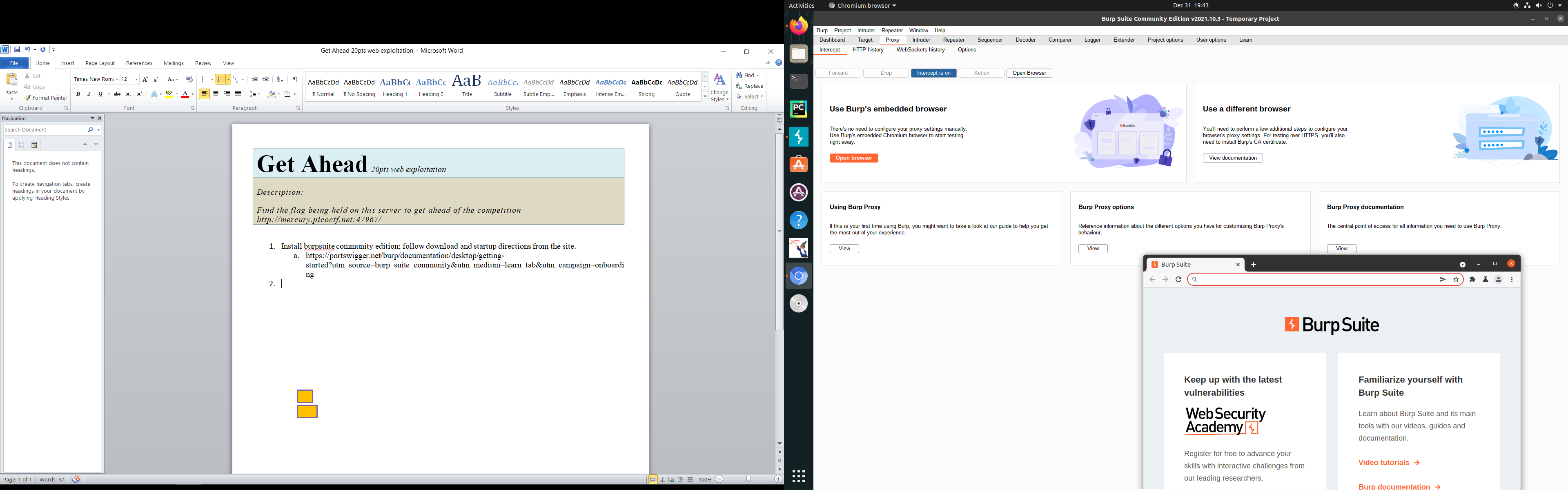
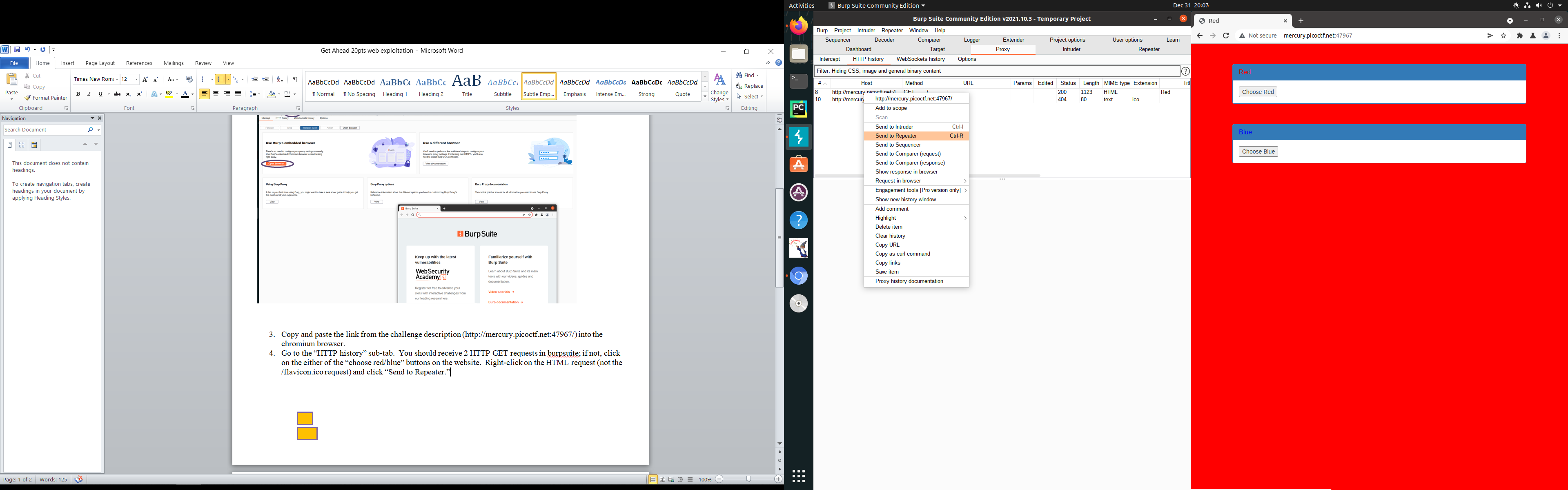
|  |
| --- |
| Get Ahead *20pts web exploitation* |
| Description:  Find the flag being held on this server to get ahead of the competition http://mercury.picoctf.net:47967/ |

1. Install burpsuite community edition; follow download and startup directions from the site.
   1. https://portswigger.net/burp/documentation/desktop/getting-started?utm\_source=burp\_suite\_community&utm\_medium=learn\_tab&utm\_campaign=onboarding
2. Once burpsuite is opened, click on the “proxy” tab at the top of the screen, and then click the “open browser” button; a built-in chromium browser should then open.

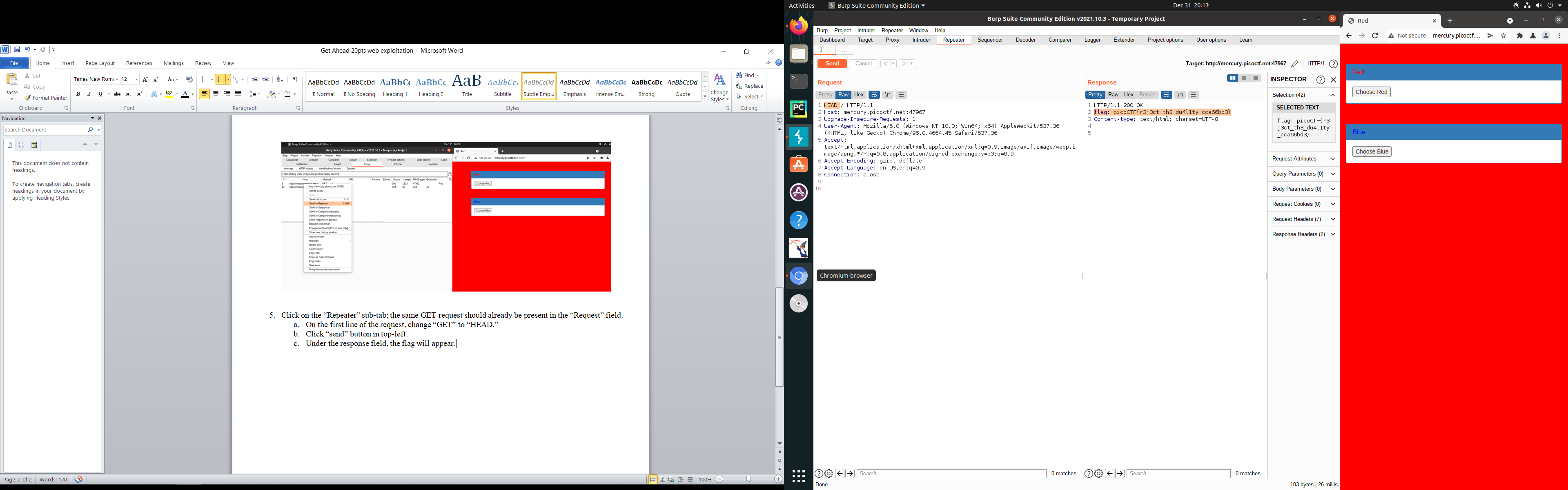


1. Copy and paste the link from the challenge description (http://mercury.picoctf.net:47967/) into the chromium browser.
2. Go to the “HTTP history” sub-tab. You should receive 2 HTTP GET requests in burpsuite; if not, click on the either of the “choose red/blue” buttons on the website. Right-click on the HTML request (not the /flavicon.ico request) and click “Send to Repeater.”



1. Click on the “Repeater” tab; the same GET request should already be present in the “Request” field.
   1. On the first line of the request, change “GET” to “HEAD.”
      1. Capitalization matters.
   2. Click “send” button in top-left.
   3. Under the response field, the flag will appear.
   4. NOTE: this can be done on any HTML GET request to the site; i.e. any of the HTML GET requests sent by pressing the buttons.

5



5c

5b

5a