Sub-domain Fuzzing

In this section, we will learn how to use `ffuf` to identify sub-domains (i.e., `*.website.com`) for any website.

Sub-domains

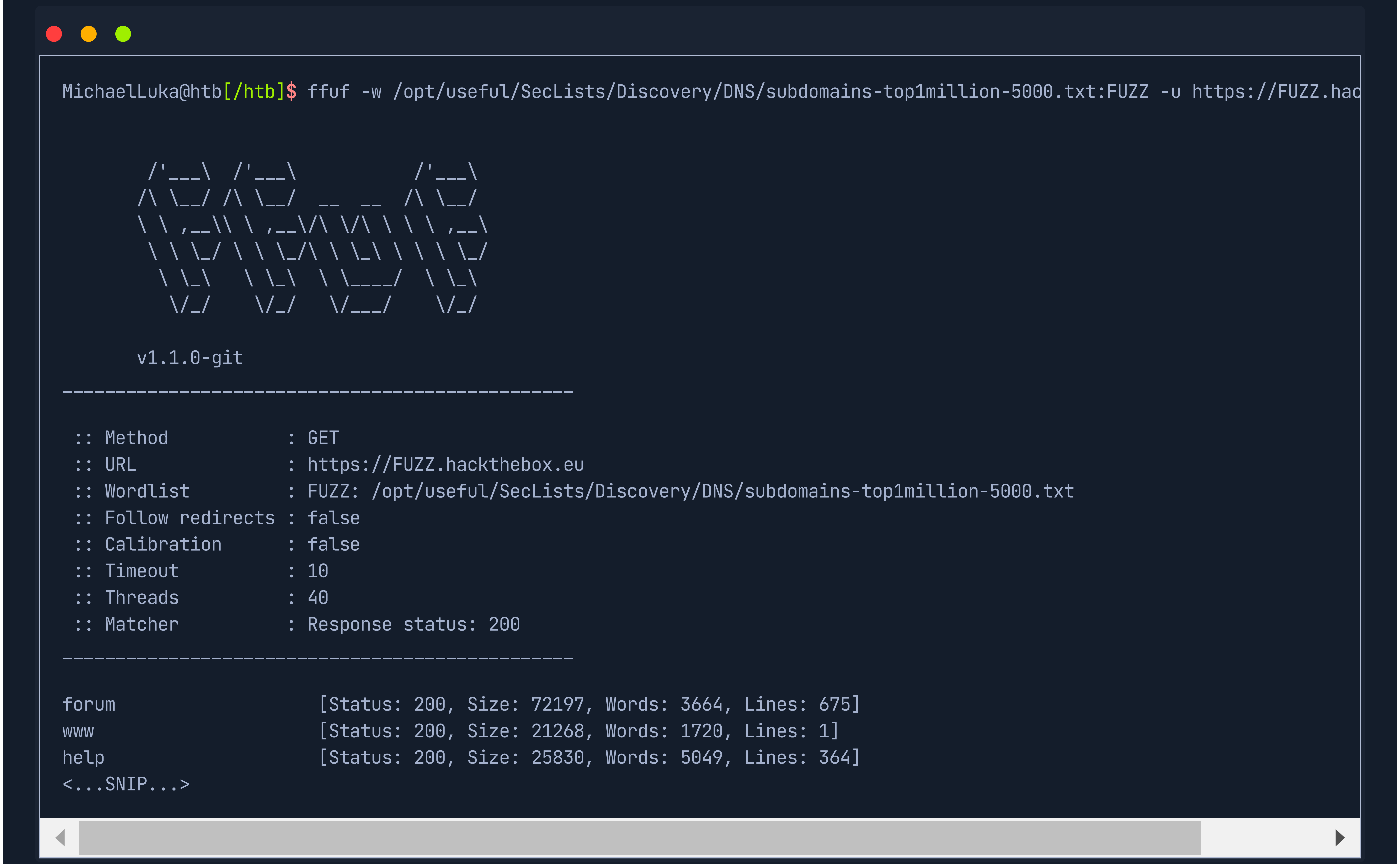
A sub-domain is any website underlying another domain. For example, `https://photos.google.com` is the `photos` sub-domain of `google.com`.

In this case, we are simply checking different websites to see if they exist by checking if they have a public DNS record that would redirect us to a working server IP. So, let's run a scan and see if we get any hits. Before we can start our scan, we need two things:

- A `wordlist`
- A `target`

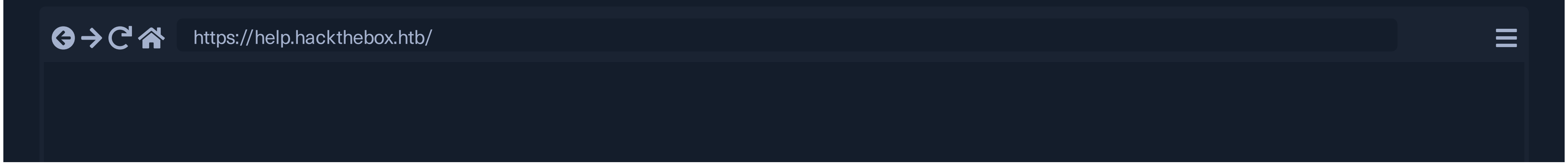
Luckily for us, in the `SecLists` repo, there is a specific section for sub-domain wordlists, consisting of common words usually used for sub-domains. We can find it in `/opt/useful/SecLists/Discovery/DNS/`. In our case, we would be using a shorter wordlist, which is `subdomains-top1million-5000.txt`. If we want to extend our scan, we can pick a larger list.

As for our target, we will use `hackthebox.eu` as our target and run our scan on it. Let us use `ffuf` and place the `FUZZ` keyword in the place of sub-domains, and see if we get any hits:

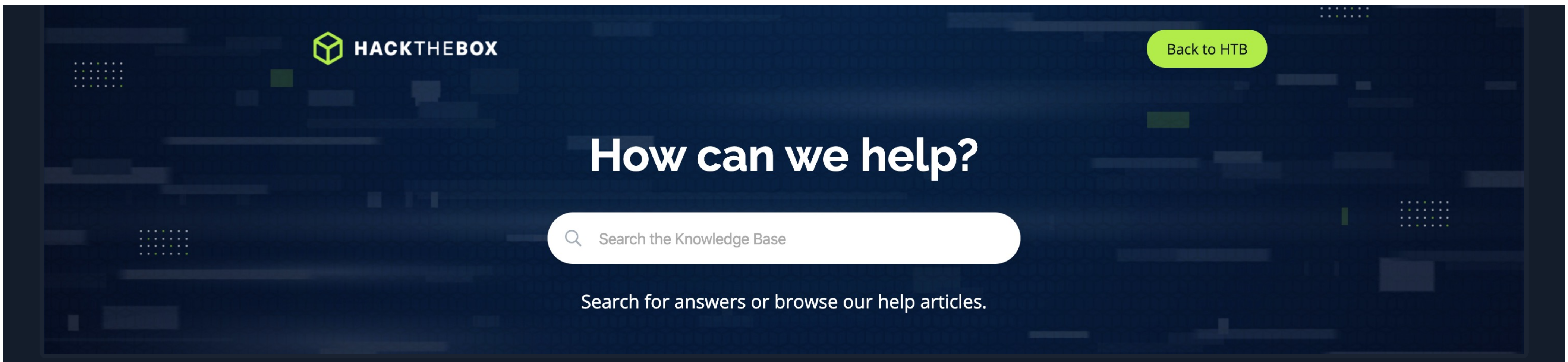


```
MichaelLuka@htb[/htb]$ ffuf -w /opt/useful/SecLists/Discovery/DNS/subdomains-top1million-5000.txt:FUZZ -u https://FUZZ.hac


        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v1.1.0-git
________________________________________________

 :: Method           : GET
 :: URL              : https://FUZZ.hackthebox.eu
 :: Wordlist         : FUZZ: /opt/useful/SecLists/Discovery/DNS/subdomains-top1million-5000.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200
________________________________________________

forum                   [Status: 200, Size: 72197, Words: 3664, Lines: 675]
www                     [Status: 200, Size: 21268, Words: 1720, Lines: 1]
help                    [Status: 200, Size: 25830, Words: 5049, Lines: 364]
<...SNIP...>
```

We see that we do get a few hits back. We can verify that these are actual sub-domains by visiting one of them:



https://help.hackthebox.htb/


HACKTHEBOX
Back to HTB
How can we help?
Search the Knowledge Base
Search for answers or browse our help articles.

We see that indeed these are working sub-domains. Now, we can try running the same thing on `academy.htb` and see if we get any hits back:

```
MichaelLuka@htb[/htb]$ ffuf -w /opt/useful/SecLists/Discovery/DNS/subdomains-top1million-5000.txt:FUZZ -u http://FUZZ.acad


        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v1.1.0-git
________________________________________________

 :: Method           : GET
 :: URL              : https://FUZZ.academy.htb/
 :: Wordlist         : FUZZ: /opt/useful/SecLists/Discovery/DNS/subdomains-top1million-5000.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403
________________________________________________

:: Progress: [4997/4997] :: Job [1/1] :: 131 req/sec :: Duration: [0:00:38] :: Errors: 4997 ::
```

We see that we do not get any hits back. Does this mean that there are no sub-domain under `academy.htb`? - No.

This means that there are no `public` sub-domains under `academy.htb`, as it does not have a public DNS record, as previously mentioned. Even though we did add `academy.htb` to our `/etc/hosts` file, we only added the main domain, so when `ffuf` is looking for other sub-domains, it will not find them in `/etc/hosts`, and will ask the public DNS, which obviously will not have them.

Start Instance

1 / 1 spawns left

Waiting to start...

Questions

Cheat Sheet

Answer the question(s) below to complete this Section and earn cubes!

+ 0 HackTheBox has an online Swag Shop. Try running a sub-domain fuzzing test on 'hackthebox.eu' to find it. What is the full domain of it?

Submit your answer here...

Submit

Hint

Previous Next

Cheat Sheet

? Go to Questions

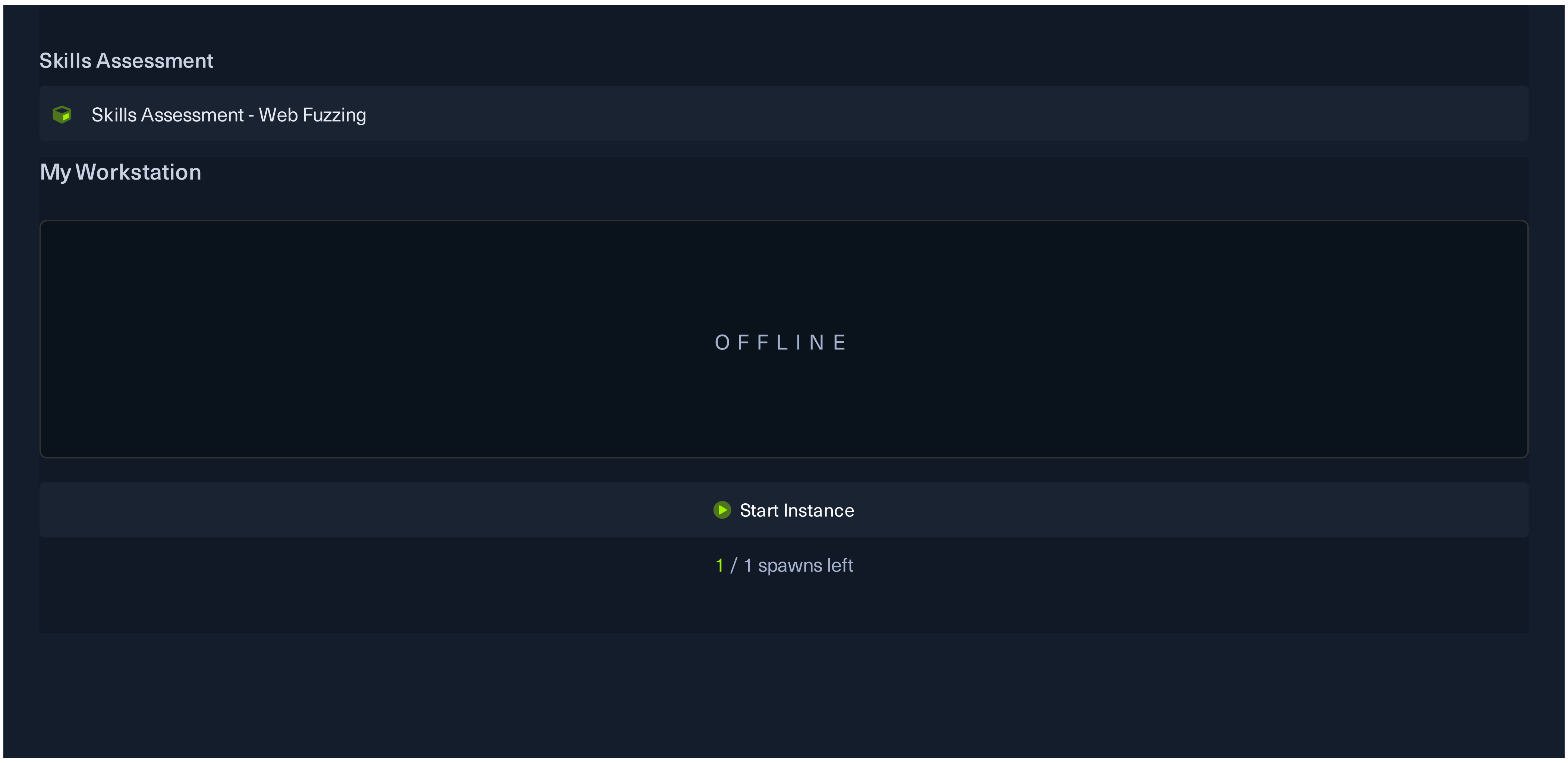
Table of Contents

Introduction

Basic Fuzzing

Domain Fuzzing

Parameter Fuzzing



Skills Assessment

Skills Assessment - Web Fuzzing

My Workstation