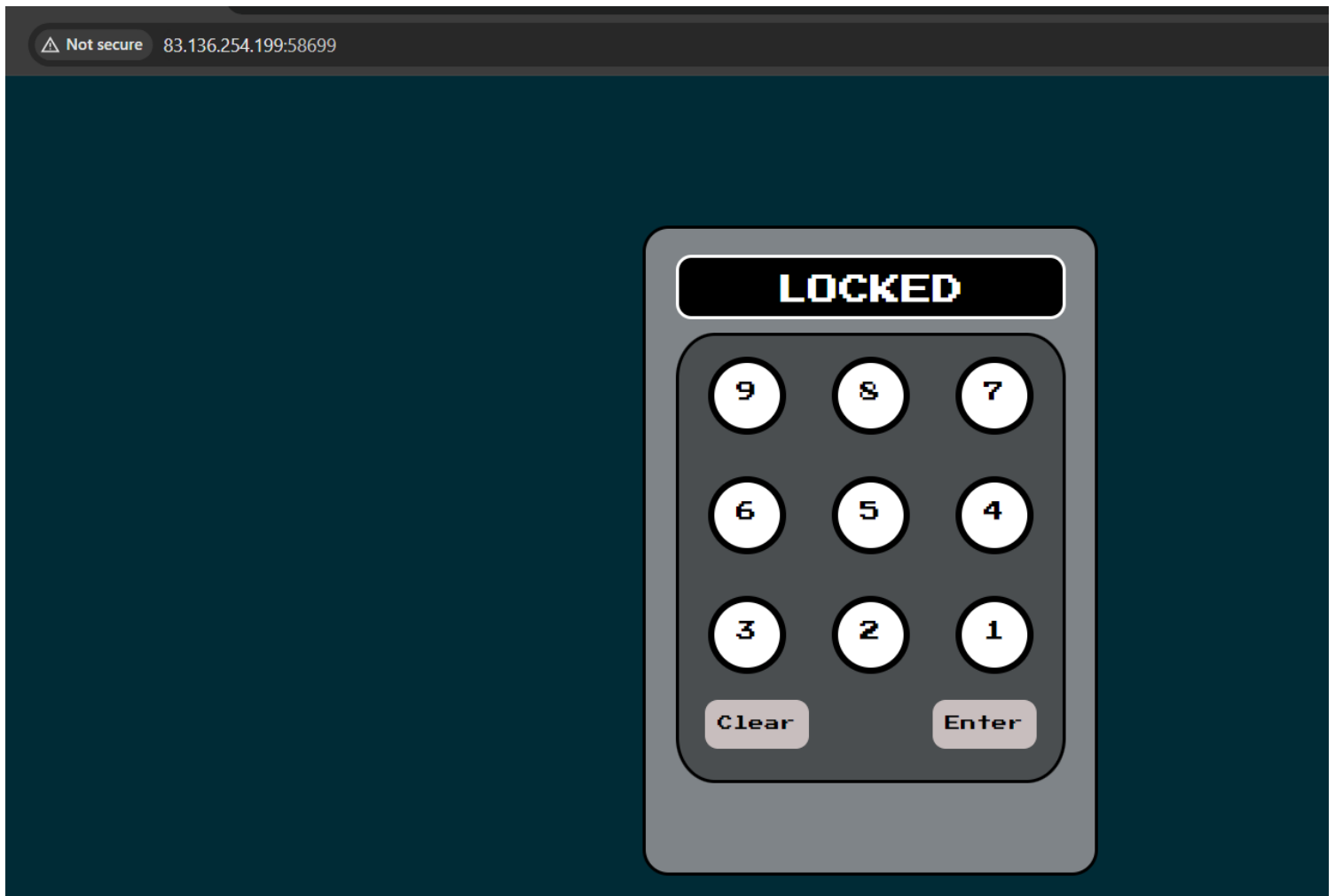


Trapped Source

1) Checked the page



2) Pin is stored in source

Line wrap ☐

```
1 <!DOCTYPE html>
2 <html lang="en">
3
4 <head>
5   <meta charset="UTF-8">
6   <title></title>
7   <link rel="stylesheet" href="/static/css/style.css">
8   <link rel="stylesheet" href="/static/css/bootstrap.min.css">
9
10 </head>
11
12 <body>
13   <script>
14     window.CONFIG = window.CONFIG || {
15       buildNumber: "v20190816",
16       debug: false,
17       modelName: "Valencia",
18       correctPin: "9880",
19     }
20   </script>
21   <div class="lockbox">
22     <div class="lockStatus">LOCKED</div>
23     <div class="lockMid">
24       <span id="btn9" class="button" onclick="unlock(9)">9</span>
25       <span id="btn8" class="button" onclick="unlock(8)">8</span>
26       <span id="btn7" class="button" onclick="unlock(7)">7</span>
27       <span id="btn6" class="button" onclick="unlock(6)">6</span>
28       <span id="btn5" class="button" onclick="unlock(5)">5</span>
29       <span id="btn4" class="button" onclick="unlock(4)">4</span>
30       <span id="btn3" class="button" onclick="unlock(3)">3</span>
31       <span id="btn2" class="button" onclick="unlock(2)">2</span>
32       <span id="btn1" class="button" onclick="unlock(1)">1</span>
33       <div class="clear" onclick="reset()">Clear</div>
34       <div class="scoreCount" onclick="checkPin()">Enter</div>
35     </div>
36   </div>
37
38   <!-- partial -->
39   <script src="/static/js/jquery.js"></script>
40   <script src="/static/js/script.js"></script>
41 </body>
42
43 </html>
```

3) Manually added the 0th button

The screenshot shows a web browser's developer tools interface. The left pane displays the HTML document structure, and the right pane shows the CSS styles for the selected element.

HTML Structure:

```

<!DOCTYPE html>
<html lang="en">
  <head> </head>
  <body>
    <script> </script>
    <div class="lockbox">
      <div class="lockStatus">LOCKED</div>
      <div class="lockMid">
        <span id="btn9" class="button" onclick="unlock(9)">9</span>
        <span id="btn8" class="button" onclick="unlock(8)">8</span>
        <span id="btn7" class="button" onclick="unlock(7)">7</span>
        <span id="btn6" class="button" onclick="unlock(6)">6</span>
        <span id="btn5" class="button" onclick="unlock(5)">5</span>
        <span id="btn4" class="button" onclick="unlock(4)">4</span>
        <span id="btn3" class="button" onclick="unlock(3)">3</span>
        <span id="btn2" class="button" onclick="unlock(2)">2</span>
        <span id="btn1" class="button" onclick="unlock(1)">1</span>
        <span id="btn0" class="button" onclick="unlock(0)">0</span>
        <div class="clear" onclick="reset()">Clear</div>
        <div class="scoreCount" onclick="checkPin()">Enter</div>
      </div>
    </div>
    <!-- partial -->
    <script src="/static/js/jquery.js"></script>
    <script src="/static/js/script.js"></script>
  </body>
</html>

```

CSS Styles:

```

element.style {
}

.style.c...
.lockMid {
  position:
    relati
  width:
    300px
  ;
  margin
    :
    auto;
  border-
    radius
    :
    10%;
  background-
    color
    :
    rgb(
  text-
    align
    :
    center
  bottom
    :
    -30px
  ;
}

```

4) Unlocked it

HTB{vi3w_cli13nt_s0urc3_s3cr3ts!}

9

8

7

6

5

4

3

2

1

0

Clear

Enter

Alternatively:

```

currentPin = []

const checkPin = () => {
  pin = currentPin.join('')

  if (CONFIG.correctPin === pin) {
    fetch('/flag', {
      method: 'POST',
      headers: {
        'Content-Type': 'application/json'
      },
      body: JSON.stringify({
        'pin': CONFIG.correctPin
      })
    })
    .then((data) => data.json())
    .then((res) => {
      $('#lockStatus').css('font-size', '8px')
      $('#lockStatus').text(res.message)
    })
    return
  }

  $('#lockStatus').text('INVALID!')
  setTimeout(() => {
    reset()
  }, 3000)
}

const unlock = (pin) => {
  currentPin.push(pin)

  if (currentPin.length > 4) return

  $('#lockStatus').text(currentPin.join(' '))
}

const reset = () => {
  currentPin.length = 0
  $('#lockStatus').css('font-size', 'x-large')

  $('#lockStatus').text('LOCKED')
}

```

We can send the post request ourselves