

PROJECT DELTA

Team Members

Anvesh Muppada (R11840667)

Saran Kumar(R11840678)

Rishabh Kumar(R11840678)

Hemanth Pavan Kashyap(R11840678)

Shireesha Kanikireddy(R11840678)

Meghana Reddy(R11840678)

Amulya Jangalapalli(R11842826)

Rakshitha Krishnan(R11840678)

under the supervision of

Dr. Abdul Serwada



Department of Computer Science
Texas Tech University

December 2022

ABSTRACT :

Cyber issues have become one of the most dangerous threats to mankind. Many mitigation steps, defence mechanisms and analysis have come to rescue users from these attacks and attackers but the attackers are somehow breaching the users and their data.

Cyber security problems are rampant in today's world, especially in websites. As an example of modern world issues, we developed a website goodguyandco.com and added some security features like Password Handling, Password Strength checker, Encryption and decryption to it. Also, by generating huge traffic on our own website we showed how a DDOS attack works and how we can mitigate the attack. We used a shell-based script to send the desired amount of huge traffic to the website. To analyse, visualize, Diagnose the traffic/ data and alerting Splunk tool is used. The ultimate goal of this project is to provide a one-stop solution to all security risks with a simplified interface.

TOOLS AND TECHNOLOGIES USED :

- AWS - VPC, EC2, NACL, SUBNETS, SECURITY GROUPS, RDS
- HTML
- CSS
- JAVASCRIPT
- SHELLSCRIPT
- SPLUNK

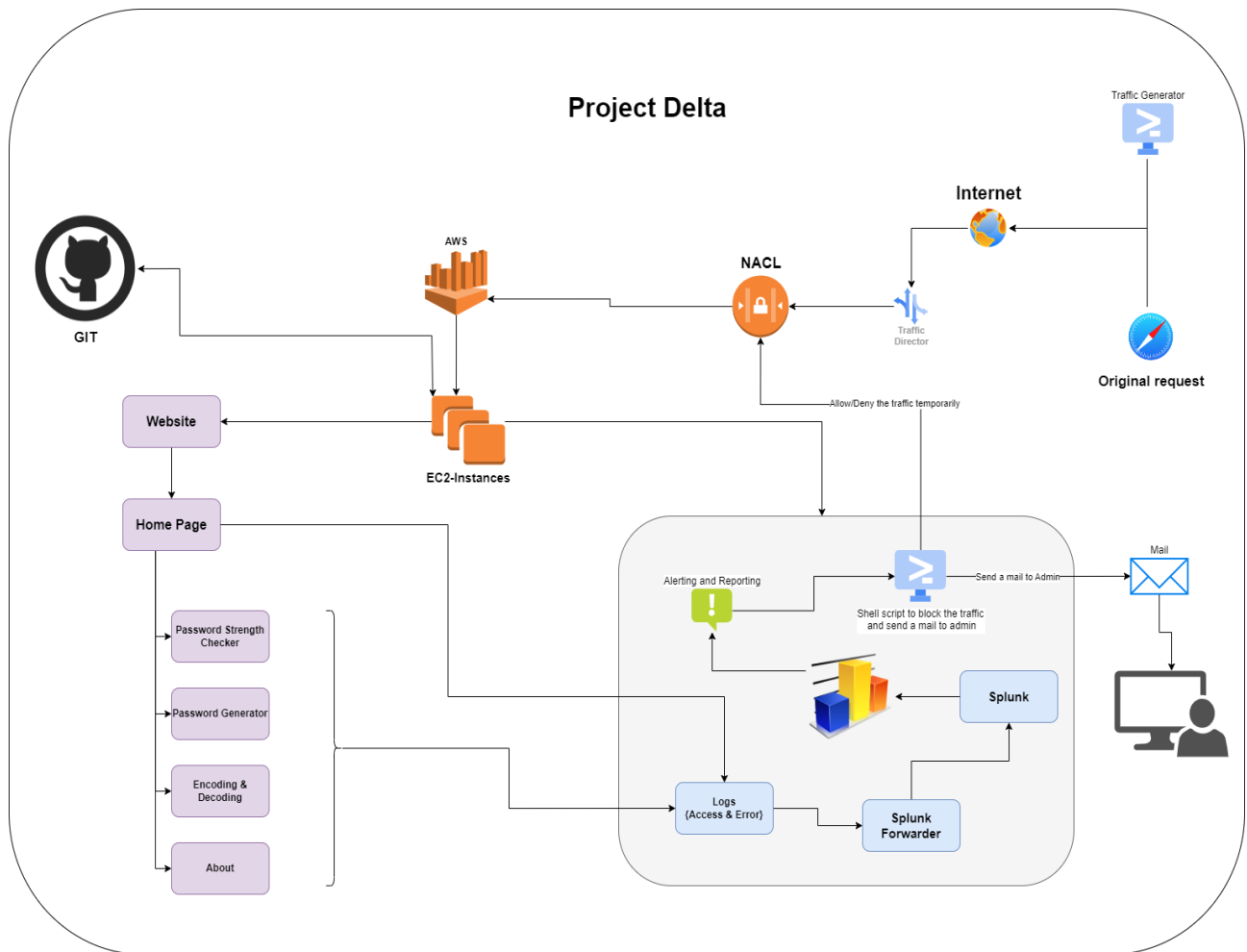
EXISTING PROBLEMS :

Passwords and DDOS attacks are one of the critical problems in cybersecurity today. 30% of online users have been victims of security breaches caused by weak passwords. Many of the users do not have proper knowledge on setting up the password for their accounts.

PROPOSED SOLUTION :

This project provides the solutions for the existing problems mentioned through a single website. Creation of a website which includes the functionalities such as Password Generator, Password Strength Checker and Encryption and Decryption. Along with that we provide an additional functionality such as network analysis using splunk.

ARCHITECTURE :



PASSWORD STRENGTH CHECKER:

Password Strength Checker is used to determine the strength of a password that has been given as input. The score determines the password strength, which might be Very Strong, Strong, Good, Weak, or Very Weak. The password is scored using a few factors, such as true and false situations.

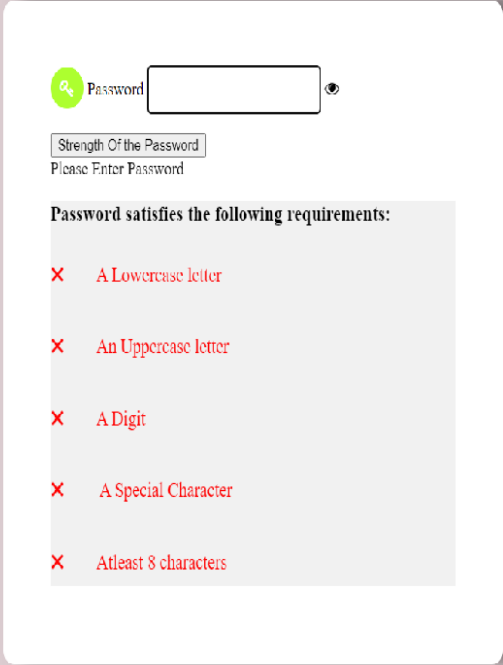
True(gaining Scoring) Scenario's:

- The password length is higher than or less than 7.
- The unique values in the string.
- Based on the count of the Uppercase letters, Lowercase letters, Special characters, numbers and the combinations of these elements.

False(Loosing Score) Scenario's:

- Forward string(the entered string is in the order of alphabets, numbers and the special characters).
- Reverse string(the entered string is in the reverse order of alphabets, length of the password, unique characters in the string and based on the count of the uppercase letters, lowercase letters, numbers and special characters).

Password Strength Checker



Strength Of the Password

Please Enter Password

Password satisfies the following requirements:

- ✗ A Lowercase letter
- ✗ An Uppercase letter
- ✗ A Digit
- ✗ A Special Character
- ✗ Atleast 8 characters

[Click Here to Generate the Password](#)

Use cases:

- Used to check the strength of the generated password and user's custom password.
- Avoids password leaks and hackings.

PASSWORD GENERATOR:

The Password Generator capability generates passwords depending on the user's preferences. There are various components, including initial letters, remaining letters, password length, and a button. The user must select an initial letter, which might be uppercase, lowercase, or a number. The remaining letters may be capital, lowercase, special characters, or numerals. The length bar is used to specify the length of the password.



The screenshot shows a web application titled "Password Generator" on a light purple background. The main interface is a light blue rounded rectangle containing several sections:

- Initial Letter** (in red text):
 - First Letter UpperCase ☐
 - First Letter LowerCase ☐
 - First Letter Number ☐
- Remaining Letters** (in red text):
 - Numbers ☐
 - LowerCase Letters ☐
 - UpperCase Letters ☐
 - Special Characters ☐
- A horizontal slider bar with a blue dot at the left end and the number "8" at the right end.
- A "Generate" button with a gear icon.

Below the main interface is a clipboard icon. At the bottom, there is a link that says "Click Here to [Check the Strength of the above Password](#)".

We created a custom code to generate passwords at random using the time technique. The time() method returns a number representing the number of seconds elapsed since 00:00:00 UTC on January 1, 1970, implying that the function will return a different value with each call. The basic concept here is that we are doing a modulus operation

on the time variable by utilizing variables such as random counter, previous random value, and maximum, which record the length of the alphabets, numerals, or special characters.

The function returns a value, which can be used as an index to get the output.