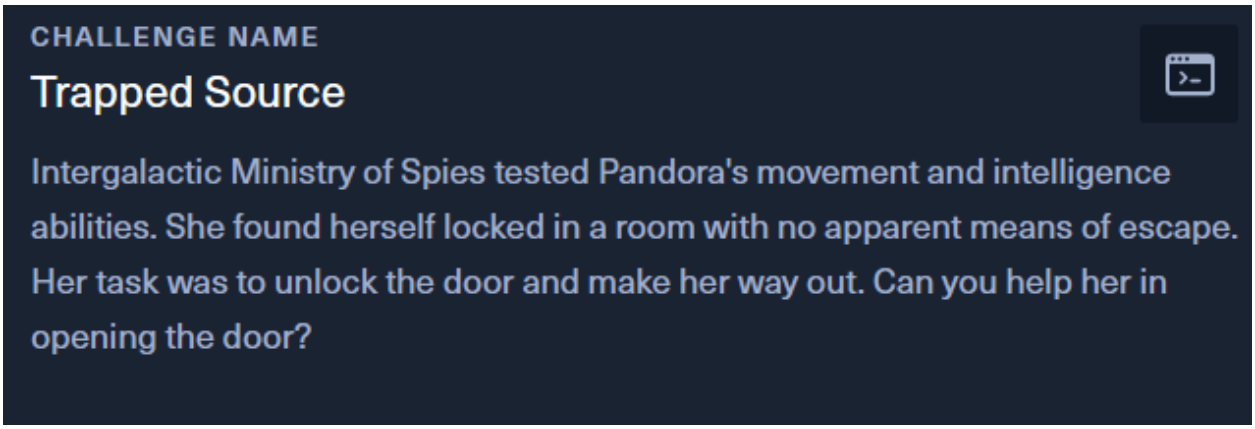
Trapped Source

Platform	HackTheBox
Category	Cyber Apocalypse 2023 - The Cursed Mission
Difficulty	very easy
Tags	source_code
Status	Rooted/Finished
Payload	
Source Code	

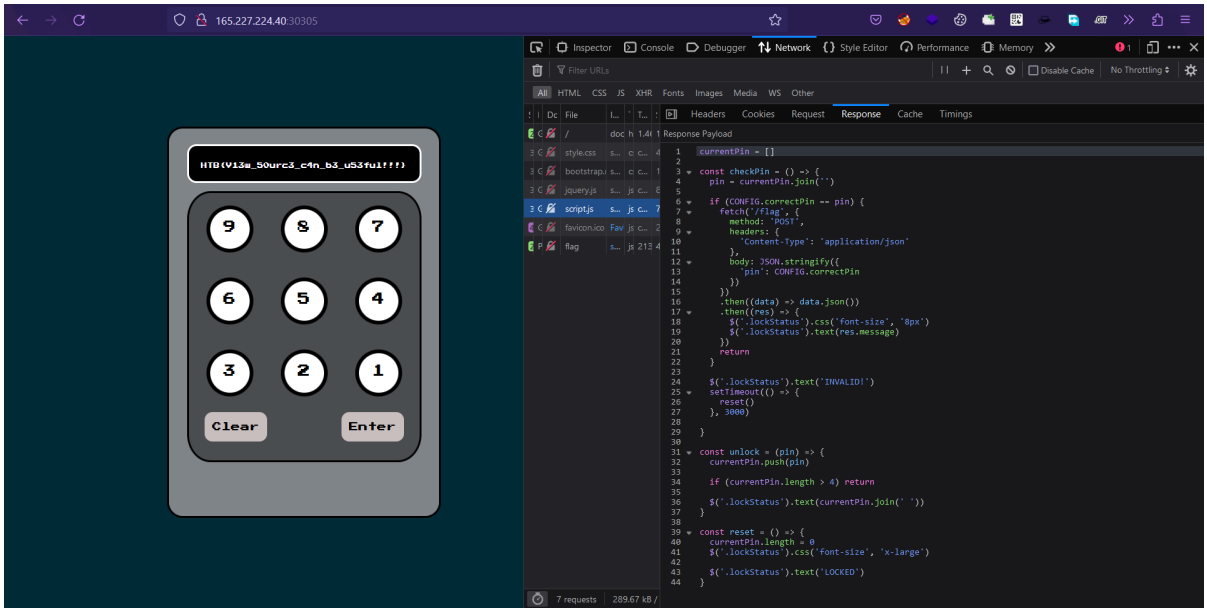
> Intro to the challenge



Set up

Information Gathering

▼ The application at-a-glance 🔍



▼ Source code review

```
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')
}
```

The Bug

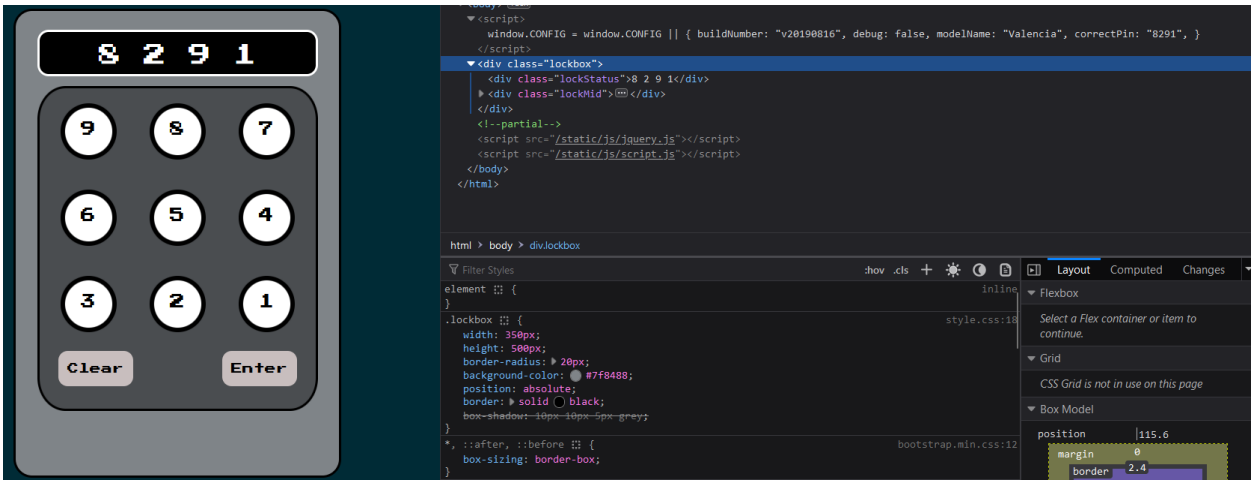
- Information Disclosure

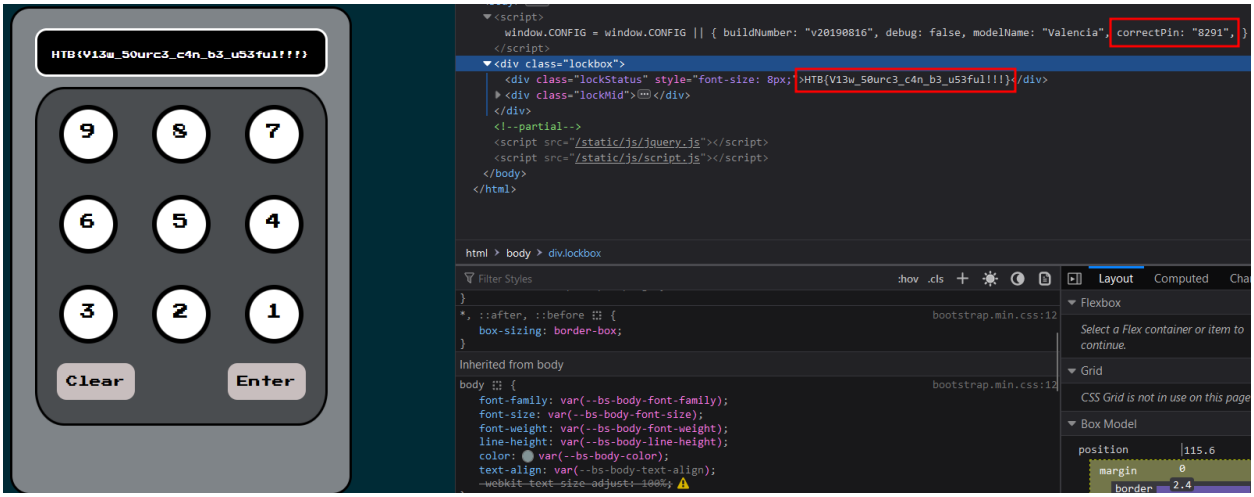
```
if (CONFIG.correctPin == pin) { //here CONFIG.correctPin == pin basically fetches the flag
    fetch('/flag', {
      method: 'POST',
      headers: {
        'Content-Type': 'application/json'
      },
      body: JSON.stringify({
        'pin': CONFIG.correctPin
      })
```

- Next I looked into the source code

```
<script>
    window.CONFIG = window.CONFIG || {
        buildNumber: "v20190816",
        debug: false,
        modelName: "Valencia",
        correctPin: "8291",
    }
</script>
```

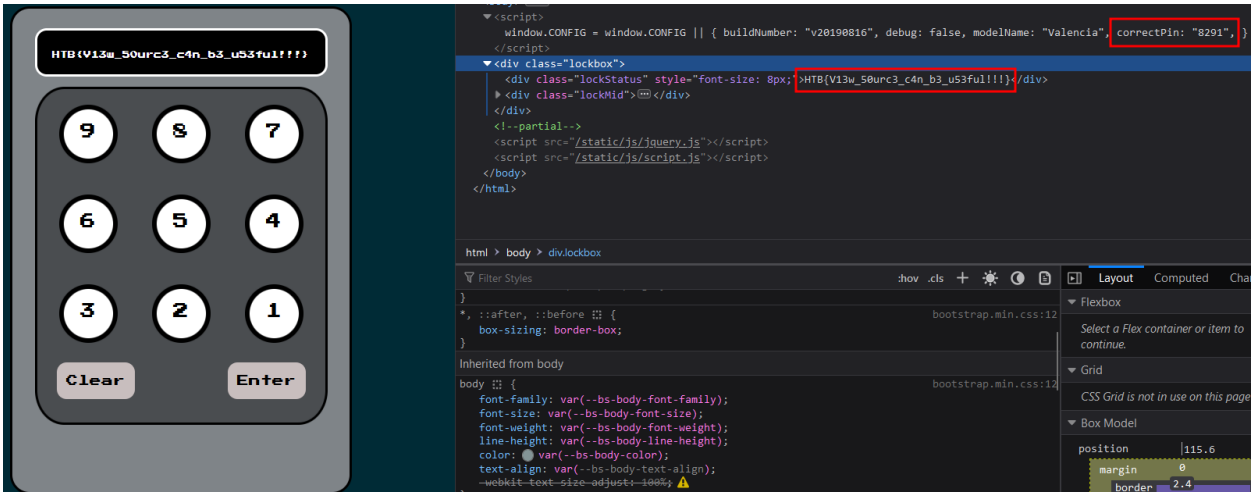
- you can see the correct pin is **8291**
- Enter the correct ping → you'll get the flag





Exploitation

Flag



Writeup

Writeup - Trapped Source [Very Easy]

Video Writeup