Research Proposal

Enhancing Authentication Security: A Python-Based System for Brute Force Attack Prevention

1. Research Summary

User authentication systems are essential for preventing unauthorized access, but the rise of the Internet and mobile apps has made it challenging to maintain security. For instance: technologies like complex passwords enhance security but reduce usability, thus leaving many systems vulnerable to attacks such as brute force (Wang, et al., 2021).

Brute force attacks are an evolving threat where criminals attempt to guess usernames and passwords (user's log-in credentials), with success rates increasing due to victims often using easily guessed information like names or common passwords such as '123456' or 'password' (Information Commissioner's Office, 2024). Despite being easy to detect, brute force attacks are difficult to prevent and continue to exploit system vulnerabilities, especially when users choose weak or common passwords or use vulnerable login systems (S, et al., N.D.).

This research is driven by the need to explore and assess current methods used to prevent brute force attacks in Python-based login systems. The main research question guiding this study is: ***What are the most effective methods to prevent or mitigate brute force attacks in Python-based login systems?*** Additional questions for further exploration include:

1. What are the common vulnerabilities in Python-based login systems that make them susceptible to brute force attacks?
2. What are the advantages and limitations of current brute force prevention mechanisms implemented in Python-based systems?
3. How can Python libraries and built-in features be utilized to enhance the security of login systems against brute force attacks?
4. How can defence mechanisms be integrated into Python-based login systems to mitigate brute force attacks without negatively affecting user experience?

The study aims to evaluate existing solutions' effectiveness and usability, identify improvements, and develop efficient approaches for organizations of all sizes, including those with limited resources.

The research problem arises from the growing prevalence of brute force attacks, despite advancements in cybersecurity measures (The Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC), 2024). Smaller organizations lacking the financial and technical resources for advanced security, are particularly vulnerable (Alwaisi & Soderi, 2024). By focusing on affordable and accessible solutions, this research aims to improve login security without relying on costly third-party services.

The rationale behind this research is clear: With over 38 million brute force attacks detected between July and September 202 (Communications Authority of Kenya, 2024), there is an urgent need for accessible and effective solutions. This project aims to provide practical, implementable solutions for smaller organizations, enhancing

authentication security while maintaining user convenience, using Python's simplicity and versatility.

This research aligns with the Secure System Design and Architecture category of CyBOK, specifically focusing on the Authentication and Authorization knowledge area (Gollmann, 2021). This aligns with the core objectives of the study, which aim to assess, improve, and develop better authentication methods for mitigating brute force attacks (CyBOK, 2021).

Implementation of enhanced brute force prevention techniques in Python-based login systems can effectively mitigate unauthorized access while maintaining usability for legitimate users.

The aims and objectives of this research are as follows:

1. To assess the effectiveness of current methods used to prevent brute force attacks in Python-based login systems.
2. To identify the limitations of existing solutions and explore potential areas of improvement.
3. To develop a Python-based solution that can be used by small organizations to enhance authentication security.
4. To evaluate the usability and effectiveness of the proposed solution, ensuring that it provides a balance between robust security and user convenience.
5. To propose optimal solutions for organizations with limited resources.

Ultimately, this research aims to contribute to a more secure, user-friendly authentication process, particularly for organizations with limited resources.

2. Methodology

This research will adopt a mixed-methods approach to evaluate existing solutions (quantitative), understand system limitations and usability (qualitative), and develop practical solutions through technical development and testing (Zou & Xu, 2023). The focus will be on evaluating the effectiveness of existing methods to prevent brute force attacks, as well as developing and testing a new solution aimed at improving security for Python-based login systems.

Research Methods and Procedures

The primary research methods used will be:

1. **Literature Review and Comparative Analysis**: A comprehensive literature review will be conducted to analyse current techniques for mitigating brute force attacks in authentication systems, focusing on Python-based solutions. This review will provide insights into:
    - Common vulnerabilities exploited by brute force attacks.
    - Existing solutions such as CAPTCHA, rate-limiting, hashing techniques, multi-factor authentication (MFA), and account lockout mechanisms.
    - Best practices for securing Python-based login systems

The aim is to assess their effectiveness, limitations, and usability, as well as directly address the research question.

2. **Python-Based Log-in System Design and Implementation**: Based on the findings of the literature review, the research will involve designing and implementing a Python-based prototype to mitigate brute force attacks. The solution will be based on Python libraries such as hashlib, time, and Flask (or other relevant tools), and will incorporate measures like rate-limiting, CAPTCHA, account lockouts, or progressive delays between login attempts.

3. **Simulation, Testing and Evaluation**: The Python prototype will be evaluated through simulated brute force attacks, with metrics like breach time, system performance, and mitigation effectiveness analysed to address the research question(s) without real-world interaction.

4. **Data Collection and Analysis:** Data will be collected from the simulation process, focusing on:

    - Number of blocked login attempts.
    - Response times for legitimate user logins.
    - System resource usage during attacks.

In this step, both quantitative and qualitative data will be collected:

- Quantitative Data: Metrics such as time to breach, failed login attempts before lockout, and system resource usage will be analyzed to compare the developed system with existing solutions.

- Qualitative Data: Feedback on usability, integration ease, and the security-convenience trade-off will assess the solution's user-friendliness.

Afterwards, quantitative analysis will objectively evaluate the performance data (e.g., attack success rates, lockout times) to analyse the effectiveness of security mechanisms, while qualitative analysis will interpret patterns and usability implications, ensuring a comprehensive understanding of the results (Zou & Xu, 2023).

5. **Usability Validation**: For validation, the research will employ a usability testing framework such as System Usability Scale (SUS) or heuristic evaluation. Metrics like task completion time, error rates, and satisfaction scores w ill ensure the solution balances security and usability.

6. **Ethical Considerations:** This study will not involve human participants directly but will ensure compliance with data protection laws (GDPR) in handling simulated data (Runeson & Höst , 2009). It will also ensure that simulated attacks do not impact real systems (Alfie, N.D).

Potential Issues, Limitations, and Challenges

Several potential issues and limitations may arise during the research process:

1. **Limited Scope of Testing**: The scope of the testing will be limited to simulated attacks in a controlled environment, which may not fully represent real-world

attack conditions. Brute force attackers may use more sophisticated techniques, making it difficult to simulate all attack vectors.

2. **Limited Simulations**: Simulated environments may not account for all real-world attack variations, which could limit the generalizability of findings (Palmieri, 2013).

   Mitigation: The testing scenarios will be designed to include a wide range of brute force attack techniques to ensure robustness.

3. **Resource Constraints**: Developing and testing a comprehensive system may be time-consuming (Özeren , 2024).

   Mitigation: The project will focus on implementing a manageable set of security measures, prioritizing those most relevant to smaller organizations.

4. **Data Validity**: Results from simulated tests might differ in real-world settings due to dynamic factors such as network configurations and user behaviour (Bailey, et al., 2013).

   Mitigation: The analysis will clearly indicate the limitations of simulation-based findings and suggest further real-world testing for future research.

5. **Technical Limitations and Scope of the Study**: The research will be focused on Python-based systems, thus limiting the findings' applicability to other languages or platforms. (Özeren , 2024).

Despite these challenges, the chosen methodology remains most appropriate as it provides a clear, systematic approach to evaluating existing solutions, developing new ones, and ensuring affordable, efficient and practical applicability.

3. Key Literature

This section provides an overview of key literature on brute force attack prevention in Python-based login systems.

Literature Review Skeleton

1. **Introduction to authentication systems and Brute Force Attacks**
    - Overview of common authentication mechanisms and brute force attack.
2. **Brute Force Attacks and their impact on Authentication Systems**
    - Types of brute force attacks and their impact.
3. **Countermeasures and Mitigation Strategies**
    - Techniques such as rate limiting, CAPTCHA, and multifactor authentication (MFA), etc.
4. **Programming Solutions for Security**
    - Role of Python in cybersecurity applications.
5. **Evaluation of Existing Solutions**
    - Challenges and Limitations of Brute Force Mitigation Methods

- Case studies and analysis of current implementations.

6. **Conclusion**

    - Summary of findings and gaps in research.

4. Human Participants

This research does not involve human participants, focusing instead on evaluating and improving brute force attack prevention in Python-based login systems through simulated tests, thus avoiding ethical concerns related to human participants.

The research will be conducted online, with data collection and system testing done remotely. All tests will be performed in a controlled, isolated environment to ensure system security and integrity (Özeren , 2024).

5. Work Packages and Timeline

To complete this research, the project is divided into several work packages, following a clear timeline from week 9 (December 16, 2024) to week 28 (May 19, 2025), with sufficient time allocated for each phase.

1. **Work Package 1: Literature Review (Weeks 9-11)**

    - **Objective**: Conduct an extensive review of existing literature on brute force attacks and their preventions, and Python-based login systems.

- **Activities**: Identify key research papers, articles, and technical reports. Summarize relevant information and critically analyse existing solutions.
- **Milestone**: Completion of the literature review by the end of week 11.

2. **Work Package 2: Research Design and Planning (Weeks 12-14)**
    - **Objective**: Finalize the research methodology and plan the approach for testing brute force prevention techniques in Python-based login systems.
    - **Activities**: Define the tools, libraries, and frameworks (e.g., Flask, Django) to be used. Establish the criteria for evaluating the effectiveness of different prevention methods.
    - **Milestone**: Final research design completed by the end of week 14.

3. **Work Package 3: System Design and Implementation (Weeks 15-20)**
    - **Objective**: Develop a Python-based authentication system with integrated brute force prevention measures.
    - **Activities**: Implement various brute force prevention techniques, such as rate limiting, CAPTCHA, and account lockout. Configure the environment and libraries.
    - **Milestone**: Fully functional login system ready for testing by the end of week 20.

4. **Work Package 4: Testing and Evaluation (Weeks 21-23)**

- **Objective**: Conduct automated tests to evaluate the effectiveness of the brute force prevention measures in the Python-based login system.
- **Activities**: Simulate brute force attacks and record the system's response to each attack. Measure the impact on system performance and security.
- **Milestone**: Testing completed by the end of week 23.

5. **Work Package 5: Analysis and Discussion (Weeks 24-26)**
    - **Objective**: Analyse the test results and discuss the effectiveness of each prevention technique.
    - **Activities**: Compare the performance and security outcomes of the implemented techniques. Identify potential improvements.
    - **Milestone**: Complete analysis and discussion by the end of week 26.

6. **Work Package 6: Final Report Writing (Weeks 27-28)**
    - **Objective**: Compile the research findings into a comprehensive dissertation.
    - **Activities**: Write, proofread and edit the dissertation.
    - **Milestone**: Finalise dissertation by the end of week 28.

7. **Work Package 7: Final Submission (Week 28)**
    - **Objective**: Submit the dissertation.
    - **Milestone**: Submit the dissertation by the end of week 28.

Gantt Chart

Below is a Gantt chart created using Visual Paradigm Online, that visually represents the timeline and work packages for the project.

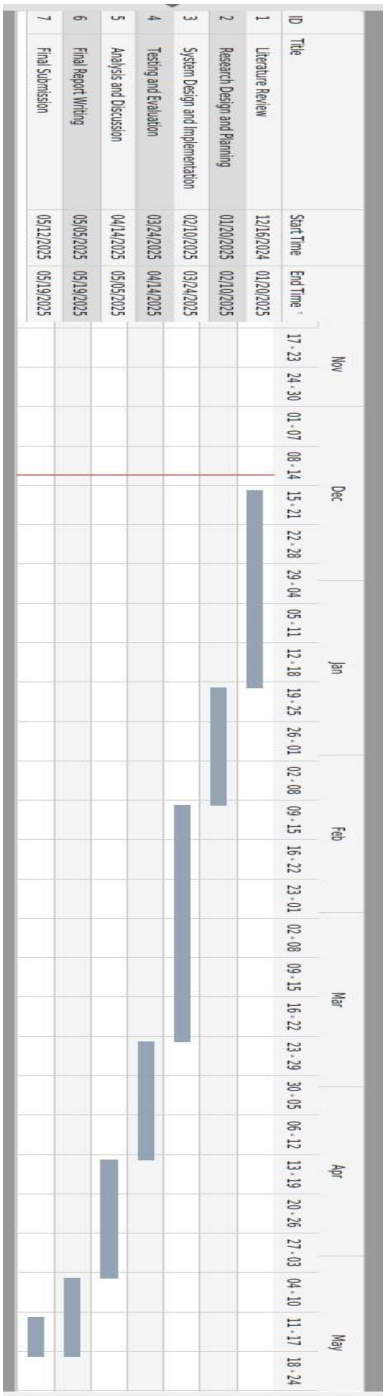

Figure 1: Gantt chart for the project timeline

Artefacts to be Produced

By the end of the project, the following artefacts will be produced:

1. **Python-based Login System**: A functional Python-based login system incorporating brute force prevention techniques.
2. **Dissertation**: A comprehensive research report, including the literature review, research methodology, results, analysis, and conclusions.

References

Alfie, N.D. *What ethical considerations are there in simulation design and use?.* [Online]
Available at: https://www.tutorchase.com/answers/ib/computer-science/what-ethical-considerations-are-there-in-simulation-design-and-use
[Accessed 07 December 2024].

Alwaisi, Z. & Soderi, S., 2024. *Towards Robust IoT Defense: Comparative Statistics of Attack Detection in Resource-Constrained Scenarios.* [Online]
Available at: https://arxiv.org/html/2410.07810v1
[Accessed 04 December 2024].

Bailey, M. et al., 2013. *Applying Ethical Principles to Information and Communication Technology Research: A Companion to the Menlo Report.* [Online]
Available at: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.dhs.gov/sites/default/files/pu

blications/CSD-MenloPrinciplesCOMPANION-20120103-r731_0.pdf

[Accessed 13 December 2024].

Communications Authority of Kenya, 2024. *Cybersecurity Report,* Nairobi: The National KE-CIRT/CC.

CyBOK, 2021. *Knowledgebase1_1.* [Online]

Available at: https://www.cybok.org/knowledgebase1_1/

[Accessed 27 March 2022].

E. et al., N.D.. *Blocking Brute Force Attacks.* [Online]

Available at: https://owasp.org/www-community/controls/Blocking_Brute_Force_Attacks

[Accessed 04 December 2024].

Gollmann, D., 2021. *Authentication, Authorisation & Accountability Knowledge Area Version 1.0.2.* [Online]

Available at: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.cybok.org/media/downloads/Authentication_Authorisation_Accountability_v1.0.2.pdf

[Accessed 4 December 2024].

Information Commissioner's Office, 2024. *Brute force attacks.* [Online]

Available at: https://ico.org.uk/about-the-ico/research-reports-impact-and-evaluation/research-and-reports/learning-from-the-mistakes-of-others-a-retrospective-review/brute-force-attacks/

[Accessed 3 December 2024].

National Cyber Security Centre, 2018. *GDPR security outcomes.* [Online]
Available at: https://www.ncsc.gov.uk/guidance/gdpr-security-outcomes
[Accessed 20 July 2022].

Özeren , S., 2024. *Breach and Attack Simulation vs. Security Validation.* [Online]
Available at: https://www.picussecurity.com/resource/blog/breach-and-attack-simulation-vs-security-validation
[Accessed 08 December 2024].

Palmieri, M., 2013. *System Testing in a Simulated Environment.* [Online]
Available at: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.diva-portal.org/smash/get/diva2:613817/FULLTEXT01.pdf
[Accessed 07 December 2024].

Runeson , P. & Höst , M., 2009. Guidelines for conducting and reporting case study research in software engineering. *Empirical Software Engineering,* Volume 14, pp. 131-164.

The Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC), 2024. *Annual Cyber Threat Report 2023-2024,* Australia: The Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC).

Wang, X., Yan, Z., Zhang, R. & Zhang, P., 2021. Attacks and defenses in user authentication systems: A survey. *Journal of Network and Computer Applications,* 15 August.Volume 188.

Zou, P. X. W. & Xu, X., 2023. *Research Methodology and Strategy: Theory and Practice.* 1st ed. West Sussex: John Wiley & Sons.

Ethical Approval

This section outlines the ethical considerations guiding the research, ensuring adherence to ethical principles and guidelines. Since the research does not involve human participants, issues like consent, do not apply. However, it will address relevant concerns related to data handling, security, and other ethical aspects of the work.

1. Consent

As the research does not involve human participants, informed consent is not required.

2. Right to Withdraw

The project does not involve human participants, the right to withdraw does not apply.

3. Confidentiality

Confidentiality is a critical concern when dealing with any data, even if it is publicly available or synthetic (National Cyber Security Centre, 2018). For this project, I will ensure that all data used during the testing phases of the system (such as login credentials or attack attempts) is entirely fictional or anonymized.

- **Data Storage**: Any data created during the simulation tests (e.g., login attempts, response times, or error logs) will be stored securely.
- **Anonymity**: All test data will be anonymized, and no personal identifiers or sensitive information will be stored or analysed. Simulated usernames and

passwords will be randomly generated and used for testing purposes only (Bailey, et al., 2013).

- **Data Sharing**: If any results from the research are shared (e.g., via reports or publications), all data will be aggregated and anonymized to ensure that no individuals can be identified from the data (Bailey, et al., 2013).

4. **Harm**

As the research does not involve human participants, there is minimal risk of harm to individuals.

5. **Data Access, Storage, and Security**

In compliance with GDPR and best practices for data privacy and security, I will ensure that all data generated throughout the research is handled with care:

Compliance with GDPR and transparency: As no personal data will be collected, GDPR concerns are minimal. I will ensure that any publicly available data complies with relevant licensing and usage conditions, and all data will be anonymized and publicly accessible (Bailey, et al., 2013). This will be verified before using any datasets or third-party tools.

To ensure that the system's testing does not inadvertently lead to misuse or negative consequences, I will follow these measures to minimize any potential risks (Bailey, et al., 2013):

- **Ethical Testing**: All testing of the Python-based login system will be conducted in a controlled and secure environment.

- **Simulated Attacks**: The brute force attack simulations will be conducted in an environment that does not interact with any live servers, websites, or real user data. This ensures that no unintended harm comes to any external systems or services.
- **System Safety**: I will ensure that all testing is done within the bounds of ethical cybersecurity practices, ensuring no harm is caused to any systems, organizations, or individuals.

6. Other Issues

Since this research does not involve human participants or vulnerable groups, there are no additional ethical concerns related to this project.

Therefore, I do not foresee any significant ethical dilemmas arising during the execution of the study. Nonetheless, I will remain committed to adhering to ethical best practices, including transparency in reporting and the secure handling of any data used.

Risk Assessment

Q1. NO

N/A

Q2. YES

Potential Risks to Researchers and Risk Management Procedures

1. **Risk of Cyber Threats**: Since the project involves working with authentication systems and testing brute force prevention methods, there is a potential risk of exposure to malicious code or tools during testing. This could lead to unintended system vulnerabilities or compromise of the research environment (Bailey, et al., 2013).

    Risk Management Procedures:

    - Conduct all testing in isolated, secure virtual environments to prevent any unintentional exposure to external systems.
    - Use only verified tools and frameworks, ensuring they come from reputable sources.
    - Implement regular system scans and updates to mitigate vulnerabilities.

2. **Data Security and Compliance**: Handling sensitive data during system testing may present risks if the data is improperly managed or inadvertently exposed (National Cyber Security Centre, 2018).

    Risk Management Procedures:

    - Utilize dummy or anonymized datasets for all testing to avoid handling real user data.
    - Adhere to GDPR guidelines and ensure all systems and practices comply with data protection policies.

3. **Technical Failures**: Hardware or software failures during development and testing could disrupt progress or lead to data loss (Bailey, et al., 2013).

    Risk Management Procedures:

    - Regularly back up project data and source code to a secure repository.
    - Maintain contingency plans, including access to alternative tools and systems, to minimize downtime in case of failures.
    - Test the login system and brute force mitigation techniques will be conducted within isolated virtual environments to ensure that any accidental breaches or weaknesses do not affect live systems or external services.

- Ensure all development and testing tools, including Python libraries and packages, are sourced from trusted platforms. I will also verify that all tools are updated and free from vulnerabilities.

4. **Time Constraints and Burnout**: Balancing research with other commitments may lead to stress or fatigue, especially during critical phases of the project (Bailey, et al., 2013).

   Risk Management Procedures:

   - Develop and adhere to a clear project timeline with realistic milestones.
   - Take regular breaks and ensure a balance between work and personal well-being.

5. **Legal and Ethical Compliance:** Any oversight in complying with legal or ethical requirements could lead to reputational risks or project delays (Bailey, et al., 2013).

   Risk Management Procedures:

   - Regularly review and adhere to the University of Essex Online ethical guidelines and ensure full compliance with approval processes.

- Consult with the dissertation supervisor and ethics committee as needed to clarify any uncertainties.

By proactively addressing these risks and implementing robust management procedures, the researcher will minimize potential threats and ensure the successful and secure execution of the project.

Q3. YES

Potential Reputational Risks and Risk Management Procedures

1. **Association with Cybersecurity Testing**: The project involves testing methods to mitigate brute force attacks, which may include working with security tools and scripts that could be misconstrued as engaging in or enabling malicious activities (Bailey, et al., 2013).

    Risk Management Procedures:

    - Ensure all testing is conducted in controlled, isolated environments with dummy data, clearly documenting the ethical and academic purpose of the research.
    - Use only legitimate tools and frameworks that align with industry standards and avoid any software or methodologies associated with unethical hacking practices.

- Explicitly clarify in project documentation that the research adheres to ethical guidelines and aims to strengthen cybersecurity, aligning with the university's values.

2. **Data Breach or Non-Compliance with Regulations**: A failure to comply with GDPR or ethical data management policies could reflect poorly on the university (National Cyber Security Centre, 2018).

   Risk Management Procedures:

   - Follow GDPR-compliant data handling procedures throughout the project.
   - Avoid the use of real-world sensitive data by exclusively utilizing anonymized or synthetic datasets.
   - Regularly consult the university's data protection guidelines to ensure full compliance.

3. **Misinterpretation of Research Outcomes**: If the results of the research are misinterpreted or misused by external parties, it could impact the university's reputation as an institution supporting ethical research.

   Risk Management Procedures:

- Clearly communicate the scope, limitations, and ethical intent of the research in all documentation and dissemination.
- Avoid publishing detailed information that could inadvertently guide malicious actors, focusing instead on broader recommendations and solutions.

By addressing these potential risks with robust management procedures, the research will uphold the integrity of the University of Essex Online while contributing positively to the field of cybersecurity.

Q4. NO

Q5. NO

All relevant ethical considerations have been thoroughly addressed, including informed consent, data privacy, confidentiality, risk minimization, and compliance with ethical research guidelines such as GDPR. The project involves no direct interaction with human participants or vulnerable groups, and all testing will occur within a secure, controlled environment using synthetic or anonymized data.

Should any unforeseen ethical concerns arise during the course of the research, they will be promptly reported to the appropriate university authorities and addressed in line with the University of Essex Online's ethical policies.