Part 1: Team Composition and Skills

Group Members:

Student 1: Muchun Wan (XSS ATTACKS)
Student 2: Benelyon Choo (Session Attack)
Student 3: Pyae Sone Soe Moe (Database Attack)

Members Profile:

Members Profile: Muchun Wan

Responsibility in Project: XSS Attacks in Testing Phase
Interest in XSS Attacks:
Muchun Wan has chosen to focus on Cross-Site Scripting (XSS) attacks for the testing phase due to a strong interest in web application security, particularly in understanding how malicious scripts can be injected into web pages and the impact they can have on users and systems. Despite lacking direct experience with XSS attacks, Muchun is eager to delve into this crucial aspect of cybersecurity, recognizing its significance in safeguarding web applications against common and potentially devastating vulnerabilities.

Learning Goals:
Muchun aims to gain a comprehensive understanding of different types of XSS vulnerabilities (stored, reflected, and DOM-based) and learn how to identify, exploit, and mitigate them effectively. Through the CTF (Capture The Flag) training phase, Muchun plans to acquire hands-on experience with real-world XSS scenarios, learning from both successes and failures to develop a robust skill set in XSS vulnerability assessment. This learning journey is driven by a keen interest in enhancing web security and contributing meaningful insights during the testing phase of the project.

Skills and Support for the Role:

1. **Analytical Thinking:** Muchun possesses strong analytical skills, essential for dissecting web applications' behaviors and identifying potential injection points for XSS attacks.
2. **Quick Learner:** With a proven ability to quickly assimilate new information and technologies, Muchun is well-equipped to dive into XSS attack methodologies and defense mechanisms.
3. **Attention to Detail:** This project requires a meticulous approach to catch subtle vulnerabilities, and Muchun's attention to detail will be crucial in spotting and exploiting complex XSS vulnerabilities.

Contribution to the Project:
Muchun is committed to turning a keen interest in XSS attacks into a tangible contribution to the project. By engaging deeply in the CTF training phase and collaborating with team members, Muchun aims to bring fresh perspectives to XSS vulnerability testing. This journey from learning to application is expected to not only enhance Muchun's skill set but also significantly contribute to identifying and mitigating XSS vulnerabilities within the Roblox application, thereby strengthening the platform's overall security posture.

Conclusion:
Muchun Wan's choice to focus on XSS attacks, driven by interest and a commitment to learning, underscores a proactive approach to personal and professional development. With support from the team and through targeted training and practical experience, Muchun is poised to make meaningful contributions to the project's success, turning theoretical knowledge into practical expertise in XSS vulnerability testing.

Members Profile: Benelyon Choo

Responsibility in Project: Session Attacks in the Testing Phase
Background and Interest:
Benelyon Choo has chosen to specialize in session attacks for the testing phase, leveraging a foundational experience in network and session security. His prior engagement with session management vulnerabilities, albeit at an introductory level, sparked a keen interest in exploring deeper into how session handling flaws can be exploited and, more importantly, how they can be prevented. Benelyon's motivation stems from an understanding of the critical role that secure session management plays in protecting user data and maintaining the integrity of web applications.

Learning and Development Goals:
While Benelyon brings some experience to the table, he recognizes the need to expand his knowledge and skills in identifying, exploiting, and mitigating session attacks. He aims to deepen his understanding of session management mechanisms, session fixation, session hijacking, and Cross-Site Request Forgery (CSRF) attacks. Through targeted learning in the CTF training phase and collaborative exploration with teammates, Benelyon seeks to enhance his ability to uncover and address sophisticated session vulnerabilities.

Skills and Strengths:

- **Technical Foundation:** Benelyon's network security background and initial foray into session vulnerabilities provide a solid technical foundation for tackling session attacks.
- **Problem-Solving:** Equipped with strong problem-solving skills, he can navigate complex security challenges and devise effective strategies for mitigating risks associated with session management.

- **Adaptability:** Benelyon's ability to adapt to rapidly changing security landscapes and his willingness to immerse himself in new learning opportunities are key to staying ahead in the field of cybersecurity.

Contribution to the Project:
Benelyon Choo is set to apply his budding expertise and learning outcomes to the project's session attack vector. His prior experience, coupled with a dedicated effort to advance his understanding of session security, positions him to contribute significantly to identifying critical session management flaws. Benelyon's focused approach will enhance the project's ability to secure the Roblox platform against session-based vulnerabilities, ensuring a safer environment for users.

Conclusion:
With a blend of experience and a strong drive to expand his knowledge, Benelyon Choo is poised to make substantial contributions to the Roblox Wildcard Domain Security Project. His focus on session attacks reflects a commitment to addressing a key area of web application security, with the goal of not just finding vulnerabilities but also fostering a secure and trustworthy platform for users.

3. Members Profile: Pyae Sone Soe Moe

Responsibility in Project: Database Attacks in Testing Phase

Background and Interest:

Pyae Sone Soe Moe brings to the team foundational expertise in database management and security, with a particular interest in safeguarding database systems against sophisticated attacks. His previous experience, primarily focused on ensuring the integrity and security of database architectures, has equipped him with a keen understanding of the vulnerabilities that databases often face. Pyae's decision to concentrate on database attacks stems from his recognition of the critical importance of database security in the broader context of application security and his desire to deepen his expertise in this area.

Learning and Development Goals:

Acknowledging the evolving landscape of database security, Pyae aims to enhance his proficiency in identifying, exploiting, and mitigating a wide range of database vulnerabilities, including but not limited to SQL injection, NoSQL injection, and other injection flaws. He is particularly interested in exploring advanced techniques for securing databases against unauthorized access and data leakage. Through hands-on practice in the CTF training phase

and collaborative learning with his peers, Pyae is committed to mastering the skills necessary to conduct thorough database vulnerability assessments.

Skills and Strengths:

1. **Technical Expertise:** Pyae's solid background in database systems provides him with the technical know-how to understand and exploit complex database vulnerabilities.
2. **Analytical Approach:** His methodical and analytical approach to problem-solving enables him to dissect and address the multifaceted nature of database security challenges.
3. **Continuous Learner:** Pyae's dedication to continuous learning and staying updated with the latest database security trends and attack vectors ensures that his skills remain sharp and relevant.

Contribution to the Project:

In focusing on database attacks, Pyae Sone Soe Moe is set to apply his technical acumen and growing expertise to identify and mitigate potential vulnerabilities within the Roblox platform's database systems. His understanding of both traditional and emerging database threats will be instrumental in fortifying the platform against data breaches and ensuring the security of user data. By leveraging his skills in conjunction with targeted training, Pyae will contribute significantly to the project's goal of enhancing the overall security posture of the Roblox platform.

Conclusion:

Pyae Sone Soe Moe's role in addressing database attacks is vital to the project's success. His blend of experience, keen interest in database security, and commitment to advancing his skills positions him as a key contributor to the team's efforts in securing the Roblox platform. Through his focused work on database vulnerabilities, Pyae aims to not only strengthen his expertise but also contribute to creating a safer and more secure environment for all Roblox users.

Part 2: The Project

Project Name: Bug Bounty Program for Roblox
Client: Roblox
Topic: Bug Bounty Program targeting the *.roblox.com wildcard domain.

Project Scope:

Our project's mission is to execute a comprehensive security audit on the *.roblox.com domain space, rigorously probing for and documenting critical security flaws that could compromise its structural integrity and the overall security of Roblox's services. This targeted assessment will focus on uncovering and evaluating high-impact vulnerabilities—such as those affecting user data protection, service availability, and application security—that pose a serious threat to the robustness of the Roblox platform and its users.

Project Out-Of-Scope and Confidentiality Requirements:

Out-of-Scope: This project will not address vulnerabilities related to the execution of non-technical attacks (e.g., social engineering, physical attacks) or issues already known to Roblox or disclosed publicly. Additionally, while the *.roblox.com wildcard domain is our primary focus, any findings directly involving Roblox's internal APIs, as distinct from web domain vulnerabilities, will be considered out-of-scope for this assessment. Our exploration will strictly adhere to the boundaries outlined in Roblox's official bug bounty program guidelines.

Scanning Limitations:
Rate Limiting: To prevent IP address blocking or banning due to aggressive scanning, the scanning activities will be rate-limited according to the guidelines provided by Roblox. This entails configuring automated vulnerability scanners to perform at a reduced speed, thereby minimizing the risk of triggering anti-scanning defenses.

Scheduling Scans: Scans will be scheduled during off-peak hours, if suggested by Roblox, to minimize the impact on the live environment. This is a common courtesy provided to ensure that the testing does not degrade service performance for users.

Confidentiality: Our team commits to the highest standards of confidentiality with regard to any vulnerabilities discovered during the assessment. All findings will be reported exclusively through the HackerOne platform, in line with Roblox's disclosure policies. No details of vulnerabilities will be disclosed to any third parties prior to an official acknowledgment or authorization from Roblox. Data integrity and security will be maintained throughout the project, with all sensitive information securely encrypted and stored, ensuring that it remains confidential and intact.

Project Strategy:

Enumeration Phase with Business Logic Assessment (Week 3)

Objective:

To systematically uncover and document both technical vulnerabilities and business logic flaws within the Roblox application, ensuring comprehensive adherence to the guidelines provided by their bug bounty policy.

Approach:

Subdomain Discovery:

Objective: Systematically identify all the subdomains associated with the *.roblox.com wildcard domain to uncover potential security vulnerabilities.

Method: Deploy a series of automated tools designed for comprehensive subdomain enumeration.

Rationale: A thorough subdomain discovery phase is essential to ensure that no part of the domain space is overlooked during the security audit.

DNS Enumeration:

Objective: Verify the existence, configuration, and properties of each subdomain to assess their security posture and identify misconfigurations.

Method: Perform detailed DNS queries and document the findings for each subdomain.

Rationale: DNS enumeration can reveal vital information about the infrastructure that may point to potential security weaknesses.

Business Logic Assessment:

Objective: Identify vulnerabilities arising from the application's business logic that could be exploited to perform unauthorized actions, bypass security measures, or manipulate application flows in unintended ways.

Method: Conduct scenario-based testing tailored to the application's core functionalities, focusing on areas like user input handling, authentication flows, and state management. Utilize threat modeling to predict and test potential misuse cases specific to the Roblox platform.

Rationale: Business logic vulnerabilities often stem from legitimate features being used in malicious or unintended ways. Understanding the intended use and flow of the application is crucial for identifying such vulnerabilities, which might not be apparent through automated scanning alone.

Documentation:

Objective: Create a detailed and organized record of all discovered subdomains and their DNS configurations to facilitate further security analysis.

Method: Maintain an up-to-date repository of documentation that includes the list of subdomains, their DNS records, and any pertinent information collected during the enumeration process.

Rationale: Proper documentation ensures that the security assessment is methodical and that findings are traceable and actionable.

Group Skills Utilization:

Muchun Wan (XSS Attacks):

Role: Leads the subdomain discovery phase, applying his knowledge in web application security.

Skills: His expertise in XSS vulnerabilities will guide the team in identifying subdomains that are more likely to be susceptible to such attacks, particularly those that involve user input and display.

Contribution: Muchun's ability to recognize and craft XSS payloads assists in prioritizing which subdomains to focus on for in-depth XSS testing.

Benelyon Choo (Session Attacks):

Role: Assists in DNS enumeration with a slight pivot towards session security.

Skills: With his specialization in session-based vulnerabilities, Benelyon's input is crucial in identifying subdomains that might have weak session management and authentication mechanisms.

Contribution: His network security background complements the DNS enumeration by focusing on the security of session tokens and cookies as they traverse through the various subdomains.

Pyae Sone Soe Moe (Database Attacks):

Role: Validates the active status of subdomains and contributes to the meticulous process of documentation.

Skills: His proficiency in database security, especially SQL injection, is valuable in recognizing which subdomains might interact with the database backend in an insecure manner.

Contribution: Pyae's attention to detail ensures that all documentation is accurate and comprehensive, capturing the nuances necessary for subsequent vulnerability assessment stages.

CTF Training Phase (Week 4 to Week 5)

Objective: To enhance the team's practical skills in identifying, exploiting, and mitigating web security vulnerabilities through Capture The Flag (CTF) exercises, specifically focusing on scenarios that resemble potential security issues within the Roblox platform.

Approach

- **Selection of CTF Platforms:** Choose online CTF platforms that offer challenges in web security, database attacks, and session management vulnerabilities. Platforms like Hack The Box, CTFd, and OverTheWire are recommended for their diverse range of challenges and learning resources.
- **Team Collaboration Exercises:** Organize internal CTF sessions where team members can collaborate on solving complex challenges. This fosters teamwork and allows members to share their specialized knowledge in real-time problem-solving scenarios.

- **Focused Training on XSS, Session, and Database Security:** Tailor the CTF challenges to include exercises on cross-site scripting (XSS) attacks, session hijacking, and SQL injections. These are directly relevant to the team members' roles and the project's focus areas.
- **Debrief and Learn:** After each CTF session, conduct a debriefing meeting to discuss the challenges, solutions, and learning points. This will help in consolidating the knowledge gained and applying it to the project strategy.

Group Skills Utilization

- **Muchun Wan:** Will lead the selection of XSS-related challenges, applying his expertise to guide the team in identifying and mitigating XSS vulnerabilities.
- **Benelyon Choo:** Focuses on challenges involving session management and security, sharing insights on protecting against session attacks.
- **Pyae Sone Soe Moe:** Curates database-related challenges, offering his expertise in preventing SQL injections and ensuring database security.

Environment Setup Phase (Week 6)

Objective: To establish a secure, controlled, and versatile testing environment that replicates the Roblox platform's critical components, allowing for safe and effective vulnerability testing.

Approach

- **Virtual Private Network (VPN):** Set up a VPN to secure the testing environment, ensuring all communications are encrypted and isolated from external networks.
- **Virtual Machines (VMs):** Deploy VMs to simulate the Roblox web and database servers. Each team member will have dedicated VMs to test different attack vectors without interfering with each other's work.
- **Docker Containers:** Use Docker containers for setting up isolated environments for specific applications or services, allowing for rapid deployment and testing of individual components.
- **Security Tools Installation:** Equip the VMs with the necessary security tools and software for enumeration, vulnerability scanning, and exploitation phases. This includes tools mentioned in the report, like OWASP ZAP, Nessus, Burp Suite, and Metasploit.
- **Test Data Generation:** Generate synthetic data that mimics the structure and type of data used by Roblox. This ensures realistic testing scenarios while adhering to data privacy and security regulations.

Group Skills Utilization:

- **Muchun Wan:** Oversees the setup of web application testing environments, ensuring they are configured for comprehensive XSS testing.
- **Benelyon Choo:** Configures network security settings, focusing on creating a secure communication channel for session testing.
- **Pyae Sone Soe Moe:** Prepares the database environments, emphasizing security configurations that prevent SQL injection and other database-related attacks.

Vulnerability Scanning Phase (Week 7)

Objective: Identify potential vulnerabilities in the subdomains using automated tools.
Approach:

- **Automated Scanning**: Implement vulnerability scanners to identify potential issues.
- **Preliminary Analysis**: Assess scan results to determine false positives and prioritize findings.
- **Prioritization**: Highlight vulnerabilities by severity, impact, and exploitability.

Group Skills Utilization:

Benelyon Choo oversees the configuration and operation of scanning tools.
Muchun Wan and **Pyae Sone Soe Moe** analyze preliminary results, with **Pyae** focusing on correlating findings with known exploits and vulnerabilities.

Manual Testing and Exploitation Phase (Week 8 to Week 9)

Objective: To manually verify and exploit confirmed vulnerabilities to assess their impact on the Roblox platform, focusing specifically on cross-site scripting (XSS) attacks, session attacks, and database attacks.

Approach:

- Manual Verification: Utilize manual penetration testing techniques to verify vulnerabilities discovered during the automated scanning phase. This includes crafting custom payloads and manually injecting them to test the application's response.
- Exploitation: Ethically exploit verified vulnerabilities to understand their potential impact on the Roblox platform. All exploitation will be conducted within a controlled environment to ensure no actual harm.
- Ethical Considerations: Strictly adhere to ethical hacking guidelines and the rules of engagement as outlined by Roblox's bug bounty program. Ensure all testing is non-disruptive and respects user privacy and data integrity.

Group Skills Utilization

- **Muchun Wan (XSS Attacks):**
  - **Role:** Takes the lead on testing for XSS vulnerabilities across identified subdomains, applying his in-depth knowledge of web application security.
  - **Skills:** Expertise in crafting and deploying various types of XSS payloads to test for both reflected and stored XSS vulnerabilities.
  - **Contribution:** Muchun's insights into advanced XSS techniques will guide the team in pinpointing and documenting XSS vulnerabilities, enhancing the security assessment's depth and breadth.
- **Benelyon Choo (Session Attacks):**
  - **Role:** Focuses on identifying and exploiting weaknesses in session management and authentication mechanisms.
  - **Skills:** Specializes in uncovering vulnerabilities such as session hijacking, fixation, and token manipulation.

    - **Contribution:** By simulating session attacks, Benelyon will assess the robustness of session management across the Roblox platform, providing critical insights into potential security gaps.
- **Pyae Sone Soe Moe (Database Attacks):**
    - **Role:** Leads the effort to test for vulnerabilities that could lead to database exposure or manipulation, such as SQL injection.
    - **Skills:** Proficient in testing for SQL injections, NoSQL injections, and other database-related vulnerabilities using both automated tools and manual testing techniques.
    - **Contribution:** Pyae's detailed approach to database security will help identify potential avenues for unauthorized data access or loss, significantly contributing to the project's overall security assessment.

Reporting Phase (Week 10)
Objective: Produce comprehensive reports for vulnerabilities with reproducible steps.
Approach:

- **Report Writing**: Document vulnerabilities with clear steps, impact assessment, and remediation recommendations.
- **Peer Review**: Internally review reports for accuracy and completeness.
- **Submission**: Submit thorough reports through HackerOne by the deadline.

Group Skills Utilization:

Pyae Sone Soe Moe leads the initial report drafting, leveraging strong organizational and documentation skills.
Muchun Wan and **Benelyon Choo** review the technical content, adding insights and ensuring clarity of the reproduction steps.
All members participate in the final review to ensure quality before submission.

Part 3: Infrastructure/Testing Environment

Project Infrastructure:

The success of our Roblox Wildcard Domain Security Project hinges on a robust and secure infrastructure tailored to support our testing tasks effectively. The infrastructure design aligns with our project strategy, enabling a seamless transition through the Enumeration, Vulnerability Scanning, Manual Testing and Exploitation, and Reporting Phases. Our choices are justified based on previous exercises, established best practices, and case studies from reputable sources within the cybersecurity community.

Computer/Network Requirements

- **Powerful Workstations:** High-performance computers with ample RAM and multi-core processors are essential to handle the intensive tasks of automated scanning and data processing. This specification is vital for running tools like OWASP ZAP and Nessus efficiently, which we have successfully utilized in past assessments.

- **Isolated Testing Environment:** A segregated network segment or virtual environment will ensure that our testing does not impact any live environments and protects our systems. This approach was effective during our practice exercises simulating an attack on a test network, as detailed in the DEF CON 27 CTF Qualifiers.

- **Secure Storage:** Encrypted storage solutions for sensitive data gathered during testing, ensuring compliance with confidentiality requirements and mirroring the practices recommended by the SANS Institute.

Tools

- **Subdomain Enumeration Tools:** Tools like Sublist3r and Amass will be used for subdomain discovery. These tools have been selected for their comprehensive database sources and DNS enumeration capabilities, aligning with our strategy's Enumeration Phase.

- **Vulnerability Scanners:** Nessus and Burp Suite will serve as our primary vulnerability scanners. Nessus provides a broad range of checks against known vulnerabilities, which is crucial for our initial scanning phase. Burp Suite's active scanning and manual testing features will be invaluable during the Manual Testing and Exploitation Phase. Both tools have been instrumental in our previous project, where we successfully identified and mitigated critical vulnerabilities.

- **Penetration Testing Frameworks:** Metasploit will be used for the exploitation and verification of vulnerabilities. Its extensive exploit database and the ability to customize exploits make it ideal for our Manual Testing Phase.

Tools for XSS Attacks Testing

XSS Attack Testing Tools: For the critical task of identifying and exploiting XSS vulnerabilities, we will utilize a suite of specialized tools:

- **OWASP ZAP:** The Zed Attack Proxy (ZAP) is an open-source web application security scanner. It's particularly effective for discovering XSS vulnerabilities as it includes advanced fuzzing and injection capabilities. Muchun Wan will employ ZAP's active scan and spider features to automate the search for XSS points.

- **XSSer:** This tool is specifically designed to detect and exploit XSS vulnerabilities. It automates the process of detecting cross-site scripting flaws and can generate various types of payloads to test the robustness of web applications against XSS attacks.

- **Burp Suite:** Known for its comprehensive testing environment, Burp Suite will be used to manually test for XSS vulnerabilities. The intruder and repeater tools allow for precise control over the injection of payloads and analysis of the application's response.

- **Custom Scripts:** In addition to established tools, Muchun Wan will write custom scripts to automate the testing process further. These scripts will be used to automate the injection of payloads and the gathering of evidence when a vulnerability is found.

Browser Developer Tools: Modern browsers come with powerful developer tools, and they will be used for manually testing XSS vulnerabilities by modifying inputs and observing how scripts are executed.

XSS Payload Lists: We will reference comprehensive XSS payload lists from trusted sources like PayloadsAllTheThings and the OWASP XSS Payloads repository to ensure a wide coverage of potential XSS patterns and filter bypasses.

Code Review Tools: Static application security testing (SAST) tools like SonarQube will also be employed to review the code for potential XSS vulnerabilities, a process that complements dynamic testing by looking at the application source code.

Tools for Session Attacks

- **Burp Suite:** This integrated platform provides a range of tools for web application security testing. Its session-handling capabilities and the ability to customize requests and responses make it ideal for testing session management vulnerabilities. Benelyon can use the Burp Suite Intruder and Repeater tools to automate custom attacks on session tokens and identify weaknesses in session handling.

- **OWASP ZAP (Zed Attack Proxy):** Similar to Burp Suite, ZAP offers session management testing features. It can be used to identify when session tokens are not properly invalidated upon logout or when they are vulnerable to fixation attacks. The session management tester component allows for automated testing of session strength and management policies.

- **BeEF (Browser Exploitation Framework):** BeEF focuses on the web browser, making it an excellent tool for testing session hijacking through client-side attacks. Benelyon can use BeEF to craft cross-site scripting (XSS) payloads that, when executed, demonstrate how an attacker could leverage XSS vulnerabilities to hijack sessions.

- **Wireshark:** This network protocol analyzer can capture and interactively browse the traffic running on a computer network. It is useful for sniffing out cookies and session tokens transmitted over unencrypted connections, allowing Benelyon to analyze how session information is handled and transferred across the network.

- **Mitmproxy:** An interactive man-in-the-middle proxy for HTTP and HTTPS traffic, mitmproxy allows for the inspection, modification, and replay of web traffic. It can be particularly useful in testing for session vulnerabilities by acting as a man-in-the-middle to capture and manipulate session tokens.

- **Custom Scripts:** Writing custom scripts (in Python, Ruby, or another scripting language) can be particularly effective for automating specific session attack vectors. Benelyon could develop scripts to automate the testing of session management policies, token entropy, and the effectiveness of token invalidation logic.

Tools for Database Attacks

- **SQLMap:** SQLMap is an open-source penetration testing tool that automates the process of detecting and exploiting SQL injection flaws and taking over database servers. It has a powerful detection engine and offers a wide range of features for penetration testers to perform extensive database testing. Pyae can use SQLMap to identify SQL injection vulnerabilities in web applications and automate the exploitation process to demonstrate the potential impact.

- **NoSQLMap:** Tailored for testing NoSQL databases, NoSQLMap is a tool designed to audit and automate injection attacks on web applications using NoSQL databases. It supports various NoSQL databases like MongoDB, CouchDB, and others. Pyae can utilize NoSQLMap to identify misconfigurations and vulnerabilities in applications that use NoSQL databases.

- **DBPwAudit:** DBPwAudit is a database password auditing tool designed for penetration testers to perform password strength testing against databases. Pyae can use this tool to assess the strength of passwords used in database user accounts, helping to highlight weak passwords that could be exploited by attackers.

- **jSQL Injection:** jSQL Injection is a lightweight application for automatic SQL database injection. It is part of the OWASP list of testing tools and can be used to identify and exploit SQL injection vulnerabilities in web applications. Pyae can leverage jSQL Injection's GUI and automated capabilities to streamline the vulnerability discovery process.

- **Metasploit Framework:** While widely known for its broader exploitation capabilities, the Metasploit Framework includes modules specifically designed for attacking database services. Pyae can use Metasploit to exploit known vulnerabilities within database software, execute arbitrary SQL queries, and even pivot to further attacks on the network.

- **Custom Scripts:** Writing custom scripts using languages such as Python or Ruby can be highly effective for tailored attacks or when testing specific aspects of database

security. Pyae might develop scripts to automate the discovery of SQL injection points, blind SQL injection testing, or to exploit specific vulnerabilities found during the assessment.

Justification

The selected infrastructure and tools support our project strategy by providing the necessary capabilities for each phase. From efficient enumeration to thorough documentation, the infrastructure allows our team to identify, analyze, and report vulnerabilities in a secure, systematic, and efficient manner.