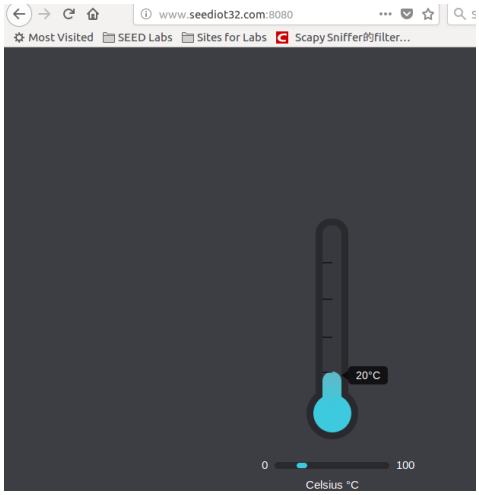
DNS Rebinding Attack Lab

1 Lab Environment Setup

User VM 10.0.2.7
Local DNS Server 10.0.2.8
Attacker VM 10.0.2.4

1.1 Task 2: Start the IoT server on the User VM



1.2 Task 3: Start the attack web server on the Attacker VM

1.3 Task 4: Configure the DNS server on the Attacker VM

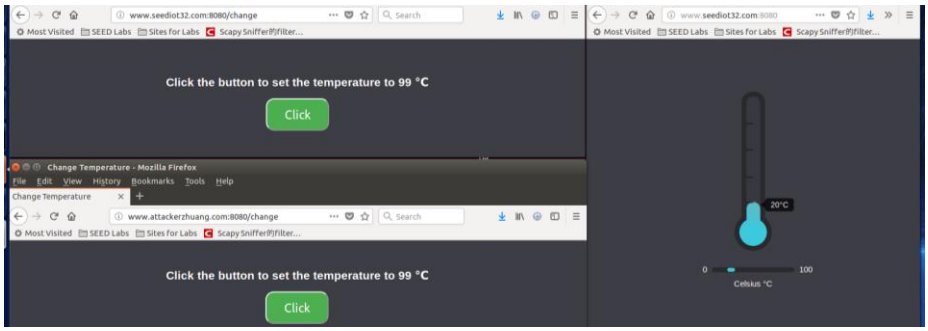
```
[11/18/20]seed@VM:~/.../attacker_vm$ dig @10.0.2.4 www.attackerZhuang.com

; <<>> DiG 9.10.3-P4-Ubuntu <<>> @10.0.2.4 www.attackerZhuang.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 2859
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.attackerZhuang.com.                IN      A

;; ANSWER SECTION:
www.attackerZhuang.com. 259200  IN      A       10.0.2.4

;; AUTHORITY SECTION:
attackerZhuang.com.     259200  IN      NS      ns.attackerZhuang.com.

;; ADDITIONAL SECTION:
ns.attackerZhuang.com.  259200  IN      A       10.0.2.4

;; Query time: 4 msec
;; SERVER: 10.0.2.4#53(10.0.2.4)
```

1.4 Task 5: Configure the Local DNS Server

```
[11/18/20]seed@VM:~$ dig xyz.attackerZhuang.com

; <<>> DiG 9.10.3-P4-Ubuntu <<>> xyz.attackerZhuang.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 2278
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;xyz.attackerZhuang.com.                IN      A

;; ANSWER SECTION:
xyz.attackerZhuang.com. 259200  IN      A       10.0.2.4

;; Query time: 3 msec
;; SERVER: 10.0.2.8#53(10.0.2.8)
```

2 Launch the Attack on the IoT Device

2.1 Task 6: Understanding the Same-Origin Policy Protection



- Page of URL www.seedIoT32.com:8080/change can successfully set the thermostat's temperature.

```
newTemperature is [99], range.value is [12]
set temperature to 99 as informed by the server.
```

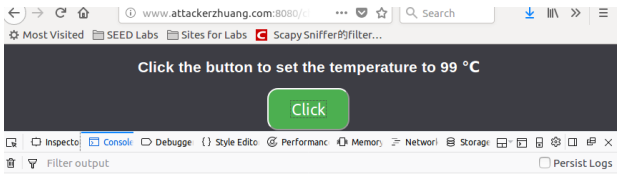
- Page of URL www.attackerZhuang.com:8080/change got this:

```
Cross-Origin Request Blocked: The Same Origin Policy disallows
reading the remote resource at http://www.seediot32.com:8080/password.
(Reason: CORS header 'Access-Control-Allow-Origin' missing).
```

同源策略限制了来自不同源（包括这里的来自不同域名的）脚本对当前 web 页面的读取或者设置某些属性（比如这里的将温度的 value 设置成 99℃）

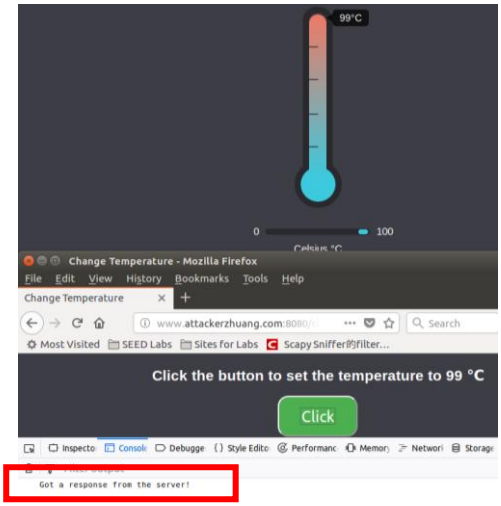
2.2 Task 7: Defeat the Same-Origin Policy Protection

2.2.1 Step 1: Modify the JavaScript code



在用户 VM 的 web console 不再出现同源策略的报错，但是温度计没有将温度调整到 99℃。不再报错是因为修改脚本已经让用户 VM 不再认为这是不同源的操作了。但操作仍不成功是因为来自用户 VM 的请求的响应到 Attacker VM 上了，所以在用户 VM 的 attacker 的 web console 上面没有显示有来自 server 的响应。

2.2.2 Step 2: Conduct the DNS rebinding



2.3 Task 8: Launch the Attack

! Remember to run command “sudo rndc flush” on local DNS server every time reload zone file.