PHP Magic Hash Walkthrough

Requirements:

Nmap

Web browser

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 which hints at a PHP login bypass.

Graphical user interface, application, website

Description automatically generated

1. The hint leads to using a PHP SHA-256 magic hash to bypass the login using the credentials “Admin:34250003024812”. The magic was found in this example at <https://github.com/spaze/hashes/blob/master/sha256.md>
2. Entering the credential reveals the flag.

Graphical user interface, text

Description automatically generated