**MODEL INSTITUTE OF ENGINEERING AND TECHNOLOGY**

**Project Report**

**PASSWORD GENERATOR BOT**

**Business Process Automation with RPA lab**

**Name: Vansh Gupta Faculty In-Charge**

**Roll No.: 2022a1R059 Asst. Prof Ms. Vani Malgar**

**Course: CSE (A2)**

**Semester: 2nd**

**Session: 2022-26**

**Table of Contents Page No.**

Abstract 03

Introduction 04

Objective 04

Problem Statement 05

Methodology 05

UiPath Packages and Activities Used 05-06

Conclusion 06

Future Enhancement 06

Detailed Process 07

Complete Workflow 08

Results 09

References 10-11

**Abstract**

In today's digital landscape, the need for strong and secure passwords is paramount to protect sensitive information and maintain data privacy. However, the manual creation of complex passwords that are both difficult to guess and resistant to cracking can be a challenging and time-consuming task for users. This research paper presents the development and implementation of a Password Generator, leveraging the capabilities of UiPath, a leading Robotic Process Automation (RPA) platform. The Password Generator automates the process of generating robust and secure passwords, eliminating the need for users to devise passwords themselves. By incorporating advanced algorithms and logic, the Password Generator generates random and unique passwords that are virtually impervious to brute-force attacks. The project not only simplifies the password creation process but also enhances overall security posture by ensuring consistent adherence to security best practices. The Password Generator offers customizable options, allowing users to specify password length, character combinations, and complexity requirements. The generated passwords meet the specified criteria and can be displayed to users or securely stored for future use. This research paper explores the methodology, technical details, and benefits of the Password Generator project, showcasing its effectiveness in empowering users to create secure passwords and bolster data security in today's digital world.

**Introduction**

* In today's digital world, maintaining strong and secure passwords is crucial to protect sensitive information and maintain data privacy. However, manually creating complex passwords that are difficult to guess and crack can be a time-consuming and challenging task. This is where a Password Generator comes to the rescue. A Password Generator is a powerful tool that automates the process of generating robust and secure passwords. It eliminates the need for users to come up with passwords on their own, ensuring that passwords are random, unique, and meet specific complexity requirements. With a password generator, users can specify the desired length of the password, including a combination of uppercase and lowercase letters, numbers, and special characters. The generator then uses sophisticated algorithms and logic to generate passwords that are virtually impossible to guess or crack through brute-force attacks. The Password Generator saves users from the hassle of remembering multiple passwords for different accounts. By generating unique passwords for each account, it enhances security and minimizes the risk of unauthorized access to personal or sensitive data. Not only does a password generator simplify the process of password creation, but it also significantly improves the overall security posture of individuals and organizations. By automating the generation of strong passwords, it ensures that security best practices are followed consistently. In this presentation, we will explore the implementation of a Password Generator using UiPath, a leading Robotic Process Automation (RPA) platform. We will delve into the workflow, technical details, and benefits of the Password Generator project, showcasing how it empowers users to create secure passwords.

**Objective**

The primary objective of this project is to create a UiPath bot that interacts with users through a password generator, presents a set of options, and executes the website. The specific objectives include:

* Design and develop a Password Generator using UiPath.
* Automate the process of generating strong and secure passwords.
* Explore the methodology and technical details of the Password Generator project.
* Investigate the customization options for password length, complexity requirements, and character combinations.
* Assess the integration capabilities of the Password Generator with other systems or password management tools.

**Problem Statement**

“The manual creation of complex and secure passwords is time-consuming and challenging, leading to weak password choices and increased vulnerability to unauthorized access and data breaches.”

**Methodology**

* **Identify Password Generation Requirements:** Begin by understanding the specific requirements for password generation, including desired password length, character combinations (uppercase, lowercase, numbers, special characters), and any additional complexity rules. This information will serve as the basis for developing the Password Generator.
* **Select a Robotic Process Automation (RPA) Platform:** Choose a suitable RPA platform, such as UiPath, which provides the necessary tools and capabilities for developing automation workflows. Consider factors like ease of use, compatibility with the desired password generation algorithm, and integration options with other systems.
* **Design the Password Generator Workflow:** Define the workflow of the Password Generator, outlining the logical steps involved in generating passwords. Consider factors like user input for password length and complexity, error handling, and storage of generated passwords. Create a flowchart or diagram to visualize the process.
* **Implement the Password Generator in UiPath:** Utilize the selected RPA platform, UiPath, to develop the automation workflow for the Password Generator. Use the platform's drag-and-drop interface and available activities to build the logic and incorporate the chosen password generation algorithm.
* **Test and Validate the Password Generator:** Conduct thorough testing of the Password Generator to ensure its functionality and adherence to the specified requirements. Test it with different inputs, including various password lengths and complexity settings, and verify that the generated passwords meet the desired criteria.
* **Enhance Security Measures:** Implement additional security measures, such as encryption of generated passwords during storage and transmission, to further safeguard sensitive information. Consider integrating secure password management tools or practices to assist users in securely storing and accessing their passwords.

**UiPath Packages and Activities Used**

The following Packages and Activities were used to develop the UiPath bot with AI capabilities:

* **UiPath Studio:** A platform for creating automation workflows.

**Open Browser:** In UiPath, the "Open Browser" activity is a built-in activity that allows you to launch and interact with a web browser within your automation workflow.

* **Type-Into: The** "Type Into" activity in UiPath is used to simulate keystrokes or input text into a target application or text field.
* **Open Browser:** Opens a URL through web browser.
* **Click:** Used to click on the elements for the clicking the elements you want to enter in website.
* **Get-Text:** It is used to extract the text over anywhere from the website.
* **Message box:** A message box, sometimes referred to as a dialog box or alert box, is a graphical user interface (GUI) element used to display important message.

**Conclusion**

In conclusion, the implementation of a Password Generator using UiPath provides an effective solution to the challenges faced in manually creating strong and secure passwords. The Password Generator automates the password creation process, generating random and complex passwords that are difficult to guess or crack. By simplifying the password creation process, promoting adherence to security best practices, and enhancing overall data security, the Password Generator empowers individuals and organizations to safeguard sensitive information and protect against unauthorized access. With its customization options, integration capabilities, and user-friendly interface, the Password Generator represents a significant step towards improving password security practices in today's digital landscape.

**Future Enhancements**

Enhanced Customization: Expand the customization options of the Password Generator to allow users to specify additional requirements such as dictionary word exclusions, exclusion of commonly used patterns, or specific character restrictions.

Multi-factor Authentication (MFA): Integrate the Password Generator with multi-factor authentication mechanisms to further strengthen the security of user accounts and ensure an additional layer of protection.

Password Strength Assessment: Implement a password strength assessment feature that evaluates the generated passwords and provides feedback to users on their strength and suggestions for further improvement.

Password Policy Integration: Integrate the Password Generator with existing password policies within organizations to ensure generated passwords adhere to specific corporate requirements, such as password expiration, complexity rules, and password history restrictions.

Secure Password Storage: Enhance the Password Generator to securely store and manage generated passwords, utilizing industry-standard encryption and storage protocols to protect against unauthorized access or data breaches.

Cross-Platform Integration: Extend the integration capabilities of the Password Generator to support a wide range of platforms, applications, and operating systems, allowing users to generate and manage passwords seamlessly across multiple devices and environments.

Machine Learning-based Password Generation: Explore the use of machine learning algorithms to improve the randomness and uniqueness of generated passwords, leveraging pattern recognition and predictive models to enhance password security.

User-Friendly Password Recovery: Develop a user-friendly password recovery mechanism that allows users to retrieve generated passwords securely in case of forgotten or lost passwords, while still maintaining the highest level of data privacy and security.

**Detailed Process to Develop This Bot**

1. Open UiPath Studio and create a new project.

2. Drag and drop a Sequence activity into the workflow.

3. Inside the sequence, add the open browser and enter the website https://delinea.com/resources/password-generator-it-tool.

4. After that add the option to data scraping.

5. After adding type into activity we have to enter the specific data to be targeted like the symbols and size of the password.

6. Then use the click activity on the “generate password” option.

7. Use the get text activity to extract the password from the browser.

8. Make it save a character “password”.

9. Add the activity name to the message box.

10. Make it display the above character password to display the password generated by the website.

11. Use Excel Scope activity.

12. Make an excel file name password to store the password that is generated by the website.

13. Use the write cell activity.

14. Give the cell location to store the password.

**1.**

**Workflow:**

**2.**

**A screenshot of a computer

Description automatically generated**

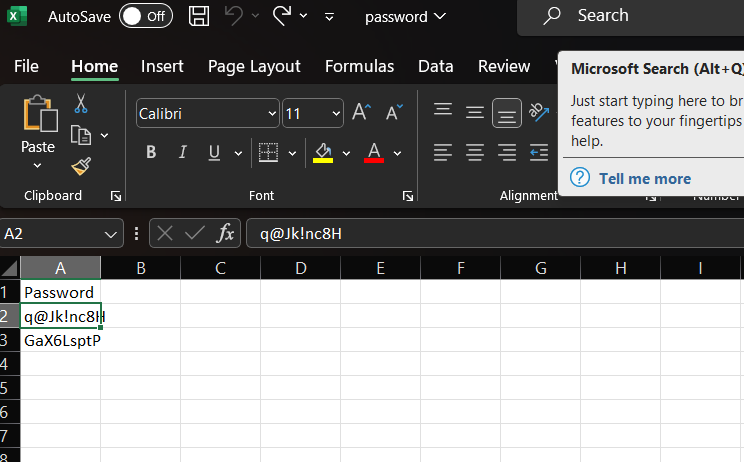
**
Description automatically generated with low confidenceA screenshot of a computer screen

Description automatically generated with medium confidence**

**3.**

A screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated

**3.**

**2.**

**1.**

**Output:**

**References:**

**Password Generation:**

* **NIST Special Publication 800-63B: Digital Identity Guidelines - This publication by the National Institute of Standards and Technology (NIST) provides guidelines and recommendations for secure password policies and generation.**

**(https://pages.nist.gov/800-63-3/).**

* **OWASP Password Storage Cheat Sheet - OWASP (Open Web Application Security Project) offers a comprehensive guide on secure password storage, including password generation techniques. (**<https://cheatsheetseries.owasp.org/cheatsheets/Password_Storage_Cheat_Sheet.html>**)**
* **Strong Password Generator - This online tool generates random, secure passwords based on user-defined criteria. It can be helpful for understanding different password generation techniques. (https://passwordsgenerator.net/).**
* **"Password Generation and Complexity" - This article from the SANS Institute discusses password generation and complexity, providing insights into best practices and considerations for creating strong passwords. (https://www.sans.org/security-awareness-training/ouch-newsletter/2018/password-generation-and-complexity).**

**Robotic Process Automation (RPA):**

* **UiPath Documentation - The official documentation provided by UiPath offers detailed information on using UiPath for RPA development, including tutorials and guides on workflow creation. (https://docs.uipath.com/).**
* **Automation Anywhere RPA - Automation Anywhere is another popular RPA platform. Their website provides resources, documentation, and tutorials on RPA implementation. (https://www.automationanywhere.com/).**
* **Blue Prism Developer Portal - Blue Prism is another leading RPA platform, and their developer portal provides resources and documentation for RPA development. (**<https://www.blueprism.com/developers/>**).**
* **"What is Robotic Process Automation (RPA)?" - This article by Automation Anywhere provides an overview of RPA, its benefits, and use cases. It can help you understand the fundamentals of RPA.**

**(https://www.automationanywhere.com/rpa/what-is-robotic-process-automation).**

* **"The Essential Guide to RPA" - This comprehensive guide by UiPath covers various aspects of RPA, including implementation strategies, best practices, and case studies. It can serve as a valuable resource for understanding RPA concepts and methodologies. (https://www.uipath.com/resources/guide-to-robotic-process-automation)**
* **"RPA Implementation: A Step-by-Step Guide" - This guide by Blue Prism offers a step-by-step approach to implementing RPA, covering key considerations, planning, and deployment strategies. It provides practical insights for successful RPA implementation. (https://www.blueprism.com/resources/white-papers/rpa-implementation-step-step-guide/)**
* **"The State of Robotic Process Automation: An Insider's Guide" - This report by Deloitte provides insights into the current landscape and trends of RPA, including its impact on organizations, challenges, and future developments.**

**(https://www2.deloitte.com/content/dam/Deloitte/nl/Documents/innovation/the-state-of-robotic-process-automation.pdf).**