

# Requesting Web Servers

**Mission 1: GET IT!**

*The next mission should be performed using a Python script or interpreter*

1. Send a get request to <http://scanme.nmap.com/> and print the following:
   1. Requested URL
   2. Response code
   3. Response text
   4. Response headers

You could get further help using the dir() and help() built-in functions:

import requests

r = requests.get("http://scanme.nmap.com/")

dir(r)

help(r)

1. Google uses the “q” parameter to search a value.
   1. Could you query “Admin” search to google?
   2. Did you receive a proper response code?
   3. Did you able to read the response text?
   4. Change the user agent header sent to “***Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.51 Safari/537.36***” and try again - Did it solve the problem of the response?
2. Access to <http://testphp.vulnweb.com/> and examine the navigation bar (you can recognize it as “home”, “categories”,etc…).
   1. Create a list of the categories (manually)
   2. As part of a web application recon, you should determine what is the largest page among them

**Mission 2: The Postman**

*The next mission should be performed using a Python script or interpreter*

1. Access to <http://testphp.vulnweb.com> and examine the “search art” feature - make a POST request to search for a “mona lisa” art.
2. In the same website - move to “login.php” URI and use the requests library to test the response when you submit the form with “test:test” credentials - how could you determine whether it worked? Is “admin:admin” are valid credentials as well?