

Where are the robots?

I attempted the picoCTF web-based question “Where Are the Robots?” This question involved the basics of web enumeration and the robots.txt file. The question itself, “Where Are the Robots?” seemed to be asking where the robots would be excluded, perhaps by the robots.txt file. I began by going to the site provided by the question, <http://fickle-tempest.picoctf.net:54178>. This site only had a standard homepage message and did not have the flag anywhere. Upon examining the HTML, I realized that the homepage did not have any hidden flags or clues other than the message itself. I then proceeded to look for the robots.txt file, a common location for hidden flags.

I went to <http://fickle-tempest.picoctf.net:54178/robots.txt> and saw the following lines of code:

```
User-agent: *
Disallow: /cc6b1.html
```

This told the robots not to look in the cc6b1.html file, but I, being a human, am allowed to look there. Upon going to <http://fickle-tempest.picoctf.net:54178/cc6b1.html>, I saw the flag right away. This illustrates the main point of the question: the robots.txt file is not a security measure and is only used to tell robots what to do. Any file listed there can be accessed by a human if the URL is known.

In doing this, I was reiterating that even the smallest detail is important and that web enumeration is the first step towards web exploitation. This exercise was also reiterating the security concept that important information should not be placed within the robots.txt file. This exercise was performed using logic and the basics of the web, which meant that no tools were required to be used, and that observation would lead you to the goal.