Fast Hands

Writeup by Speer

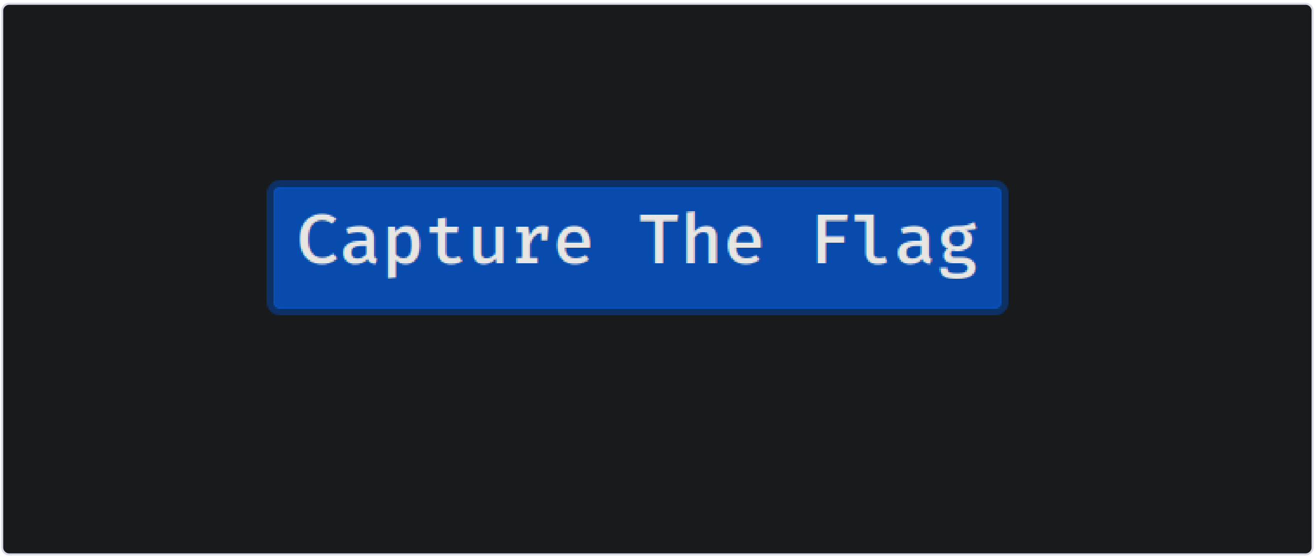
Category: Warmups

Author: JohnHammond

Description

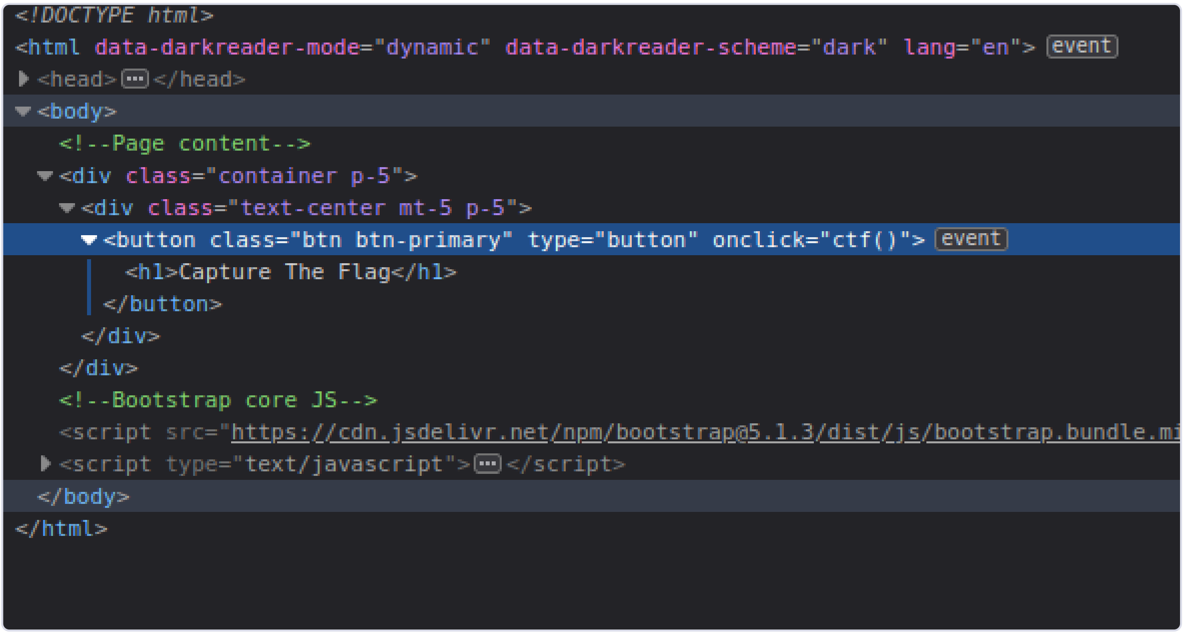
You can capture the flag, but you gotta be fast!

Going to the site I find a button:



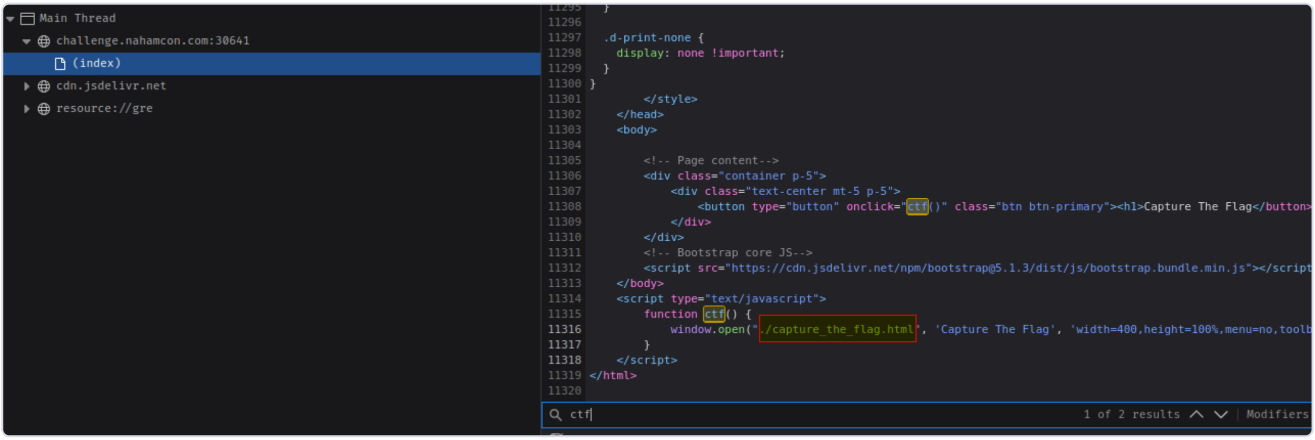
When clicking this it opens a new window that then loads and closes itself.

In inspector we can see the event:



```
<!DOCTYPE html>
<html data-darkreader-mode="dynamic" data-darkreader-scheme="dark" lang="en"> event
 ▶<head>⋯</head>
 ▼<body>
    <!--Page content-->
   ▼<div class="container p-5">
     ▼<div class="text-center mt-5 p-5">
       ▼<button class="btn btn-primary" type="button" onclick="ctf()"> event
          <h1>Capture The Flag</h1>
        </button>
      </div>
    </div>
    <!--Bootstrap core JS-->
    <script src="https://cdn.jsdelivr.net/npm/bootstrap@5.1.3/dist/js/bootstrap.bundle.mi
   ▶<script type="text/javascript">⋯</script>
  </body>
</html>
```

checking the function in debugger:

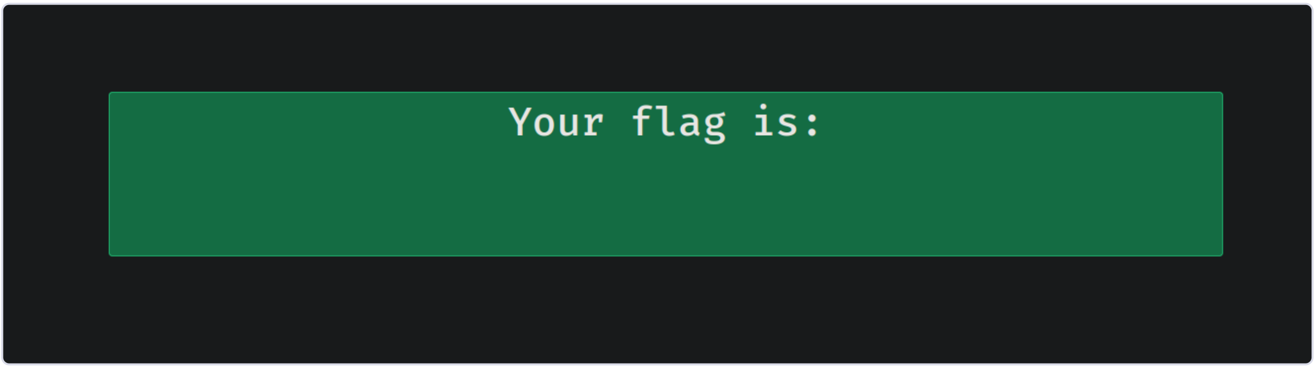


```
  }

  .d-print-none {
    display: none !important;
  }
}
        </style>
    </head>
    <body>

        <!-- Page content-->
        <div class="container p-5">
            <div class="text-center mt-5 p-5">
                <button type="button" onclick="ctf()" class="btn btn-primary"><h1>Capture The Flag</button>
            </div>
        </div>
        <!-- Bootstrap core JS-->
        <script src="https://cdn.jsdelivr.net/npm/bootstrap@5.1.3/dist/js/bootstrap.bundle.min.js"></script
    </body>
    <script type="text/javascript">
        function ctf() {
            window.open("./capture_the_flag.html", 'Capture The Flag', 'width=400,height=100%,menu=no,toolb
        }
    </script>
</html>
```

it opens:

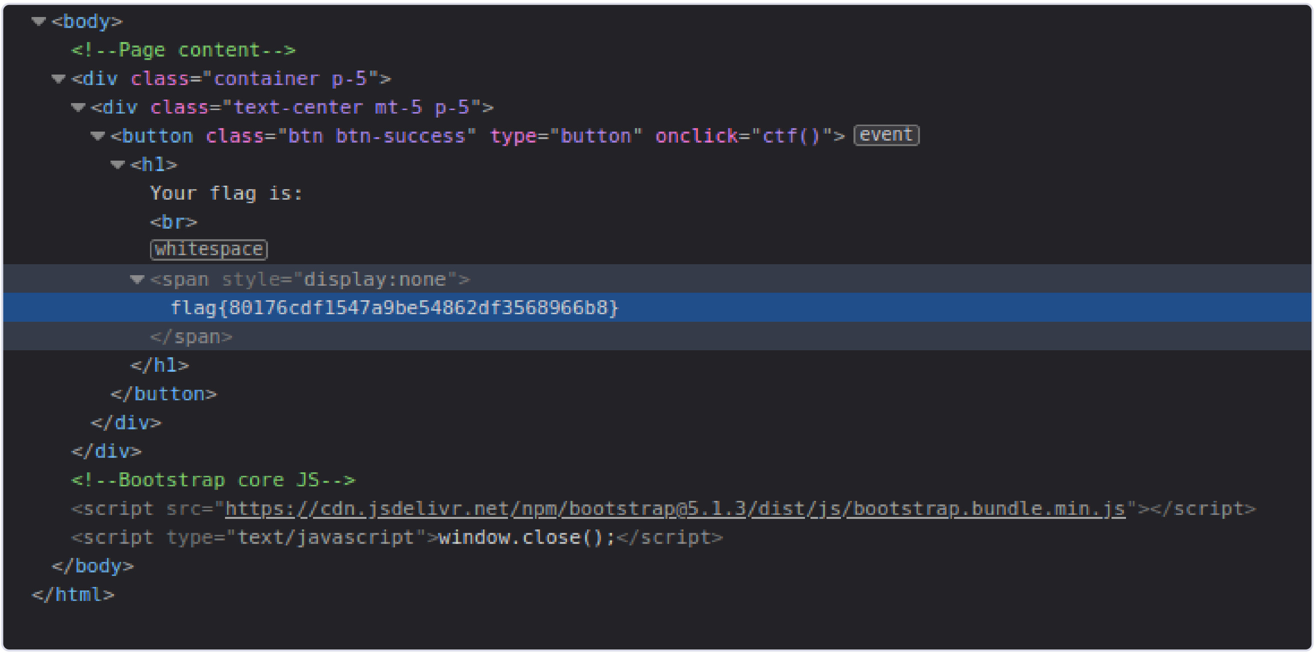
`./capture_the_flag.html`

which leads to another empty page with this in the middle:



Your flag is:

If I look in the body tags I can see the hidden flag:



```
<body>
  <!--Page content-->
  <div class="container p-5">
    <div class="text-center mt-5 p-5">
      <button class="btn btn-success" type="button" onclick="ctf()"> event
        <h1>
          Your flag is:
          <br>
          whitespace
          <span style="display:none">
            flag{80176cdf1547a9be54862df3568966b8}
          </span>
        </h1>
      </button>
    </div>
  </div>
  <!--Bootstrap core JS-->
  <script src="https://cdn.jsdelivr.net/npm/bootstrap@5.1.3/dist/js/bootstrap.bundle.min.js"></script>
  <script type="text/javascript">window.close();</script>
</body>
</html>
```

`flag{80176cdf1547a9be54862df3568966b8}`