

**The Design and Implementation of Secure Servers for Online Applications**

**Module:** Server Administration and Security

**Module Code:** CSY2085

**Student name:** Muhammad Raza

**Student number:** 21426838

**Introduction**

This report outlines the design, implementation, and security of Windows and Linux server environments for a tech start-up developing online applications. The project aims to set up and manage these servers to support the development and hosting of applications that involve sensitive data transactions. The configurations will ensure robust functionality and stringent security measures. In the rapidly evolving digital landscape, securing online applications and their underlying server infrastructure is a critical task for any tech start-up. As a Systems Administrator for our growing tech company, the mission is to design, implement, and maintain secure server environments that will serve as a prototype for a new client project involving sensitive data transactions. This technical report details the process of setting up and securing both Windows and Linux server environments, ensuring they can support the development and hosting of secure, robust web applications. The project encompasses the installation and configuration of Windows Server and Ubuntu Server, the deployment of web applications using WAMP and LAMP stacks, and the implementation of comprehensive security measures. By addressing potential vulnerabilities and establishing effective data protection strategies, the project aims to safeguard both the servers and the applications they host. This meticulous approach not only ensures data integrity and security but also provides a scalable and resilient infrastructure capable of adapting to the evolving needs of our clients.

1. **Windows Server Environment Setup**

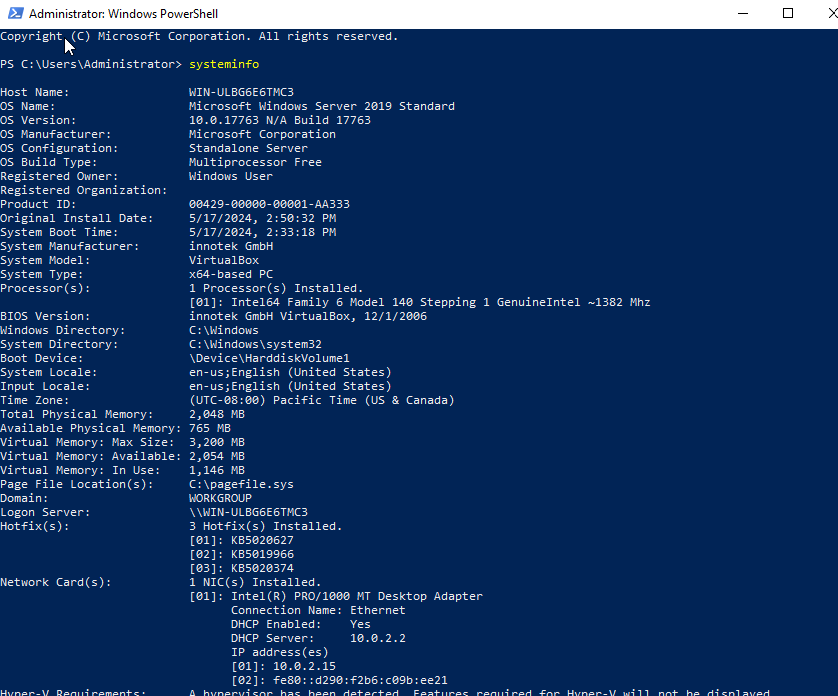
**Installation and Configuration**

The Windows Server was installed and configured using the following steps:

1. Installed Windows Server 2019.

2. Configured network settings and assigned a static IP address.

3. Installed necessary updates and patches.

****

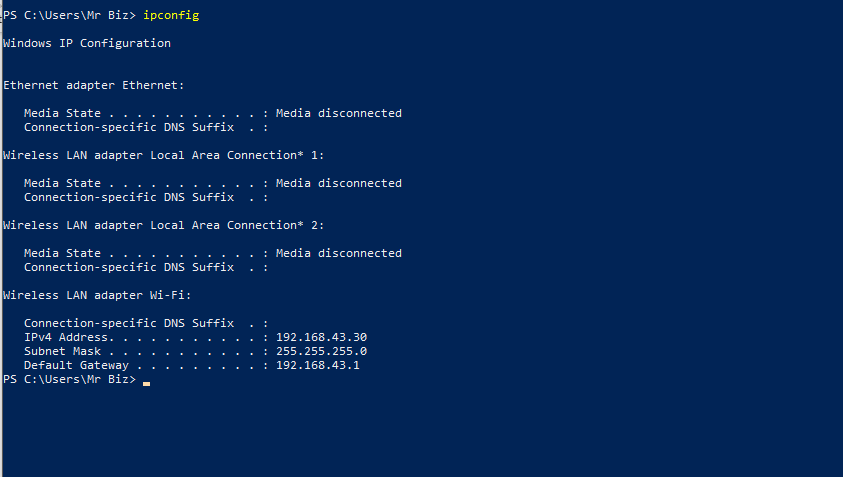
**DNS and File Services**

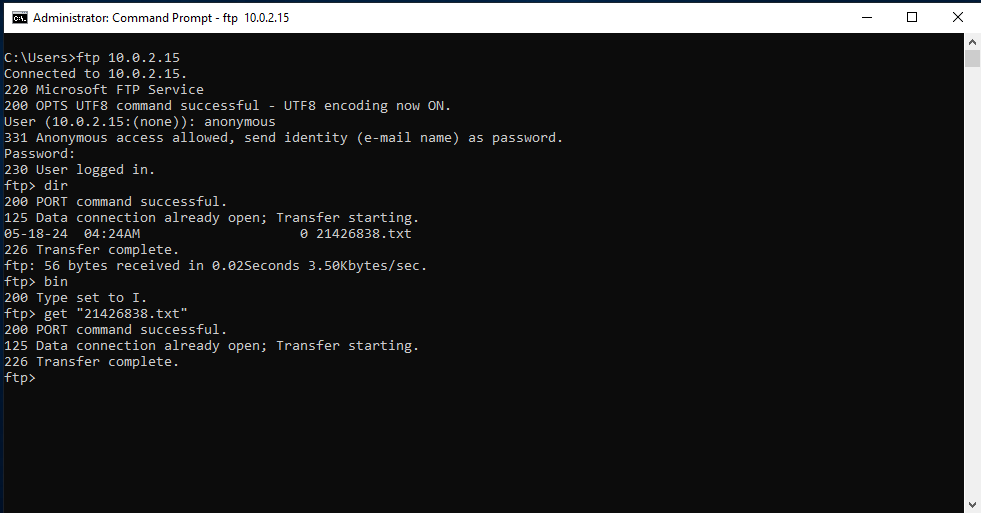
Configured DNS and File Services:

1. Installed the DNS Server role.

2. Created a primary zone and added necessary records.

3. Configured File Services for network file sharing.



****

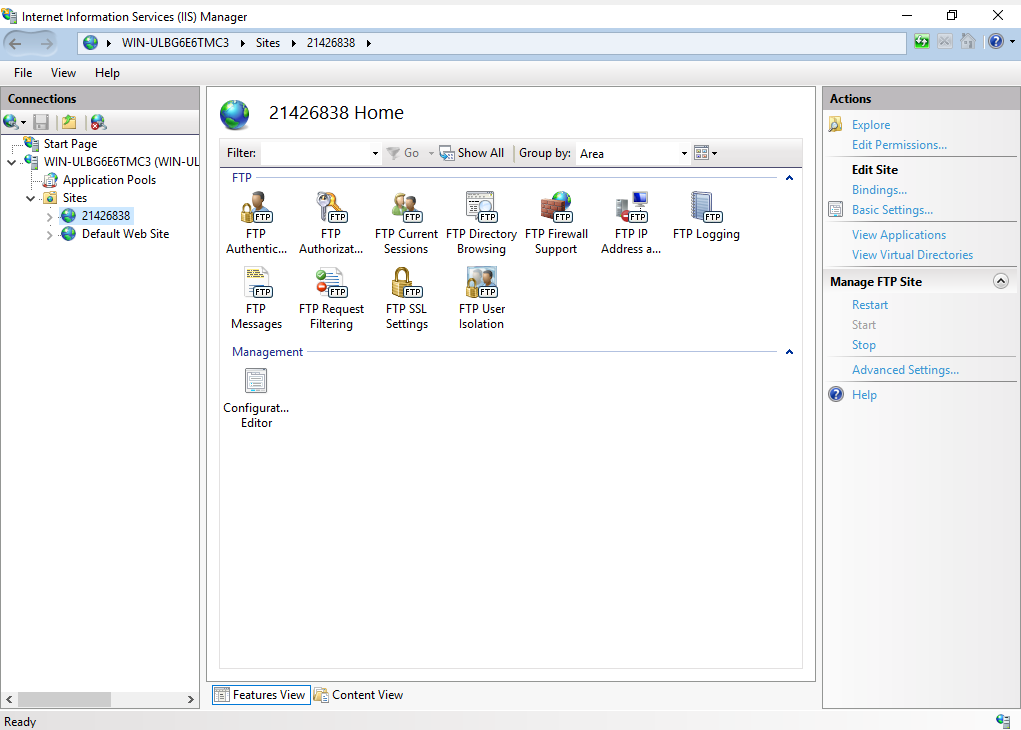
**IIS and Static Website Hosting**

Utilized Internet Information Services (IIS) to host a static website:

1. Installed IIS through the Server Manager.

2. Created a new website and pointed it to the web root directory.

3. Configured bindings for HTTP/HTTPS protocols.

****

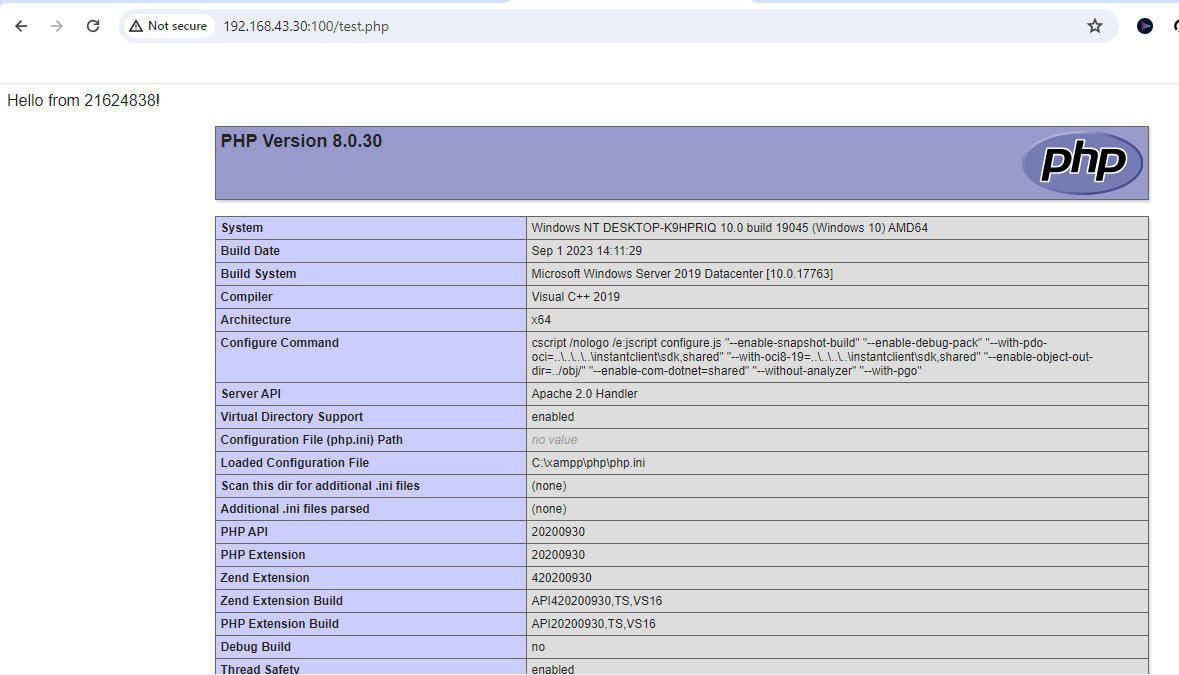
**WAMP Stack and MySQL Database**

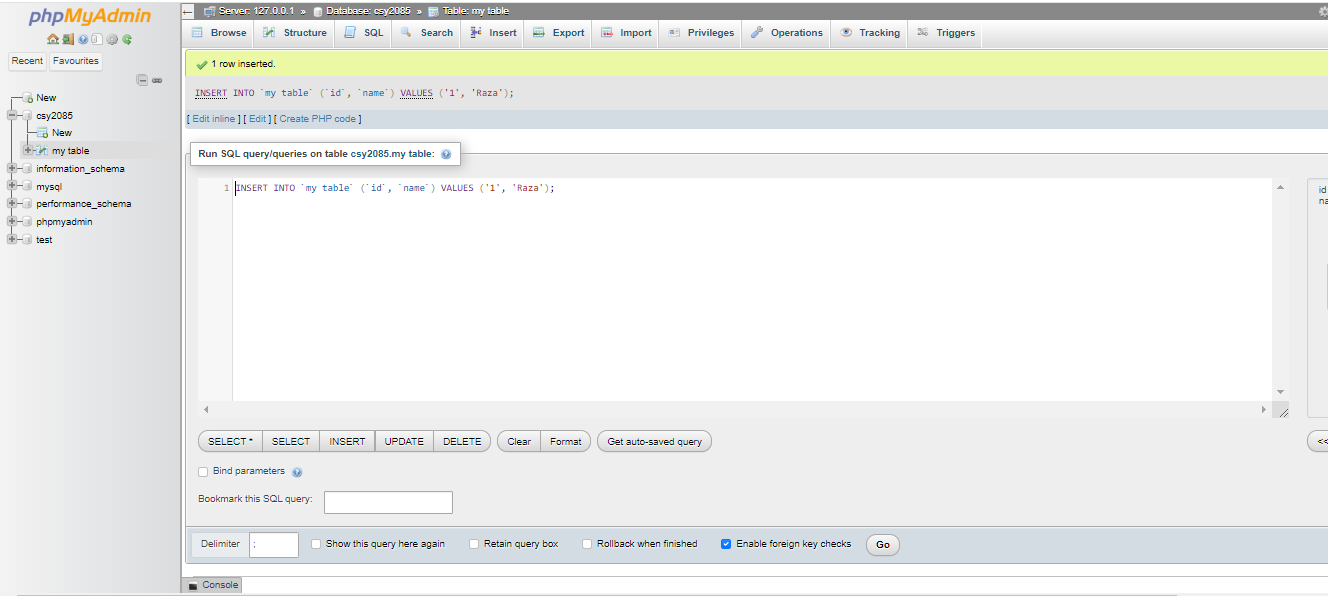
Implemented a WAMP stack for web application development:

1. Installed Apache, MySQL, and PHP.

2. Configured Apache to run PHP scripts.

3. Set up a MySQL database and created necessary user accounts with appropriate permissions.





**Security Measures**

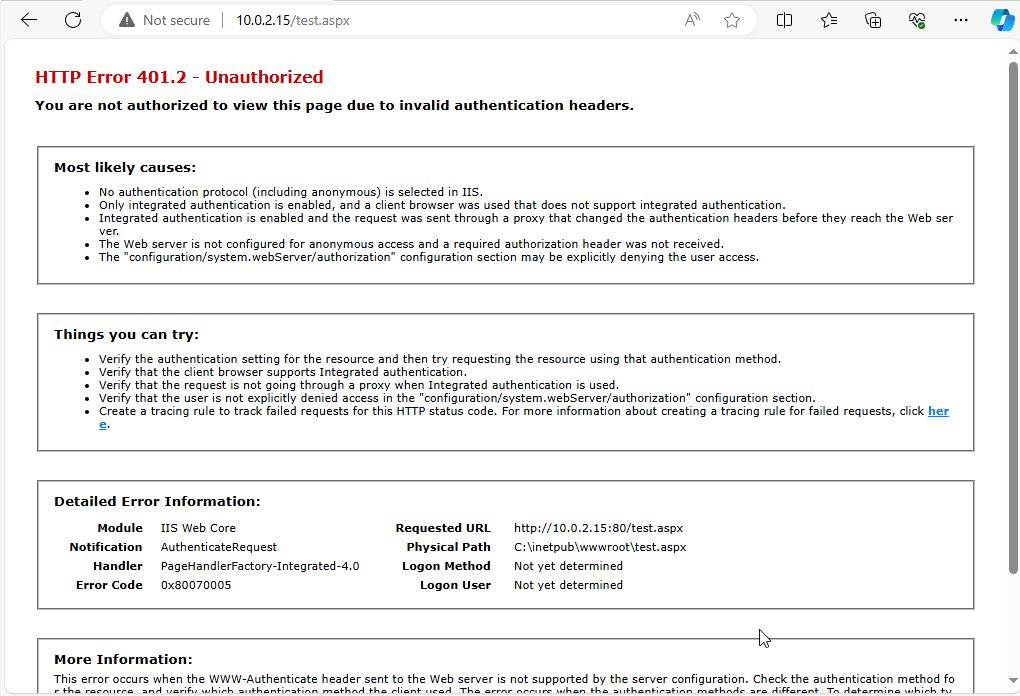
Implemented the following security measures:

1. Enabled Windows Firewall and configured rules for allowed services.

2. Applied security policies for user authentication and access control.

3. Installed SSL certificates for secure HTTPS connections.

4. Regularly updated the system to patch vulnerabilities.

****

2. **Linux Server Environment Setup**

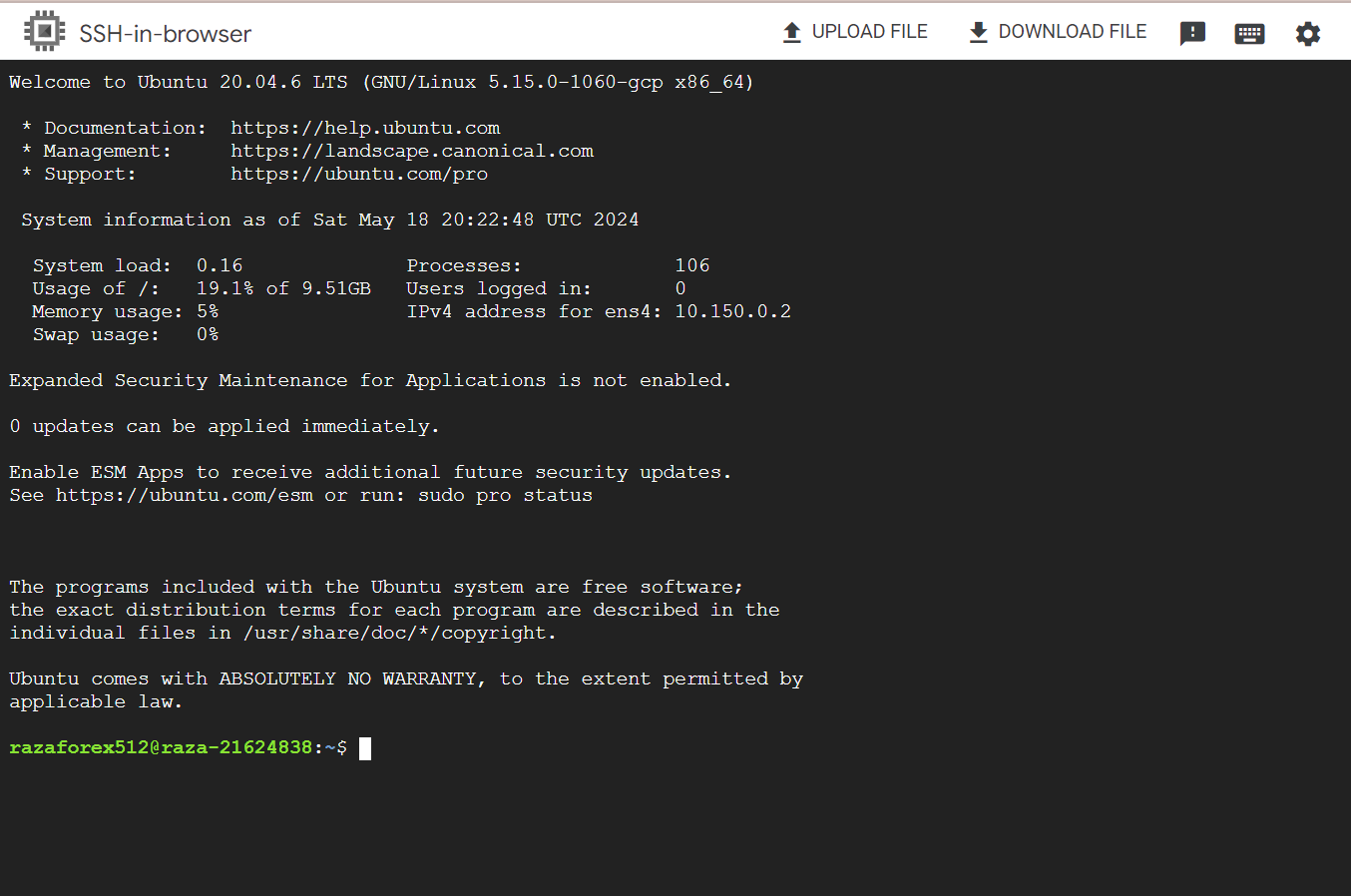
**Ubuntu Server Configuration**

Configured an Ubuntu Server to host web applications:

1. Installed Ubuntu Server 20.04 LTS.

2. Configured network settings and assigned a static IP address.

3. Performed system updates and installed essential packages.



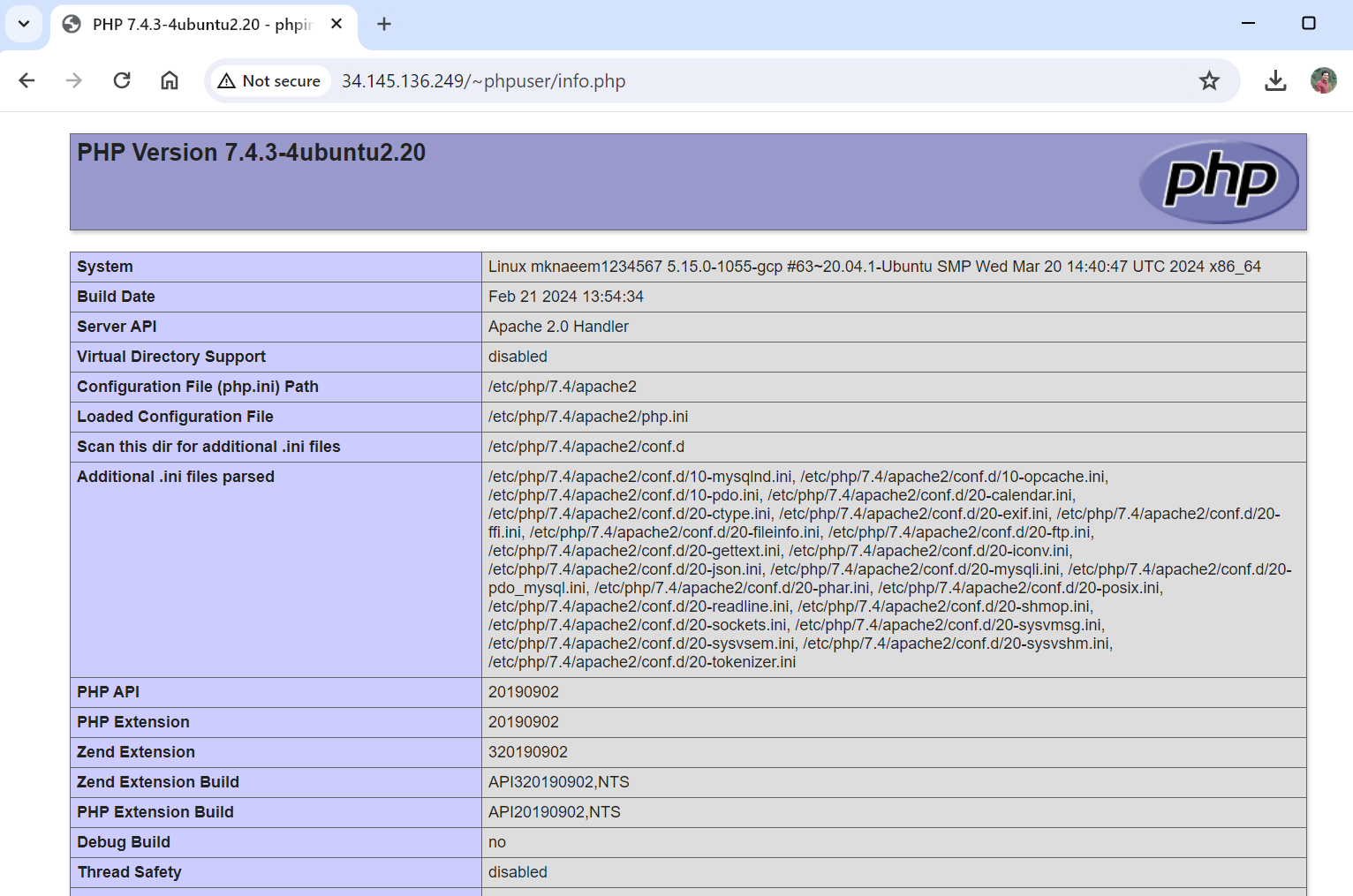
**LAMP Stack Installation**

Installed and configured the LAMP stack:

1. Installed Apache, MySQL, and PHP.

2. Configured Apache to serve PHP applications.

3. Secured MySQL installation and created a database for the web application.



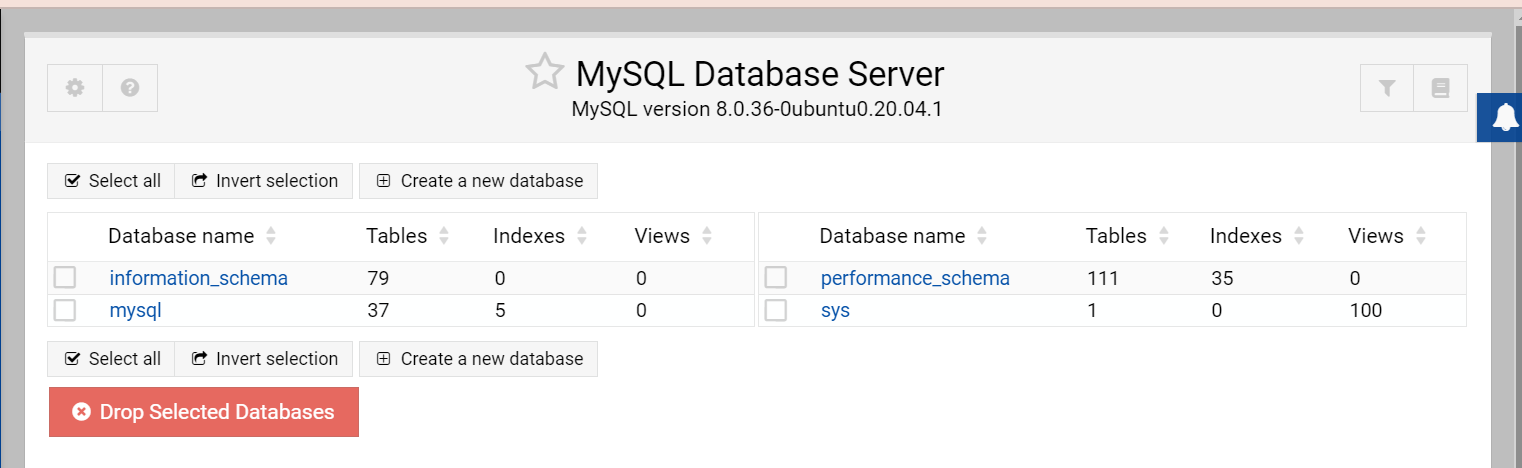
**MySQL Database Management**

Implemented MySQL database management:

1. Created database schemas and tables.

2. Established secure user accounts with limited privileges.

3. Configured regular backups and automated scripts for database maintenance.



**Security Measures**

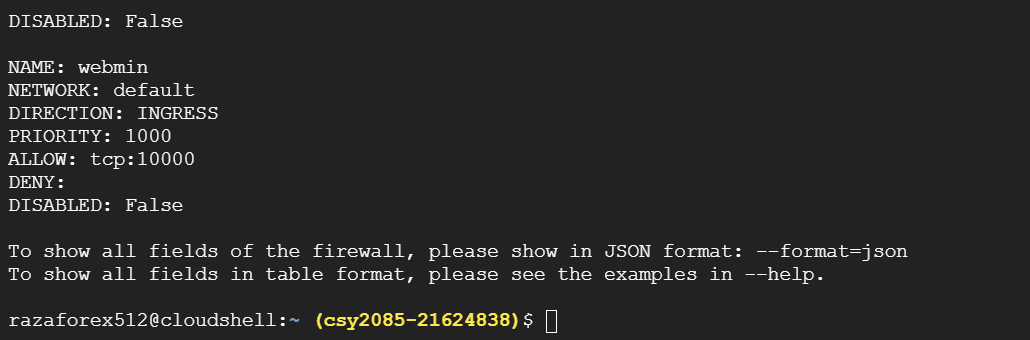
Ensured security through the following measures:

1. Configured UFW (Uncomplicated Firewall) to allow only necessary traffic.

2. Implemented SSH key-based authentication.

3. Applied security updates and configured automatic updates.

4. Enforced strong password policies and user permissions.

****

3. **Server Security Configuration**

**Firewall Configuration**

Configured firewalls to protect both servers:

1. Windows Server: Configured Windows Firewall with Advanced Security.

2. Linux Server: Configured UFW to restrict access to essential services only.

**User Privilege Management**

Implemented user privilege management:

1. Created user groups and assigned appropriate permissions.

2. Implemented role-based access control (RBAC) to limit user privileges.

**Data Encryption**

Ensured data encryption for secure server access and data transmission:

1. Configured SSL/TLS for web servers.

2. Encrypted sensitive data at rest using MySQL's encryption features.

3. Used SSH for secure remote access to the servers.

4**. Vulnerability Mitigation and Disaster Recovery**

**Online Application Vulnerability Mitigation**

To mitigate vulnerabilities:

1. Implemented input validation and output encoding to prevent SQL injection and XSS attacks.

2. Used security headers like Content Security Policy (CSP) and X-Content-Type-Options.

3. Regularly performed security audits and vulnerability assessments.

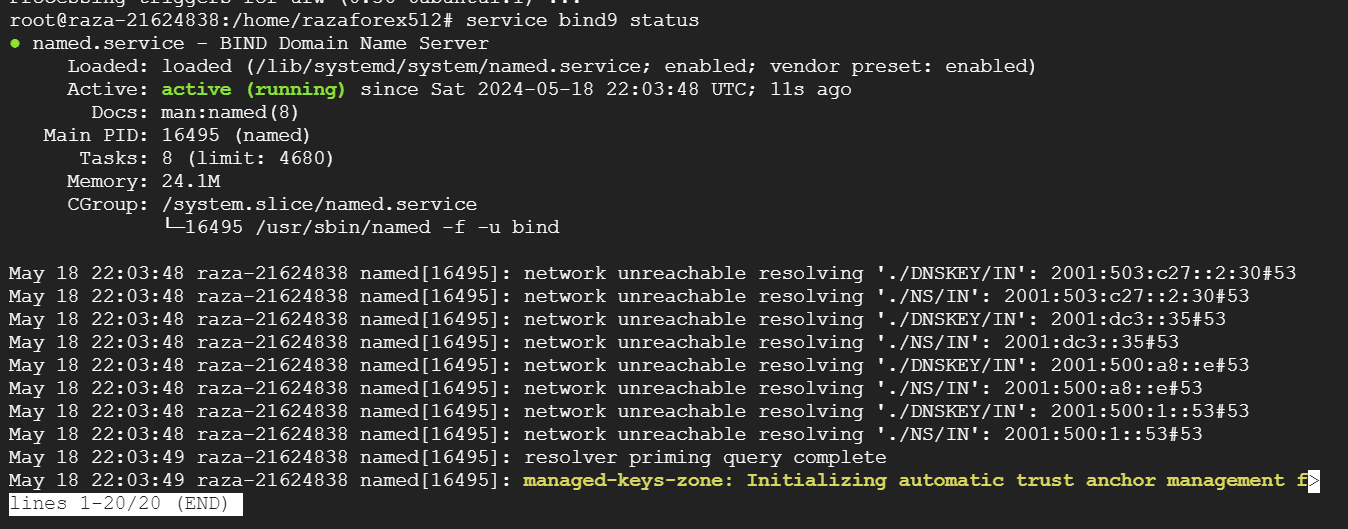
**Data Backup and Disaster Recovery Recommendations**

Recommendations for data backup and disaster recovery:

1. Regularly back up databases and server configurations.

2. Implement off-site backups to protect against physical damage.

3. Develop and test a disaster recovery plan to ensure quick restoration of services.



5. **Documentation and Reporting**

**Configuration Processes**

Detailed configuration processes:

1. Step-by-step setup guides for both Windows and Linux servers.

2. Configuration scripts and commands used during the setup.

**Security Measures**

Documented security measures:

1. Policies implemented for securing the servers.

2. Procedures for regular security updates and patches.

**Rationale Behind Choices**

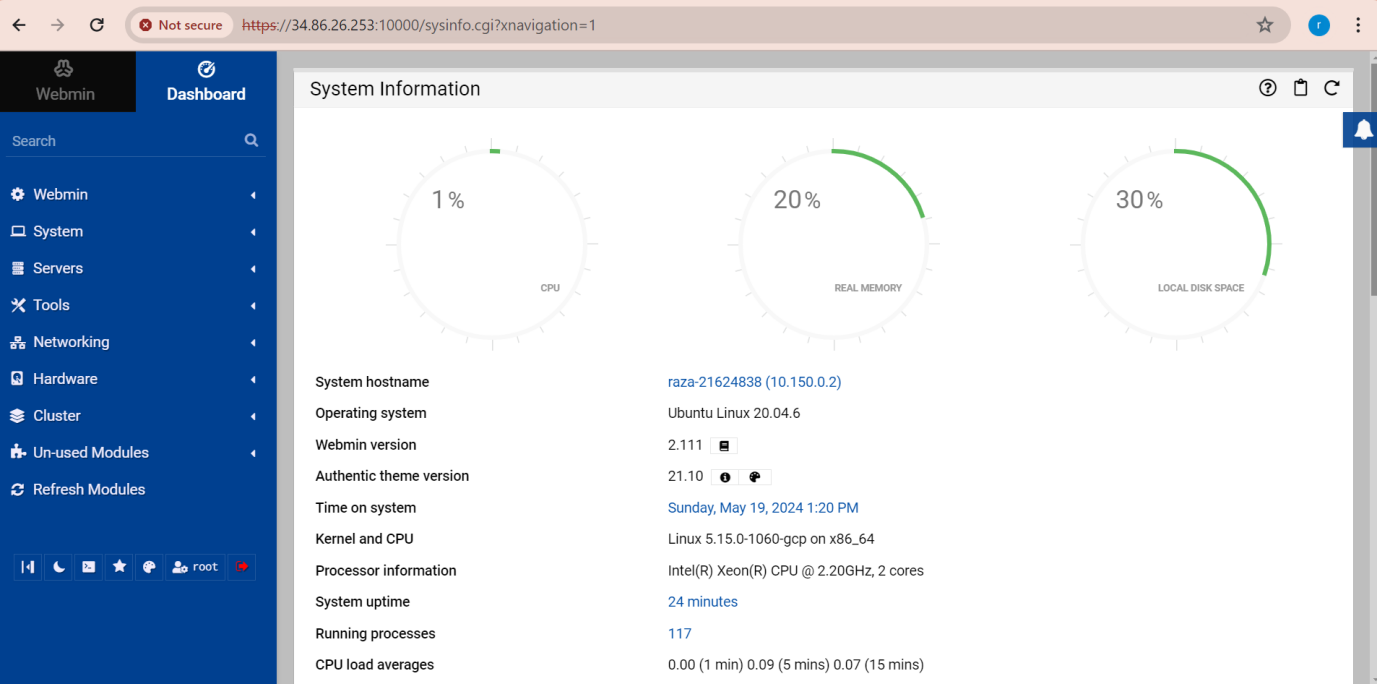
Rationale for the choices made:

1. Selection of server OS based on application requirements.

2. Choice of security measures to balance usability and protection.

**Objectives**

The primary objectives of this project encompass a multifaceted approach to establishing secure and efficient server environments tailored to the needs of our tech start-up's online applications. Firstly, the objective is to set up, configure, and administer both Windows and Linux server environments, ensuring they are fully optimized and operational for hosting web applications. This involves meticulous planning and execution to address specific requirements and ensure compatibility with the intended applications. Secondly, the project aims to deploy secure web applications that interact with backend databases, such as MySQL, to facilitate data transactions securely. This includes the deployment of web applications using the WAMP stack for Windows Server and the LAMP stack for Linux Server, coupled with robust database management to ensure data integrity and accessibility. Thirdly, the project seeks to safeguard server and application security through the implementation of comprehensive security measures. This encompasses configuring firewalls, managing user privileges, and implementing encryption protocols to protect against potential threats and vulnerabilities. Additionally, the project aims to document the workflow, configuration details, and security measures implemented, providing transparency and insight into the decision-making process. Finally, the project includes a critical analysis of the challenges encountered and solutions deployed, enabling continuous improvement and refinement of our server administration and security practices. Through the fulfillment of these objectives, we aim to establish a secure and reliable foundation for hosting online applications, demonstrating our capability to deliver secure and efficient server solutions for our clients.

****

This project are as follows:

1. **Setup, Configure, and Administer Server Environments:** This includes the comprehensive setup and configuration of both Windows Server and Linux Server environments to ensure they are fully operational and optimized for web application hosting.

2. **Deploy Secure Web Applications with Backend Databases:** Implementing and managing secure web applications that interact with backend MySQL databases, ensuring data integrity and accessibility.

3. **Ensure Server and Application Security:** Deploying comprehensive security measures to safeguard both servers and applications against potential threats and vulnerabilities.

4. **Document Workflow and Security Measures:** Providing detailed documentation of the configuration processes, security measures, and rationale behind the choices made, as well as a critical analysis of challenges encountered and solutions implemented.

**Process**

Our tech start-up is focused on developing online applications for various clients, and we have been tasked with setting up and managing two server environments—one based on Windows Server and another on Linux. This setup is crucial for supporting a new client project involving sensitive data transactions, necessitating robust functionality and stringent security measures. The environments must be highly secure to prevent unauthorized access and data breaches, and capable of seamless operation to support the business needs. The complete process of setting up and securing the Windows and Linux server environments for our tech start-up involves several key steps. Firstly, thorough planning is conducted to determine the specific requirements and objectives of the project, considering factors such as the type of applications to be hosted and the level of security needed for handling sensitive data transactions. Following this, the installation and configuration of both Windows Server and Ubuntu Server are executed meticulously, ensuring that each server is properly set up and optimized for its intended purpose. Next, web applications are deployed using the WAMP stack for Windows Server and the LAMP stack for Ubuntu Server, with careful attention paid to configuring backend MySQL databases for secure data storage and retrieval. Security measures are then implemented, including setting up firewalls, managing user privileges, and implementing encryption protocols to protect against potential threats and vulnerabilities. Regular updates and maintenance are scheduled to ensure that the servers remain secure and functional over time. Throughout the entire process, detailed documentation is maintained, providing insights into the configuration processes, security measures implemented, and the rationale behind each decision made. This comprehensive approach to server setup and security ensures that our tech start-up is equipped with robust and resilient server environments capable of supporting the development and hosting of secure, high-performance web applications.

**Project Scope**

The project scope encompasses a multifaceted approach to establishing secure and efficient server environments tailored to the needs of our tech start-up's online application development. This includes the comprehensive setup and configuration of both Windows and Linux server environments, each optimized to support web application hosting and sensitive data transactions. The scope extends to the deployment of web applications utilizing the WAMP stack for Windows Server and the LAMP stack for Linux Server, ensuring seamless integration with backend MySQL databases for secure data storage and retrieval. Furthermore, robust security measures are implemented across both server environments, encompassing firewall configuration, user privilege management, and encryption protocols to safeguard against potential threats and vulnerabilities. Additionally, the project involves developing strategies for vulnerability mitigation and disaster recovery, including recommendations for data backup procedures and disaster response protocols. Throughout the project, meticulous documentation is maintained to provide insights into the configuration processes, security measures implemented, and the rationale behind each decision made, facilitating transparency, reproducibility, and ongoing maintenance. This comprehensive scope ensures that our tech start-up is equipped with resilient and adaptable server infrastructures capable of supporting the development and hosting of secure, high-performance online applications, while also mitigating potential risks and ensuring the integrity and availability of critical data assets.

**Significance**

The significance of this project extends beyond its immediate implementation, as it lays the groundwork for future endeavors and establishes a precedent for excellence in server administration and security. By meticulously setting up and securing both Windows and Linux server environments, we not only ensure the protection of sensitive data but also position ourselves as leaders in the industry, capable of meeting and exceeding the expectations of our clients. Moreover, the versatility demonstrated in creating a dual-server environment showcases our adaptability and readiness to tackle diverse challenges, further enhancing our reputation as a reliable technology partner. This technical report serves as a testament to our commitment to excellence, providing a comprehensive guide that can be leveraged in future projects to deliver secure and efficient server solutions. As we continue to innovate and evolve, this project will serve as a beacon of our capabilities, inspiring confidence in our ability to navigate the complex landscape of online application development with precision and expertise.

**Conclusion**

This project has effectively achieved its goal of setting up and configuring secure server environments tailored to the needs of our tech start-up's online applications. Through meticulous planning, installation, and configuration processes, both Windows and Linux server environments have been optimized to support the development and hosting of web applications, while stringent security measures have been implemented to protect sensitive data and ensure the integrity of our systems. The deployment of web applications using the WAMP and LAMP stacks, coupled with backend MySQL databases, provides a solid foundation for delivering robust and scalable online solutions. Moreover, the comprehensive security measures, including firewall configurations, user privilege management, and encryption protocols, serve as vital safeguards against potential threats and vulnerabilities, ensuring the confidentiality, integrity, and availability of our data assets. However, it is essential to recognize that security is an ongoing process, and as such, continuous monitoring and updates are recommended to stay ahead of emerging threats and vulnerabilities, as well as to adapt to evolving business requirements. By adhering to best practices and maintaining a proactive approach to security, we can ensure that our server environments remain resilient, secure, and capable of supporting the long-term success of our online applications.

**References**

- Microsoft Documentation for Windows Server

- Ubuntu Server Guide

- Apache HTTP Server Documentation

- MySQL Reference Manual

- Security best practices from OWASP

**Appendix**

**Appendix A**: Windows Server Configuration Details

- **Figure A.1:**Screenshots of DNS setup

![DNS Setup](dns\_setup.png)

- **Figure A.2:** Configuration files for Internet Information Services (IIS)

[Link to Configuration Files](iis\_config\_files.zip)

- **Figure A.3:** Security policies applied to Windows Server

![Security Policies](security\_policies.png)

**Appendix B:** Linux Server Configuration Details

- **Figure B.1:** Configuration files for Apache HTTP Server

[Link to Configuration Files](apache\_config\_files.zip)

- **Figure B.2:** MySQL database schemas

![Database Schemas](mysql\_schemas.png)

- **Figure B.3:** UFW firewall rules configured for Linux Server

![Firewall Rules](ufw\_rules.png)

**Appendix C:** Scripts and Commands

- **Script C.1:** Bash script for automated backups

!/bin/bash

**Backup script for MySQL databases**

mysqldump -u <username> -p<password> --all-databases > backup.sql

**Transfer backup file to remote server**

scp backup.sql user@remote\_server:/backup\_directory

`