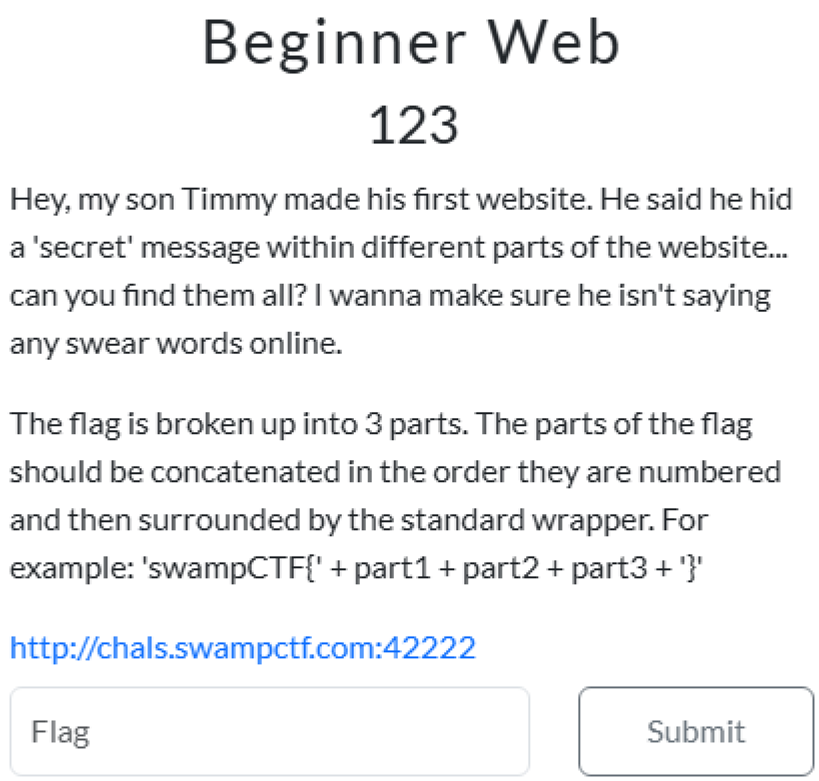


Beginner Web

123

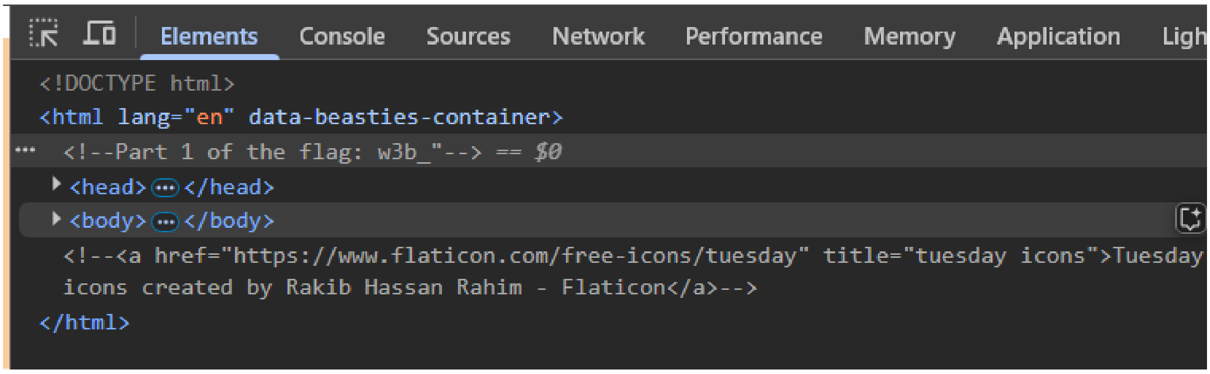
Hey, my son Timmy made his first website. He said he hid a 'secret' message within different parts of the website... can you find them all? I wanna make sure he isn't saying any swear words online.

The flag is broken up into 3 parts. The parts of the flag should be concatenated in the order they are numbered and then surrounded by the standard wrapper. For example: 'swampCTF{' + part1 + part2 + part3 + '}'

http://chals.swampctf.com:42222

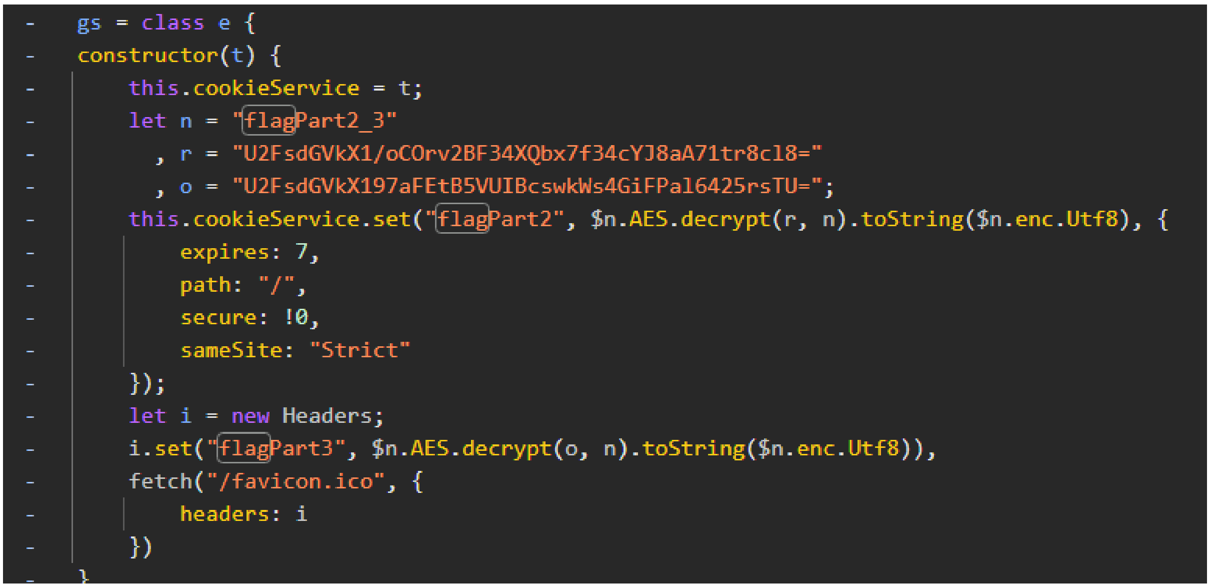
The challenge is asking us to find the hidden flags in the website

1. I inspect the website and we got the part 1



```
<!DOCTYPE html>
<html lang="en" data-beasties-container>
  <!--Part 1 of the flag: w3b_"--> == $0
  ▶ <head> ⋯ </head>
  ▶ <body> ⋯ </body>
  <!--<a href="https://www.flaticon.com/free-icons/tuesday" title="tuesday icons">Tuesday
  icons created by Rakib Hassan Rahim - Flaticon</a>-->
</html>
```

2. I saw something inside a js file in source, and it’s the based64 of the flag and I saw that the flag is encrypted in AES in CBC mode



```
-   gs = class e {
-   constructor(t) {
-       this.cookieService = t;
-       let n = "flagPart2_3"
-         , r = "U2FsdGVkX1/oCOrv2BF34XQbx7f34cYJ8aA71tr8cl8="
-         , o = "U2FsdGVkX197aFEtB5VUIBcswkWs4GiFPal6425rsTU=";
-       this.cookieService.set("flagPart2", $n.AES.decrypt(r, n).toString($n.enc.Utf8), {
-           expires: 7,
-           path: "/",
-           secure: !0,
-           sameSite: "Strict"
-       });
-       let i = new Headers;
-       i.set("flagPart3", $n.AES.decrypt(o, n).toString($n.enc.Utf8)),
-       fetch("/favicon.ico", {
-           headers: i
-       })
-   }
```

3. then this is the script I used to decrypt the flag

```
const CryptoJS = require("crypto-js");

function decryptFlagParts() {

   const key = "flagPart2_3";

   const encryptedPart2 = "U2FsdGVkX1/oCOrv2BF34XQbx7f34cYJ8aA71tr8cl8=";
   const encryptedPart3 = "U2FsdGVkX197aFEtB5VUIBcswkWs4GiFPal6425rsTU=";
   const flagPart2 = CryptoJS.AES.decrypt(encryptedPart2,
key).toString(CryptoJS.enc.Utf8);
   const flagPart3 = CryptoJS.AES.decrypt(encryptedPart3,
key).toString(CryptoJS.enc.Utf8);
   console.log("Flag Part 2:", flagPart2);
   console.log("Flag Part 3:", flagPart3);

   const part1 = "w3b_";

   const flag = "swampCTF{" + part1 + flagPart2 + flagPart3 + "}";

   console.log("Complete Flag:", flag);
}

decryptFlagParts();
```

Flag : swampCTF{w3b_br0w53r5_4r3_c0mpl1c473d}