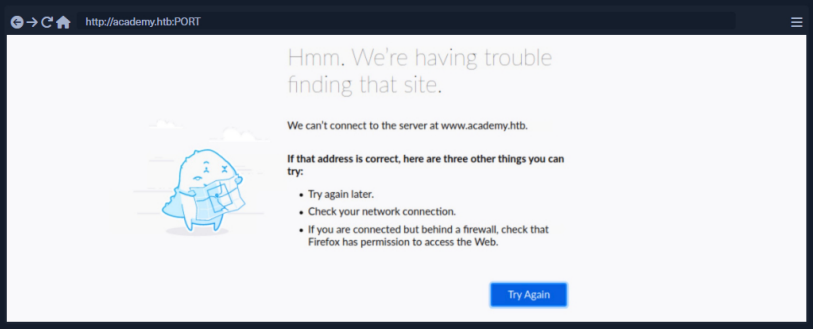
DNS Records

Once we accessed the page under `/blog`, we got a message saying `Admin panel moved to academy.htb`. If we visit the website in our browser, we get `can't connect to the server at www.academy.htb`:



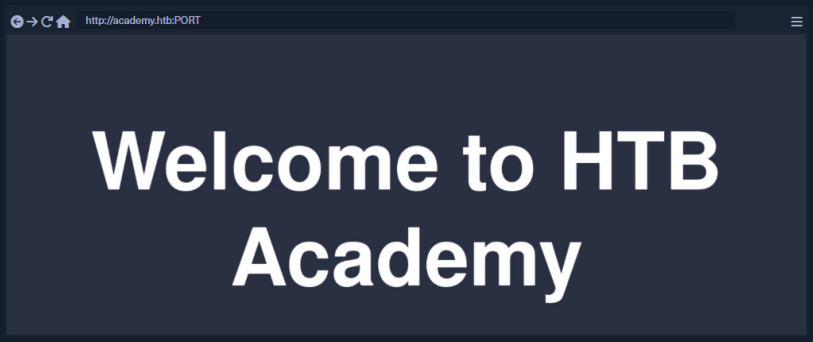
This is because the exercises we do are not public websites that can be accessed by anyone but local websites within HTB. Browsers only understand how to go to IPs, and if we provide them with a URL, they try to map the URL to an IP by looking into the local `/etc/hosts` file and the public DNS `Domain Name System`. If the URL is not in either, it would not know how to connect to it.

If we visit the IP directly, the browser goes to that IP directly and knows how to connect to it. But in this case, we tell it to go to `academy.htb`, so it looks into the local `/etc/hosts` file and doesn't find any mention of it. It asks the public DNS about it (such as Google's DNS `8.8.8.8`) and does not find any mention of it, since it is not a public website, and eventually fails to connect. So, to connect to `academy.htb`, we would have to add it to our `/etc/hosts` file. We can achieve that with the following command:

DNS Records

```
MisaelMacias@htb[/htb]$ sudo sh -c 'echo "SERVER_IP  academy.htb" >> /etc/hosts'
```

Now we can visit the website (don't forget to add the PORT in the URL) and see that we can reach the website:



However, we get the same website we got when we visit the IP directly, so `academy.htb` is the same domain we have been testing so far. We can verify that by visiting `/blog/index.php`, and see that we can access the page.

When we run our tests on this IP, we did not find anything about `admin` or panels, even when we did a full `recursive` scan on our target. `So, in this case, we start looking for sub-domains under '*.academy.htb' and see if we find anything, which is what we will attempt in the next section.`

← Previous Next → Mark Complete & Next

Cheat Sheet

Table of Contents

Introduction
Introduction
Web Fuzzing

Basic Fuzzing
Directory Fuzzing
Page Fuzzing
Recursive Fuzzing

Domain Fuzzing
DNS Records
Sub-domain Fuzzing
Vhost Fuzzing
Filtering Results

Parameter Fuzzing
Parameter Fuzzing - GET
Parameter Fuzzing - POST
Value Fuzzing

Skills Assessment
Skills Assessment - Web Fuzzing

My Workstation

OFFLINE

Start Instance

∞ / 1 spawns left