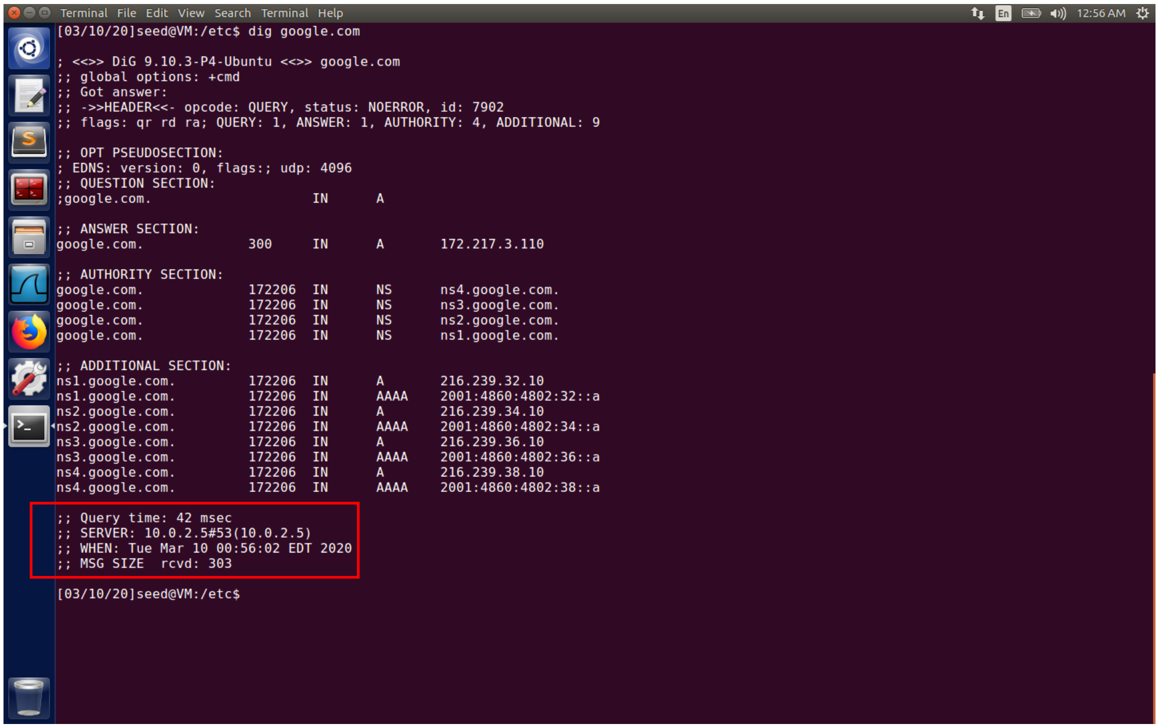
Remote DNS Rebinding Lab

Task 1: Configure the User VM

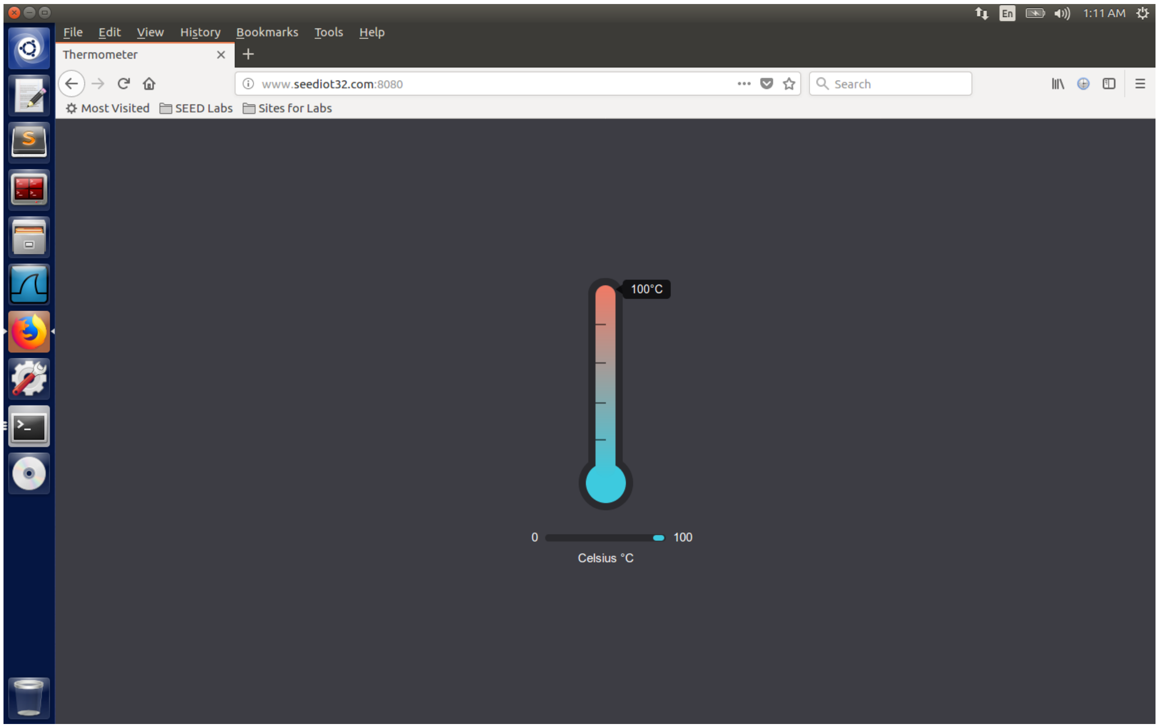
Testing `dig` command after configuring the user VM. It shows that DNS reply comes from the local DNS server we set before (10.0.2.5).



```
[03/10/20]seed@VM:/etc$ dig google.com

; <<>> DiG 9.10.3-P4-Ubuntu <<>> google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 7902
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 4, ADDITIONAL: 9

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

;; ANSWER SECTION:
google.com.             300     IN      A       172.217.3.110

;; AUTHORITY SECTION:
google.com.             172206  IN      NS      ns4.google.com.
google.com.             172206  IN      NS      ns3.google.com.
google.com.             172206  IN      NS      ns2.google.com.
google.com.             172206  IN      NS      ns1.google.com.

;; ADDITIONAL SECTION:
ns1.google.com.         172206  IN      A       216.239.32.10
ns1.google.com.         172206  IN      AAAA    2001:4860:4802:32::a
ns2.google.com.         172206  IN      A       216.239.34.10
ns2.google.com.         172206  IN      AAAA    2001:4860:4802:34::a
ns3.google.com.         172206  IN      A       216.239.36.10
ns3.google.com.         172206  IN      AAAA    2001:4860:4802:36::a
ns4.google.com.         172206  IN      A       216.239.38.10
ns4.google.com.         172206  IN      AAAA    2001:4860:4802:38::a

;; Query time: 42 msec
;; SERVER: 10.0.2.5#53(10.0.2.5)
;; WHEN: Tue Mar 10 00:56:02 EDT 2020
;; MSG SIZE  rcvd: 303

[03/10/20]seed@VM:/etc$
```

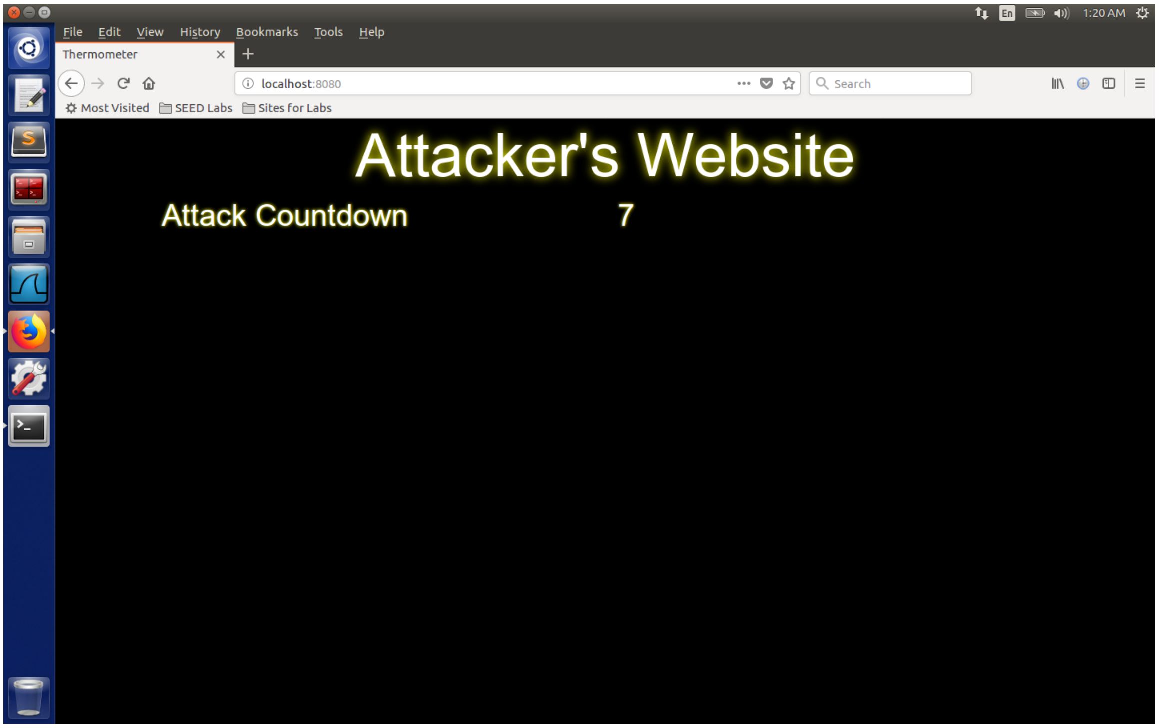
Task 2: Start the IoT server on the User VM

After we set the IoT server, we are able to see this thermostat page.



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

After we set the attacker VM, we are able to see this attacker’s page.

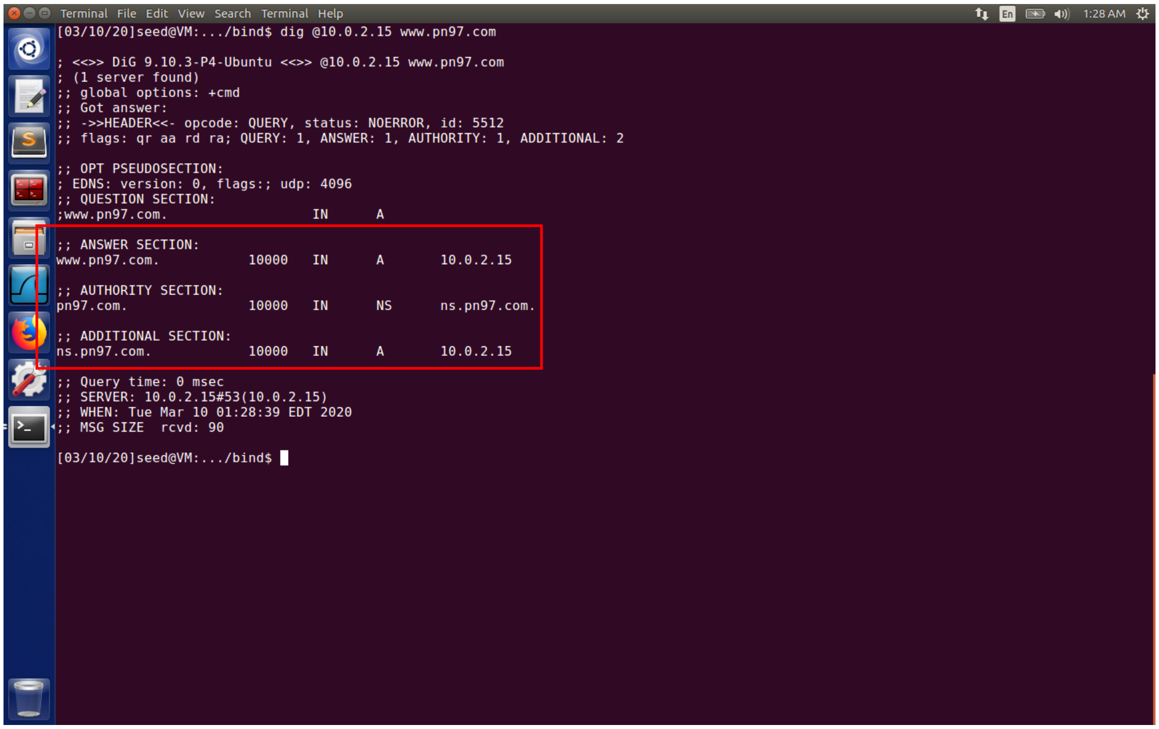


Attacker's Website

Attack Countdown 7

Task 4: Configure the DNS server on the Attacker VM

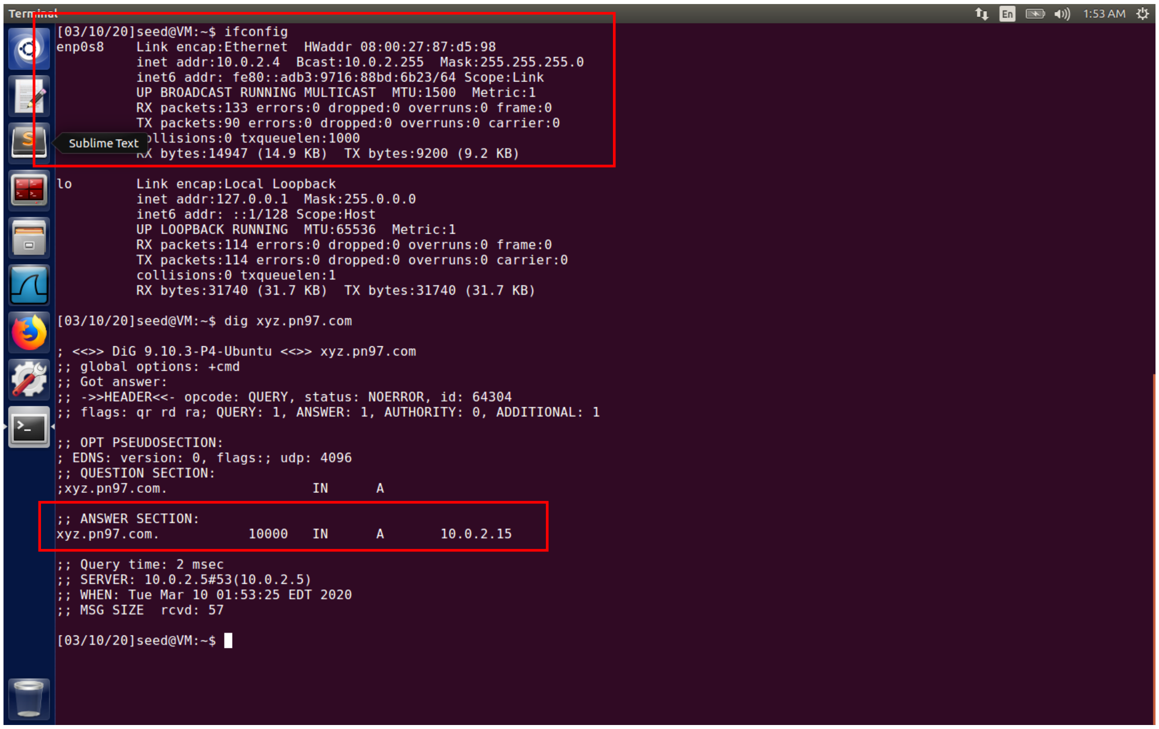
After we try the `dig` command, we successfully bind the `pn97.com` domain to our attacker's ip address 10.0.2.15.



```
[03/10/20]seed@VM:.../bind$ dig @10.0.2.15 www.pn97.com

; <<>> DiG 9.10.3-P4-Ubuntu <<>> @10.0.2.15 www.pn97.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 5512
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.pn97.com.                  IN      A

;; ANSWER SECTION:
www.pn97.com.           10000   IN      A       10.0.2.15

;; AUTHORITY SECTION:
pn97.com.               10000   IN      NS      ns.pn97.com.

;; ADDITIONAL SECTION:
ns.pn97.com.            10000   IN      A       10.0.2.15

;; Query time: 0 msec
;; SERVER: 10.0.2.15#53(10.0.2.15)
;; WHEN: Tue Mar 10 01:28:39 EDT 2020
;; MSG SIZE  rcvd: 90

[03/10/20]seed@VM:.../bind$
```

Task 5: Configure the Local DNS Server

After we try the `dig` command on our user machine for `pn97.com`, it shows the ip address is 10.0.2.5, which is our attacker’s ip address.



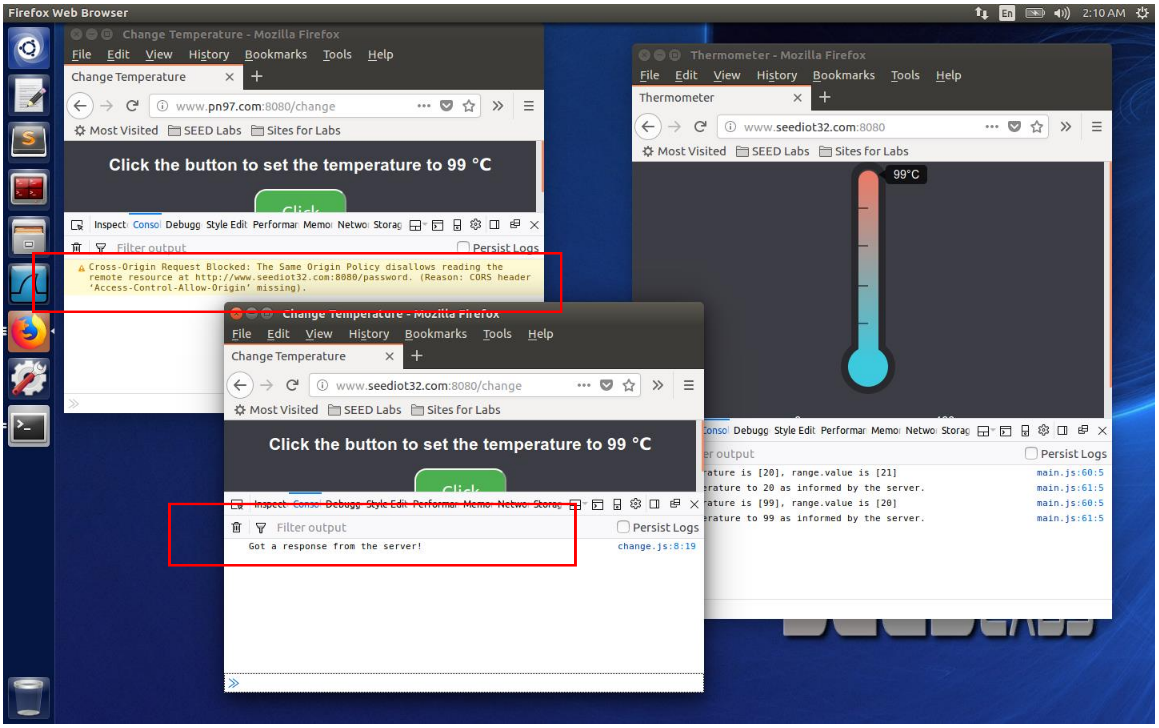
```
[03/10/20]seed@VM:~$ ifconfig
enp0s8    Link encap:Ethernet  HWaddr 08:00:27:87:d5:98
          inet addr:10.0.2.4  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::adb3:9716:88bd:6b23/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:133 errors:0 dropped:0 overruns:0 frame:0
          TX packets:90 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:14947 (14.9 KB)  TX bytes:9200 (9.2 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:114 errors:0 dropped:0 overruns:0 frame:0
          TX packets:114 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:31740 (31.7 KB)  TX bytes:31740 (31.7 KB)

[03/10/20]seed@VM:~$ dig xyz.pn97.com

; <<>> DiG 9.10.3-P4-Ubuntu <<>> xyz.pn97.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 64304
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;xyz.pn97.com.                  IN      A

;; ANSWER SECTION:
xyz.pn97.com.           10000   IN      A       10.0.2.15

;; Query time: 2 msec
;; SERVER: 10.0.2.5#53(10.0.2.5)
;; WHEN: Tue Mar 10 01:53:25 EDT 2020
;; MSG SIZE  rcvd: 57

[03/10/20]seed@VM:~$ 
```

Task 6. Understanding the Same-Origin Policy Protection

After we click the button on the second and third pages:

The second page (change page on user machine / IoT server): We could set temperature on our IoT server by clicking the button on this page.

The third page (change page on attacker's machine): We cannot set temperature on our IoT server by clicking the button on this page. It is because they are from different source (10.0.2.4 and 10.0.2.15) and break the same-origin policy, the request will not be handled by the IoT thermometer page.



Firefox Web Browser
2:10 AM
Change Temperature - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Change Temperature
www.pn97.com:8080/change
Most Visited SEED Labs Sites for Labs
Click the button to set the temperature to 99 °C
Click
Inspect Consol Debugg Style Edit Performan Memo Netwo Storag
Filter output
Persist Logs
Thermometer - Mozilla Firefox
Thermometer
www.seediot32.com:8080
99°C
www.seediot32.com:8080/change

```
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).
```

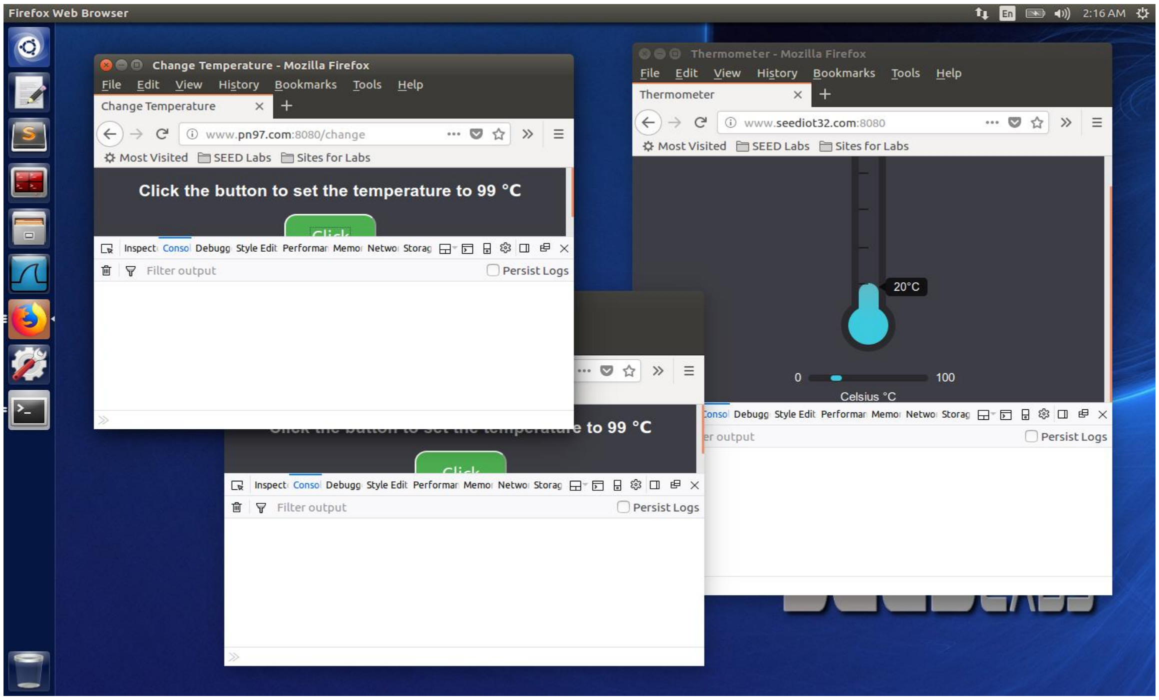
```
Got a response from the server!                                    change.js:8:19
```

```
rature is [20], range.value is [21]                    main.js:60:5
erature to 20 as informed by the server.               main.js:61:5
rature is [99], range.value is [20]                    main.js:60:5
erature to 99 as informed by the server.               main.js:61:5
```

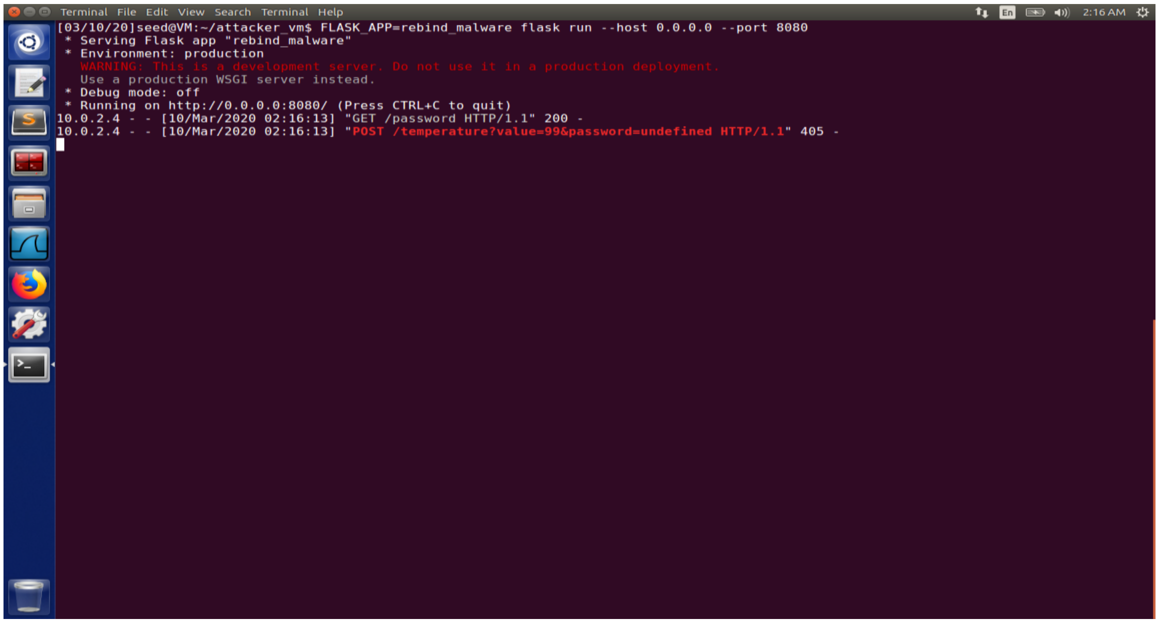
Task 7. Defeat the Same-Origin Policy Protection

Step 1

After changing the `url_prefix` in javascript code. We no longer see error message when clicking the button on the attacker's page. This is because after we change the code, the request is sent to `pn97.com` instead of `seediot32.com`. They are under the same domain and do not break the same-origin policy.

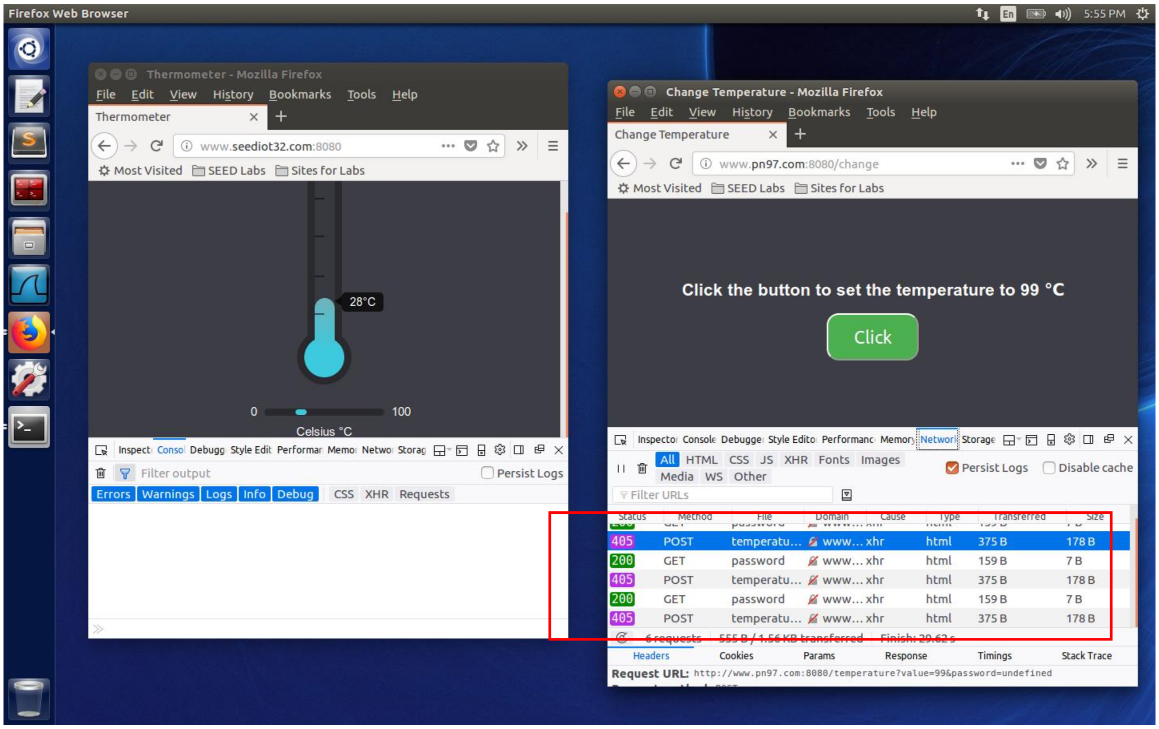

Firefox Web Browser
2:16 AM
Change Temperature - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Change Temperature
www.pn97.com:8080/change
Most Visited SEED Labs Sites for Labs
Click the button to set the temperature to 99 °C
Click
Inspect Console Debugger Style Editor Performance Memory Network Storage
Filter output
Persist Logs
Thermometer - Mozilla Firefox
Thermometer
www.seediot32.com:8080
20°C
0
100
Celsius °C

However, because the request is sent back to attacker's page that does not serve this kind of http request, it return with a 405 http error code (on the attacker's machine).



```
[03/10/20]seed@VM:~/attacker_vm$ FLASK_APP=rebind_malware flask run --host 0.0.0.0 --port 8080
 * Serving Flask app "rebind_malware"
 * Environment: production
   WARNING: This is a development server. Do not use it in a production deployment.
   Use a production WSGI server instead.
 * Debug mode: off
 * Running on http://0.0.0.0:8080/ (Press CTRL+C to quit)
10.0.2.4 - - [10/Mar/2020 02:16:13] "GET /password HTTP/1.1" 200 -
10.0.2.4 - - [10/Mar/2020 02:16:13] "POST /temperature?value=99&password=undefined HTTP/1.1" 405 -
```

On our user machine, 405 error code received.


Firefox Web Browser
5:55 PM
Thermometer - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Thermometer
www.seediot32.com:8080
Most Visited
SEED Labs
Sites for Labs
28°C
0
100
Celsius °C
Inspect Conso Debugg Style Edit Performar Memo Netwo Storag
Filter output
Persist Logs
Errors Warnings Logs Info Debug CSS XHR Requests
Change Temperature - Mozilla Firefox
Change Temperature
www.pn97.com:8080/change
Click the button to set the temperature to 99 °C
Click
Inspecto Console Debugge Style Edito Performanc Memory Networ Storage
All HTML CSS JS XHR Fonts Images Media WS Other
Persist Logs
Disable cache
Filter URLs
Headers Cookies Params Response Timings Stack Trace

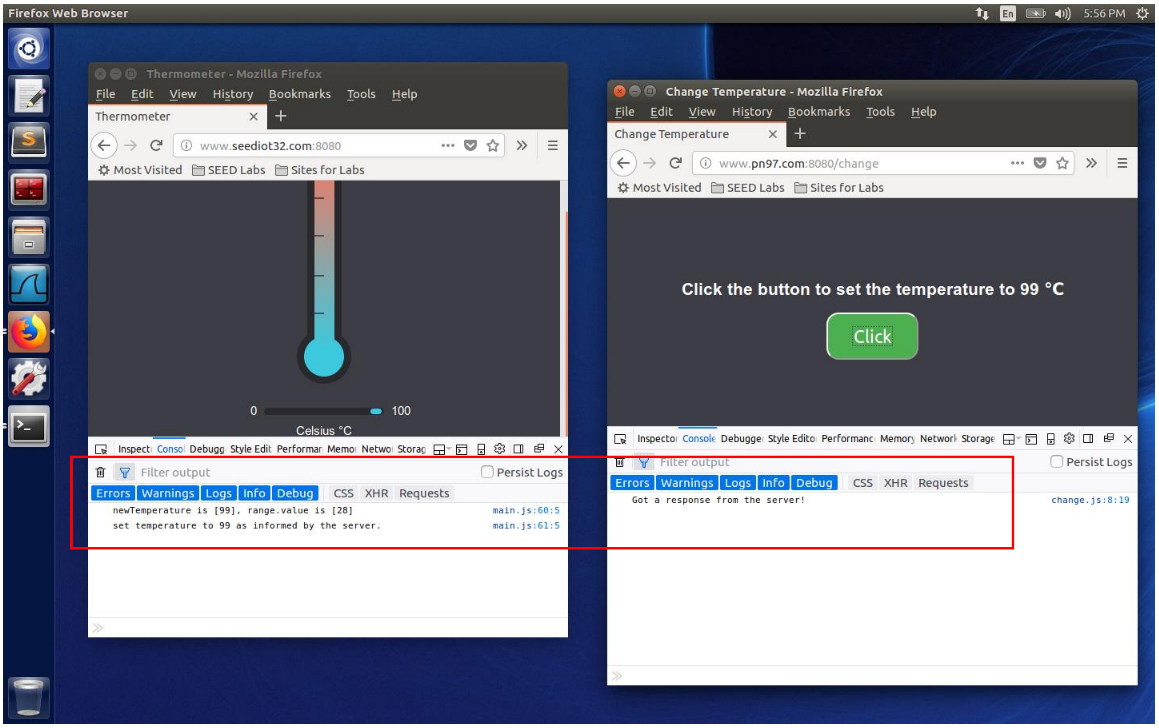
Status	Method	File	Domain	Cause	Type	Transferred	Size
405	POST	temperatu…	www…	xhr	html	375 B	178 B
200	GET	password	www…	xhr	html	159 B	7 B
405	POST	temperatu…	www…	xhr	html	375 B	178 B
200	GET	password	www…	xhr	html	159 B	7 B
405	POST	temperatu…	www…	xhr	html	375 B	178 B

6 requests | 555 B / 1.56 KB transferred | Finish: 29.62 s

Request URL: http://www.pn97.com:8080/temperature?value=99&password=undefined

Step 2

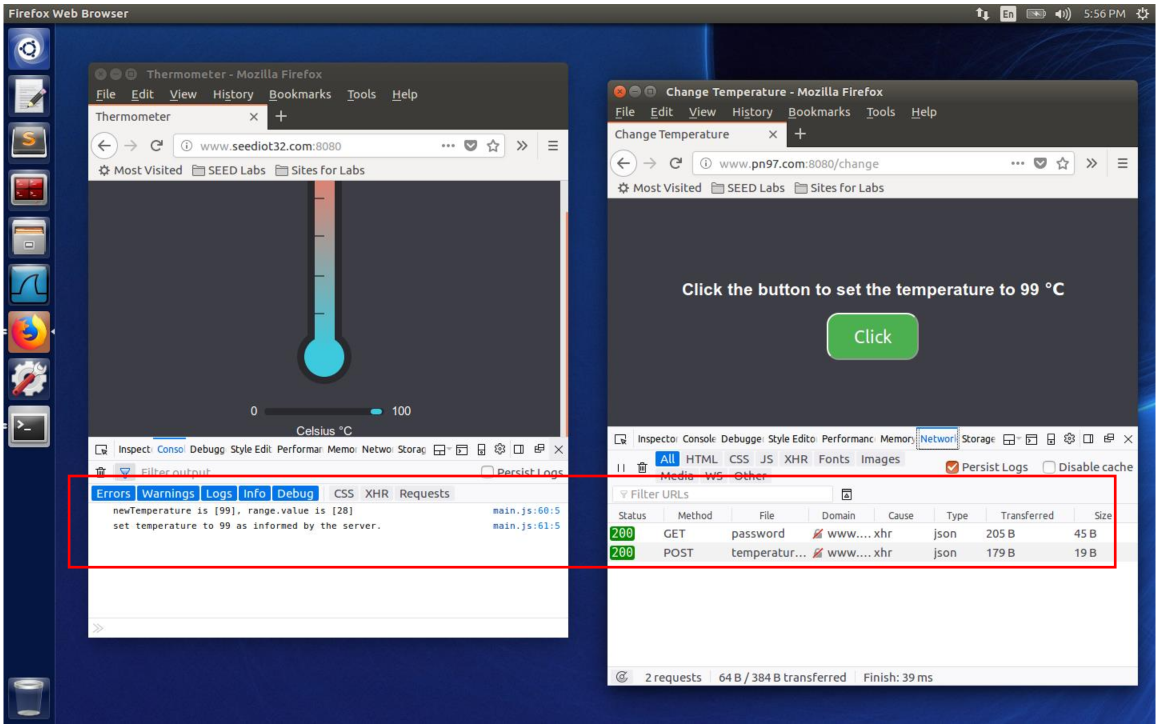
After we changed twice of the zone file on attacker's machine, we finally get the result. First of all, change the DNS reply address to 10.0.2.15, which is our attacker's ip address. Ensure that our user machine open the change page from `pn97.com` correctly. Then we change the DNS reply address to 10.0.2.4, which is our user machine's ip address. By doing this, we could send http request (on `pn97.com` change page) to thermometer page without break the same-origin policy and set the temperature to 99℃.



Click the button to set the temperature to 99 °C

```
newTemperature is [99], range.value is [28]          main.js:60:5
set temperature to 99 as informed by the server.     main.js:61:5
```

```
Got a response from the server!                      change.js:8:19
```



Click the button to set the temperature to 99 °C

```
newTemperature is [99], range.value is [28]          main.js:60:5
set temperature to 99 as informed by the server.     main.js:61:5
```

☑ Persist Logs ☐ Disable cache

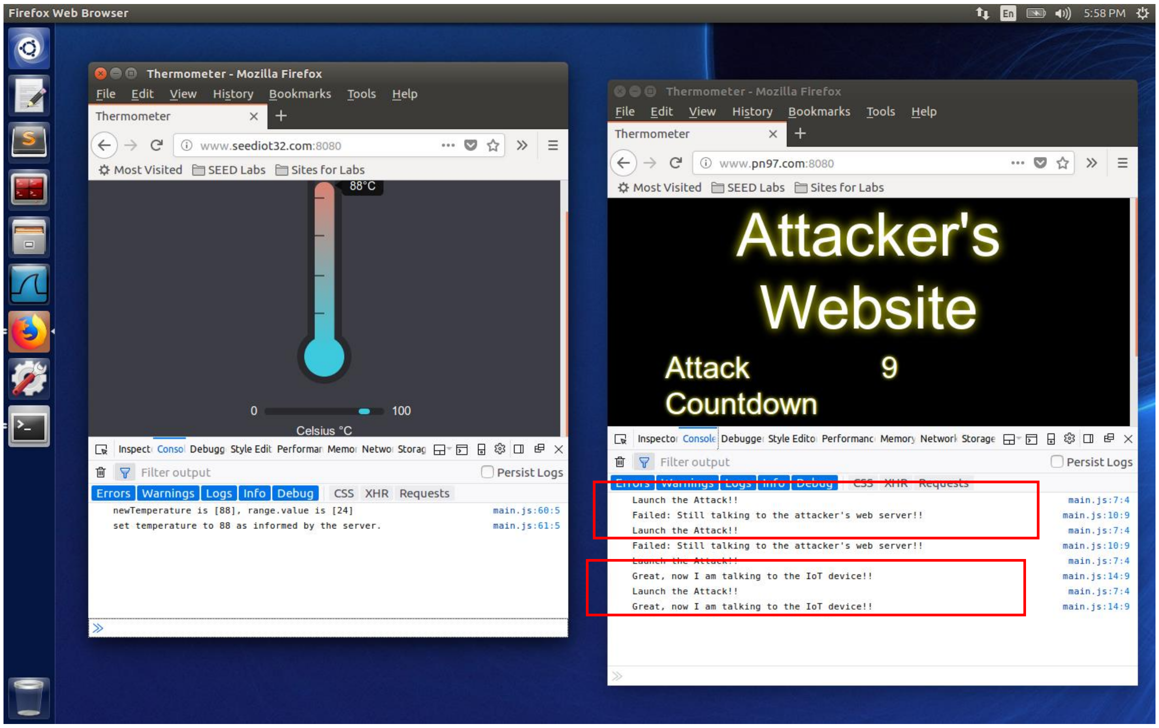
Status	Method	File	Domain	Cause	Type	Transferred	Size
200	GET	password	www.…	xhr	json	205 B	45 B
200	POST	temperatur…	www.…	xhr	json	179 B	19 B

2 requests | 64 B / 384 B transferred | Finish: 39 ms

Task 8. Launch the Attack

Launch the same attack by using this attacker page with countdown.

As we can see, before we change the DNS reply to 10.0.2.4, our http request is blocked. After we change the DNS reply to 10.0.2.4, our http request sent to the thermometer page and set the temperature periodically.



Firefox Web Browser
5:58 PM
Thermometer - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Thermometer
www.seediot32.com:8080
Most Visited
SEED Labs
Sites for Labs
88°C
0
100
Celsius °C
Inspect Conso Debugg Style Edit Performan Memo Netwo Storag
Filter output
Persist Logs
Errors Warnings Logs Info Debug CSS XHR Requests
www.pn97.com:8080
Attacker's Website
Attack Countdown
9
Inspector Console Debugger Style Editor Performance Memory Network Storage

```
newTemperature is [88], range.value is [24]          main.js:60:5
set temperature to 88 as informed by the server.     main.js:61:5
```

```
Launch the Attack!!                                  main.js:7:4
Failed: Still talking to the attacker's web server!! main.js:10:9
Launch the Attack!!                                  main.js:7:4
Failed: Still talking to the attacker's web server!! main.js:10:9
Launch the Attack!!                                  main.js:7:4
Great, now I am talking to the IoT device!!          main.js:14:9
Launch the Attack!!                                  main.js:7:4
Great, now I am talking to the IoT device!!          main.js:14:9
```