

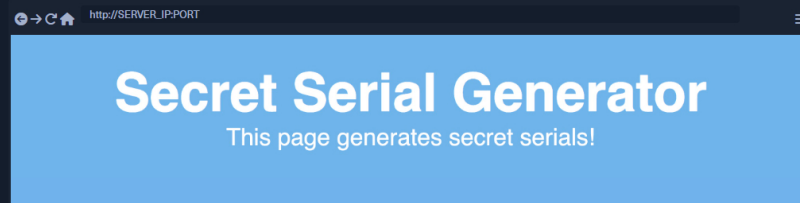
## Source Code

Most websites nowadays utilize JavaScript to perform their functions. While **HTML** is used to determine the website's main fields and parameters, and **CSS** is used to determine its design, **JavaScript** is used to perform any functions necessary to run the website. This happens in the background, and we only see the pretty front-end of the website and interact with it.

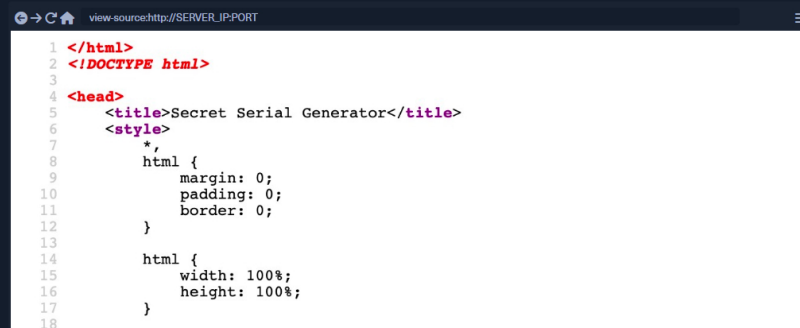
Even though all of this source code is available at the client-side, it is rendered by our browsers, so we do not often pay attention to the HTML source code. However, if we wanted to understand a certain page's client-side functionalities, we usually start by taking a look at the page's source code. This section will show how we can uncover the source code that contains all of this and understand its general usage.

## HTML

We will start by starting the exercise below, open Firefox in our PwnBox, and visit the url shown in the question:



As we can see, the website says **Secret Serial Generator**, without having any input fields or showing any clear functionality. So, our next step is to peek at its source code. We can do that by pressing **[CTRL + U]**, which should open the source view of the website:



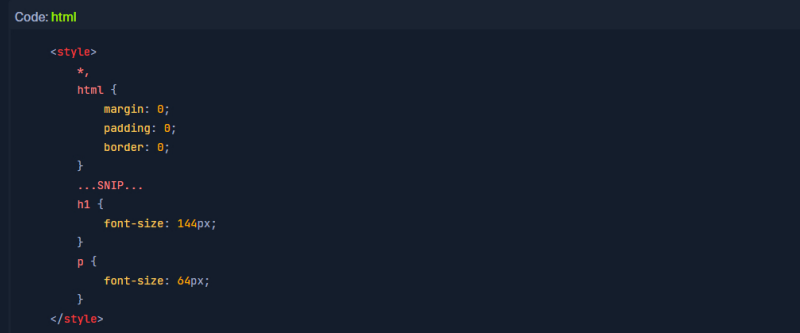
As we can see, we can view the **HTML** source code of the website.

The HTML source code can hold various information, such as comments, to further facilitate a better understanding of the code. Developers may leave sensitive information, which can be further taken advantage of. It is worth reading through the HTML comments.

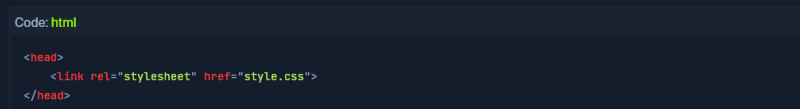
## CSS

**CSS** code is either defined **internally** within the same **HTML** file between **<style>** elements, or defined **externally** in a separate **.css** file and referenced within the **HTML** code.

In this case, we see that the **CSS** is internally defined, as seen in the code snippet below:



If a page **CSS** style is externally defined, the external **.css** file is referred to with the **<link>** tag within the HTML head, as follows:

[Cheat Sheet](#)[Go to Questions](#)

### Table of Contents

#### Introduction

- [Introduction](#) ✓
- [Source Code](#) ✓

#### Obfuscation

- [Code Obfuscation](#) ✓
- [Basic Obfuscation](#) ✓
- [Advanced Obfuscation](#) ✓
- [Deobfuscation](#) ✓

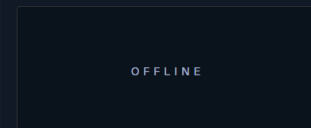
#### Deobfuscation Examples

- [Code Analysis](#) ✓
- [HTTP Requests](#) ✓
- [Decoding](#) ✓

#### Skills Assessment

- [Skills Assessment](#) ✓
- [Summary](#) ✓

#### My Workstation

[Start Instance](#)

00 / 1 spawns left

## JavaScript

The same concept applies to **JavaScript**. It can be internally written between `<script>` elements or written into a separate `.js` file and referenced within the `HTML` code.

We can see in our `HTML` source that the `.js` file is referenced externally:

Code: `html`


```
<script src="secret.js"></script>
```

We can check out the script by clicking on `secret.js`, which should take us directly into the script. When we visit it, we see that the code is very complicated and cannot be comprehended:

Code: `javascript`


```
eval(function (p, a, c, k, e, d) { e = function (c) { '...SNIP... |true|function'.split('|'), 0, {}))
```

The reason behind this is `code obfuscation`. What is it? How is it done? Where is it used?

**Connect to Pwnbox**  
Your own web-based Parrot Linux Instance to play our labs.

Pwnbox Location


UK 100ms

 Terminate Pwnbox to switch location

Start Instance

∞ / 1 spawns left

Waiting to start...

☒ Enable step-by-step solutions for all questions 


### Questions

Answer the question(s) below to complete this Section and earn cubes!



Cheat Sheet


Target(s): [Click here to spawn the target system!](#)

**+ 1**  Repeat what you learned in this section, and you should find a secret flag, what is it?


HTB{4lw4y5\_r34d\_7h3\_50urc3}

 Submit

 Hint

 Previous

Next 

 Mark Complete & Next

