

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">
  <link rel="stylesheet" href="assets/css/style.css">
  <title>Password Generator</title>
```

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

```
1.  ↵
2.  <!DOCTYPE html>↵
3.  <html lang="en">↵
4.  ↵
5.  <head>↵
6.      <meta charset="UTF-8">↵
7.      <meta name="viewport" content="width=device-width, initial-scale=1.0">↵
8.      <meta name="description"↵
9.          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.">↵
10.     <meta name="keywords"↵
11.         content="password generator, strong password, new password, create new password, random password, generate
new password, generate passwords, free password generator">↵
12.     <link rel="stylesheet" href="assets/css/style.css">↵
13.     <title>Password Generator</title>↵
14.     <link rel="apple-touch-icon" sizes="180x180" href="assets/favicon/apple-touch-icon.png">↵
15.     <link rel="icon" type="image/png" sizes="32x32" href="assets/favicon/favicon-32x32.png">↵
16.     <link rel="icon" type="image/png" sizes="16x16" href="assets/favicon/favicon-16x16.png">↵
17. </head>↵
18. ↵
19. <body>↵
20.     <header>↵
21.         <a href="index.html" aria-label="Go to homepage">↵
22.             <h1>Password Generator</h1>↵
23.         </a>↵
24.         <!-- menu -->↵
25.         <nav>↵
26.             <ul id="menu">↵
27.                 <li><a href="#generator-section">Password Generator</a></li>↵
28.                 <li><a href="#lowercase">Saved Passwords</a></li>↵
29.                 <li><a href="#link">FAQ</a></li>↵
30.             </ul>↵
31.         </nav>↵
32.     </header>↵
33.     <main>↵
34.         <!-- password generator area -->↵
35.         <section id="generator-section">↵
36.             <div class="generator-outer-container">↵
37.                 <div class="generator-inner-container">↵
38.                     <h2>Password Generator</h2>↵
39.                     <br>↵
40.                     <p>Looking for a reliable password? Try the Password Generator to craft complicated passwords↵
```

```

41.         ensuring the safety of your information!</p><
42.     <br>
43.     <!-- password display -->
44.     <div id="password-output"></div>
45.     <br>
46.     <div class="button-container">
47.         <button type="button" id="generate-button" class="button" aria-label="Generate
password">Generate</button>
48.         <button type="button" id="save-button" class="button" aria-label="Save password">Save
Password</button>
49.     </div>
50.     <br>
51.     <label for="length">Password Length: <span id="length-value">12</span></label>
52.     <input type="range" id="length" name="length" min="4" max="80" value="12">
53.     <br>
54.     <label>Character Types:</label>
55.     <!-- password generator characters -->
56.     <form>
57.         <label for="lowercase" aria-label="Include lowercase letters in password"><input
type="checkbox">
58.             id="lowercase" name="lowercase" checked> Lowercase (a-z)</label>
59.         <label for="uppercase" aria-label="Include uppercase letters in password"><input
type="checkbox">
60.             id="uppercase" name="uppercase" checked> Uppercase (A-Z)</label>
61.         <label for="numbers" aria-label="Include numbers in password"><input type="checkbox">
62.             id="numbers" name="numbers" checked> Numbers (0-9)</label>
63.         <label for="symbols" aria-label="Include symbols in password"><input type="checkbox">
64.             id="symbols" name="symbols" checked> Symbols (!@#$$%^&*)</label>
65.     </form>
66.     </div>
67. </div>
68. </section>
69. <!-- saved passwords area -->
70. <section id="saved-passwords-section">
71.     <div class="saved-passwords-container">
72.         <h2>Your Saved Passwords</h2>
73.         <p id="link">You can save up to 10 passwords.</p>
74.         <button id="delete-all">Delete All Passwords <i class="fa-solid fa-trash-can fa-lg"></i></button>
75.         <div id="saved-passwords"></div>
76.     </div>
77. </section>
78. <!-- FAQ area -->
79. <section id="faq-section">
80.     <h2>Frequently Asked Questions</h2>
81.     <div id="faq-container">
82.         <!-- question -->
83.         <div class="accordion">

```

```

84. <button class="accordion-header" aria-label="Expand/Collapse question">↵
85.   <span>↵
86.     What makes a password strong?↵
87.   </span>↵
88.   <i class="fa-solid fa-chevron-down arrow"></i>↵
89. </button>↵
90. <div class="accordion-body">↵
91.   <p>↵
92.     Creating a strong password is essential for safeguarding your accounts against
93.     unauthorized↵
94.     access. A strong password typically consists of at least 12 characters and includes a mix
95.     of↵
96.     uppercase letters,↵
97.     lowercase letters, numbers, and special characters to increase complexity and make it
98.     harder↵
99.     to guess or crack. Avoid using easily predictable patterns or sequences, and refrain
100.    from↵
101.    including personal↵
102.    information like your name, birthday, or common words related to your interests.
103.    Instead,↵
104.    opt for random combinations of characters or words. It's important to use different↵
105.    passwords for different accounts↵
106.    to prevent a breach in one account compromising others. Additionally, remember to
107.    change↵
108.    your passwords regularly to maintain security. Lastly, enabling two-factor
109.    authentication↵
110.    (2FA) wherever possible adds↵
111.    an extra layer of protection to your accounts.↵
112.   </p>↵
113. </div>↵
114. </div>↵
115. <!-- question -->↵
116. <div class="accordion">↵
117.   <button class="accordion-header" aria-label="Expand/Collapse question">↵
118.     <span>↵
119.       Why should my password be unique?↵
120.     </span>↵
121.     <i class="fa-solid fa-chevron-down arrow"></i>↵
122.   </button>↵
123.   <div class="accordion-body">↵
124.     <p>↵
125.       Having a unique password for each of your accounts is essential because it prevents a↵
126.       security breach in one account from compromising all your other accounts. If you use
127.       the↵
128.       same password across multiple↵
129.       accounts and one of those accounts is compromised, hackers could potentially gain access
130.       to↵

```

```

122.         all your other accounts. Unique passwords also protect against credential stuffing
attacks,↵
123.         where hackers use leaked↵
124.         username and password combinations from one website to try to access other websites. By↵
125.         using unique passwords, you minimize the risk of unauthorized access to your accounts
and↵
126.         enhance overall security.↵
127.     </p>↵
128. </div>↵
129. </div>↵
130. <!-- question -->↵
131. <div class="accordion">↵
132.     <button class="accordion-header" aria-label="Expand/Collapse question">↵
133.         <span>↵
134.             Why should my password be random?↵
135.         </span>↵
136.         <i class="fa-solid fa-chevron-down arrow"></i>↵
137.     </button>↵
138.     <div class="accordion-body">↵
139.         <p>↵
140.             Creating a random password enhances its security by making it more difficult for
attackers↵
141.             to guess or crack. Randomness adds complexity, which strengthens the password's
resilience↵
142.             against various hacking↵
143.             techniques. When passwords are predictable or follow a pattern, they become more
susceptible↵
144.             to dictionary attacks, brute-force attacks, and other automated password cracking
methods.↵
145.             Random passwords are↵
146.             harder to guess because they lack recognizable patterns or associations with personal↵
147.             information, such as birthdays or names. This randomness increases the entropy of the↵
148.             password, making it exponentially↵
149.             more challenging for attackers to decipher through trial and error. Therefore,
generating↵
150.             passwords with random combinations of characters significantly bolsters their
effectiveness↵
151.             in protecting your↵
152.             accounts and sensitive information from unauthorized access.↵
153.         </p>↵
154.     </div>↵
155. </div>↵
156. <!-- question -->↵
157. <div class="accordion">↵
158.     <button class="accordion-header" aria-label="Expand/Collapse question">↵
159.         <span>↵
160.             How do password generators work?↵

```

```

161.         </span>↵
162.         <i class="fa-solid fa-chevron-down arrow"></i>↵
163.     </button>↵
164.     <div class="accordion-body">↵
165.         <p>↵
166.             Password generators use algorithms to create random or pseudo-random sequences of
characters↵
167.             based on specified criteria. These criteria typically include factors such as password↵
168.             length, character types↵
169.             (uppercase letters, lowercase letters, numbers, special characters), and any additional↵
170.             constraints specified by the user. The process begins with the generation of a seed
value,↵
171.             which serves as the starting↵
172.             point for generating random numbers. These random numbers are then mapped to characters↵
173.             according to the chosen character types. Once the characters are selected, they are
combined↵
174.             into a string to form the↵
175.             password. Users may have the option to customize the generated password further, such
as↵
176.             avoiding ambiguous characters or enforcing specific patterns. Ultimately, password↵
177.             generators automate the creation of↵
178.             strong, random passwords, providing users with a convenient and effective means of
enhancing↵
179.             the security of their online accounts and sensitive information.↵
180.         </p>↵
181.     </div>↵
182. </div>↵
183. <!-- question -->↵
184. <div class="accordion">↵
185.     <button class="accordion-header" aria-label="Expand/Collapse question">↵
186.         <span>↵
187.             Is a Password Generator safe to use?↵
188.         </span>↵
189.         <i class="fa-solid fa-chevron-down arrow"></i>↵
190.     </button>↵
191.     <div class="accordion-body">↵
192.         <p>↵
193.             A password generator can indeed be safe to use, provided you take certain precautions.↵
194.             Firstly, it's essential to choose a reliable source for the generator. Trusted password↵
195.             managers often offer built-in↵
196.             generators that create strong, random passwords using secure methods like cryptographic↵
197.             algorithms. Additionally, be mindful of the environment in which you use the generator.↵
198.             Online generators, especially↵
199.             those without HTTPS or hosted on dubious websites, may pose security risks, potentially↵
200.             leading to intercepted or compromised passwords. Lastly, remember that the security of
your↵
201.             passwords doesn't solely↵

```

```

202.      depend on the generator itself but also on how you handle and store those passwords.↵
203.      Utilizing a secure, encrypted password manager to store your generated passwords is
        crucial↵
204.      for maintaining their safety.↵
205.      By following these guidelines and exercising caution, a password generator can indeed be
        a↵
206.      valuable tool for enhancing your online security.↵
207.      </p>↵
208.      </div>↵
209.    </div>↵
210.    <!-- question -->↵
211.    <div class="accordion">↵
212.      <button class="accordion-header" aria-label="Expand/Collapse question">↵
213.        <span>↵
214.          What are the requirements for a strong password?↵
215.        </span>↵
216.        <i class="fa-solid fa-chevron-down arrow"></i>↵
217.      </button>↵
218.      <div class="accordion-body">↵
219.        <p>↵
220.          A strong password is one that possesses several key characteristics to withstand
        various↵
221.          forms of cyber threats. Firstly, it should be of sufficient length, typically at least
        12↵
222.          characters, as longer↵
223.          passwords are inherently more difficult to crack. Secondly, complexity is crucial—
        mixing↵
224.          uppercase and lowercase letters, numbers, and special characters creates a more secure↵
225.          password. Additionally,↵
226.          unpredictability is essential; avoiding easily guessable information like common phrases
        or↵
227.          personal details strengthens the password's resilience. It's also crucial to use a
        unique↵
228.          password for each account↵
229.          or service to prevent widespread compromise if one password is breached. Steer clear of↵
230.          patterns or sequences, opting instead for truly random combinations of characters.
        Regularly↵
231.          updating passwords,↵
232.          particularly for sensitive accounts, further bolsters security. By adhering to these↵
233.          principles, individuals can create robust passwords that significantly reduce the risk
        of↵
234.          unauthorized access and protect↵
235.          their online accounts and personal information.↵
236.        </p>↵
237.      </div>↵
238.    </div>↵
239.    <!-- question -->↵

```

```

240. <div class="accordion">↵
241.   <button class="accordion-header" aria-label="Expand/Collapse question">↵
242.     <span>↵
243.       Can password generators be hacked?↵
244.     </span>↵
245.     <i class="fa-solid fa-chevron-down arrow"></i>↵
246.   </button>↵
247.   <div class="accordion-body">↵
248.     <p>↵
249.       Password generators themselves are not typically vulnerable to hacking, as they are
250.       tools↵
251.       designed to create passwords using secure algorithms. However, certain risks exist,↵
252.       primarily due to external factors.↵
253.       For instance, if you use a compromised password generator application or website
254.       infected↵
255.       with malware, the generated passwords could be compromised. Additionally, poorly
256.       implemented↵
257.       random number generation↵
258.       algorithms may result in predictable passwords. Furthermore, using online generators
259.       without↵
260.       secure connections (HTTPS) could expose generated passwords to interception by
261.       malicious↵
262.       actors. There's also a↵
263.       risk of encountering fake or malicious generators that aim to capture generated
264.       passwords.↵
265.       To mitigate these risks, it's crucial to use reputable password generators from trusted↵
266.       sources, ensure secure↵
267.       connections when generating passwords online, and regularly update software to address
268.       any↵
269.       potential vulnerabilities. Moreover, employing trusted password managers with built-in↵
270.       generators enhances security↵
271.       by providing a controlled and secure environment for generating and storing passwords.↵
272.     </p>↵
273.   </div>↵
274. </div>↵
275. <!-- question -->↵
276. <div class="accordion">↵
277.   <button class="accordion-header" aria-label="Expand/Collapse question">↵
278.     <span>↵
279.       What are the top 10 worst passwords?↵
280.     </span>↵
281.     <i class="fa-solid fa-chevron-down arrow"></i>↵
282.   </button>↵
283.   <div class="accordion-body">↵
284.     <p>↵
285.       The top 10 worst passwords often include easily guessable or common phrases that offer↵

```



```

279.         little to no security. As of recent reports, some of the most commonly used weak
passwords↵
280.         include:↵
281.     </p>↵
282.     <br>↵
283.     <br>↵
284.     <ol>↵
285.         <li>123456</li>↵
286.         <li>password</li>↵
287.         <li>123456789</li>↵
288.         <li>12345678</li>↵
289.         <li>12345</li>↵
290.         <li>1234567</li>↵
291.         <li>qwerty</li>↵
292.         <li>1234567890</li>↵
293.         <li>abc123</li>↵
294.         <li>password123</li>↵
295.     </ol>↵
296.     <br>↵
297.     <p>↵
298.         These passwords are highly insecure because they are either sequential, easily guessable,
or↵
299.         widely used, making them vulnerable to brute-force attacks or dictionary attacks. It's↵
300.         crucial to avoid such weak↵
301.         passwords and instead opt for strong, unique passwords that incorporate a mix of
uppercase↵
302.         and lowercase letters, numbers, and special characters. Additionally, using a password↵
303.         manager can help generate and↵
304.         securely store complex passwords for better online security.↵
305.     </p>↵
306. </div>↵
307. </div>↵
308. </div>↵
309. </section>↵
310. </main>↵
311. <footer>↵
312.     <p>Password Generator</p>↵
313.     <br>↵
314.     <div class="social">↵
315.         <a href="https://www.facebook.com/" target="_blank" rel="noopener" aria-label="Go to our Facebook page">
<i>
316.             class="fa-brands fa-facebook fa-2x1"></i></a>↵
317.         <a href="https://www.instagram.com/" target="_blank" rel="noopener" aria-label="Go to our Instagram
page"><i>
318.             class="fa-brands fa-instagram fa-2x1"></i></a>↵
319.         <a href="https://twitter.com/" target="_blank" rel="noopener" aria-label="Go to our X/Twitter page"><i>
320.             class="fa-brands fa-x-twitter fa-2x1"></i></a>↵

```

```
321.         </div>↵
322.     </footer>↵
323.     <script src="https://kit.fontawesome.com/1014f68af8.js" crossorigin="anonymous"></script>↵
324.     <script src="assets/js/script.js"></script>↵
325. </body>↵
326. ↵
327. </html>
```

Used the HTML parser.

Total execution time 13 milliseconds.

[About this checker](#) • [Report an issue](#) • Version: 24.4.15