Nu Html Checker

This tool is an ongoing experiment in better HTML checking, and its behavior remains subject to change

Showing results for contents of text-input area

Checker Input

Show ☑ source □ outline □ image report Options…

Check by text input □ css

```

<!DOCTYPE html>
<html lang="en">

<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <meta name="description"
        content="Password generator. Completely free and safe to use. Generate
strong passwords for every account and get the latest best practices on how to
maintain password security and privacy online.">
    <meta name="keywords"
        content="password generator, strong password, new password, create new
password, random password, generate new password, generate passwords, free
password generator">
```

Check

Use the Message Filtering button below to hide/show particular messages, and to see total counts of errors and warnings.

Message Filtering

Document checking completed. No errors or warnings to show.

Source

```
↩
<!DOCTYPE html>↩
<html lang="en">↩
↩
<head>↩
    <meta charset="UTF-8">↩
    <meta name="viewport" content="width=device-width, initial-scale=1.0">↩
    <meta name="description"↩
        content="Password generator. Completely free and safe to use. Generate
strong passwords for every account and get the latest best practices on how to
maintain password security and privacy online.">↩
    <meta name="keywords"↩
        content="password generator, strong password, new password, create new
password, random password, generate new password, generate passwords, free
password generator">↩
    <link rel="stylesheet" href="assets/css/style.css">↩
    <title>Password Generator</title>↩
    <link rel="apple-touch-icon" sizes="180x180" href="assets/favicon/apple-
touch-icon.png">↩
```

```
    <link rel="icon" type="image/png" sizes="32x32" href="assets/favicon/favicon-32x32.png">↩
    <link rel="icon" type="image/png" sizes="16x16" href="assets/favicon/favicon-16x16.png">↩
</head>↩
↩
<body>↩
    <header>↩
        <a href="index.html" aria-label="Go to homepage">↩
            <h1><img src="assets/images/logo.png" alt="Password Generator Logo." id="logo">Password Generator</h1>↩
        </a>↩
        <!-- menu -->↩
        <nav>↩
            <ul id="menu">↩
                <li><a href="#generator-section">Password Generator</a></li>↩
                <li><a href="#lowercase">Saved Passwords</a></li>↩
                <li><a href="#link">FAQ</a></li>↩
            </ul>↩
        </nav>↩
    </header>↩
    <main>↩
        <!-- password generator area -->↩
        <section id="generator-section">↩
            <div class="generator-outer-container">↩
                <div class="generator-inner-container">↩
                    <h2>Password Generator</h2>↩
                    <br>↩
                    <p>Looking for a reliable password? Try the Password Generator to craft complicated passwords↩
                        ensuring the safety of your information!</p>↩
                    <br>↩
                    <!-- password display -->↩
                    <div id="password-output"></div>↩
                    <br>↩
                    <div class="button-container">↩
                        <button type="button" id="generate-button" class="button" aria-label="Generate password">Generate</button>↩
                        <button type="button" id="save-button" class="button" aria-label="Save password">Save Password</button>↩
                    </div>↩
                    <br>↩
                    <label for="length">Password Length: <span id="length-value">12</span></label>↩
                    <input type="range" id="length" name="length" min="4" max="80" value="12">↩
                    <br>↩
                    <label>Character Types:</label>↩
                    <!-- password generator characters -->↩
                    <form>↩
                        <label for="lowercase" aria-label="Include lowercase letters in password"><input type="checkbox"↩
                                id="lowercase" name="lowercase" checked> Lowercase (a-z)</label>↩
                        <label for="uppercase" aria-label="Include uppercase letters in password"><input type="checkbox"↩
                                id="uppercase" name="uppercase" checked> Uppercase (A-Z)</label>↩
                        <label for="numbers" aria-label="Include numbers in password"><input type="checkbox"↩
                                id="numbers" name="numbers" checked> Numbers (0-9)</label>↩
                        <label for="symbols" aria-label="Include symbols in password"><input type="checkbox"↩
                                id="symbols" name="symbols" checked> Symbols (!@#$%^&*)</label>↩
                    </form>↩
                </div>↩
            </div>↩
        </section>↩
        <!-- saved passwords area-->↩
        <section id="saved-passwords-section">↩
            <div class="saved-passwords-container">↩
                <h2>Your Saved Passwords</h2>↩
                <p id="link">You can save up to 10 passwords.</p>↩
                <button id="delete-all">Delete All Passwords <i class="fa-solid fa-trash-can fa-lg"></i></button>↩
                <div id="saved-passwords"></div>↩
            </div>↩
        </section>↩
        <!-- FAQ area -->↩
        <section id="faq-section">↩
            <h2>Frequently Asked Questions</h2>↩
            <div id="faq-container">↩
                <!-- question -->↩
                <div class="accordion">↩
                    <button class="accordion-header" aria-label="Expand/Collapse question">↩
                        <span>↩
                            What makes a password strong?↩
                        </span>↩
                        <i class="fa-solid fa-chevron-down arrow"></i>↩
                    </button>↩
                    <div class="accordion-body">↩
                        <p>↩
                            Creating a strong password is essential for safeguarding your accounts against unauthorized↩
                            access. A strong password typically consists of at least 12 characters and includes a mix of↩
                            uppercase letters,↩
                            lowercase letters, numbers, and special characters to increase complexity and make it harder↩
                            to guess or crack. Avoid using easily predictable patterns or sequences, and refrain from↩
                            including personal↩
                            information like your name, birthday, or common words related to your interests. Instead,↩
                            opt for random combinations of characters or words. It's important to use different↩
                            passwords for different accounts↩
                            to prevent a breach in one account compromising others. Additionally, remember to change↩
                            your passwords regularly to maintain security. Lastly, enabling two-factor authentication↩
                            (2FA) wherever possible adds↩
                            an extra layer of protection to your accounts.↩
                        </p>↩
                    </div>↩
                </div>↩
                <!-- question -->↩
                <div class="accordion">↩
                    <button class="accordion-header" aria-label="Expand/Collapse question">↩
                        <span>↩
                            Why should my password be unique?↩
                        </span>↩
                        <i class="fa-solid fa-chevron-down arrow"></i>↩
                    </button>↩
                    <div class="accordion-body">↩
                        <p>↩
                            Having a unique password for each of your accounts is essential because it prevents a↩
                            security breach in one account from compromising all your other accounts. If you use the↩
                            same password across multiple↩
                            accounts and one of those accounts is compromised, hackers could potentially gain access to↩
                            all your other accounts. Unique passwords also protect against credential stuffing attacks,↩
                            where hackers use leaked↩
                            username and password combinations from one website to try to access other websites. By↩
                            using unique passwords, you minimize the risk of unauthorized access to your accounts and↩
                            enhance overall security.↩
                        </p>↩
                    </div>↩
                </div>↩
                <!-- question -->↩
                <div class="accordion">↩
                    <button class="accordion-header" aria-label="Expand/Collapse question">↩
                        <span>↩
                            Why should my password be random?↩
                        </span>↩
                        <i class="fa-solid fa-chevron-down arrow"></i>↩
                    </button>↩
                    <div class="accordion-body">↩
                        <p>↩
                            Creating a random password enhances its security by making it more difficult for attackers↩
                            to guess or crack. Randomness adds complexity, which strengthens the password's resilience↩
                            against various hacking↩
                            techniques. When passwords are predictable or follow a pattern, they become more susceptible↩
                            to dictionary attacks, brute-force attacks, and other automated password cracking methods.↩
                            Random passwords are↩
                            harder to guess because they lack recognizable patterns or associations with personal↩
                            information, such as birthdays or names. This randomness increases the entropy of the↩
                            password, making it exponentially↩
                            more challenging for attackers to decipher through trial and error. Therefore, generating↩
                            passwords with random combinations of characters significantly bolsters their effectiveness↩
                            in protecting your↩
                            accounts and sensitive information from unauthorized access.↩
                        </p>↩
                    </div>↩
                </div>↩
                <!-- question -->↩
                <div class="accordion">↩
                    <button class="accordion-header" aria-label="Expand/Collapse question">↩
                        <span>↩
                            How do password generators work?↩
                        </span>↩
                        <i class="fa-solid fa-chevron-down arrow"></i>↩
                    </button>↩
                    <div class="accordion-body">↩
                        <p>↩
                            Password generators use algorithms to create random or pseudo-random sequences of characters↩
                            based on specified criteria. These criteria typically include factors such as password↩
                            length, character types↩
                            (uppercase letters, lowercase letters, numbers, special characters), and any additional↩
                            constraints specified by the user. The process begins with the generation of a seed value,↩
                            which serves as the starting↩
                            point for generating random numbers. These random numbers are then mapped to characters↩
                            according to the chosen character types. Once the characters are selected, they are combined↩
                            into a string to form the↩
                            password. Users may have the option to customize the generated password further, such as↩
                            avoiding ambiguous characters or enforcing specific patterns. Ultimately, password↩
                            generators automate the creation of↩
                            strong, random passwords, providing users with a convenient and effective means of enhancing↩
                            the security of their online accounts and sensitive information.↩
                        </p>↩
                    </div>↩
                </div>↩
                <!-- question -->↩
                <div class="accordion">↩
                    <button class="accordion-header" aria-label="Expand/Collapse question">↩
                        <span>↩
                            Is a Password Generator safe to use?↩
                        </span>↩
                        <i class="fa-solid fa-chevron-down arrow"></i>↩
                    </button>↩
                    <div class="accordion-body">↩
                        <p>↩
                            A password generator can indeed be safe to use, provided you take certain precautions.↩
                            Firstly, it's essential to choose a reliable source for the generator. Trusted password↩
                            managers often offer built-in↩
                            generators that create strong, random passwords using secure methods like cryptographic↩
                            algorithms. Additionally, be mindful of the environment in which you use the generator.↩
                            Online generators, especially↩
                            those without HTTPS or hosted on dubious websites, may pose security risks, potentially↩
                            leading to intercepted or compromised passwords. Lastly, remember that the security of your↩
                            passwords doesn't solely↩
                            depend on the generator itself but also on how you handle and store those passwords.↩
                            Utilizing a secure, encrypted password manager to store your generated passwords is crucial↩
                            for maintaining their safety.↩
                            By following these guidelines and exercising caution, a password generator can indeed be a↩
                            valuable tool for enhancing your online security.↩
                        </p>↩
                    </div>↩
                </div>↩
                <!-- question -->↩
                <div class="accordion">↩
                    <button class="accordion-header" aria-label="Expand/Collapse question">↩
                        <span>↩
                            What are the requirements for a strong password?↩
                        </span>↩
                        <i class="fa-solid fa-chevron-down arrow"></i>↩
                    </button>↩
                    <div class="accordion-body">↩
                        <p>↩
                            A strong password is one that possesses several key characteristics to withstand various↩
                            forms of cyber threats. Firstly, it should be of sufficient length, typically at least 12↩
                            characters, as longer↩
                            passwords are inherently more difficult to crack. Secondly, complexity is crucial—mixing↩
                            uppercase and lowercase letters, numbers, and special characters creates a more secure↩
                            password. Additionally,↩
                            unpredictability is essential; avoiding easily guessable information like common phrases or↩
                            personal details strengthens the password's resilience. It's also crucial to use a unique↩
                            password for each account↩
                            or service to prevent widespread compromise if one password is breached. Steer clear of↩
                            patterns or sequences, opting instead for truly random combinations of characters. Regularly↩
                            updating passwords,↩
                            particularly for sensitive accounts, further bolsters security. By adhering to these↩
                            principles, individuals can create robust passwords that significantly reduce the risk of↩
                            unauthorized access and protect↩
                            their online accounts and personal information.↩
                        </p>↩
                    </div>↩
                </div>↩
                <!-- question -->↩
                <div class="accordion">↩
                    <button class="accordion-header" aria-label="Expand/Collapse question">↩
                        <span>↩
                            Can password generators be hacked?↩
                        </span>↩
                        <i class="fa-solid fa-chevron-down arrow"></i>↩
                    </button>↩
                    <div class="accordion-body">↩
                        <p>↩
                            Password generators themselves are not typically vulnerable to hacking, as they are tools↩
                            designed to create passwords using secure algorithms. However, certain risks exist,↩
                            primarily due to external factors.↩
                            For instance, if you use a compromised password generator application or website infected↩
                            with malware, the generated passwords could be compromised. Additionally, poorly implemented↩
                            random number generation↩
                            algorithms may result in predictable passwords. Furthermore, using online generators without↩
                            secure connections (HTTPS) could expose generated passwords to interception by malicious↩
                            actors. There's also a↩
                            risk of encountering fake or malicious generators that aim to capture generated passwords.↩
                            To mitigate these risks, it's crucial to use reputable password generators from trusted↩
                            sources, ensure secure↩
                            connections when generating passwords online, and regularly update software to address any↩
                            potential vulnerabilities. Moreover, employing trusted password managers with built-in↩
                            generators enhances security↩
                            by providing a controlled and secure environment for generating and storing passwords.↩
                        </p>↩
                    </div>↩
                </div>↩
                <!-- question -->↩
                <div class="accordion">↩
                    <button class="accordion-header" aria-label="Expand/Collapse question">↩
                        <span>↩
                            What are the top 10 worst passwords?↩
                        </span>↩
                        <i class="fa-solid fa-chevron-down arrow"></i>↩
                    </button>↩
                    <div class="accordion-body">↩
                        <p>↩
                            The top 10 worst passwords often include easily guessable or common phrases that offer↩
                            little to no security. As of recent reports, some of the most commonly used weak passwords↩
                            include:↩
                        </p>↩
                        <br>↩
                        <br>↩
                        <ol>↩
                            <li>123456</li>↩
                            <li>password</li>↩
                            <li>123456789</li>↩
                            <li>12345678</li>↩
                            <li>12345</li>↩
                            <li>1234567</li>↩
                            <li>qwerty</li>↩
                            <li>1234567890</li>↩
                            <li>abc123</li>↩
                            <li>password123</li>↩
                        </ol>↩
                        <br>↩
                        <p>↩
                            These passwords are highly insecure because they are either sequential, easily guessable, or↩
                            widely used, making them vulnerable to brute-force attacks or dictionary attacks. It's↩
                            crucial to avoid such weak↩
                            passwords and instead opt for strong, unique passwords that incorporate a mix of uppercase↩
                            and lowercase letters, numbers, and special characters. Additionally, using a password↩
                            manager can help generate and↩
                            securely store complex passwords for better online security.↩
                        </p>↩
                    </div>↩
                </div>↩
            </div>↩
        </section>↩
    </main>↩
    <footer>↩
        <p>Password Generator</p>↩
        <br>↩
        <div class="social">↩
            <a href="https://www.facebook.com/" target="_blank" rel="noopener" aria-label="Go to our Facebook page"><i↩
                    class="fa-brands fa-facebook fa-2xl"></i></a>↩
            <a href="https://www.instagram.com/" target="_blank" rel="noopener" aria-label="Go to our Instagram page"><i↩
                    class="fa-brands fa-instagram fa-2xl"></i></a>↩
            <a href="https://twitter.com/" target="_blank" rel="noopener" aria-label="Go to our X/Twitter page"><i↩
                    class="fa-brands fa-x-twitter fa-2xl"></i></a>↩
        </div>↩
    </footer>↩
    <script src="https://kit.fontawesome.com/1014f68af8.js" crossorigin="anonymous"></script>↩
    <script src="assets/js/script.js"></script>↩
    <script src="https://cdn.jsdelivr.net/npm/sweetalert2@11"></script>↩
</body>↩
↩
</html>
```

Used the HTML parser.

Total execution time 14 milliseconds.

About this checker • Report an issue • Version: 24.4.4