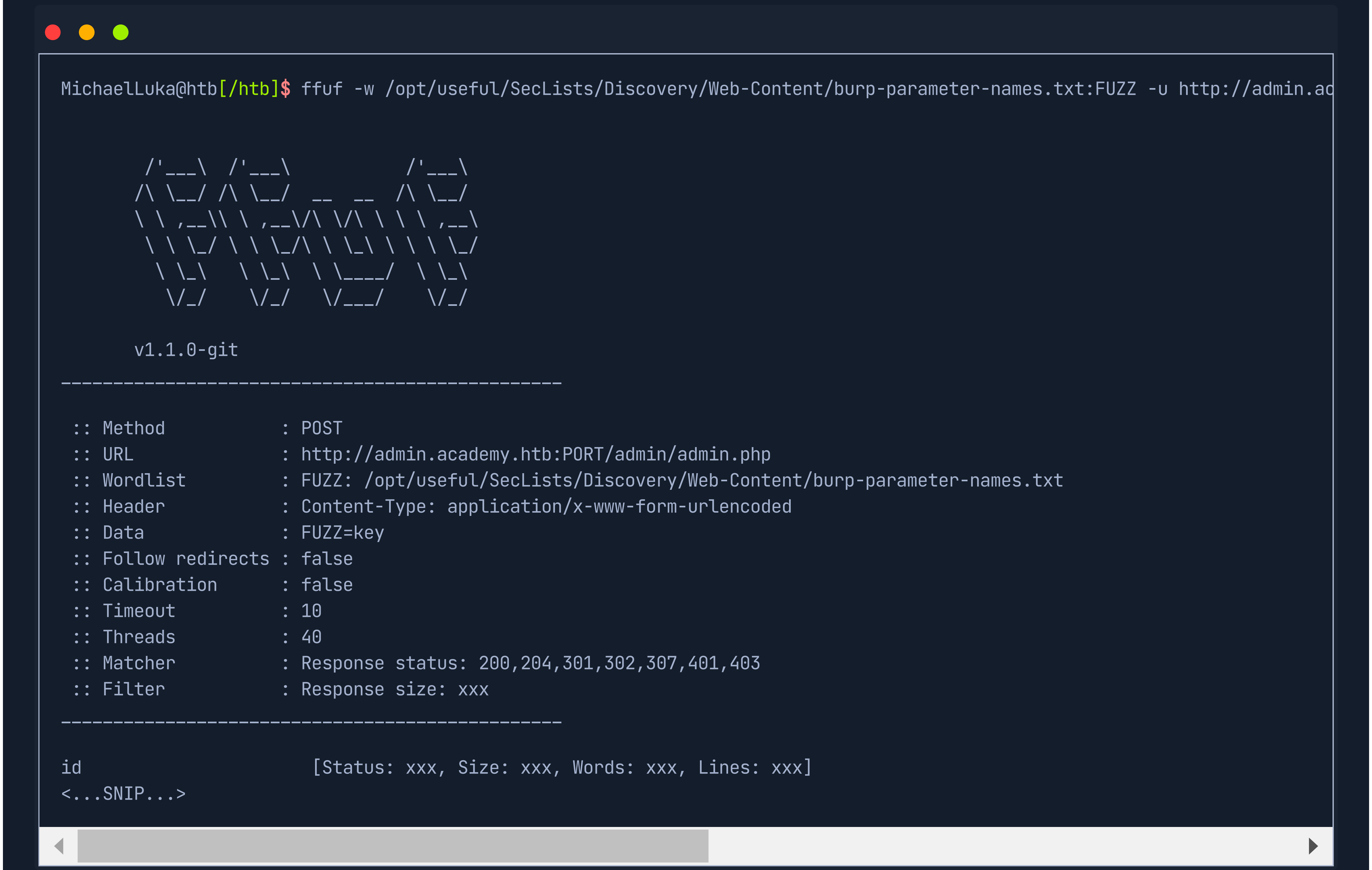
Parameter Fuzzing - POST

The main difference between POST requests and GET requests is that POST requests are not passed with the URL and cannot simply be appended after a ? symbol. POST requests are passed in the data field within the HTTP request. Check out the Web Requests module to learn more about HTTP requests.

To fuzz the data field with ffuf, we can use the -d flag, as we saw previously in the output of ffuf -h. We also have to add -X POST to send POST requests.

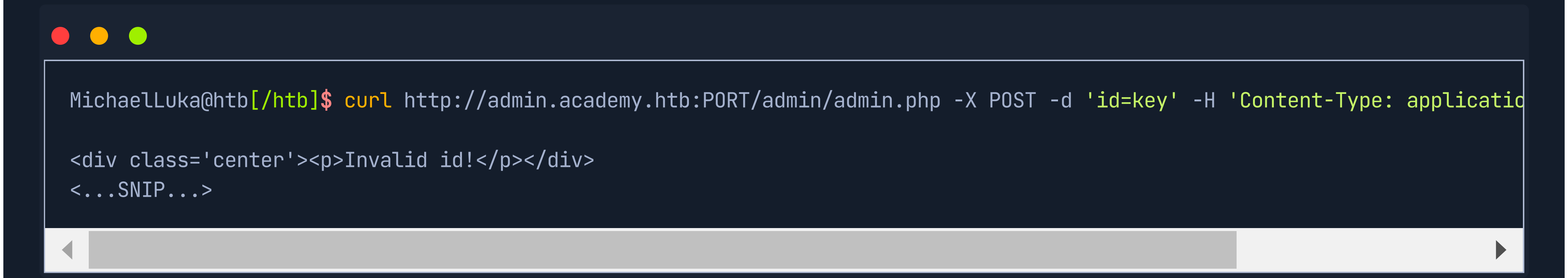
Tip: In PHP, "POST" data "content-type" can only accept "application/x-www-form-urlencoded". So, we can set that in "ffuf" with "-H 'Content-Type: application/x-www-form-urlencoded'".

So, let us repeat what we did earlier, but place our FUZZ keyword after the -d flag:



```
MichaelLuka@htb[/htb]$ ffuf -w /opt/useful/SecLists/Discovery/Web-Content/burp-parameter-names.txt:FUZZ -u http://admin.ac


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

       v1.1.0-git
________________________________________________

 :: Method           : POST
 :: URL              : http://admin.academy.htb:PORT/admin/admin.php
 :: Wordlist         : FUZZ: /opt/useful/SecLists/Discovery/Web-Content/burp-parameter-names.txt
 :: Header           : Content-Type: application/x-www-form-urlencoded
 :: Data             : FUZZ=key
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403
 :: Filter           : Response size: xxx
________________________________________________

id                      [Status: xxx, Size: xxx, Words: xxx, Lines: xxx]
<...SNIP...>
```

As we can see this time, we got a couple of hits, the same one we got when fuzzing GET and another parameter, which is id. Let's see what we get if we send a POST request with the id parameter. We can do that with curl, as follows:



```
MichaelLuka@htb[/htb]$ curl http://admin.academy.htb:PORT/admin/admin.php -X POST -d 'id=key' -H 'Content-Type: applicatio

<div class='center'><p>Invalid id!</p></div>
<...SNIP...>
```

As we can see, the message now says Invalid id!.

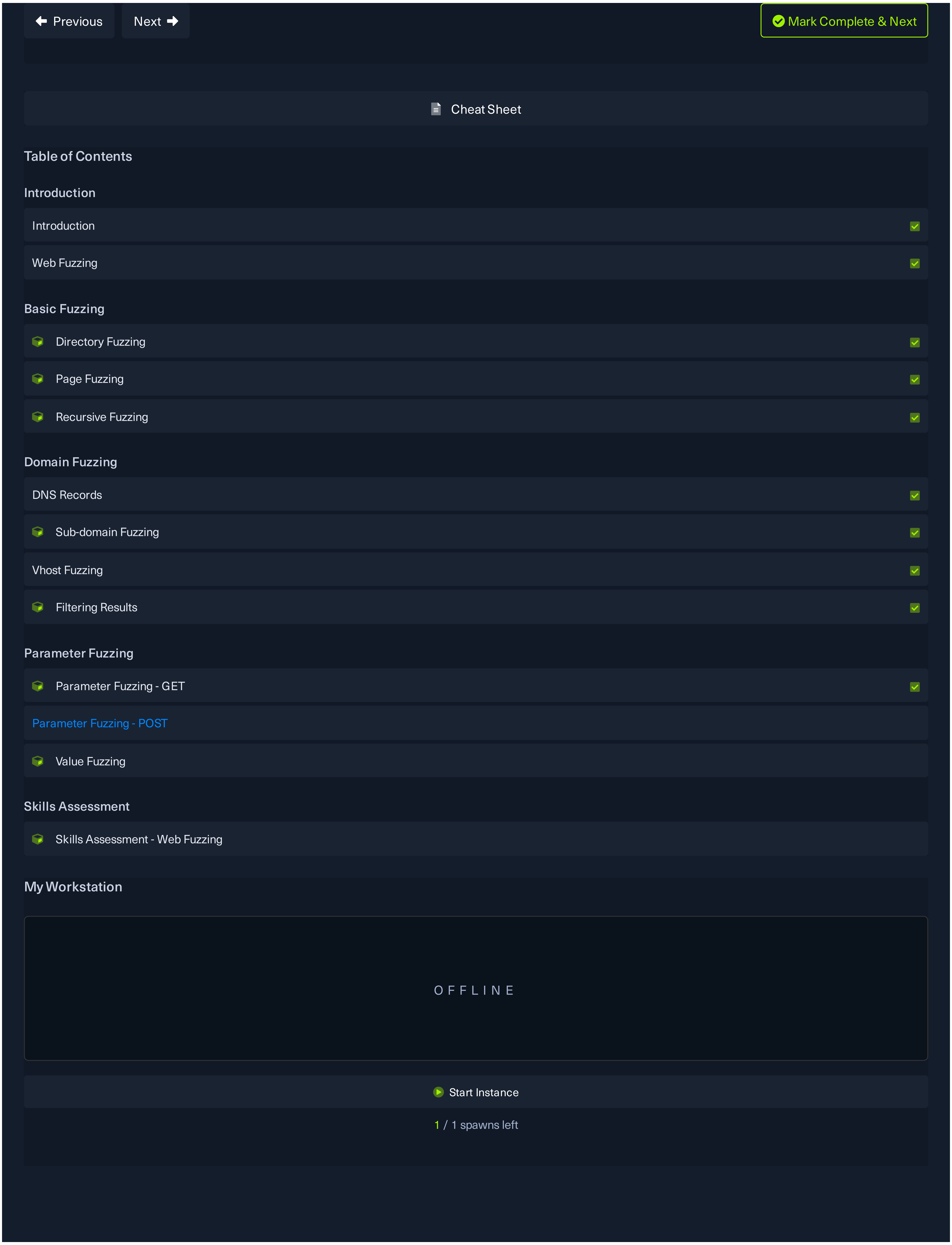


Table of Contents

Introduction

Basic Fuzzing

Domain Fuzzing

Parameter Fuzzing

Skills Assessment

My Workstation

OFFLINE

1 / 1 spawns left