Challenge URL: /dvwa/vulnerabilities/upload/
Objective: Execute any PHP function of your choosing on the target system (such as phpinfo() or system()) thanks to this file upload vulnerability.
Tools needed: A reverse shell, netcat

Did you remember to read this section's README?

The Guide

Note: This challenge is extremely similar to Challenge 4. We'll be using the PHP reverse shell and netcat listener from before, so make sure those are good to go before proceeding.

Right off the bat, DVWA presents a simple file upload form.

Let's not waste any time, and immediately try to upload Challenge 4's reverse shell, **php-reverse-shell.php**.

It can't be this easy, can it? The form tells you exactly where the newly-uploaded shell is! Let's try navigating to it.

http://dvwa/dvwa/hackable/uploads/php-reverse-shell.php

Looks like the shell worked first try. I tested with the `whoami` command we learned in Challenge 2, and we got the same output as before. I guess it really was that easy!

Challenge complete! Feeling like a hacker yet?