Password Strength Tester

subtitle:analysing and improving password security

Fatoumata dicko
Farah adam donga
Yasmine duchelle
Daniella esther

date:12/july/2024

INTRODUCTION

A Password Strength Tester is a cybersecurity project designed to evaluate the strength and security of user-created passwords. This tool helps users create stronger, more secure passwords by analyzing various factors such as length, complexity, and entropy. It provides immediate feedback on password strength, often categorizing them as weak, moderate, or strong, and suggests improvements if needed. The tool typically checks for the inclusion of uppercase and lowercase letters, numbers, and special characters, and may also ensure the password is not easily guessable or commonly used. By encouraging better password practices, a Password Strength Tester enhances overall security for individuals and organizations.

features of our password strength tester

There is an interactive web page that acts as a user interface . It is easy to use and understands. It contains a chat box where the user can enter the password to be checked. The user can also reset the page and type a new password at any time to check its strength.

HOW IT WORKS

The password checker collects a password and rates its strength on a scale of 1 to 4 from weakest to strongest. Based on the strength, it provides feedback to ameliorate the password and suggests stronger passwords.

BENEFITS

1-Enhanced SecurityStronger Passwords: Encourages users to create complex, robust passwords that are harder to crack.Protection Against Attacks: Reduces the risk of brute force, dictionary, and other common types of attacks.

2-User Awareness and EducationPassword Best Practices: Educates users on the importance of including a mix of characters, numbers, and symbols.Security Mindset: Promotes a culture of security awareness among users, leading to better overall security habits.

3-Immediate Feedback and ImprovementInstant Analysis: Provides real-time feedback on password strength, allowing users to make immediate improvements.Actionable Suggestions: Offers clear recommendations for enhancing password strength, guiding users in creating more secure passwords.

BENEFITS

4-Preventing Common Pitfalls Avoids Common Passwords: Detects and discourages the use of commonly used passwords, which are easily guessable. Checks Password History: Some advanced testers can compare against a database of breached passwords to ensure users aren't reusing compromised passwords.

5-Increased Trust and Compliance Compliance with Policies: Helps organizations enforce password policies and comply with industry standards and regulations. User Trust: Builds trust with users by demonstrating a commitment to their security.

6-Scalability and IntegrationEasy Integration: Can be integrated into websites, applications, and systems to ensure password strength across all user interactions.Scalable Solution: Suitable for individual users as well as organizations of all sizes.

DEMO

File Edit Format View Help

```
<!DOCTYPE html>
<html>
<head>
    <title>Password Strength Result</title>
</head>
<body>
    <h1>Password Strength Result</h1>
    <p>Score: {{ score }} (0=weak, 4=strong)</p>
    <p>Feedback:</p>
    <ul>
        {% for suggestion in feedback['suggestions'] %}
            <li>{{ suggestion }}</li>
        {% endfor %}
    </ul>
    {% if suggestions %}
    <h2>Suggestions for Stronger Passwords:</h2>
    <ul>
        {% for suggestion in suggestions %}
            <li>{{ suggestion }}</li>
        {% endfor %}
    </ul>
    {% endif %}
    <a href="/">Check another password</a>
</body>
</html>
```

index - Notepad

File Edit Format View Help

```
<!DOCTYPE html>
<html>
<head>
    <title>Password Strength Checker</title>
</head>
<body>
    <h1>Password Strength Checker</h1>
    <form action="/check_password" method="post">
        <label for="password">Enter Password:</label>
        <input type="password" id="password" name="password" required>
        <input type="submit" value="Check Strength">
    </form>
</body>
</html>
```

password_checker

Home Share View

jenovic mapwasa › password_checker

Quick access
Downloads
Desktop
Documents
password_checker
templates
OneDrive - Personal
This PC

Name	Date modified	Type
templates	7/14/2024 4:35 PM	File folder
venv	7/14/2024 4:49 PM	File folder
app	7/14/2024 5:50 PM	Python File
cmd result	7/14/2024 6:06 PM	PNG File
index	7/14/2024 5:59 PM	PNG File
python app	7/14/2024 6:00 PM	PNG File
result	7/14/2024 5:58 PM	PNG File

Not secure 192.168.1.19:5000

Password Strength Checker

Enter Password: Check Strength

Not secure 192.168.1.19:5000/check_password

Password Strength Result

Score: 2 (0=weak, 4=strong)

Feedback:

- Add another word or two. Uncommon words are better.

Suggestions for Stronger Passwords:

- Tr0ub4dor&3
- correcthorsebatterystaple
- X3@mp!ePa$$w0rd
- D0g.....
- tH!sIsAV3ry$tr0nGP@$$w0rd
- c0rr3ctH0rs3b@tt3rY5taple
- myF@v0r!t3F00dI$P!zz@
- 3@tM0reFrU!t$

ck another password

Command Prompt - python app.py

```
Microsoft Windows [Version 10.0.19045.4651]
(c) Microsoft Corporation. All rights reserved.

C:\Users\jenov>cd password_checker

C:\Users\jenov\password_checker>python app.py
 * Serving Flask app 'app'
 * Debug mode: on
WARNING: This is a development server. Do not use it in a production deployment. Use a production WSGI server inst
 * Running on all addresses (0.0.0.0)
 * Running on http://127.0.0.1:5000
 * Running on http://192.168.1.19:5000
Press CTRL+C to quit
 * Restarting with stat
 * Debugger is active!
 * Debugger PIN: 115-344-580
127.0.0.1 - - [14/Jul/2024 17:51:30] "POST /check_password HTTP/1.1" 200 -
127.0.0.1 - - [14/Jul/2024 17:51:35] "GET / HTTP/1.1" 200 -
127.0.0.1 - - [14/Jul/2024 17:51:36] "GET / HTTP/1.1" 200 -
127.0.0.1 - - [14/Jul/2024 17:51:45] "POST /check_password HTTP/1.1" 200 -
192.168.1.20 - - [14/Jul/2024 17:53:23] "GET / HTTP/1.1" 200 -
192.168.1.20 - - [14/Jul/2024 17:53:32] "POST /check_password HTTP/1.1" 200 -
192.168.1.20 - - [14/Jul/2024 17:54:37] "POST /check_password HTTP/1.1" 200 -
192.168.1.20 - - [14/Jul/2024 17:54:41] "GET / HTTP/1.1" 200 -
```

app.py - C:/Users/jenov/password_checker/app.py (3.12.4)

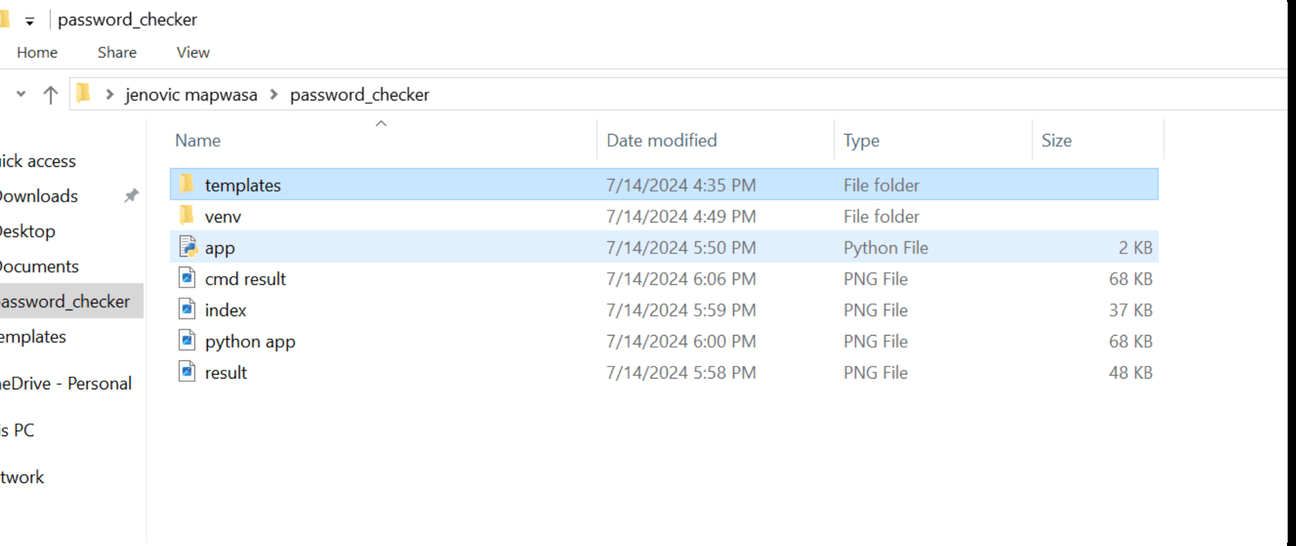
File Edit Format Run Options Window Help

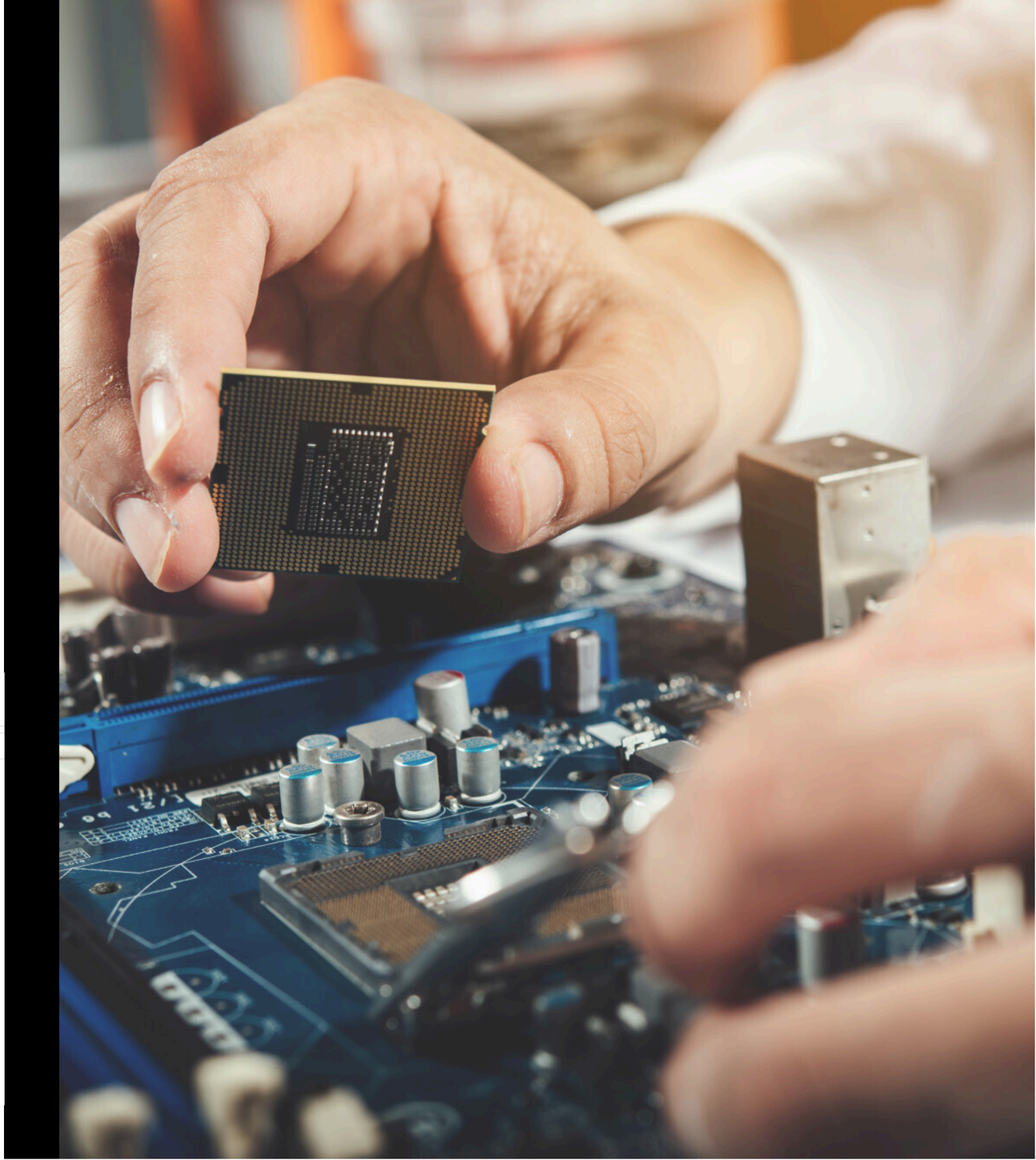
```
from flask import Flask, request, render_template
from zxcvbn import zxcvbn

app = Flask(__name__)

# Predefined strong passwords
strong_passwords = [
    "Tr0ub4dor&3",
    "correcthorsebatterystaple",
    "X3@mp!ePa$$w0rd",
    "D0g.....",
    "tH!sIsAV3ry$tr0nGP@$$w0rd",
    "c0rr3ctH0rs3b@tt3rY5taple",
    "myF@v0r!t3F00dI$P!zz@",
    "3@tM0reFrU!t$"
]

# Function to generate password suggestions
def generate_password_suggestions(password):
    result = zxcvbn(password)
    score = result['score']
    if score < 4:
        return strong_passwords
    else:
        return []

@app.route('/')
def index():
    return render_template('index.html')

@app.route('/check_password', methods=['POST'])
def check_password():
    password = request.form['password']
    result = zxcvbn(password)
    score = result['score']
    feedback = result['feedback']
    suggestions = generate_password_suggestions(password)
    return render_template('result.html', score=score, feedback=feedback, suggestions=suggestions)

if __name__ == '__main__':
    app.run(host='0.0.0.0',port=5000,debug=True)
```

TECHNICAL DETAILS

The Flask module was used to create the web application to run the password strength checker.

A realistic password strength estimator tool called 'zxcvbn' was used to check the password strength and generate suggestions. The zxcvbn python library was used in the code. A virtual python environment was equally used in this project.





CHALLENGES AND SOLUTIONS

CHALLENGES:

User Resistance

Balancing Complexity and Usability

Technical Implementation

Performance Impact

Evolving Threat Landscape

User Privacy and Data Security

Solutions:

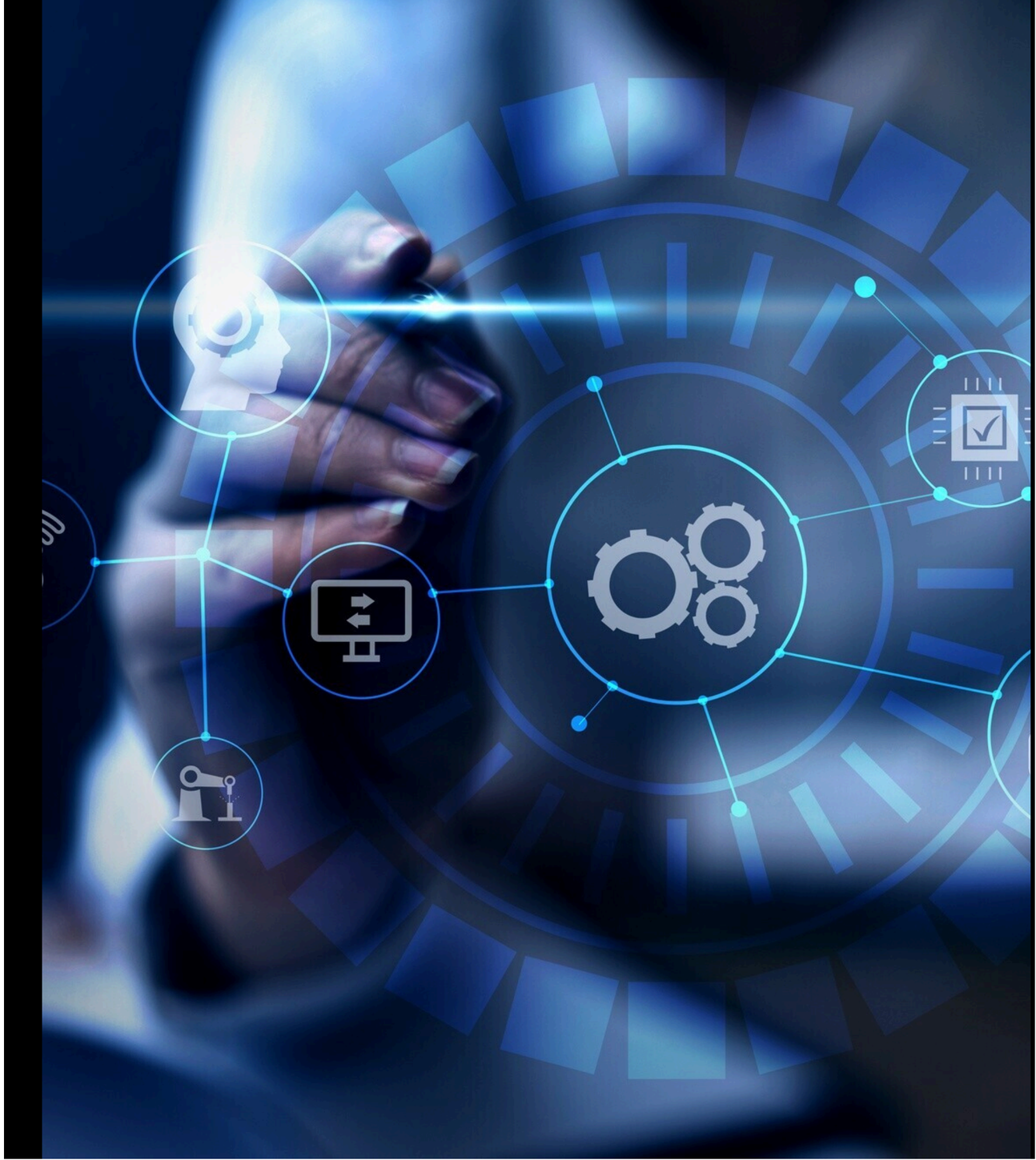
Education and Awareness

User-Friendly Design

Technical Optimization

Regular Updates and Maintenance

Secure Data Handling



Conclusion: Secure Your Accounts

In conclusion, the password strength tester is a valuable tool to assess and improve the security of your online accounts. Implement the strategies discussed to safeguard your digital identity and protect against unauthorized access.

Thanks!