ThinkPHP Walkthrough

Requirements:

Nmap

Metasploit

Difficulty:

Easy

Walkthrough:

1. Build and host the docker server.
   * docker build -t <NAME> .
   * docker run -p 80:80 <NAME>
2. Run NMAP to find the open port.

Text

Description automatically generated

1. Navigate to the website hosted on port 80.

Graphical user interface, website

Description automatically generated

1. The website hints that it is running ThinkPHP which is confirmed by navigating to “/index.php?s=a”.

Text

Description automatically generated

1. Researching this version of ThinkPHP reveals a multitude of RCE vulnerabilities. Metasploit is seen to have an exploit script that can be used to get access.

A screenshot of a computer screen

Description automatically generated with medium confidence

Text

Description automatically generated

Text

Description automatically generated

1. The flag can then be found in the home directory.

Text

Description automatically generated