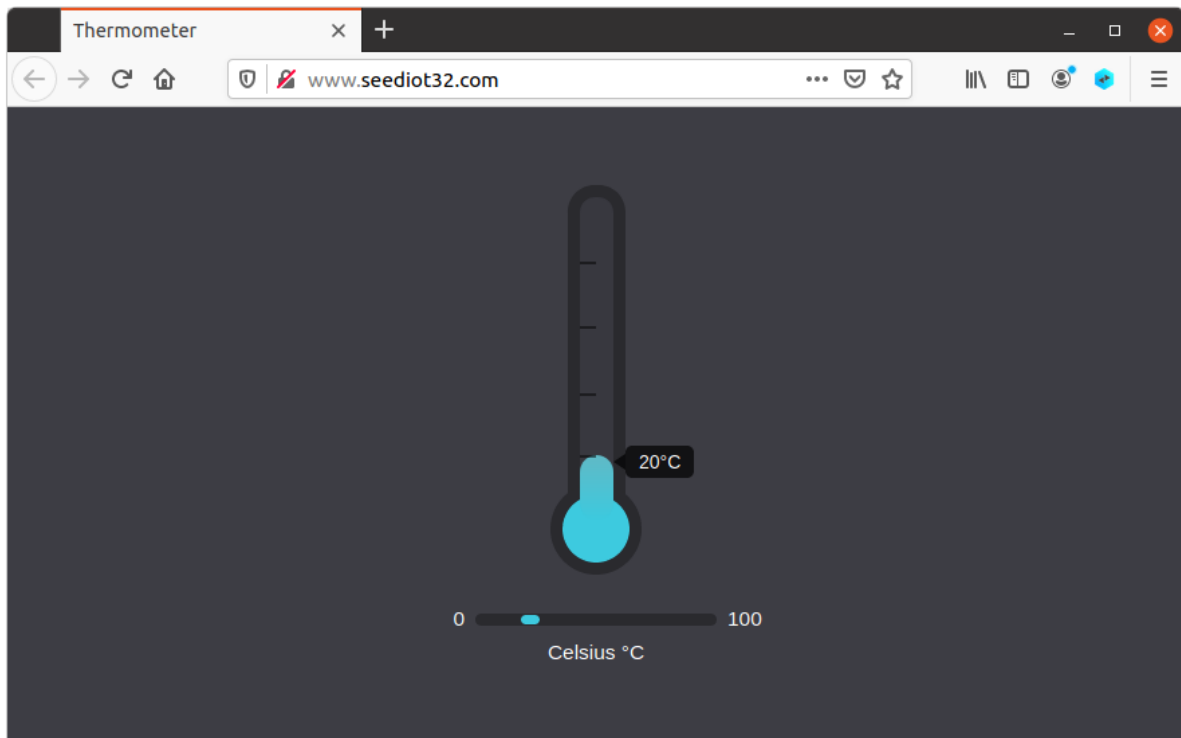


姓名：蔡佩蓉

學號：109511286

## DNS Rebinding Attack Lab (Lab8)



```
seed@VM: ~/.../Labsetup
[06/11/24]seed@VM:~/.../Labsetup$ dig www.attacker32.com

; <<>> DiG 9.16.1-Ubuntu <<>> www.attacker32.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 13044
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL:
1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: bb87becb9a58eab9010000006668a09d5376f978bbafaf2f (good)
;; QUESTION SECTION:
;www.attacker32.com.                IN      A

;; ANSWER SECTION:
www.attacker32.com.                259200  IN      A      10.9.0.180

;; Query time: 11 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Tue Jun 11 15:08:13 EDT 2024
;; MSG SIZE rcvd: 91
```

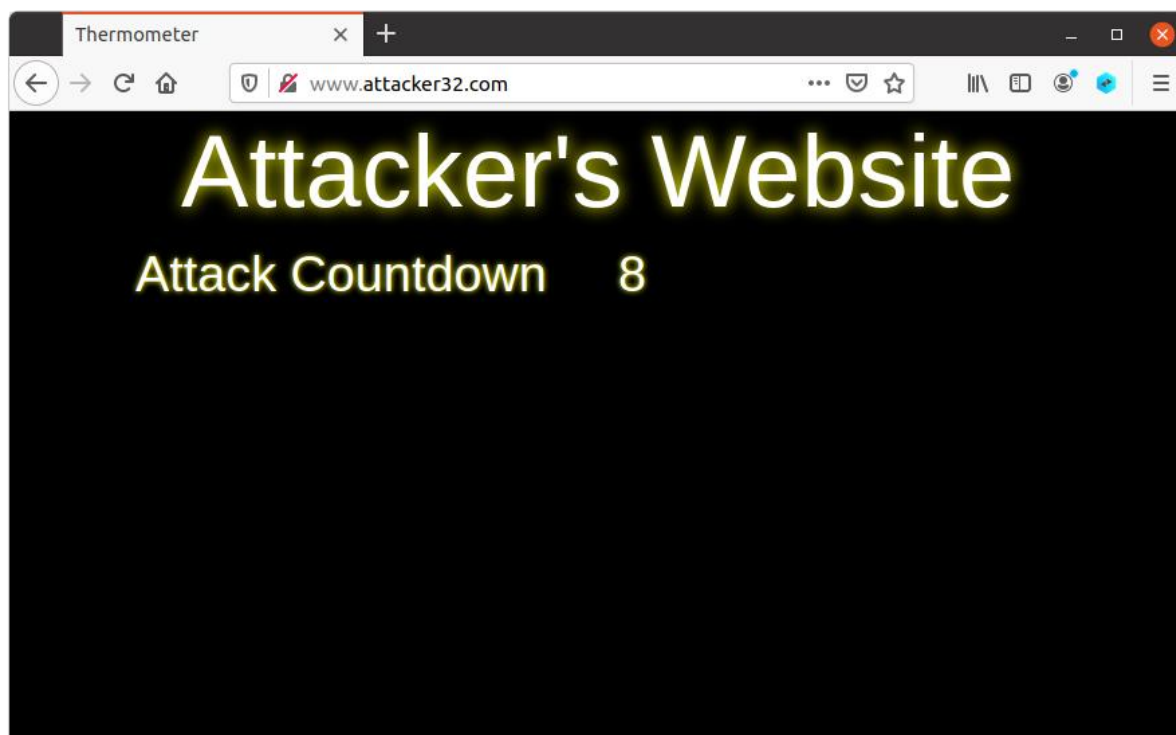
```
seed@VM: ~/.../Labsetup
[06/11/24]seed@VM:~/.../Labsetup$ dig ns.attacker32.com

; <<>> DiG 9.16.1-Ubuntu <<>> ns.attacker32.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 40062
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL:
1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: aa8f5693f2c9f2b0010000006668a0ac58ee6b352b4647f0 (good)
;; QUESTION SECTION:
;ns.attacker32.com.                IN      A

;; ANSWER SECTION:
ns.attacker32.com.                259200  IN      A      10.9.0.153

;; Query time: 95 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Tue Jun 11 15:08:28 EDT 2024
;; MSG SIZE rcvd: 90
```



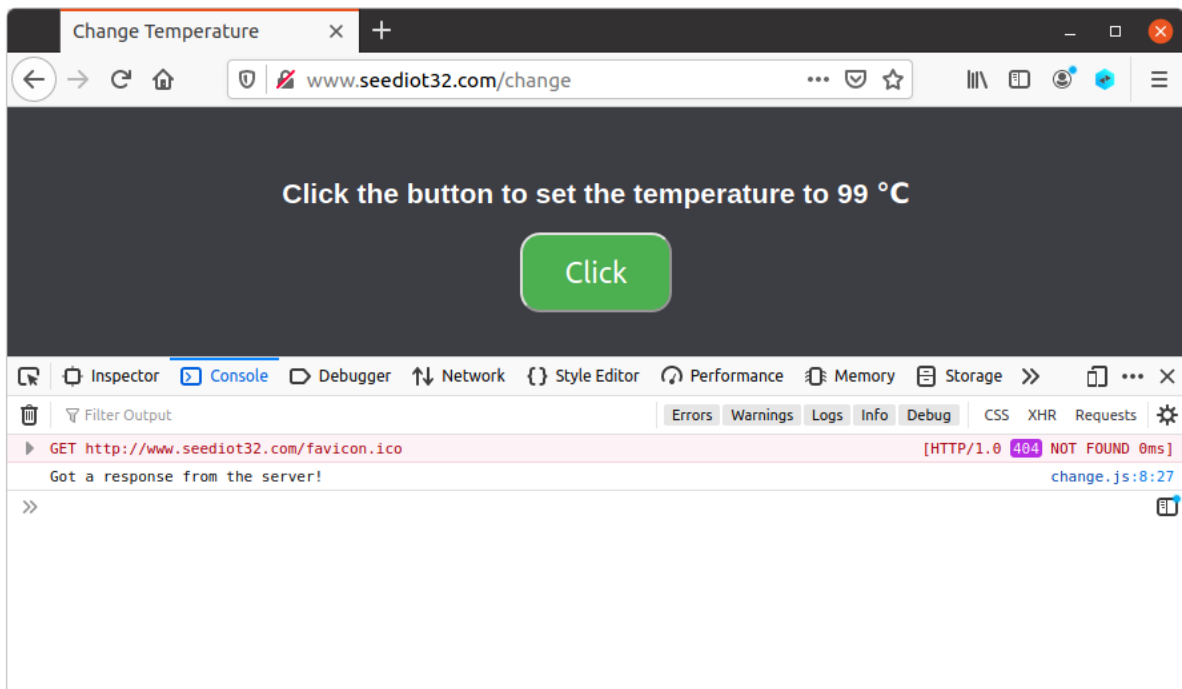
## Task 1: Understanding the Same-Origin Policy Protection

The screenshot shows a web browser window titled "Thermometer" with the address bar displaying `www.seediot32.com`. The main content area features a thermometer graphic with a blue-to-red gradient, showing a temperature of 99°C. Below the thermometer is a horizontal slider ranging from 0 to 100, labeled "Celsius °C".

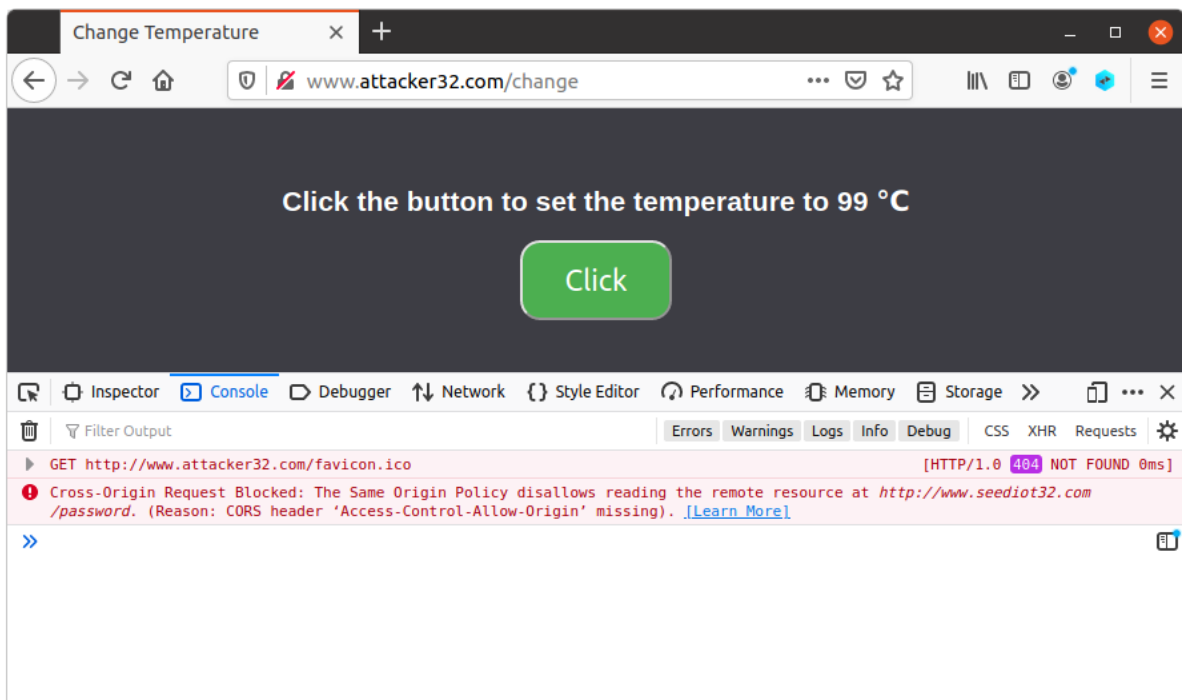
The browser's developer console is open, showing the following log entries:

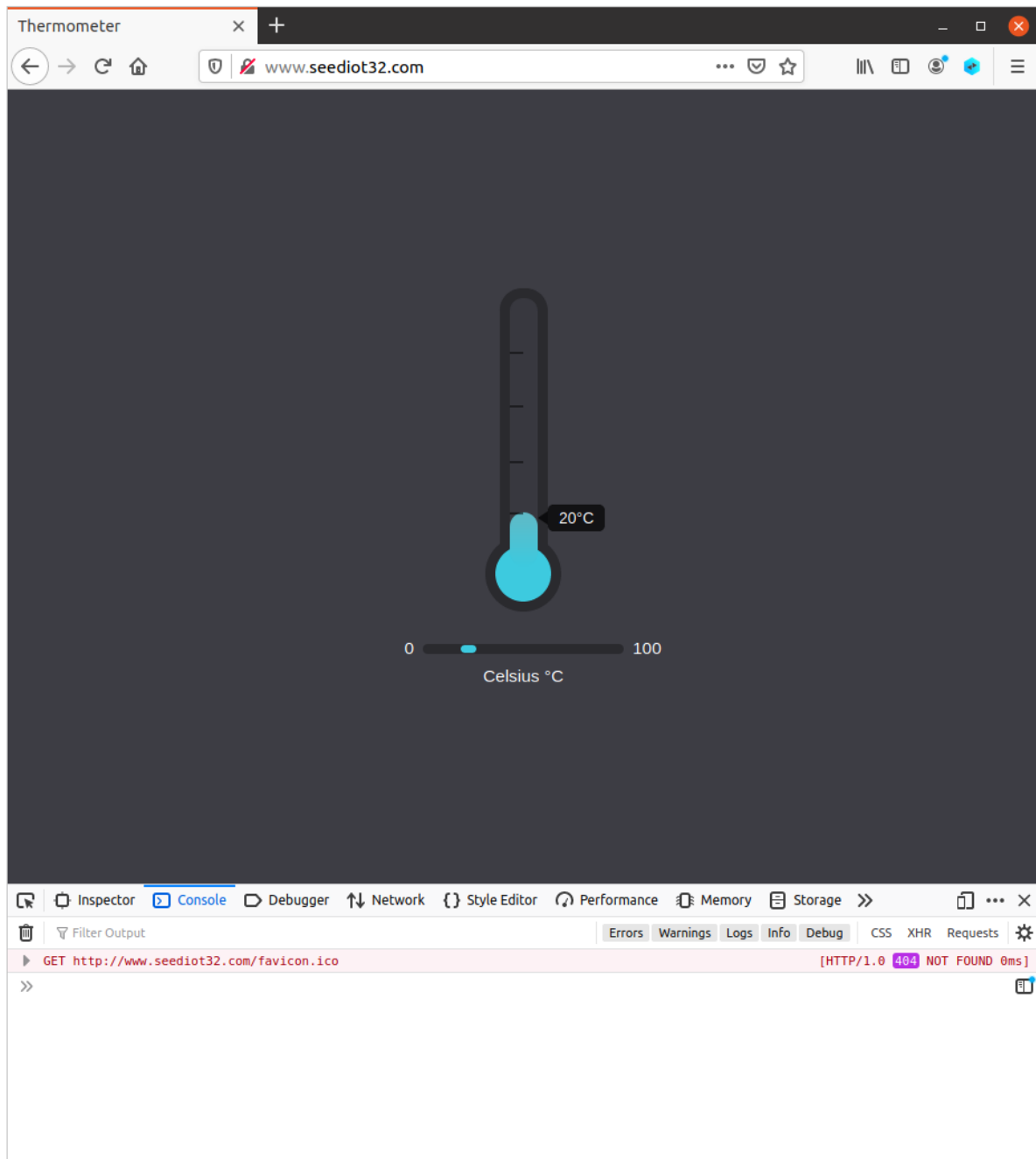
- `GET http://www.seediot32.com/favicon.ico [HTTP/1.0 404 NOT FOUND 0ms]`
- `newTemperature is [99], range.value is [20]`
- `set temperature to 99 as informed by the server.`

The console also shows the file names `main.js:60:13` and `main.js:61:13` for the respective log entries.



Observation: The temperature on the first page (<http://www.seedIoT32.com>) updated to 99 Celsius after clicking the button, indicating that the change was successfully communicated to the IoT server.



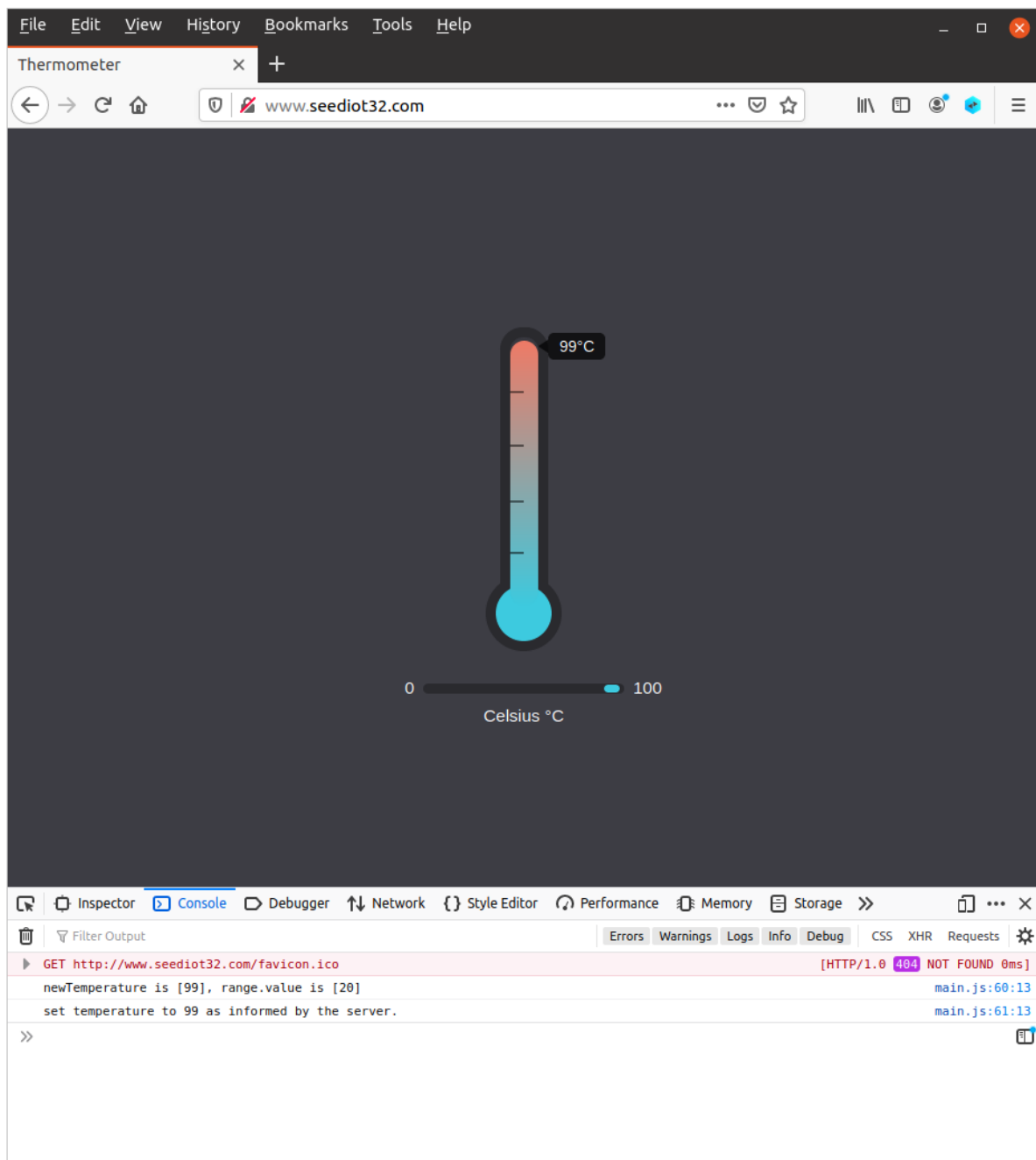


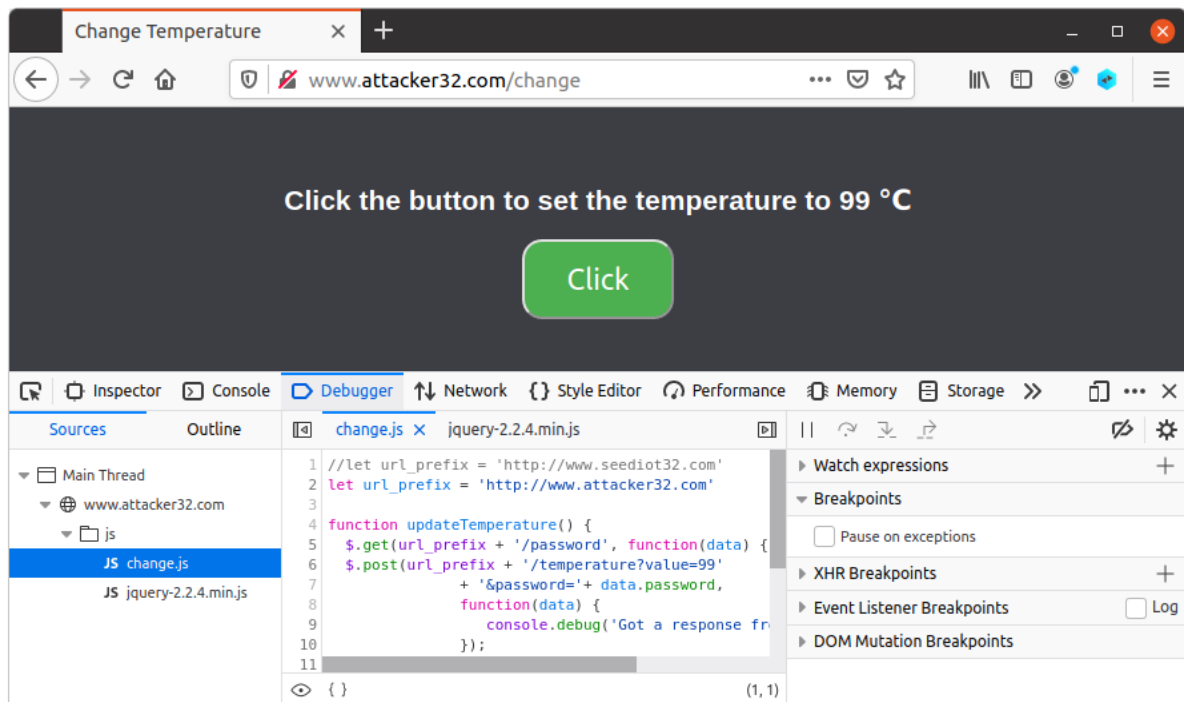
Observation: The temperature on the first page does not update to 99 Celsius, indicating that the change attempt from this page was unsuccessful.

This page (<http://www.seedIoT32.com/change>) successfully changed the thermostat's temperature because it shares the same origin with the IoT server. The origin of this URL is <http://www.seedIoT32.com>, which matches the origin of the IoT server, allowing the request to be processed and the temperature to be changed.

This page (<http://www.attacker32.com/change>) failed to change the thermostat's temperature because it violates the Same-Origin Policy. The origin <http://www.attacker32.com> is different from the origin of the IoT server (<http://www.seedIoT32.com>), leading to the request being blocked by the browser's SOP. (protecting the server from potentially harmful interactions initiated by external websites.)

## Task 2: Defeat the Same-Origin Policy Protection





```
seed@VM: ~/.../Labsetup
[06/11/24] seed@VM:~/.../Labsetup$ dig www.attacker32.com

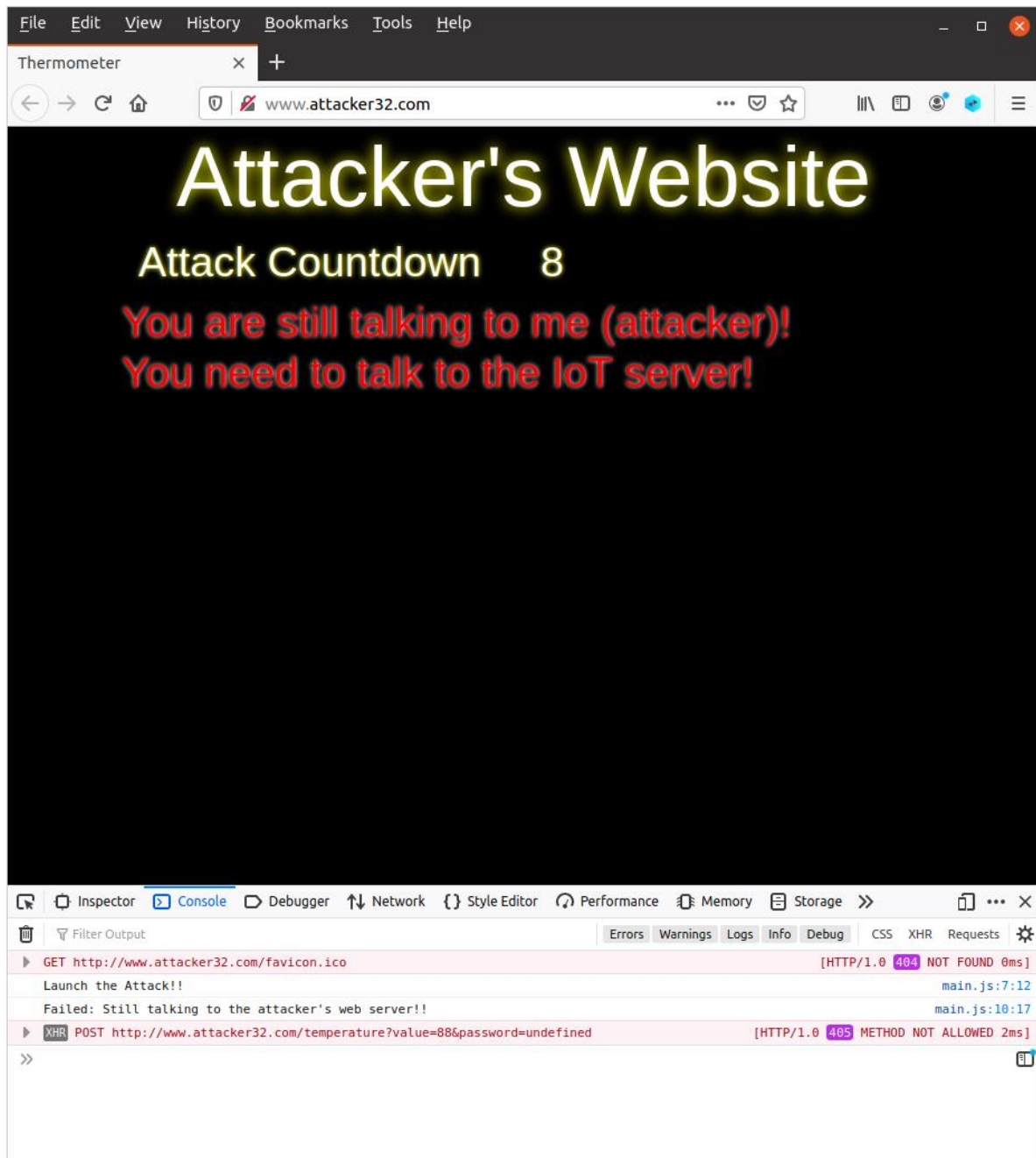
; <<>> DiG 9.16.1-Ubuntu <<>> www.attacker32.com
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 33743
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL:
1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: a05352ce744a1b82010000006668aa9c0139667bc754d393 (good)
;; QUESTION SECTION:
;www.attacker32.com.                IN      A

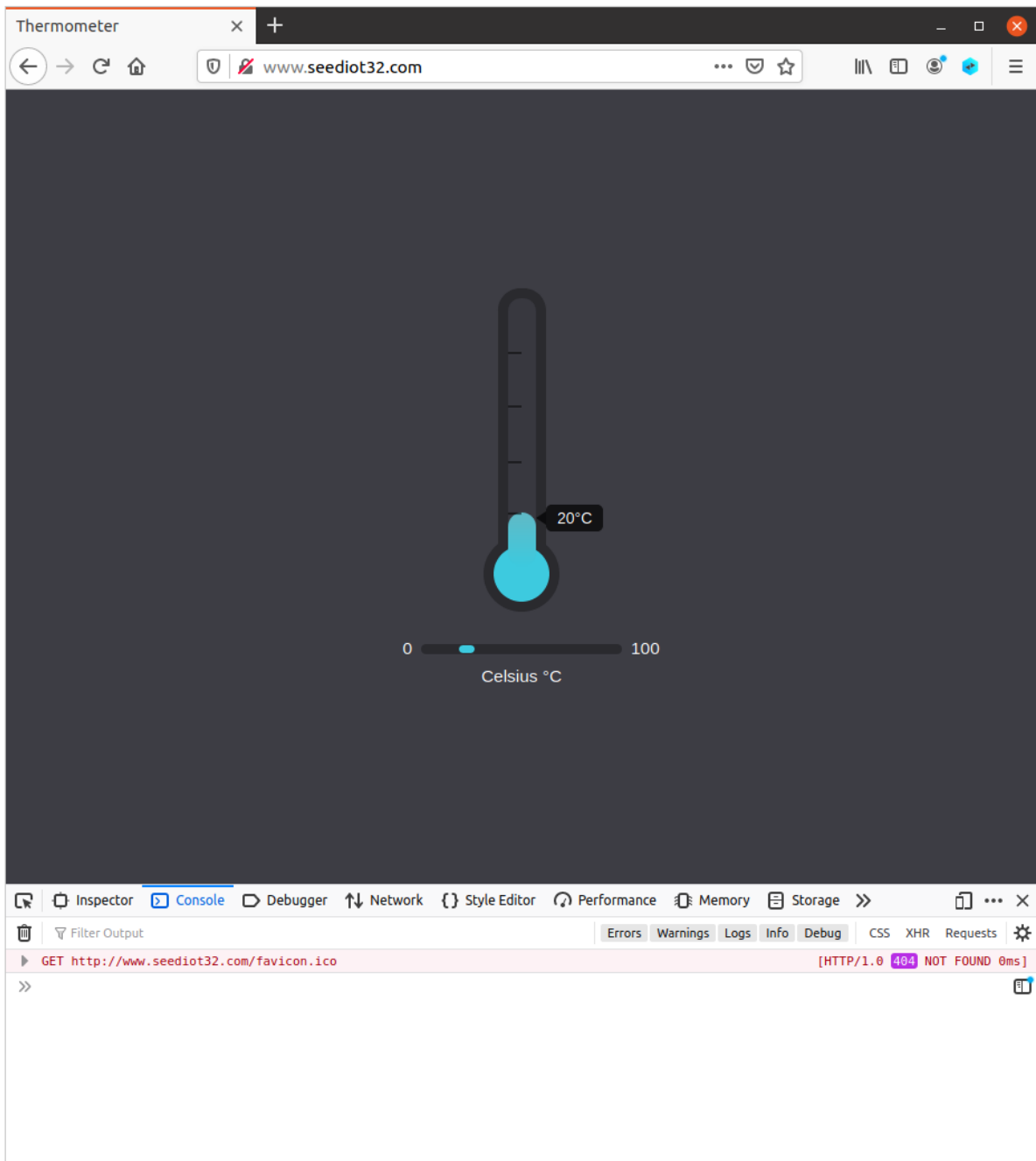
;; ANSWER SECTION:
www.attacker32.com.                259200  IN      A      192.168.60.80

;; Query time: 12 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Tue Jun 11 15:50:52 EDT 2024
;; MSG SIZE rcvd: 91
```

### Task 3: Launch the Attack







Thermometer x +

www.attacker32.com

# Attacker's Website

Attack Countdown 6

You are now talking to the IoT server!

Inspector Console Debugger Network Style Editor Performance Memory Storage

Filter Output Errors Warnings Logs Info Debug CSS XHR Requests

Failed: Still talking to the attacker's web server!! main.js:10:17

XHR POST http://www.attacker32.com/temperature?value=88&password=undefined [HTTP/1.0 405 METHOD NOT ALLOWED 4ms]

Launch the Attack!! main.js:7:12

Failed: Still talking to the attacker's web server!! main.js:10:17

XHR POST http://www.attacker32.com/temperature?value=88&password=undefined [HTTP/1.0 401 UNAUTHORIZED 2ms]

Launch the Attack!! main.js:7:12

Great, now I am talking to the IoT device!! main.js:14:17

>>


Thermometer

← → ↻ 🏠

🔒 [www.seediot32.com](http://www.seediot32.com)

⋮ 🛡️ ☆

🔍 📄 🌐 🔄 ☰



🔍

Inspector

Console

Debugger

↕ Network

{ } Style Editor

🕒 Performance

🧠 Memory

📁 Storage

⏏

⋮

✕

🗑️

🔍 Filter Output

Errors

Warnings

Logs

Info

Debug

CSS

XHR

Requests

⚙️

▶ GET <http://www.seediot32.com/favicon.ico> [HTTP/1.0 404 NOT FOUND 0ms]

newTemperature is [88], range.value is [20]

main.js:60:13

set temperature to 88 as informed by the server.

main.js:61:13

>>

📄