

DNS Rebinding Attack Lab

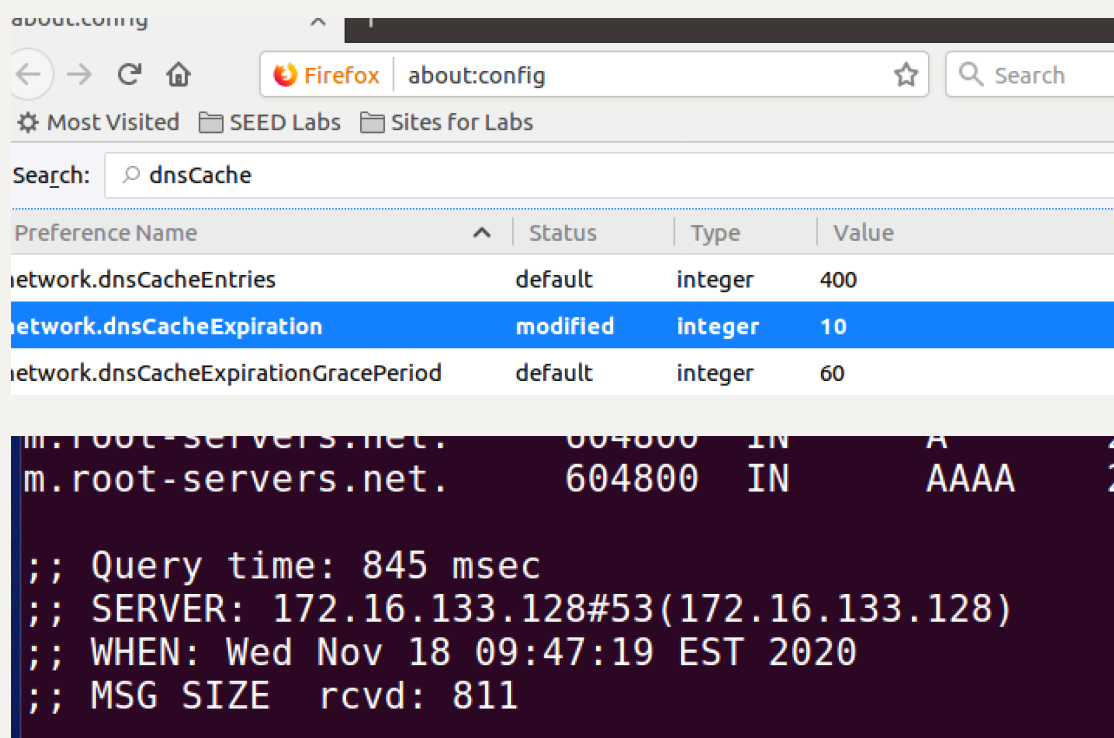
18307130089 吴嘉琪

user machine:172.16.133.130

Attacker:172.16.133.129

local DNS server:172.16.133.128

Task 1: Configure the User VM、



The screenshot shows the Firefox `about:config` page with the search bar set to `dnsCache`. The following table lists the relevant preferences:

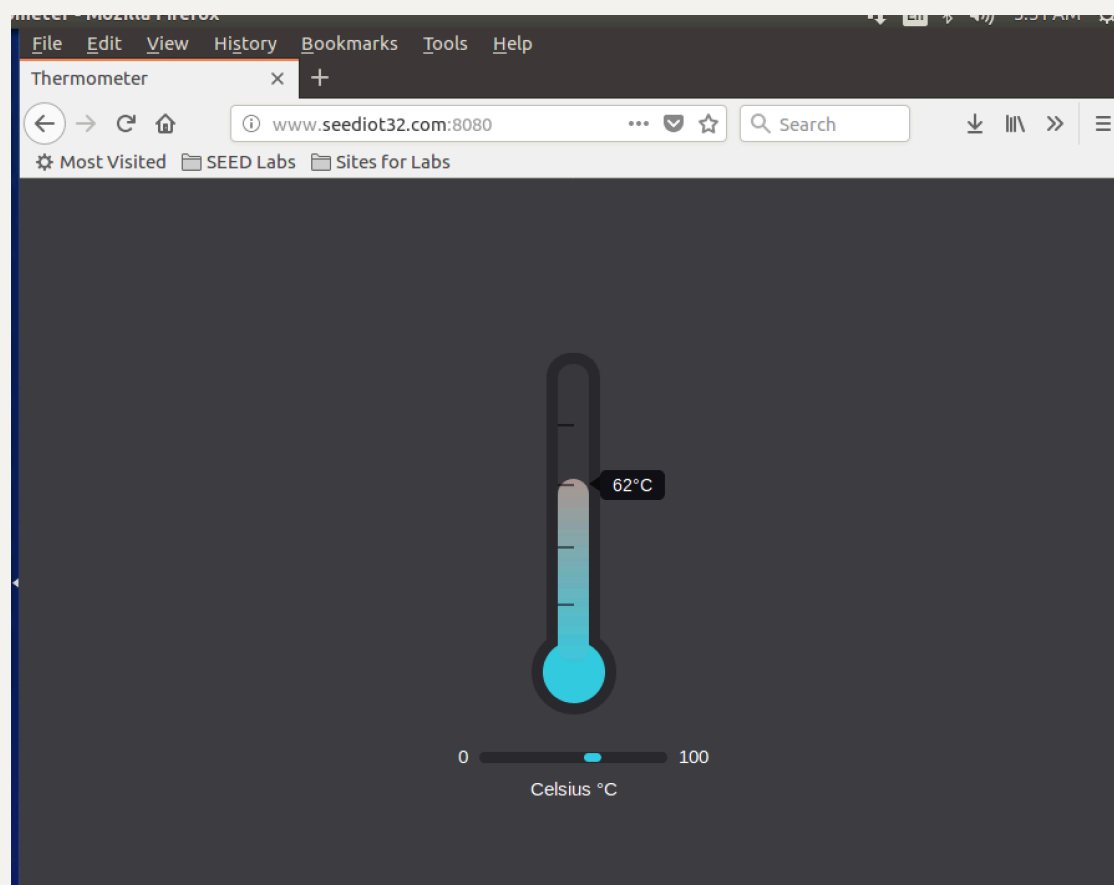
Preference Name	Status	Type	Value
<code>network.dnsCacheEntries</code>	default	integer	400
<code>network.dnsCacheExpiration</code>	modified	integer	10
<code>network.dnsCacheExpirationGracePeriod</code>	default	integer	60

Below the table, a terminal window displays the output of a DNS query:

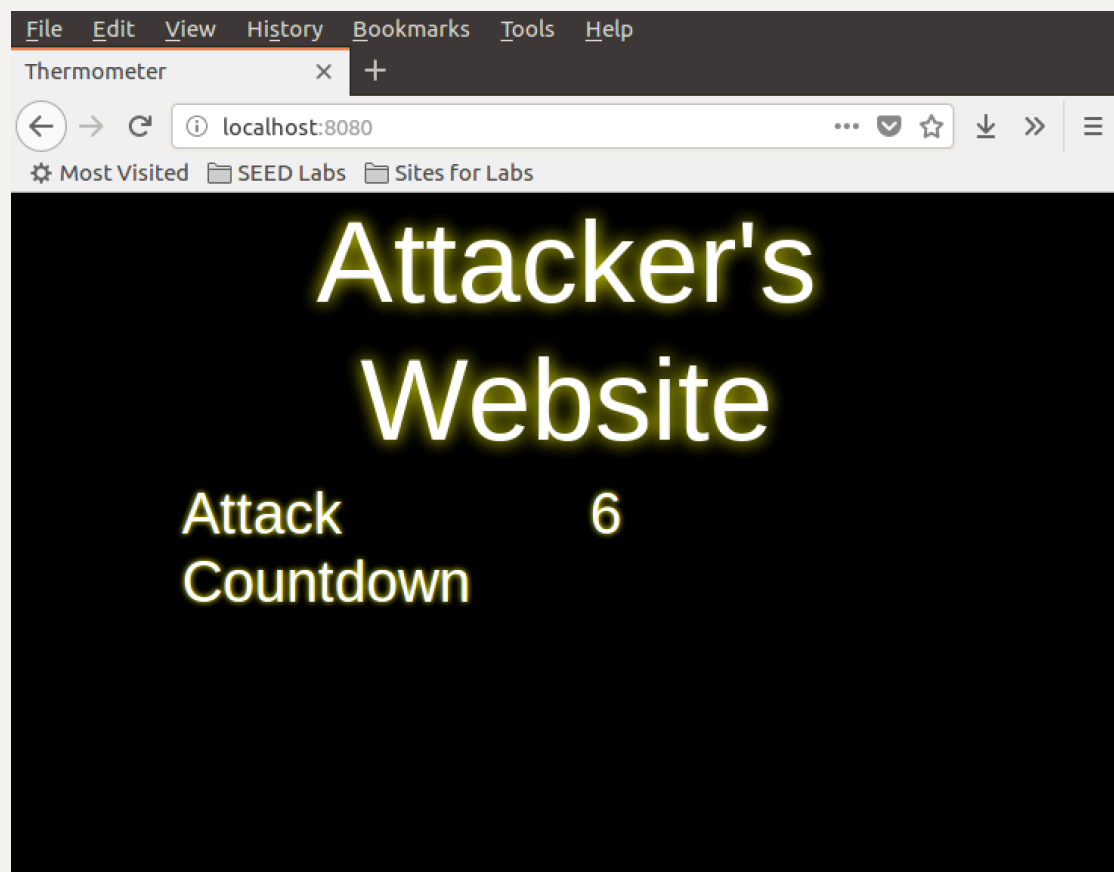
```
m.root-servers.net. 604800 IN A 2
m.root-servers.net. 604800 IN AAAA 2

;; Query time: 845 msec
;; SERVER: 172.16.133.128#53(172.16.133.128)
;; WHEN: Wed Nov 18 09:47:19 EST 2020
;; MSG SIZE rcvd: 811
```

Task 2: Start the IoT server on the User VM



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



Task 4: Configure the DNS server on the Attacker VM

attacker上配置完成后, user上运行 `dig @10.0.2.8 www.attacker32.com`

```
;; ->HEADER<<- opcode: QUERY, status: NOERROR, id: 33224
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.attacker32.com.          IN      A

;; ANSWER SECTION:
www.attacker32.com.          259200  IN      A      172.16.133.129

;; AUTHORITY SECTION:
attacker32.com.              259200  IN      NS      ns.attacker32.com.

;; ADDITIONAL SECTION:
ns.attacker32.com.           259200  IN      A      172.16.133.129

;; Query time: 2 msec
;; SERVER: 172.16.133.129#53(172.16.133.129)
;; WHEN: Thu Nov 19 03:40:10 EST 2020
;; MSG SIZE rcvd: 96
```

Task 5: Configure the Local DNS Server

配置完成后在user上运行 `dig xyz.attacker32.com`, 发现返回的answer session确实是attacker上zone file里所配置的信息;

```
[11/19/20]seed@VM:~$ dig xyz.attacker32.com

; <<>> DiG 9.10.3-P4-Ubuntu <<>> xyz.attacker32.com
;; global options: +cmd
;; Got answer:
;; ->HEADER<<- opcode: QUERY, status: NOERROR, id: 41307
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 13, ADDITIONAL: 27

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;xyz.attacker32.com.          IN      A

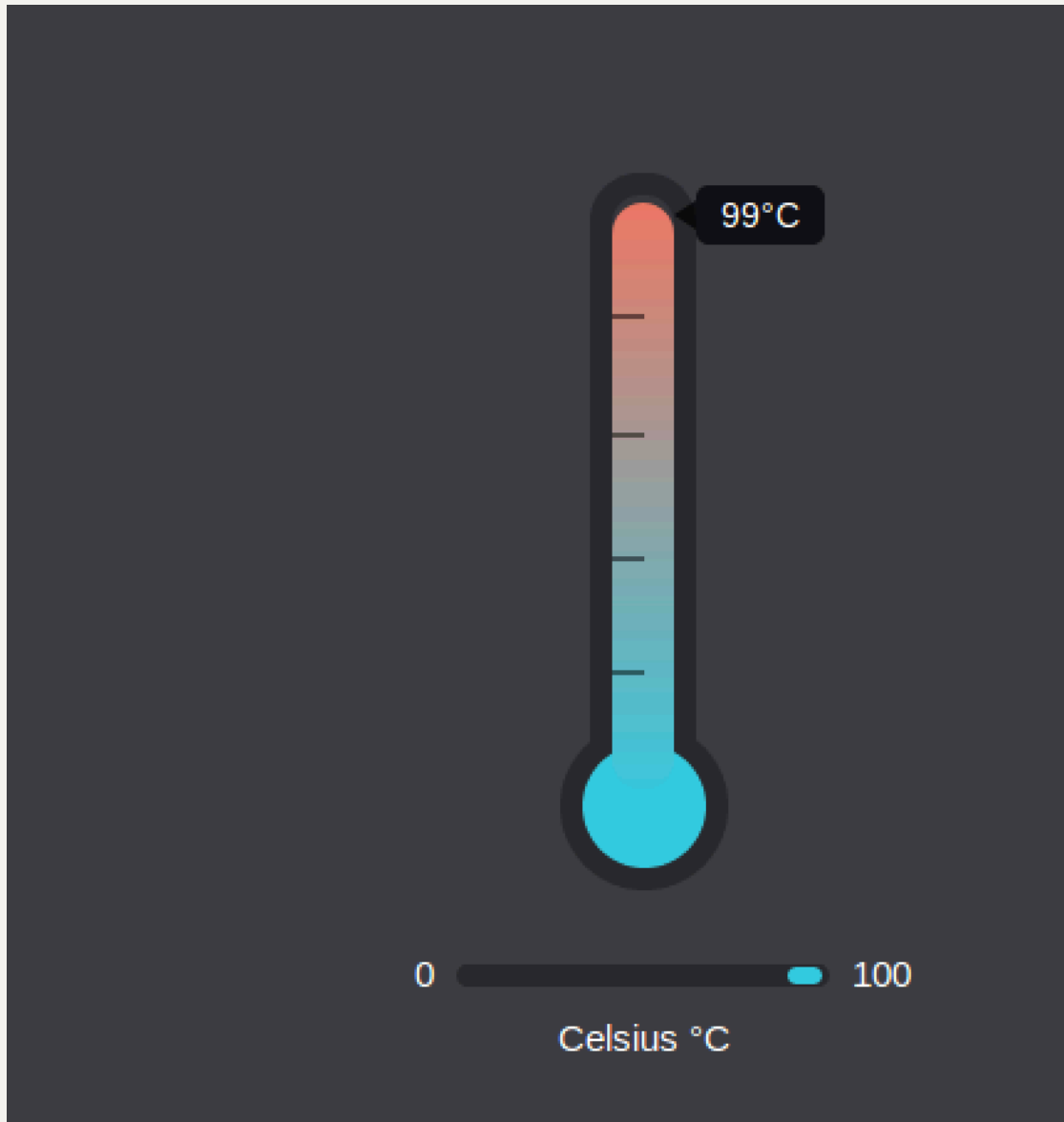
;; ANSWER SECTION:
xyz.attacker32.com.          259200  IN      A      172.16.133.129

;; AUTHORITY SECTION:
```

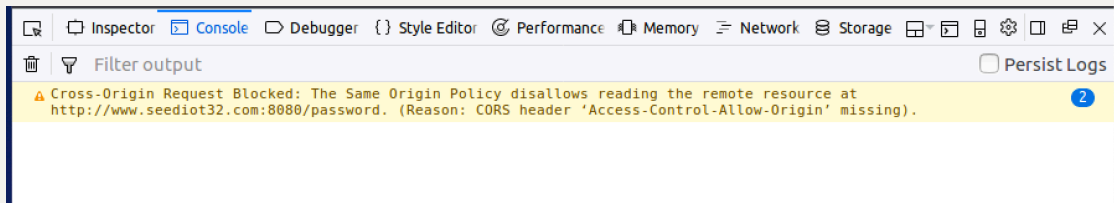
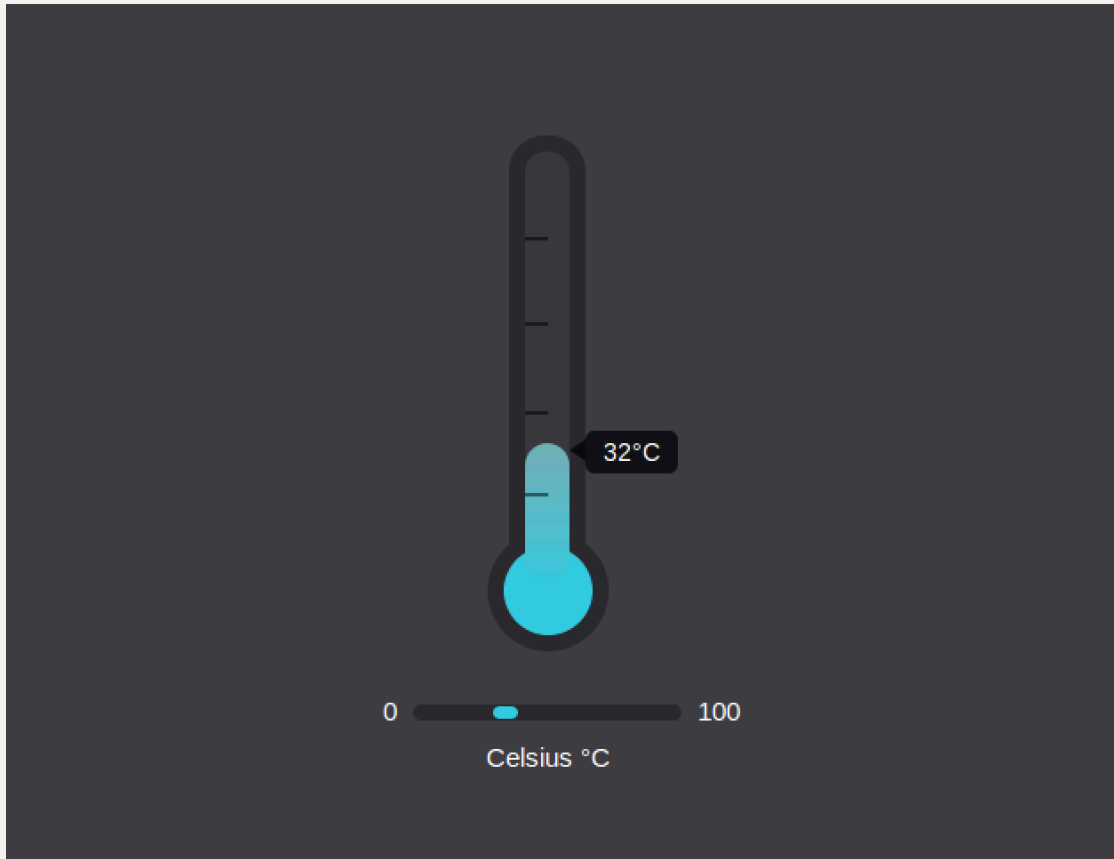
Task 6. Understanding the Same-Origin Policy Protection

Click the button on the second and third pages, and describe your observation. Which page can successfully set the thermostat's temperature? Please explain why.

点击<http://www.seedIoT32.com:8080/change> 的按钮，温度成功升到99

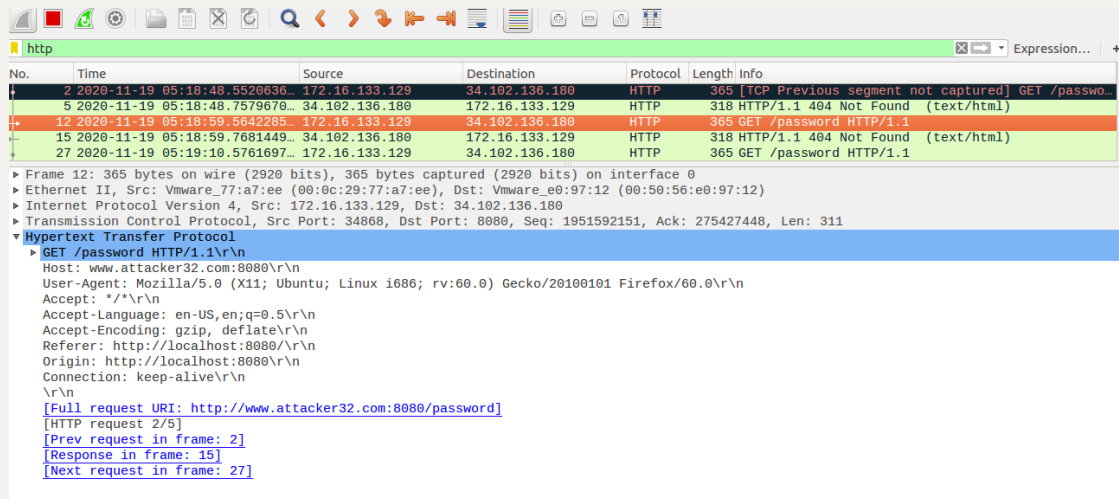


点击<http://www.attacker32.com:8080/change>的按钮，温度没有变化；



"We emulate such a vulnerable IoT device using a simple web server, which serves two APIs: password and temperature. The IoT device can set the room temperature. To do that, we need to send out an HTTP request to the server's temperature API; the request should include two pieces of data: the target temperature value and a password. The password is a secret that changes periodically, but it can be fetched using the password API. Therefore, to successfully set the temperature, users need to first get the password, and then attach the password in the temperature API."

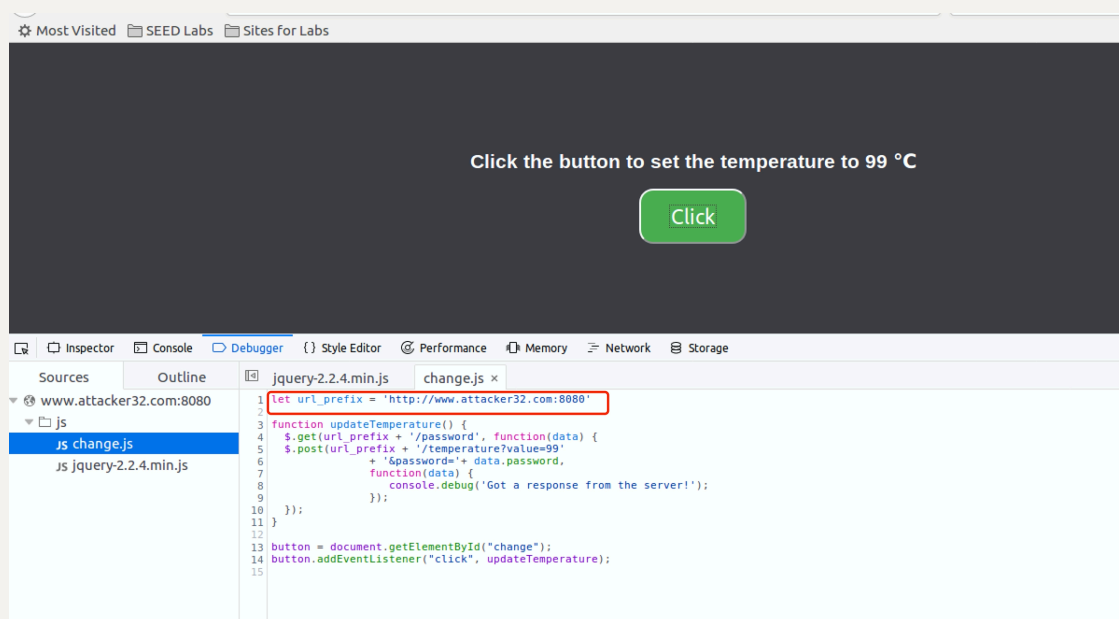
浏览器报错，表示拦截了一个cross-origin request，说明失败原因是来自<http://www.attacker32.com:8080/change>的request URL(与attacker server同源) 与seediot server不属于同一个origin，因此没有权限读取其password;而且没有使用CORS来指定跨源访问，因此不被允许。



Task 7. Defeat the Same-Origin Policy Protection

so as long as we use www.attacker32.com in the URL, we are complying with the SOP policy, but that does not mean we are restricted to communicate with the www.attacker32.com web server.

修改attacker端的js后，重启attacker的server，刷新页面，再次尝试；不再报错



We first map www.attacker32.com to the IP address of the attacker VM, so the user can get the actual page from <http://www.attacker32.com/change>. Before we click on the button on the page, we remap the www.attacker32.com hostname to the IP address of the IoT server, so the request triggered by the button will go to the IoT server. That is exactly what we want.

在点击click之前，将attacker域名重定向到IoT服务器的ip：

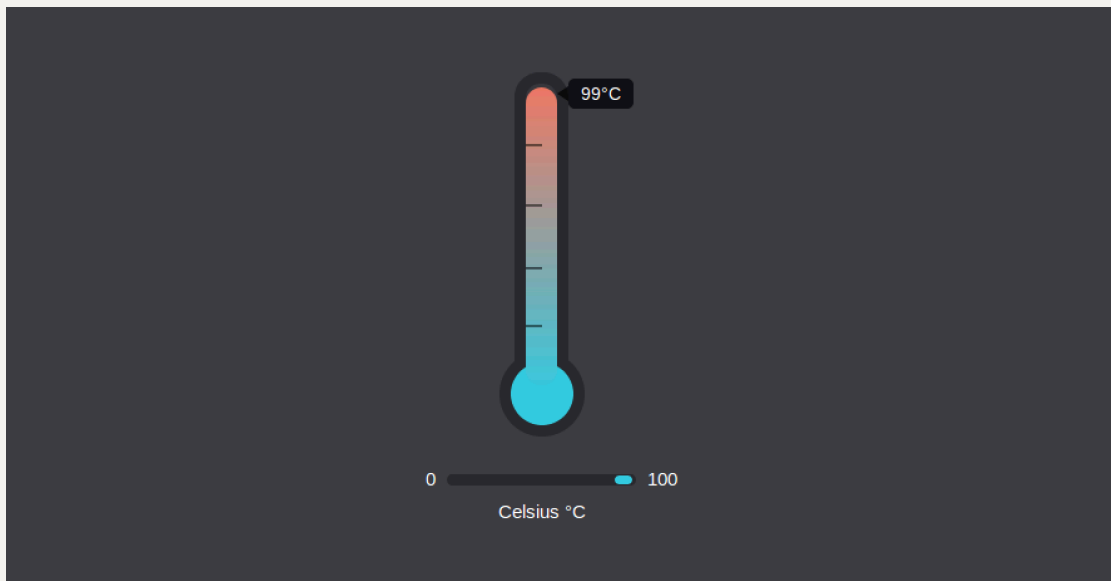
```
[11/19/20]seed@VM:~$ dig www.attacker32.com

; <<>> DiG 9.10.3-P4-Ubuntu <<>> www.attacker32.com
;; global options: +cmd
;; Got answer:
;; ->HEADER<<- opcode: QUERY, status: NOERROR, id: 39921
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.attacker32.com.          IN      A
;
; ANSWER SECTION:
www.attacker32.com.          10000   IN      A      172.16.133.130
;

;; Query time: 3 msec
;; SERVER: 172.16.133.128#53(172.16.133.128)
;; WHEN: Thu Nov 19 05:53:18 EST 2020
;; MSG SIZE rcvd: 63
```

这样，www.attacker32.com的request实际上会请求ip地址为172.16.133.130的主机，也就是 IoT server；这样就能在不违反SOP原则的情况下，得到正确的密码，并且成功设置温度：



Task 8. Launch the Attack

没有将attacker的dns rebinding时，页面会有错误提示：



将attacker32的域名rebinding到IoT server后，成功设置温度：

