

# How Websites Work

To exploit a website, you first need to know how they are created.

## Task 1 How websites work

Question	Answer
What term best describes the component of a web application rendered by your browser?	Front End

## Task 2 HTML

One of the images on the cat website is broken - fix it, and the image will reveal the hidden text answer!

Answer: **HTMLHERO**

→ I noticed The cat-2 image (line 10) is missing its image extension

### HTML Code

```
1 <!DOCTYPE html>
2 <html>
3   <head>
4     <title>TryHackMe HTML Editor</title>
5   </head>
6   <body>
7     <h1>Cat Website!</h1>
8     <p>See images of all my cats!</p>
9     <img src='img/cat-1.jpg'>
10    <img src='img/cat-2.'>
11    <!-- Add dog image here -->
12  </body>
13 </html>
```

Render HTML Code

Type HTML into the box above, then click the "Render HTML" button to see how it looks

↓

Rendered HTML Code

→ I added the extension "jpg" and clicked on "Render HTML Code" button

### HTML Code

```
1 <!DOCTYPE html>
2 <html>
3   <head>
4     <title>TryHackMe HTML Editor</title>
5   </head>
6   <body>
7     <h1>Cat Website!</h1>
8     <p>See images of all my cats!</p>
9     <img src='img/cat-1.jpg'>
10    <img src='img/cat-2.jpg'>
11    <!-- Add dog image here -->
12  </body>
13 </html>
```

Render HTML Code

Type HTML into the box above, then click the "Render HTML" button to see how it looks

↓



Rendered HTML Code

→ Then, I got the hidden text answer

### Rendered HTML Code

Cat Website!

See images of all my cats!



Add a dog image to the page by adding another img tag (<img>) on line 11. The dog image location is img/dog-1.png. What is the text in the dog image?

Answer: **DOGHTML**

→ I added **<img src='img/dog-1.png'>** to the page on line 11

### HTML Code

```
1 <!DOCTYPE html>
2 <html>
3   <head>
4     <title>TryHackMe HTML Editor</title>
5   </head>
6   <body>
7     <h1>Cat Website!</h1>
8     <p>See images of all my cats!</p>
9     <img src='img/cat-1.jpg'>
10    <img src='img/cat-2.jpg'>
11    <img src='img/dog-1.png'>
12  </body>
13 </html>
```

Render HTML Code

Type HTML into the box above, then click the "Render HTML" button to see how it looks



↓


Rendered HTML Code

→ Then i got the text image

## Cat Website!

See images of all my cats!





### Task 3 JavaScript

Click the "View Site" button on this task. On the right-hand side, add JavaScript that changes the demo element's content to "Hack the Planet"

Answer: **JSISFUN**

→ I added the JavaScript to line 9 and clicked the "Render HTML+JS Code" button.

Javascript: **document.getElementById("demo").innerHTML = "Hack The Planet"**

#### HTML + Javascript Code

```
1 <!DOCTYPE html>
2 <html>
3   <head>
4     <title>TryHackMe Editor</title>
5   </head>
6   <body>
7     <div id="demo">Hi there!</div>
8     <script type="text/javascript">
9       document.getElementById("demo").innerHTML = "Hack
The Planet"
10    </script>
11  </body>
12 </html>
```

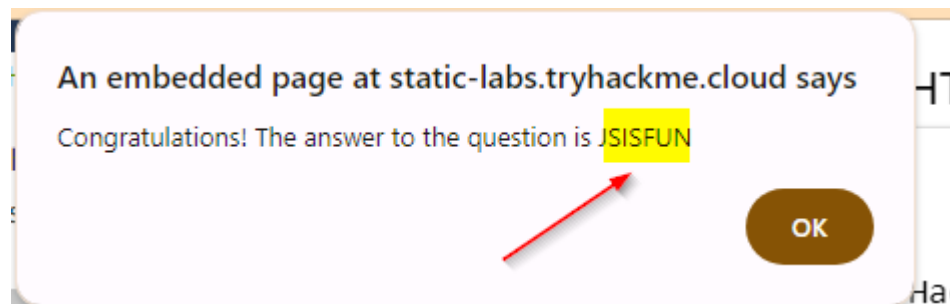
Type HTML/JS into the box above, then click the "Render HTML+JS" button to see how it looks

↓

#### Rendered HTML Code

Hack The Planet

→ Then i got the flag



Add the button HTML from this task that changes the element's text to "Button Clicked" on the editor on the right, update the code by clicking the "Render HTML+JS Code" button and then click the button.

→ I added the javascript: **<button onclick='document.getElementById("demo").innerHTML = "Button Clicked";'>Click Me!</button>**

### HTML + Javascript Code

```
1 <!DOCTYPE html>
2 <html>
3   <head>
4     <title>TryHackMe Editor</title>
5   </head>
6   <body>
7     <div id="demo">Hi there!</div>
8     <button
9       onclick='document.getElementById("demo").innerHTML = "Button
10      Clicked";'>Click Me!</button>
11     <script type="text/javascript">
12       document.getElementById("demo").innerHTML = "Hack
13       The Planet"
14     </script>
15   </body>
16 </html>
```

Render HTML+JS Code

Type HTML/JS into the box above, then click the "Render HTML+JS" button to see how it looks

↓

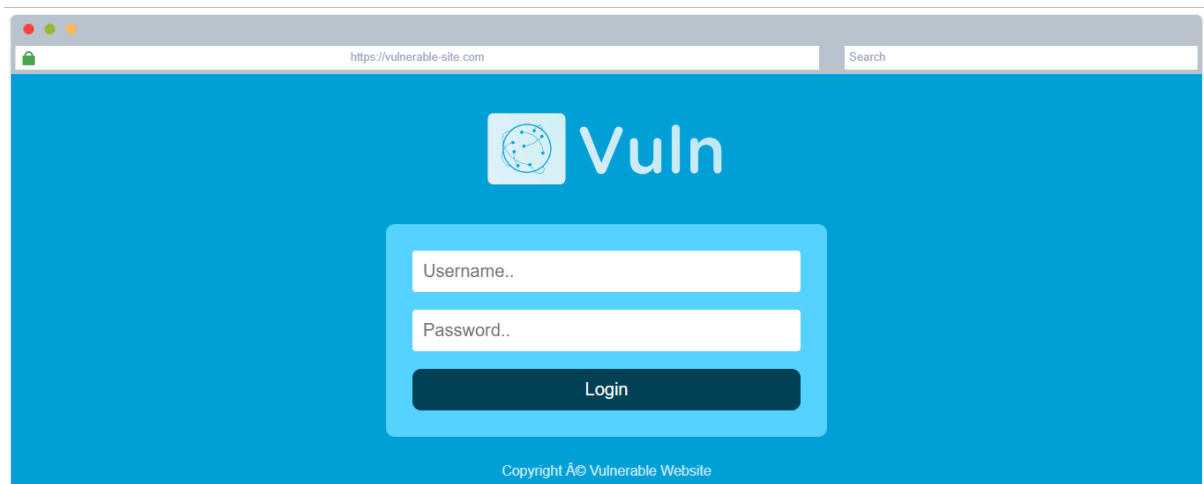
Rendered HTML Code

## Task 4 Sensitive Data Exposure

View the website on this link. What is the password hidden in the source code?

Hint: The link requires internet access, so you can not use it with a free AttackBox but instead open it from your own machine.

**Answer: testpasswd**



→ I right clicked on the page to view the page source and found the password

```
Line wrap ☐
1 <!DOCTYPE html>
2 <html>
3
4 <head>
5   <title>How websites work</title>
6   <link rel="stylesheet" href="css/style.css"></link>
7 </head>
8
9 <body>
10   <div id="html-code-box">
11     <div id="html-bar">
12       <span id="html-url">https://vulnerable-site.com</span>
13     </div>
14     <div class="theme" id="html-code">
15       <div class="logo-pos"></div>
16       <p id="login-msg"></p>
17       <form method="post" id="form" autocomplete="off">
18         <div class="form-field">
19           <input class="input-text" type="text" name="username" placeholder="Username..">
20         </div>
21         <div class="form-field">
22           <input class="input-text" type="password" name="password" placeholder="Password..">
23         </div>
24         <button onclick="login()" type="button" class="login">Login</button>
25       </form>
26       <div class="footer">Copyright Â© Vulnerable Website</div>
27     </div>
28   </div>
29   <script src="js/script.js"></script>
30 </body>
31 </html>
```

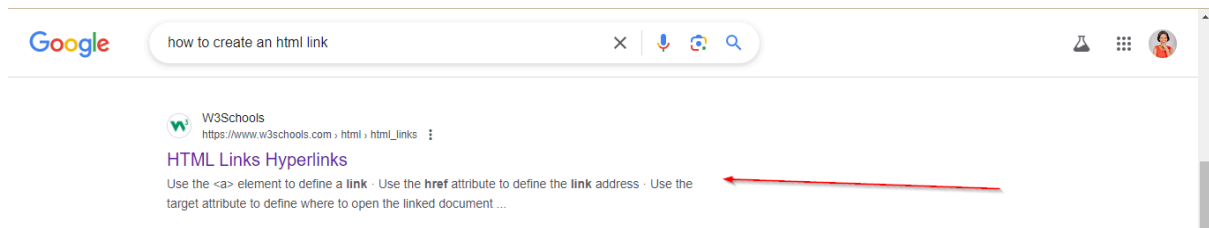
TODO: Remove test credentials!  
Username: admin  
Password: testpasswd

## Task 5 HTML Injection

View the website on this task and inject HTML so that a malicious link to <http://hacker.com> is shown.

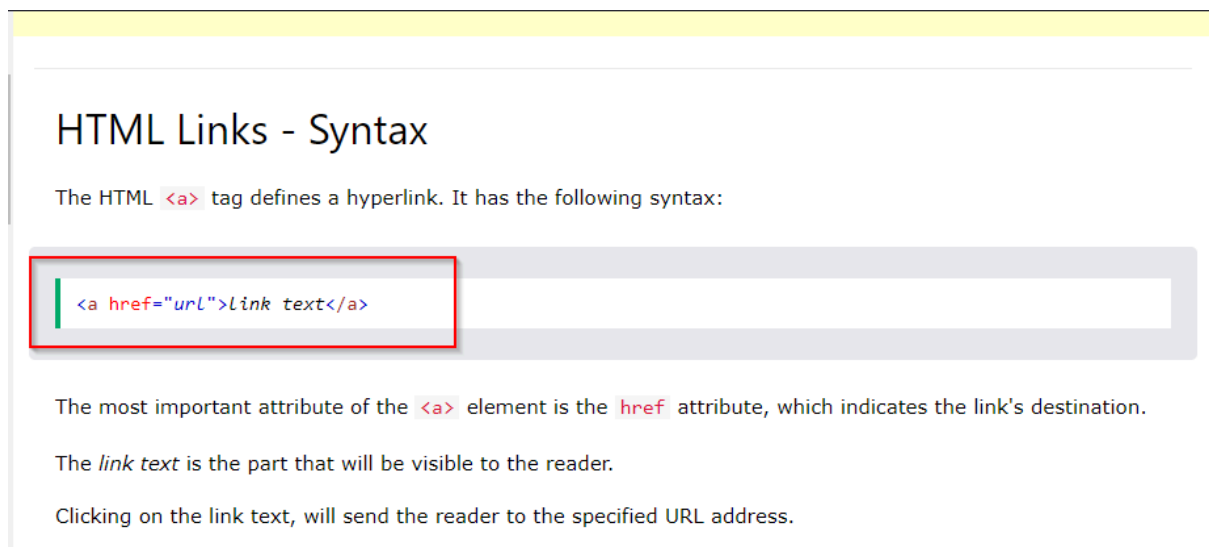
Answer: **HTML\_INJ3CTION**

Hint: Google how to create a HTML link and use it as input to the "What's your name" field.



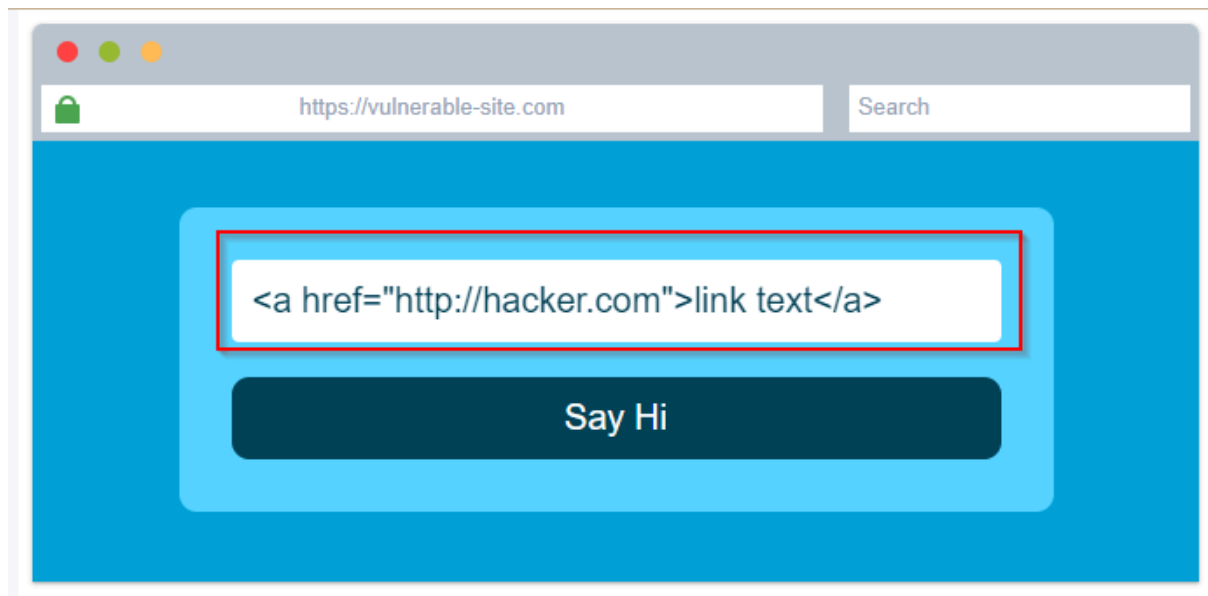
→ Then i got the syntax in the w3schools page

Syntax: **<a href="url">link text</a>**

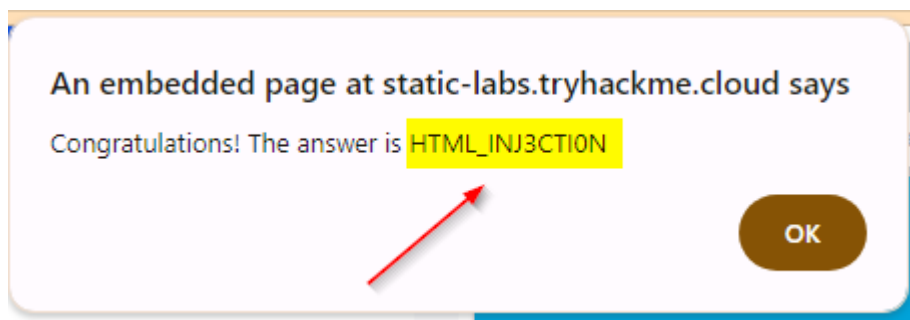


→ HTML Link i injected is : **<a href="http://hacker.com">link text</a>**

→ Then i clicked on "Say Hi"



→ Finally, i got the flag



**END!!!**