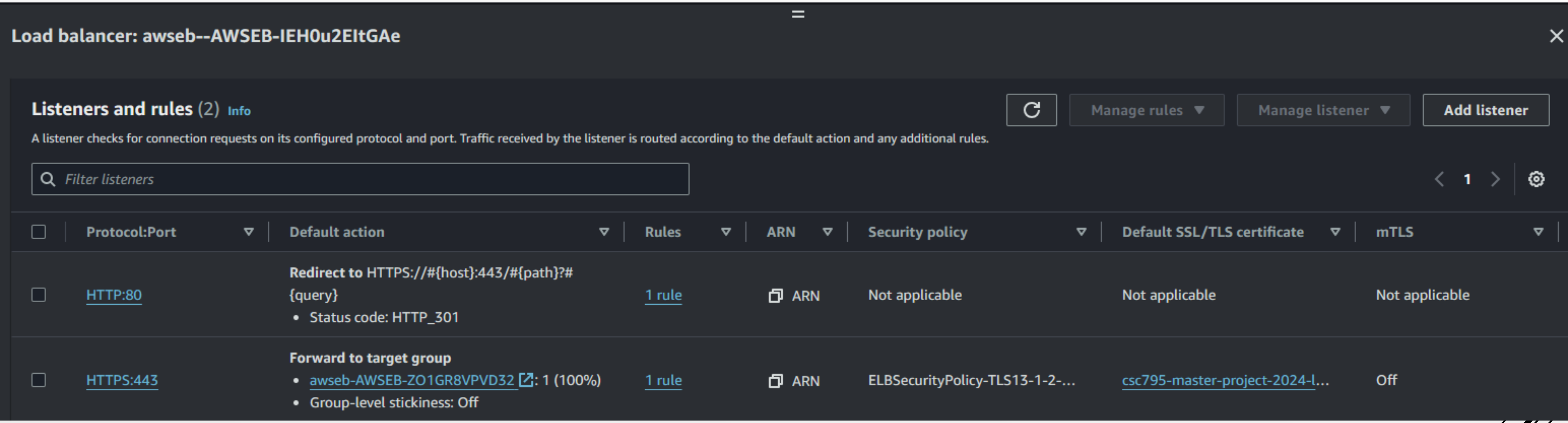


Certificates (1)

□	Certificate ID	Domain name	Type	Status	In use	Renewal eligibility	Key algorithm
□	fc3b16be-378a-4726-95e3-5e4158c7afd2	csc795-master-project-2024-leo-davis.com	Amazon Issued	✓ Issued	Yes	Eligible	RSA 2048

METHODOLOGY
IMPLEMENTATION – DOMAIN NAME REGISTRATION AND SSL CONFIGURATION

- Configure all traffic going to port 80 to be redirected to port 443.



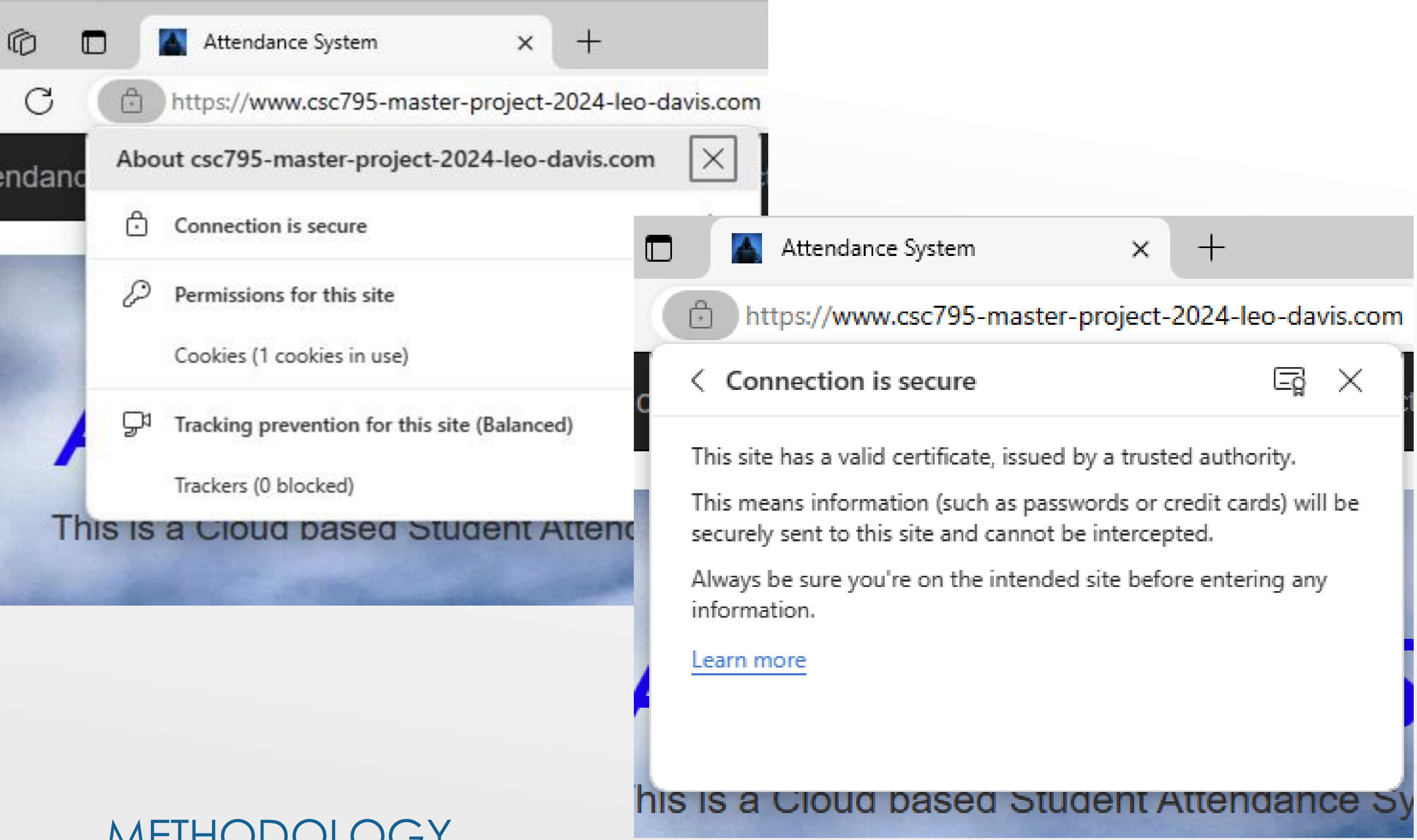
Listeners and rules (2) Info

A listener checks for connection requests on its configured protocol and port. Traffic received by the listener is routed according to the default action and any additional rules.

□	Protocol:Port	Default action	Rules	ARN	Security policy	Default SSL/TLS certificate	mTLS
□	HTTP:80	**Redirect to** HTTPS://#{host}:443/#{path}?#{query} • Status code: HTTP_301	1 rule	ARN	Not applicable	Not applicable	Not applicable
□	HTTPS:443	**Forward to target group** • awseb-AWSEB-ZO1GR8VPVD32: 1 (100%) • Group-level stickiness: Off	1 rule	ARN	ELBSecurityPolicy-TLS13-1-2-...	csc795-master-project-2024-l...	Off

METHODOLOGY

IMPLEMENTATION – SSL REDIRECT



Attendance System
https://www.csc795-master-project-2024-leo-davis.com

About csc795-master-project-2024-leo-davis.com

Connection is secure

Permissions for this site

Cookies (1 cookies in use)

Tracking prevention for this site (Balanced)

Trackers (0 blocked)

This is a Cloud based Student Attend

Attendance System
https://www.csc795-master-project-2024-leo-davis.com

Connection is secure

This site has a valid certificate, issued by a trusted authority.

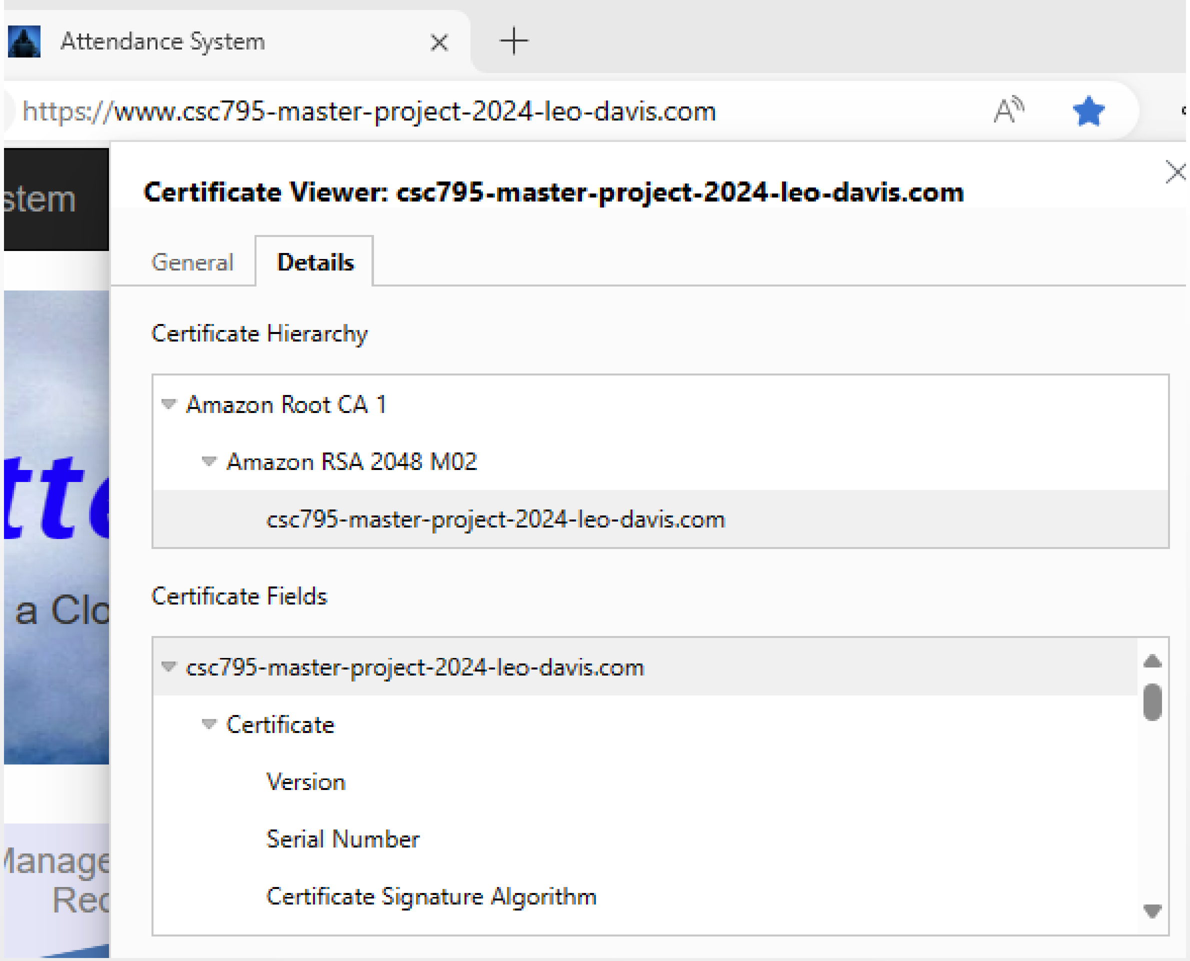
This means information (such as passwords or credit cards) will be securely sent to this site and cannot be intercepted.

Always be sure you're on the intended site before entering any information.

Learn more

his is a Cloud based Student Attendance Sy

METHODOLOGY
IMPLEMENTATION – SSL VERIFICATION



Attendance System

https://www.csc795-master-project-2024-leo-davis.com

Certificate Viewer: csc795-master-project-2024-leo-davis.com

General | Details

Certificate Hierarchy

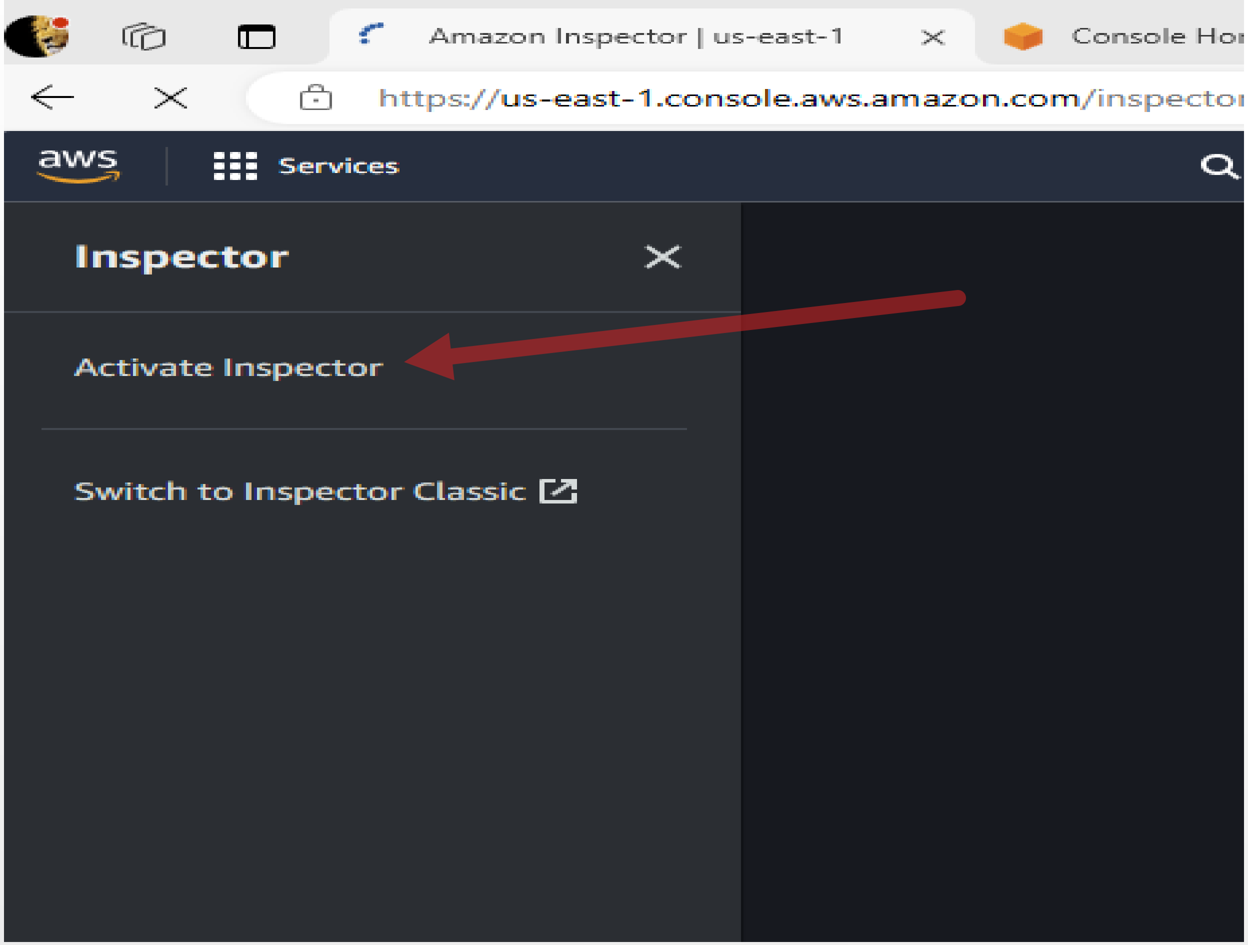
- Amazon Root CA 1
  - Amazon RSA 2048 M02
    - csc795-master-project-2024-leo-davis.com

Certificate Fields

- csc795-master-project-2024-leo-davis.com
  - Certificate
    - Version
    - Serial Number
    - Certificate Signature Algorithm

METHODOLOGY

IMPLEMENTATION – REVIEW CERTIFICATE DETAILS



Amazon Inspector | us-east-1

Console Ho

https://us-east-1.console.aws.amazon.com/inspecto

Inspector

Activate Inspector

Switch to Inspector Classic

METHODOLOGY

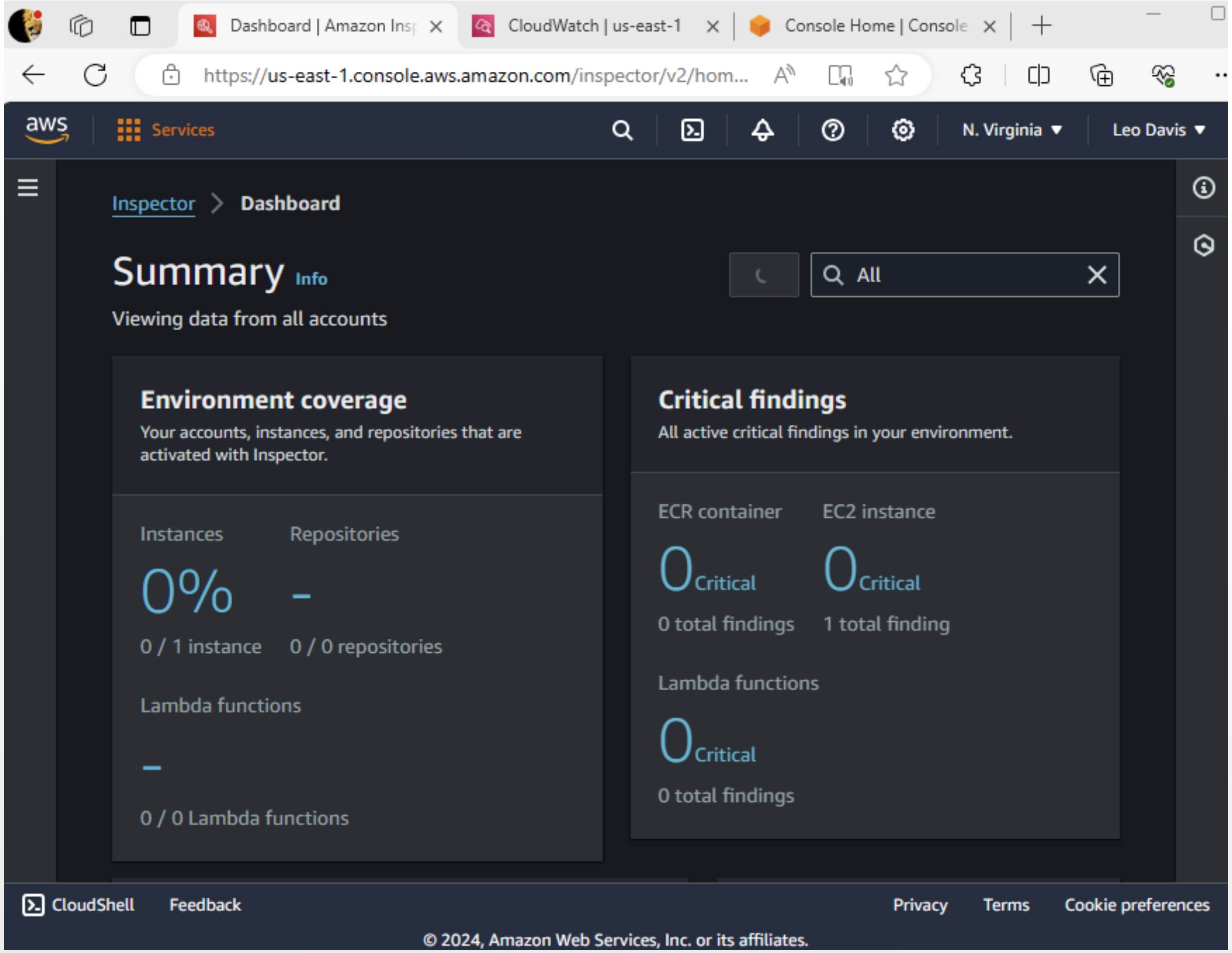
IMPLEMENTATION – ACTIVATE AMAZON INSPECTOR

- Utilizes automated security scanning tools like AWS Inspector
- Employs AWS logging and monitoring tools for identifying security threats or misconfigurations.

METHODOLOGY
DATA COLLECTION

- Automated Vulnerability Management
- Risk scoring and correlation to CVE information
- Integrates with other AWS Services such as Security Hub and AWS Systems Manager.

METHODOLOGY
DATA COLLECTION – AMAZON INSPECTOR



Inspector > Dashboard

Summary Info

Viewing data from all accounts

All

Environment coverage

Your accounts, instances, and repositories that are activated with Inspector.

Instances	Repositories
0%	-
0 / 1 instance	0 / 0 repositories

Lambda functions

-

0 / 0 Lambda functions

Critical findings

All active critical findings in your environment.

ECR container	EC2 instance
0 Critical	0 Critical
0 total findings	1 total finding

Lambda functions

0 Critical

0 total findings

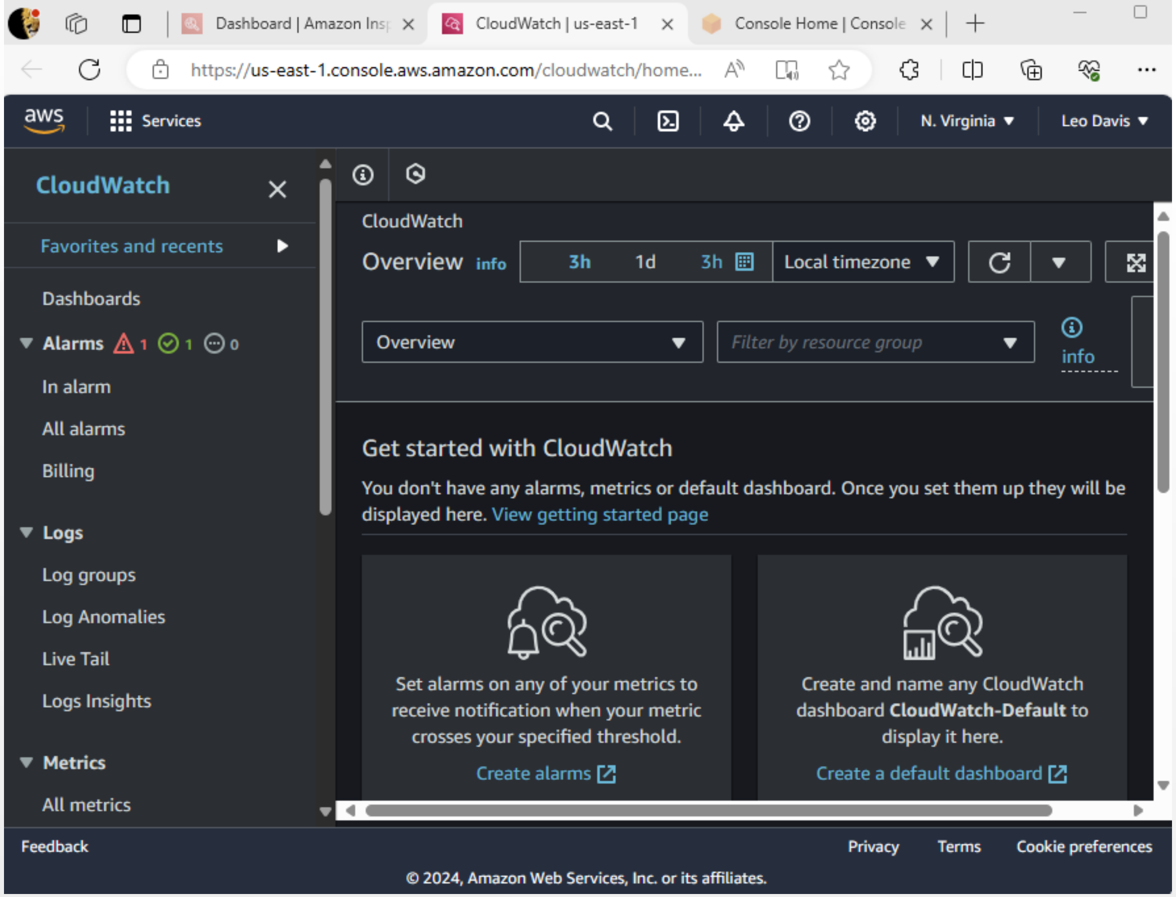
© 2024, Amazon Web Services, Inc. or its affiliates.

METHODOLOGY
DATA COLLECTION – AMAZON INSPECTOR

- Enables end-to-end observability by visualizing and analyzing data.
- Promotes operational efficiency through automation.
- Provides an integrated view of AWS and other resources quickly.
- Enhances end-user experiences with proactive monitoring and actionable insights.

METHODOLOGY

DATA COLLECTION – AMAZON CLOUDWATCH



Get started with CloudWatch

You don't have any alarms, metrics or default dashboard. Once you set them up they will be displayed here. View getting started page

Set alarms on any of your metrics to receive notification when your metric crosses your specified threshold.

Create alarms

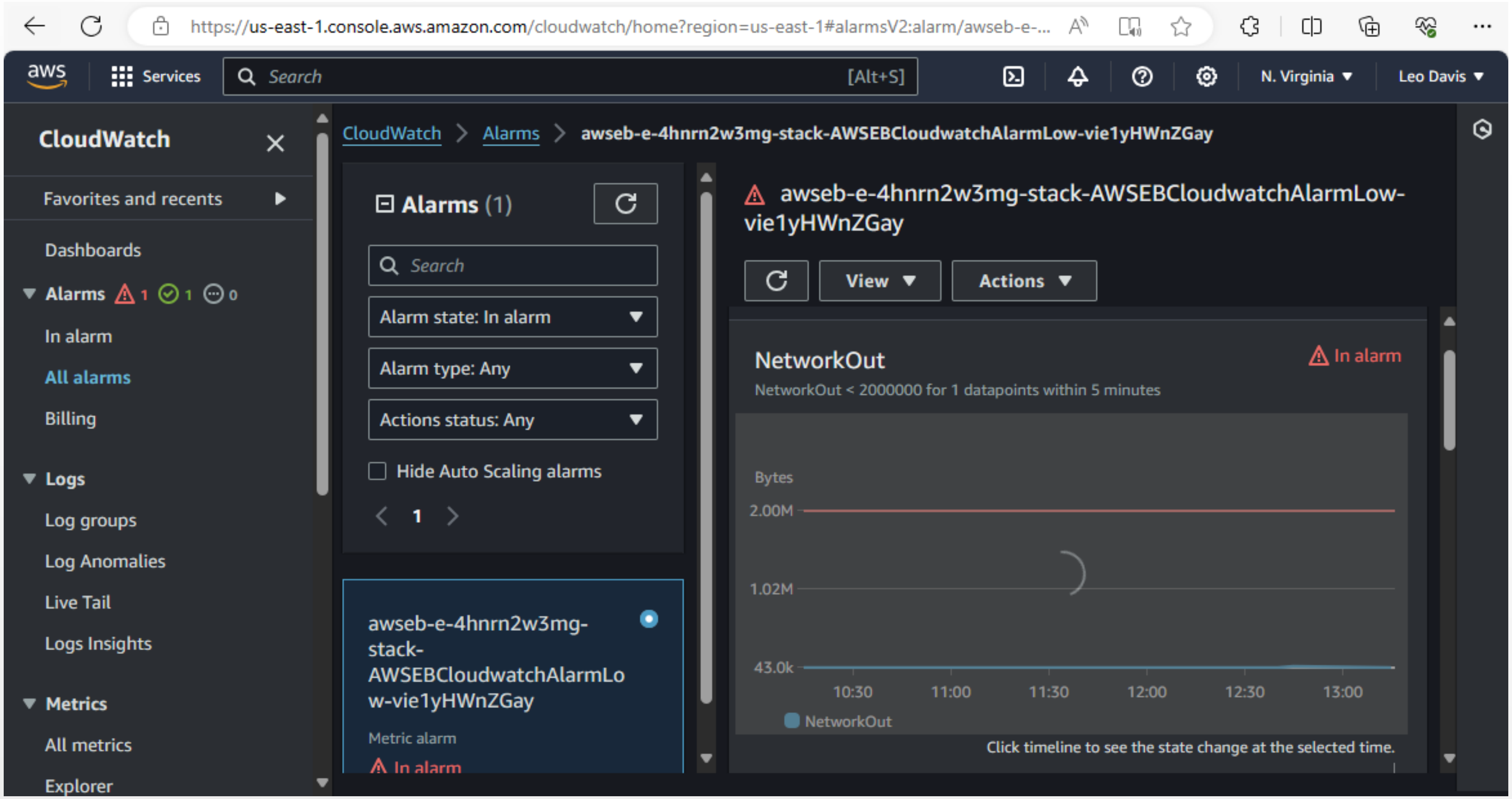
Create and name any CloudWatch dashboard **CloudWatch-Default** to display it here.

Create a default dashboard

© 2024, Amazon Web Services, Inc. or its affiliates.

METHODOLOGY

DATA COLLECTION – AMAZON CLOUDWATCH



https://us-east-1.console.aws.amazon.com/cloudwatch/home?region=us-east-1#alarmsV2:alarm/awseb-e-...

CloudWatch > Alarms > awseb-e-4hnrn2w3mg-stack-AWSEBCloudwatchAlarmLow-vie1yHWnZGay

Alarms (1)

Alarm state: In alarm

Alarm type: Any

Actions status: Any

□ Hide Auto Scaling alarms

awseb-e-4hnrn2w3mg-stack-AWSEBCloudwatchAlarmLow-vie1yHWnZGay

Metric alarm

⚠ In alarm

⚠ awseb-e-4hnrn2w3mg-stack-AWSEBCloudwatchAlarmLow-vie1yHWnZGay

NetworkOut

⚠ In alarm

NetworkOut < 2000000 for 1 datapoints within 5 minutes

Click timeline to see the state change at the selected time.

METHODOLOGY
DATA COLLECTION – AMAZON CLOUDWATCH ALARM

- Analyzes the database migration process and domain name configuration for security compliance.
- Utilizes Elastic Beanstalk's monitoring tools for performance analysis and sets up auto-scaling for handling varying loads efficiently.
- Evaluates the SSL certificate setup and HTTPS redirection for securing data in transit.
- Assesses Amazon Inspector setup for security and compliance, recommending regular reviews and mitigation implementations.

METHODOLOGY ANALYSIS

- Section 1. Introduction
- Section 2. Literature Review
- Section 3. Methodology
- Section 4. Results and Findings
- Section 5. Conclusion

RESULTS AND FINDINGS OVERVIEW

- CASE STUDIES AND ANALYSIS
- COMPARIATIVE ANALYSIS OF SECURITY PRACTICES
- MITIGATION STRATEGIES AND BEST PRACTICES

- Case Study 1: Deploying a Secure Django App on AWS
- Case Study 2: Overcoming Elastic Beanstalk Security Challenges

RESULTS AND FINDINGS

CASE STUDIES AND ANALYSIS

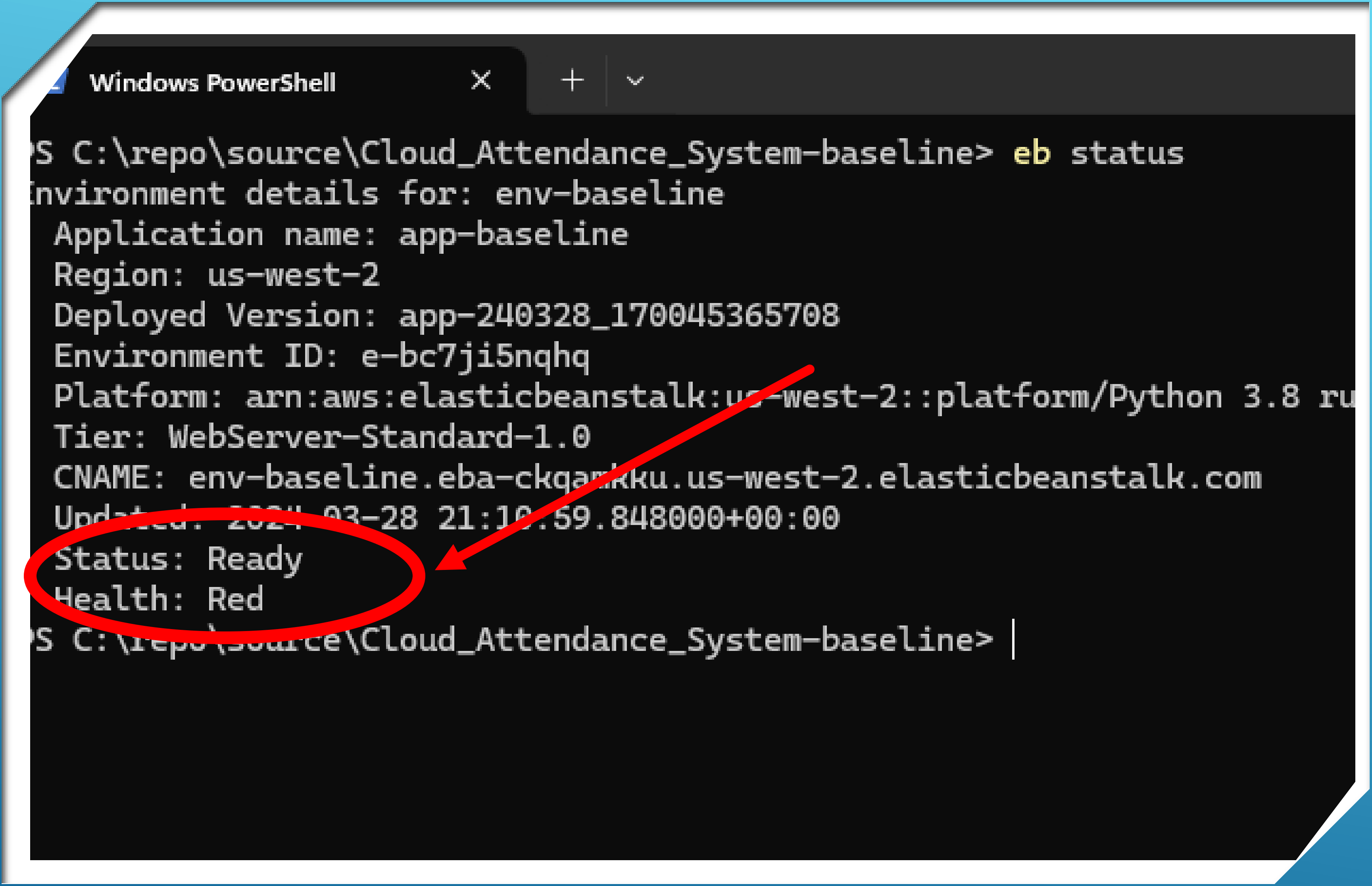
- Data Collection Methods
  - Vulnerability Scanning
  - Logs and Alarms
- Analysis Techniques
  - Scan, Patch, Rescan
  - Continuous Monitoring

RESULTS AND FINDINGS

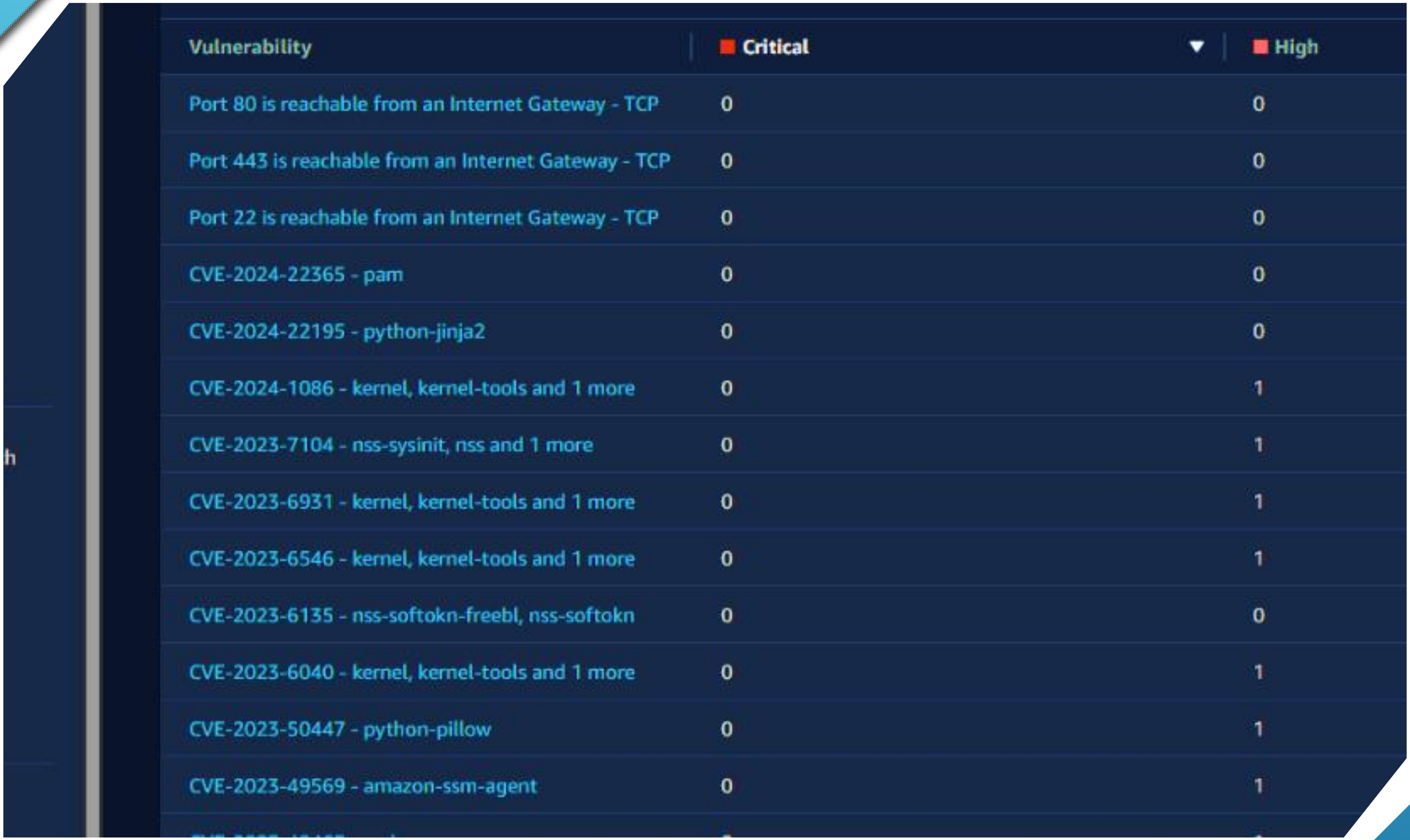
COMPARATIVE ANALYSIS OF SECURITY PRACTICES

RESULTS AND FINDINGS

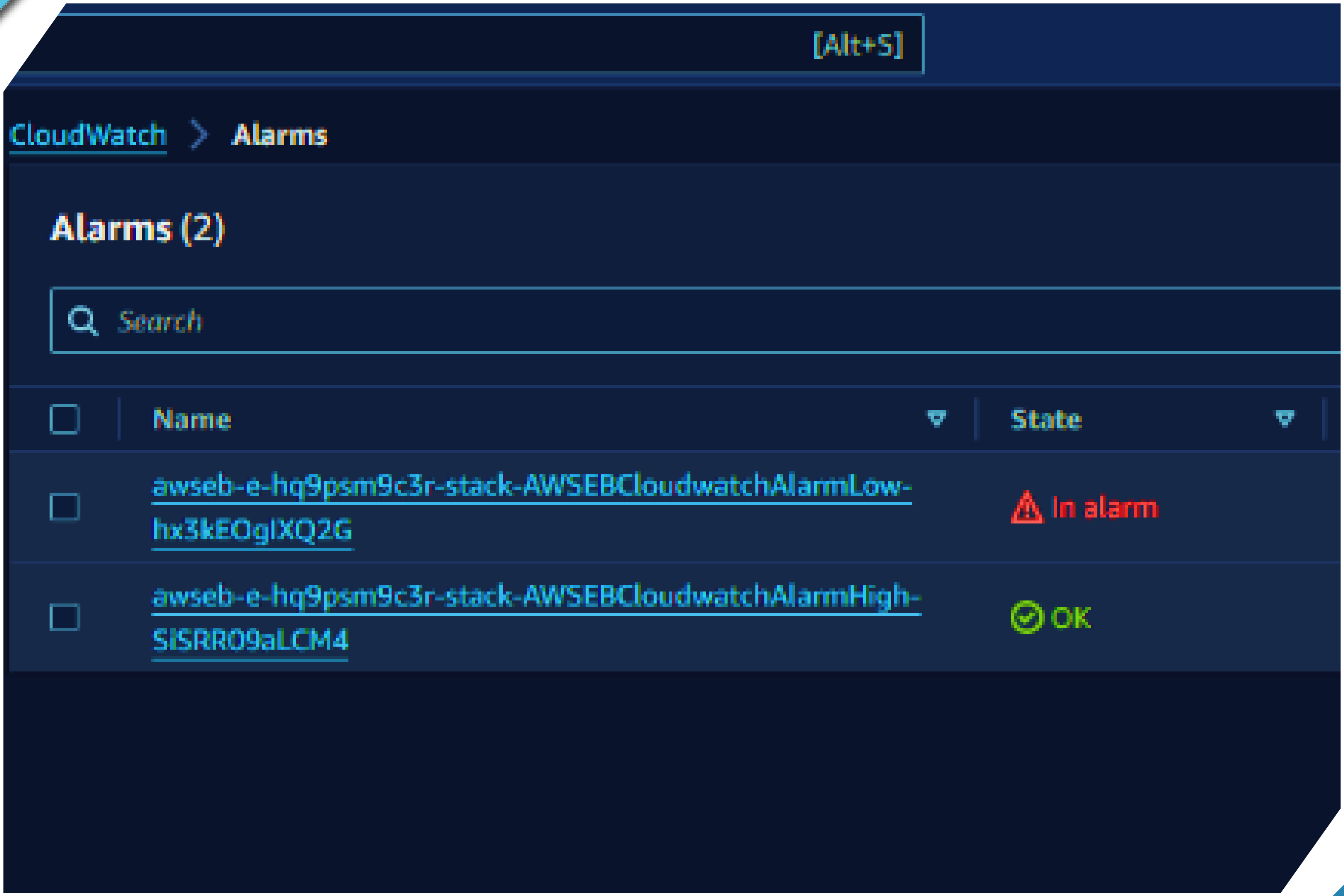
BEFORE



```
PS C:\repo\source\Cloud_Attendance_System-baseline> eb status
Environment details for: env-baseline
  Application name: app-baseline
  Region: us-west-2
  Deployed Version: app-240328_170045365708
  Environment ID: e-bc7ji5nqhq
  Platform: arn:aws:elasticbeanstalk:us-west-2::platform/Python 3.8 ru
  Tier: WebServer-Standard-1.0
  CNAME: env-baseline.eba-ckqamkku.us-west-2.elasticbeanstalk.com
  Updated: 2024-03-28 21:10:59.848000+00:00
  Status: Ready
  Health: Red
PS C:\repo\source\Cloud_Attendance_System-baseline>
```



Vulnerability	🟥 Critical ▼	🟥 High
Port 80 is reachable from an Internet Gateway - TCP	0	0
Port 443 is reachable from an Internet Gateway - TCP	0	0
Port 22 is reachable from an Internet Gateway - TCP	0	0
CVE-2024-22365 - pam	0	0
CVE-2024-22195 - python-jinja2	0	0
CVE-2024-1086 - kernel, kernel-tools and 1 more	0	1
CVE-2023-7104 - nss-sysinit, nss and 1 more	0	1
CVE-2023-6931 - kernel, kernel-tools and 1 more	0	1
CVE-2023-6546 - kernel, kernel-tools and 1 more	0	1
CVE-2023-6135 - nss-softokn-freebl, nss-softokn	0	0
CVE-2023-6040 - kernel, kernel-tools and 1 more	0	1
CVE-2023-50447 - python-pillow	0	1
CVE-2023-49569 - amazon-ssm-agent	0	1



CloudWatch > Alarms

Alarms (2)

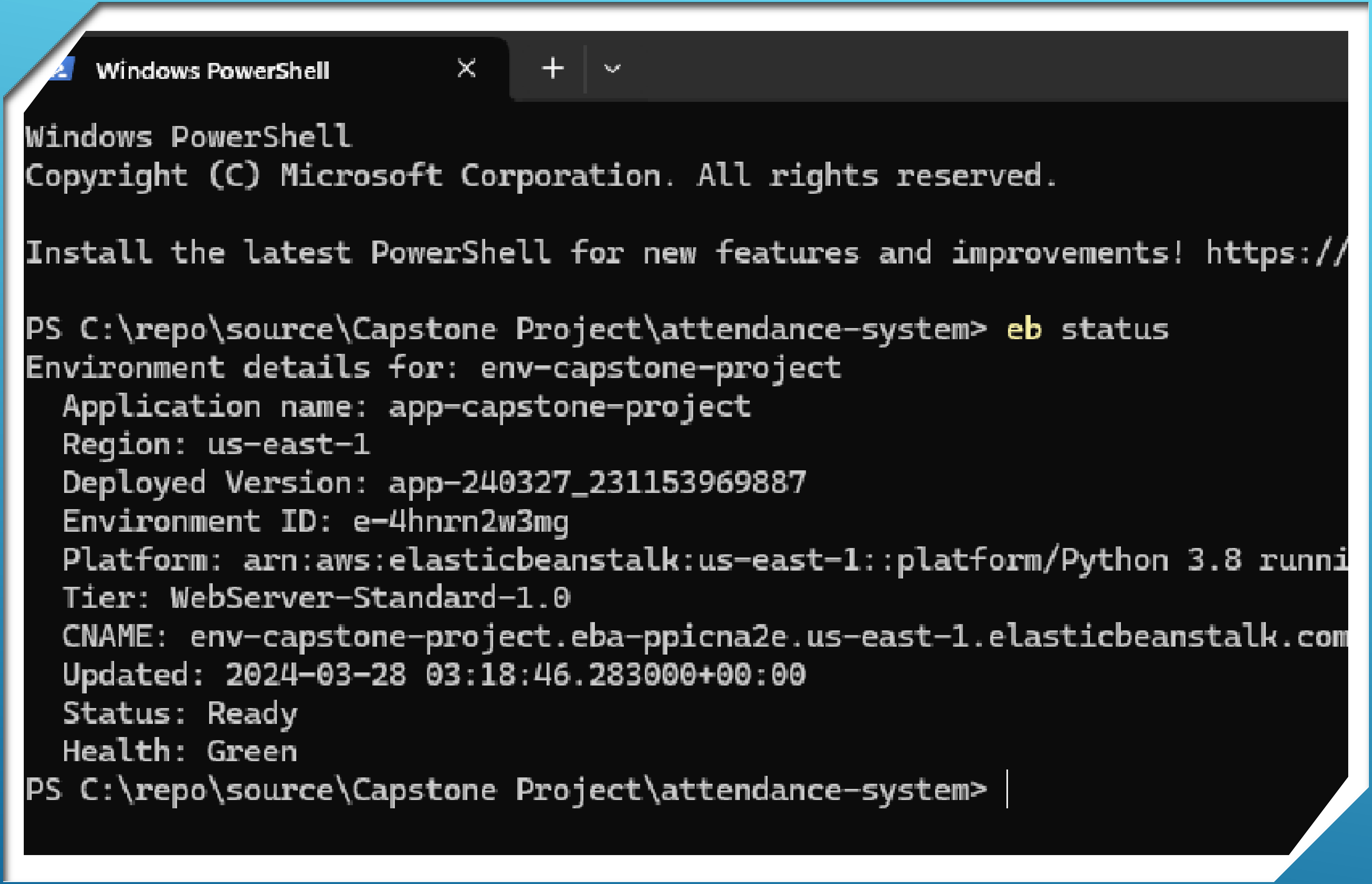
□	Name	State
□	awseb-e-hq9psm9c3r-stack-AWSEBCloudwatchAlarmLow-hx3kEOglXQ2G	⚠ In alarm
□	awseb-e-hq9psm9c3r-stack-AWSEBCloudwatchAlarmHigh-SISRRO9aLCM4	✓ OK

Vulnerability	Severity	Description
CVE-2024-1086 - kernel, kernel tools, and one more	High	A use-after-free vulnerability in the Linux kernel's netfilter: nf_tables component can be exploited to achieve local privilege escalation. The nft_verdict_init() function allows positive values as drop errors within the hook verdict. Hence, the nf_hook_slow() function can cause a double-free vulnerability when NF_DROP is issued with a drop error that resembles NF_ACCEPT. We recommend upgrading past commit f342de4e2f33e0e39165d8639387aa6c19dff660.
CVE-2023-7104 - nss-sysinit, NSS and 1 more	High	A vulnerability was found in SQLite SQLite3 up to 3.43.0 and classified as critical. This issue affects the function sessionReadRecord of the file ext/session/sqlite3session.c of the component makes all test Handler. The manipulation leads to a heap-based buffer overflow. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-248999. NOTE: https://sqlite.org/forum/forumpost/5bcbf4571c NOTE: Fixed by: https://sqlite.org/src/info/0e4e7a05c4204b47
CVE-2023-6931 - kernel, kernel-tools and 1 more	High	A heap out-of-bounds write vulnerability in the Linux kernel's Performance Events system component can be exploited to achieve local privilege escalation. A perf_event's read_size can overflow, leading to an heap out-of-bounds increment or write in perf_read_group(). We recommend upgrading past commit 382c27f4ed28f803b1f1473ac2d8db0afc795a1b.
CVE-2023-42465 - sudo	Low	Sudo before 1.9.15 might allow row hammer attacks (for authentication bypass or privilege escalation) because application logic sometimes is based on not equaling an error value (instead of equaling a success value), and because the values do not resist a single bit flips.

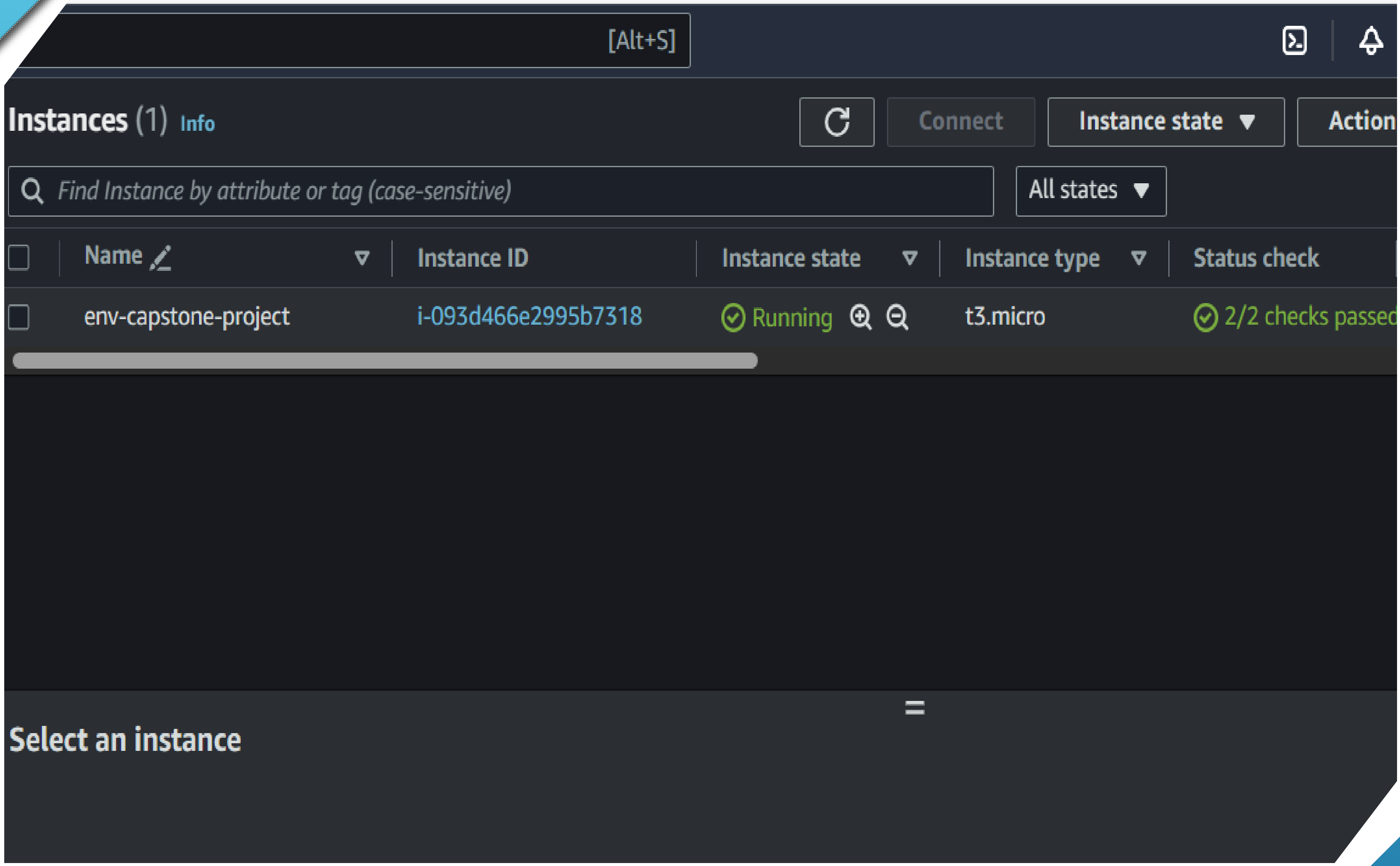
Vulnerability	REMEDIATION STEPS
CVE-2024-1086 - kernel, kernel tools, and one more	Upgrade your installed software packages to the proposed fixed in version and release. ▪ yum update kernel ▪ yum update kernel-tools ▪ yum update kernel-headers
CVE-2023-7104 - nss-sysinit, NSS and 1 more	Upgrade your installed software packages to the proposed fixed in version and release. ▪ yum update nss-sysinit ▪ yum update nss ▪ yum update nss-tools
CVE-2023-6931 - kernel, kernel-tools and 1 more	Upgrade your installed software packages to the proposed fixed in version and release. ▪ yum update kernel ▪ yum update kernel-tools ▪ yum update kernel-headers
CVE-2023-42465 - sudo	Upgrade your installed software packages to the proposed fixed in version and release. ▪ yum update sudo

RESULTS AND FINDINGS

AFTER



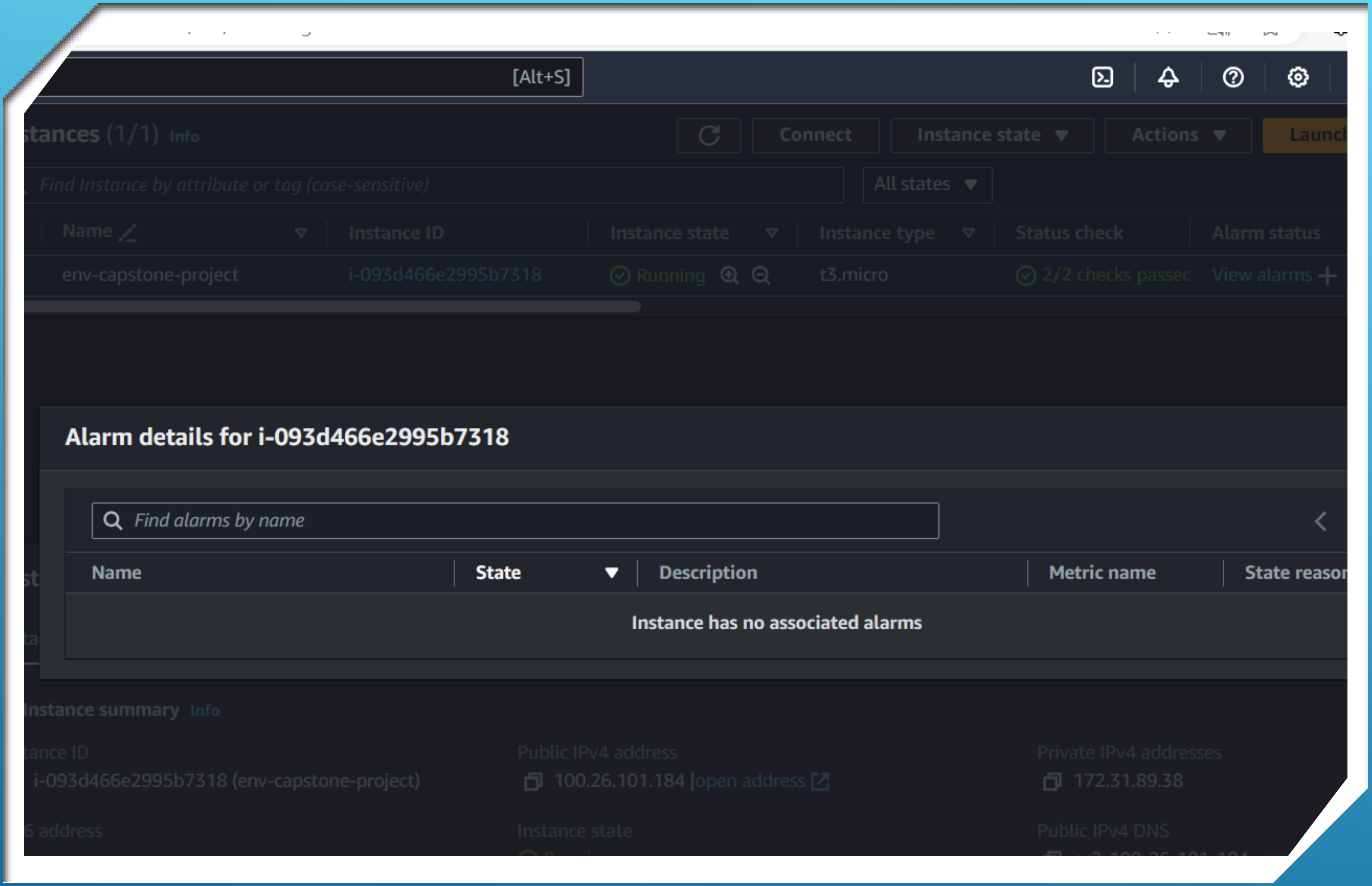
```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://

PS C:\repo\source\Capstone Project\attendance-system> eb status
Environment details for: env-capstone-project
  Application name: app-capstone-project
  Region: us-east-1
  Deployed Version: app-240327_231153969887
  Environment ID: e-4hnrn2w3mg
  Platform: arn:aws:elasticbeanstalk:us-east-1::platform/Python 3.8 runni
  Tier: WebServer-Standard-1.0
  CNAME: env-capstone-project.eba-ppicna2e.us-east-1.elasticbeanstalk.com
  Updated: 2024-03-28 03:18:46.283000+00:00
  Status: Ready
  Health: Green
PS C:\repo\source\Capstone Project\attendance-system>
```



Instances (1)

□	Name	Instance ID	Instance state	Instance type	Status check
□	env-capstone-project	i-093d466e2995b7318	✓ Running	t3.micro	✓ 2/2 checks passed

Select an instance



stances (1/1) Info

Name	Instance ID	Instance state	Instance type	Status check	Alarm status
env-capstone-project	i-093d466e2995b7318	Running	t3.micro	2/2 checks passed	View alarms +

Alarm details for i-093d466e2995b7318

Name	State	Description	Metric name	State reasor

Instance has no associated alarms

Instance summary Info

tance ID
i-093d466e2995b7318 (env-capstone-project)

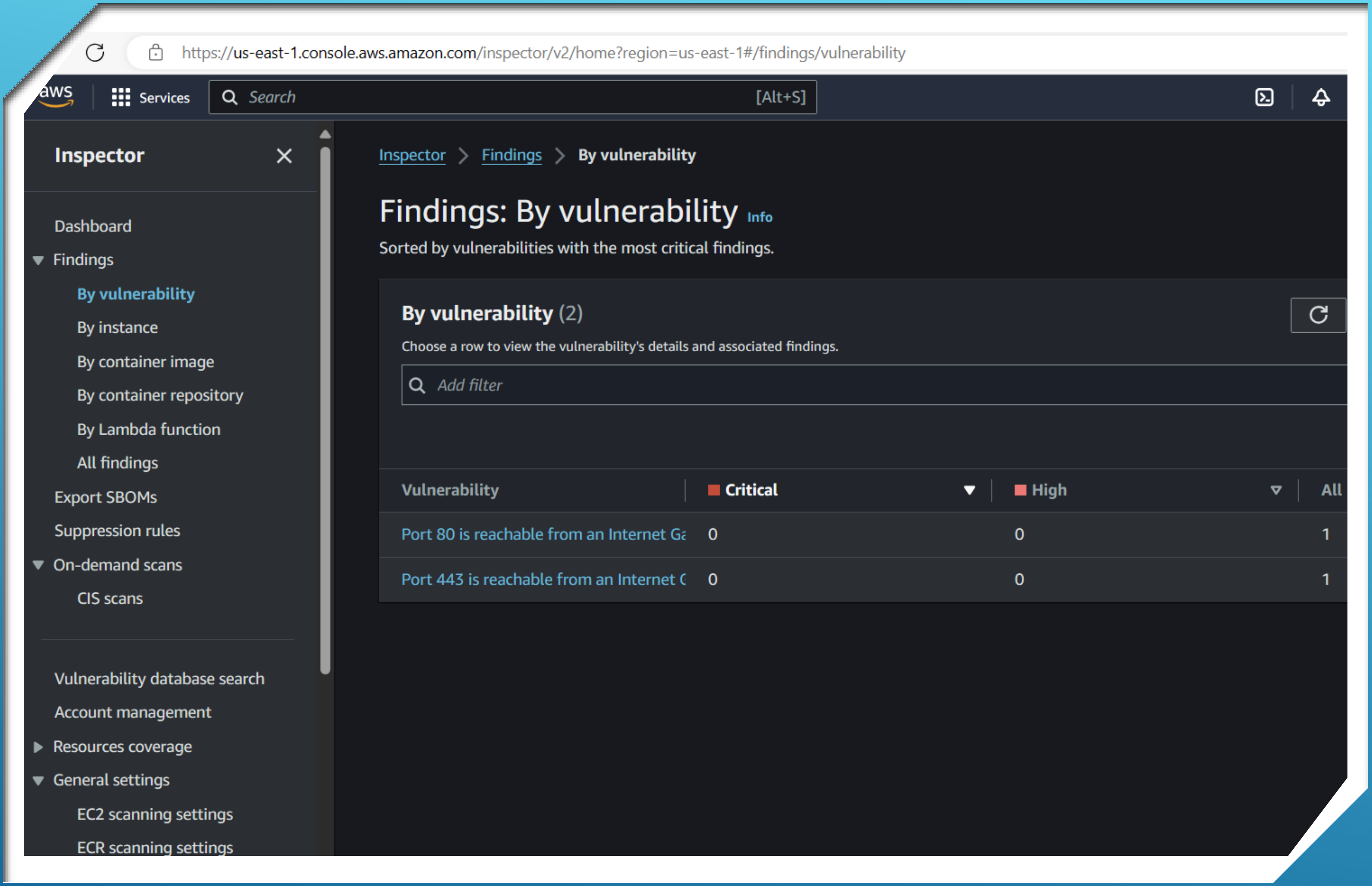
Public IPv4 address
100.26.101.184 | open address

Private IPv4 addresses
172.31.89.38

6 address

Instance state

Public IPv4 DNS



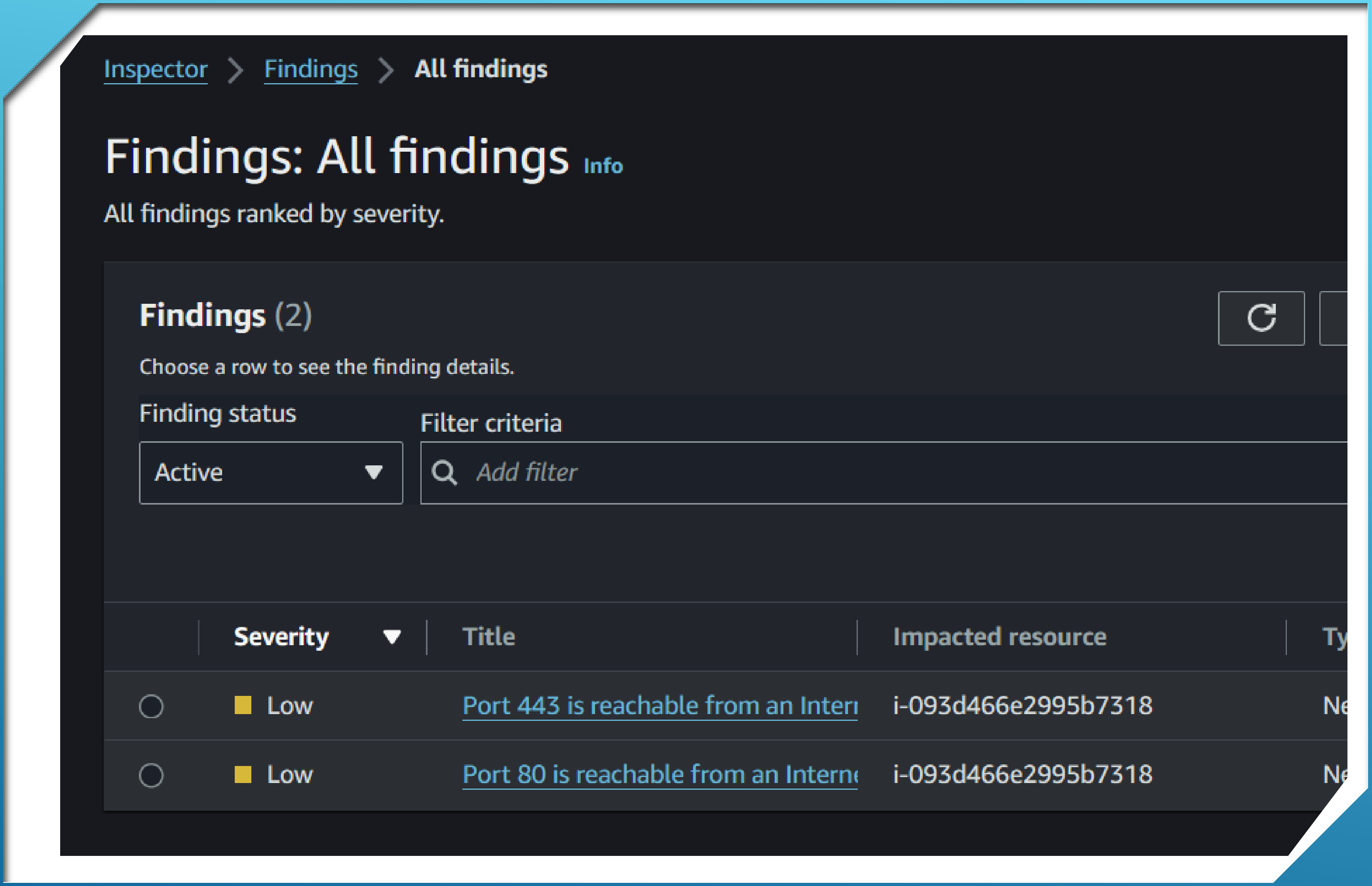
Findings: By vulnerability

Sorted by vulnerabilities with the most critical findings.

By vulnerability (2)

Choose a row to view the vulnerability's details and associated findings.

Vulnerability	🟥 Critical	🟥 High	All
Port 80 is reachable from an Internet Ga	0	0	1
Port 443 is reachable from an Internet (	0	0	1



Inspector > Findings > All findings

Findings: All findings Info

All findings ranked by severity.

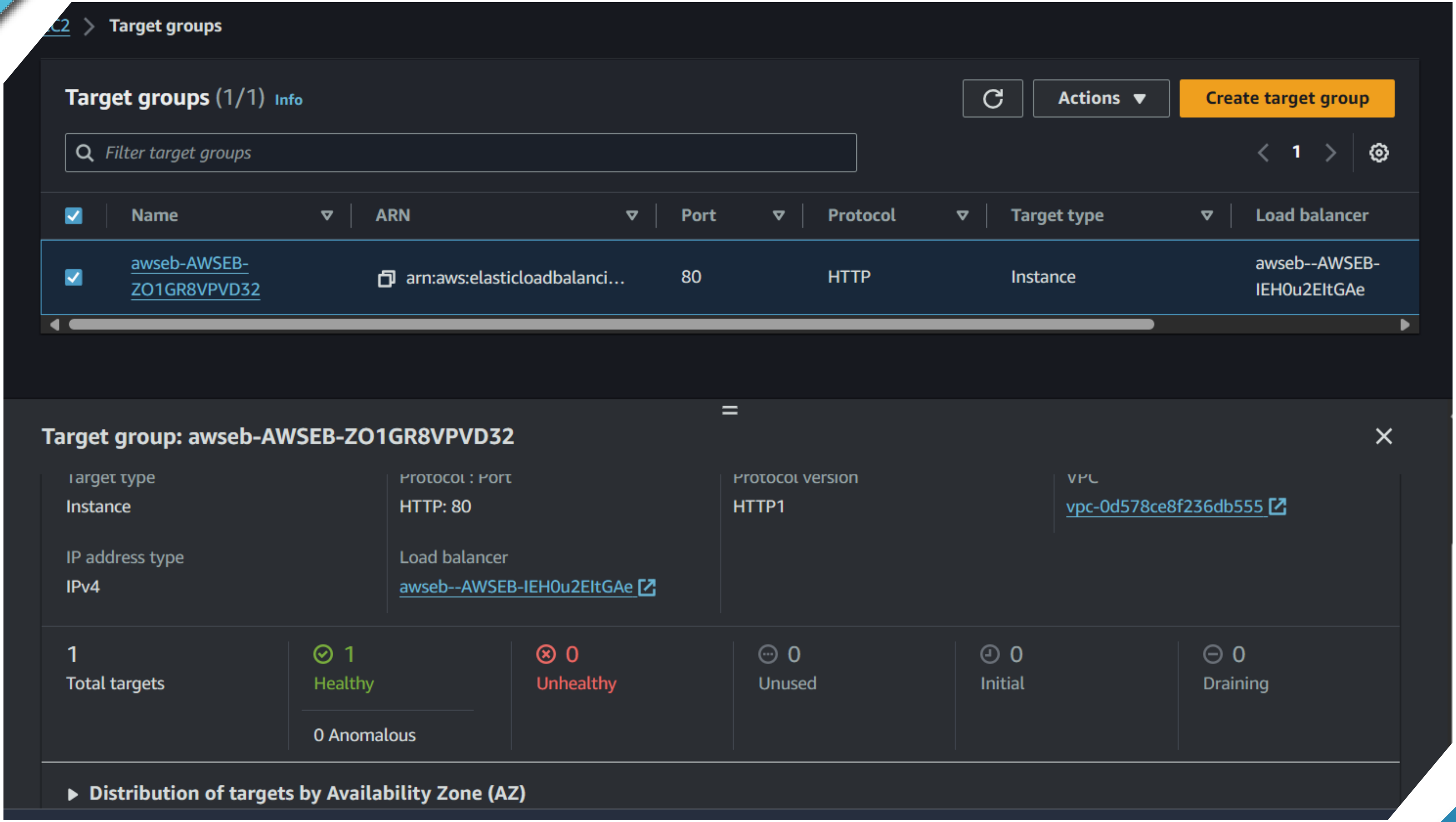
Findings (2)

Choose a row to see the finding details.

Finding status: Active ▼

Filter criteria: Add filter

	Severity ▼	Title	Impacted resource	Ty
○	🟨 Low	Port 443 is reachable from an Interi	i-093d466e2995b7318	Ne
○	🟨 Low	Port 80 is reachable from an Interne	i-093d466e2995b7318	Ne



C2 > Target groups

Target groups (1/1) Info

☑	Name	ARN	Port	Protocol	Target type	Load balancer
☑	awseb-AWSEB-ZO1GR8VPVD32	arn:aws:elasticloadbalanci...	80	HTTP	Instance	awseb--AWSEB-IEH0u2EItGAe

Target group: awseb-AWSEB-ZO1GR8VPVD32

Target type	Protocol : Port	Protocol version	VPC
Instance	HTTP: 80	HTTP1	vpc-0d578ce8f236db555
IP address type	Load balancer		
IPv4	awseb--AWSEB-IEH0u2EItGAe		

1	✓ 1	⊗ 0	0	0	0
Total targets	Healthy 0 Anomalous	Unhealthy	Unused	Initial	Draining

▶ Distribution of targets by Availability Zone (AZ)

- Secure Coding Practices for Django
- AWS Security Tools and Features
- Elastic Beanstalk Security Tools and Features
- Continuous Monitoring and Incident Response

RESULTS AND FINDINGS

MITIGATION STRATEGIES AND BEST PRACTICES

- Section 1. Introduction
- Section 2. Literature Review
- Section 3. Methodology
- Section 4. Results and Findings
- Section 5. Conclusion

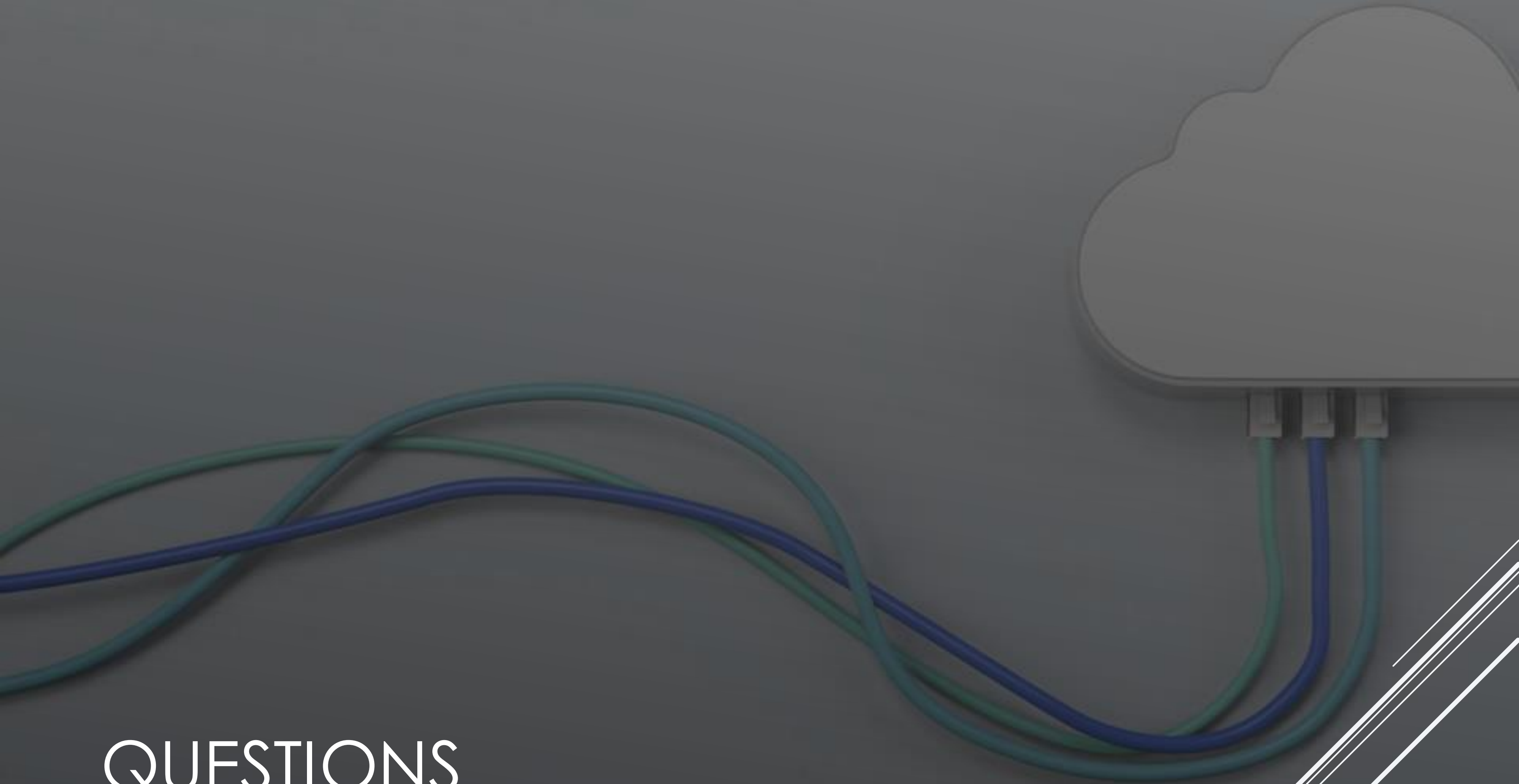
- Cloud computing has significantly evolved and become central to the digital economy, driving innovation and reshaping security frameworks.
- Deploying Django web applications on AWS reveals potential critical security vulnerabilities in the EC2 instance, highlighting the need for secure configuration management and rigorous security practices.
- Recommendations for enhancing security include using Amazon Inspector to identify and patch vulnerabilities in the EC2 instance, database encryption, regular updates, and continuous security assessments.

CONCLUSION
OVERVIEW

- Automated Code Review
- Vulnerability Patching
- Penetration Testing
- AWS Web Application Firewall (WAF)
- Advanced Threat Detection

CONCLUSION

FUTURE RESEARCH



QUESTIONS

REFERENCES

[1] Flexera, "Flexera State of the Cloud Report 2023," 2023. [Online]. Available: https://resources.flexera.com/web/pdf/Flexera-State-of-the-Cloud-Report-2023.pdf. [Accessed 21 Nov 2023].

[2] N. Bharathi, "Data Science in the Cloud: Who wins the cloud war?," Kaggle, 2019. [Online]. Available: https://www.kaggle.com/code/nitishabharathi/data-science-in-the-cloud-who-wins-the-cloud-war. [Accessed 29 Oct 2023].

[3] C. O'Hanlon, "A conversation with Werner Vogels - ACM queue," ACM Digital Library, 2006. [Online]. Available: https://queue.acm.org/detail.cfm?id=1142065. [Accessed 11 2023].

[4] A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee and M. Zaharia, "Above the clouds: A Berkeley view of cloud computing," in UCB/EECS, Berkeley, CA, 2009.

[5] I. Ruiz-Agundez, Y.K. Penya and P. G. Bringas, "Cloud Computing Services Accounting," International Journal of Advanced Computer Research (IJACR), vol. 2, pp. 7 - 17, 2012.

[6] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson and D. Song, "Provable Data Possession at Untrusted Stores," 2007.

[7] H. Shacham and B. Waters, "Compact Proofs of Retrievability," Journal of Cryptology, pp. 442-483, 2013.

[8] A. Juels and Kaliski, "PORs: Proofs of Retrievability for Large Files," pp. 584-597, 2007.

[9] K. D. Bowers, A. Juels and A. Oprea, "Proofs of retrievability: Theory and implementation," pp. 43-54, 2009.

[10] Q. Wang, C. Wang, K. Ren, W. Lou and J. Li, "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing," IEEE Transactions on Parallel and Distributed Systems, vol. 22, pp. 847-859, 2011.

REFERENCES CONTINUED…

[11] G. K. Patra and N. Chakraborty, "Securing cloud infrastructure for high-performance scientific computations using cryptographic techniques," International Journal of Advanced Computer Research, vol. 4, pp. 66-72, 2014.

[12] N. Pachorkar and R. Ingle, "Multi-dimensional Affinity-aware VM Placement Algorithm in Cloud Computing," International Journal of Advanced Computer Research, vol. 3, pp. 121-125, 2013.

[13] A. Holovaty and S. Willison, "The Django Web Framework," 2005. [Online]. Available: https://www.djangoproject.com/start/. [Accessed 29 01 2024].

[14] "Django documentation," Django Software Foundation, 2005-2024. [Online]. Available: https://docs.djangoproject.com/en/3.2/. [Accessed 30 01 2024].

[15] J. Kaplan-Moss and A. Holovaty, The Definitive Guide to Django: Web Development Done Right, 2nd Ed., Apress, 2009.

[16] T. Christie, "Django REST Framework," 2013. [Online]. Available: http://www.django-rest-framework.org/. [Accessed 29 01 2024].

[17] Gartner, "Magic quadrant for cloud infrastructure and platform services," 2021. [Online]. Available: https://www.gartner.com/en/documents/3997265/magic-quadrant-for-cloud-infrastructure-and-platform-services. [Accessed 29 01 2024].

[18] Amazon, "AWS Elastic Beanstalk - Deploy Web Applications,," Amazon Web Services, Inc., 2011. [Online]. Available: https://aws.amazon.com/elasticbeanstalk/. [Accessed 29 01 2024].

[19] J. Varia, "Architecting for the Cloud: Best practices," AWS Whitepaper, 2014.

[20] P. Kaushik, A. M. Rao, D. P. Singh, S. Vashisht and S. Gupta, "Cloud Computing and comparison based on service and performance between amazon AWS, microsoft azure, and google cloud," 2021.

REFERENCES CONTINUED…

[21]	D. M. Saraswat and D. R. C. Tripathi, "Cloud Computing: Comparison and Analysis of," in Proceedings of the SMART–2020, IEEE Conference, Moradabad, India, 2020.
[22]	L. Miller, Cloud Security and Compliance For Dummies, Hoboken, NJ: John Wiley & Sons, Inc., 2019.
[23]	A. Safhi, A. Al-Zahrani and A. Mubaraki, "Major Security Threats and Attacks That Facing Cloud Computing with the Main Defence Strategies," Communications in Mathematics and Applications, vol. 13, pp. 315-329, 2022.
[24]	A. Gupta and V. Chourey, "Cloud Computing: Security Threats & Control Strategy Using Tri-Mechanism," in IEEE International Technologies (ICCICCT), 2014.
[25]	S. Naqvi, A. Michot and Van, "Analysing impact of scalability and heterogeneity on the performance of federated cloud security services," in Security and Privacy in Computing and Communications (TrustCom, 2012.
[26]	M. Jenkins, "Accelerating DevOps with AWS Elastic Beanstalk," DevOps Journal, 2018.
[27]	F. A. AlSelami, "Major Cloud Computing Security Challenges with Innovative Approaches," Technical Gazette, vol. 17, no. 1, 2023.
[28]	Y. Alemami, "Cloud Data Security and Various Cryptographic Algorithms," International Journal of Electrical and Computer Engineering, vol. 13, no. 3, pp. 1867-1879, 2023.
[29]	A. Gobeo, C. Fowler and W. J. Buchanan, "GDPR and Cyber Security for Business Information Systems," GDPR and Cyber Security for Business Information Systems, pp. i-xix, 2020.
[30]	S. Rodigari, D. O'Shea, P. McCarthy, M. McCarry and S. McSweeney, "Performance Analysis of Zero-Trust multi-cloud," in 2021 IEEE 14th International Conference on Cloud Computing (CLOUD), Cork, Ireland, 2021.

REFERENCES CONTINUED…

[31] R. Khande, S. Rajapurkar, P. Barde, H. Balsara and A. Datkhile, "Data Security in AWS S3 Cloud Storage," no. https://doi.org/10.1109/ICCCNT56998.2023.10306922., pp. 1-6.

[32] U. D. o. H. a. H. Services, "Guidance on HIPAA & Cloud Computing," HHS.gov, 23 December 2022. [Online]. Available: https://www.hhs.gov/hipaa/for-professionals/special-topics/health-information-technology/cloud-computing/index.html. [Accessed 23 11 2023].

[33] "Complete guide to GDPR compliance," Horizon 2020 Framework Programme of the European Union, 2018. [Online]. Available: https://gdpr.eu/. [Accessed 29 01 2024].

[34] B. Kumar and J. Boaddh, "A Meta-Analysis on Secure Cloud Computing," International Journal of Advanced Technology and Engineering Exploration, vol. 3, pp. 15-20, 2016.

[35] A. R. Khan and L. K. Alnwihel, "A Brief Review on Cloud Computing," Engineering, Technology & Applied Science Research, vol. 13, no. 1, pp. 9997-10004, 2023.

[36] A. Bedse, P. Padiya, A. Vidhate and R. Adik, "Security Techniques in Cloud Computing for," Grenze International Journal of Engineering and Technology, vol. 9, no. 1, pp. 622-627, 2023.

[37] P. Mell and T. Grance, "National Institute of Standards and Technology," September 2011. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-145.pdf. [Accessed 29 01 2024].

[38] S. Jajodia, Secure Cloud Computing, New York, NY: Springer, 2014.

[39] S. D. Galav and D. S. M. Ghosh, "Data Confidentiality for Secure Cloud Computing Through Homomorphic Encryption," International Journal of Advanced Research in Computer Science, vol. 6, no. 1, pp. 146-148, 2015.

[40] O. Foundation, "OWASP API Security Project," Open Worldwide Application Security Project, 2023. [Online]. Available: https://owasp.org/www-project-api-security/. [Accessed 29 01 2024].

REFERENCES CONTINUED…

[41] J. B. Michael, "Placing Trust in Automated Software Development Processes," Computer, vol. 55, no. 7, pp. 78-81, 2022.

[42] S. Mishra, M. Kumar, N. Singh and S. Dwivedi, "A Survey on AWS Cloud Computing Security Challenges & Solutions," 2022.

[43] A. Sun, G. Gao, T. Ji and X. Tu, "One Quantifiable Security Evaluation Model for Cloud Computing Platform," in 2018 Sixth International Conference on Advanced Cloud and Big Data (CBD), Lanzhou, China, 2018.

[44] R. Patil, L. Paikrao and V. H, "Security as a Service Model for Virtualization Vulnerabilities in Cloud Computing," 2018 International Conference On Advances in Communication and Computing Technology (ICACCT), no. doi: 10.1109/ICACCT.2018.8529573, pp. 559-562, 2018.

[45] D. Project, "Security in Django," Django, 2005-2024. [Online]. Available: https://docs.djangoproject.com/en/5.0/topics/security/. [Accessed 29 01 2024].

[46] A. W. Services, "What is Django?," AWS Documentation, 2011 - 2024. [Online]. Available: https://aws.amazon.com/what-is/django/. [Accessed 29 01 2024].

[47] A. W. Services, "AWS Shield Documentation," AWS, 2011 - 2024. [Online]. Available: https://aws.amazon.com/documentation-overview/shield/. [Accessed 29 01 2024].

[48] J. D. Meier, A. Mackman, M. Dunner, S. Vasireddy, R. Escamilla and A. Murukan, "Security practices for ASP.NET applications," 29th IEEE International Conference on Software Engineering, pp. 123-132, 2017.

[49] A. Aborujilah, J. Adamu, S. M. Shariff and Z. Awang Long, "Descriptive Analysis of Built-in Security Features in Web Development Frameworks," in 2022 16th International Conference on Ubiquitous Information Management and Communication (IMCOM), Seoul, Korea, 2022.

[50] W. W. W. Consortium, "Content Security Policy Level 3," WC3, 21 2 2024. [Online]. Available: https://www.w3.org/TR/CSP3/. [Accessed 28 02 2024].

REFERENCES CONTINUED…

[51] A. W. Services, "AWS CloudFormation Documentation," AWS, 2011 - 2024. [Online]. Available: https://aws.amazon.com/documentation-overview/cloudformation/. [Accessed 29 01 2024].

[52] N. Case, "Top 10 security items to improve in your AWS account," AWS Security Blog, 20 03 2020. [Online]. Available: https://aws.amazon.com/blogs/security/top-10-security-items-to-improve-in-your-aws-account/. [Accessed 29 01 2024].

[53] A. W. Services, "Identity and access management for Elastic Beanstalk," AWS, 2011 - 2024. [Online]. Available: https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/security-iam.html. [Accessed 29 01 2024].

[54] A. W. Services, "Security best practices for Amazon S3," AWS, 2011 - 2024. [Online]. Available: https://docs.aws.amazon.com/AmazonS3/latest/userguide/security-best-practices.html. [Accessed 29 01 2024].

[55] A. W. Services, "Control traffic to subnets using network ACLs," AWS, 2011 - 2024. [Online]. Available: https://docs.aws.amazon.com/vpc/latest/userguide/vpc-network-acls.html. [Accessed 29 01 2024].

[56] A. W. Services, "Amazon Aurora Documentation," AWS, 2011 - 2024. [Online]. Available: https://aws.amazon.com/documentation-overview/aurora/. [Accessed 29 01 2024].

[57] A. W. Services, "AWS Lambda Documentation," AWS, 2011 - 2024. [Online]. Available: https://aws.amazon.com/documentation-overview/lambda/. [Accessed 29 01 2024].

[58] Amazon, "AWS Elastic Beanstalk Documentation," AWS Documentation, 2023. [Online]. Available: https://docs.aws.amazon.com/elastic-beanstalk/. [Accessed 29 01 2024].

[59] J. Wettinger, V. Andrikopoulos, F. Leymann and S. Strauch, "Middleware-oriented deployment automation for cloud applications," IEEE Transactions on Cloud Computing, vol. 6, no. 10.1109/TCC.2016.2535325, pp. 1054-1066, 2018.

[60] C. R. Pushpaleela, S. Sankar, K. Viswanathan and K. S. Aathithya, "Application modernization strategies for AWS cloud," 2022

REFERENCES CONTINUED…

[61] G. McGrath, J. Short, S. Ennis, B. Judson and P. Brenner, "Cloud event programming paradigms: Applications and analysis," IEEE International Conference on Cloud Computing, no. doi: https://doi.org/10.1109/CLOUD.2016.0060., pp. 400-406, 2016.

[62] A. Kaur, G. Raj, S. Yadav and T. Choudhury, "Performance evaluation of AWS and IBM cloud platforms for security mechanism," no. doi: https://doi.org/10.1109/CTEMS.2018.8769215., pp. 516-520, 2018.

[63] A. W. Services, "Artificial Intelligence and Machine Learning," AWS, 2011 - 2024. [Online]. Available: https://docs.aws.amazon.com/wellarchitected/latest/financial-services-industry-lens/artificial-intelligence-and-machine-learning.html. [Accessed 29 01 2024].

[64] A. W. Services, "Encryption in transit," AWS, 2018. [Online]. Available: https://docs.aws.amazon.com/glue/latest/dg/encryption-in-transit.html. [Accessed 29 01 2024].

[65] K. Janarthanan, "Cloud_Attendance_System," kujalk, 18 Dec. 2020. [Online]. Available: https://github.com/kujalk/Cloud_Attendance_System. [Accessed 15 12 2023].