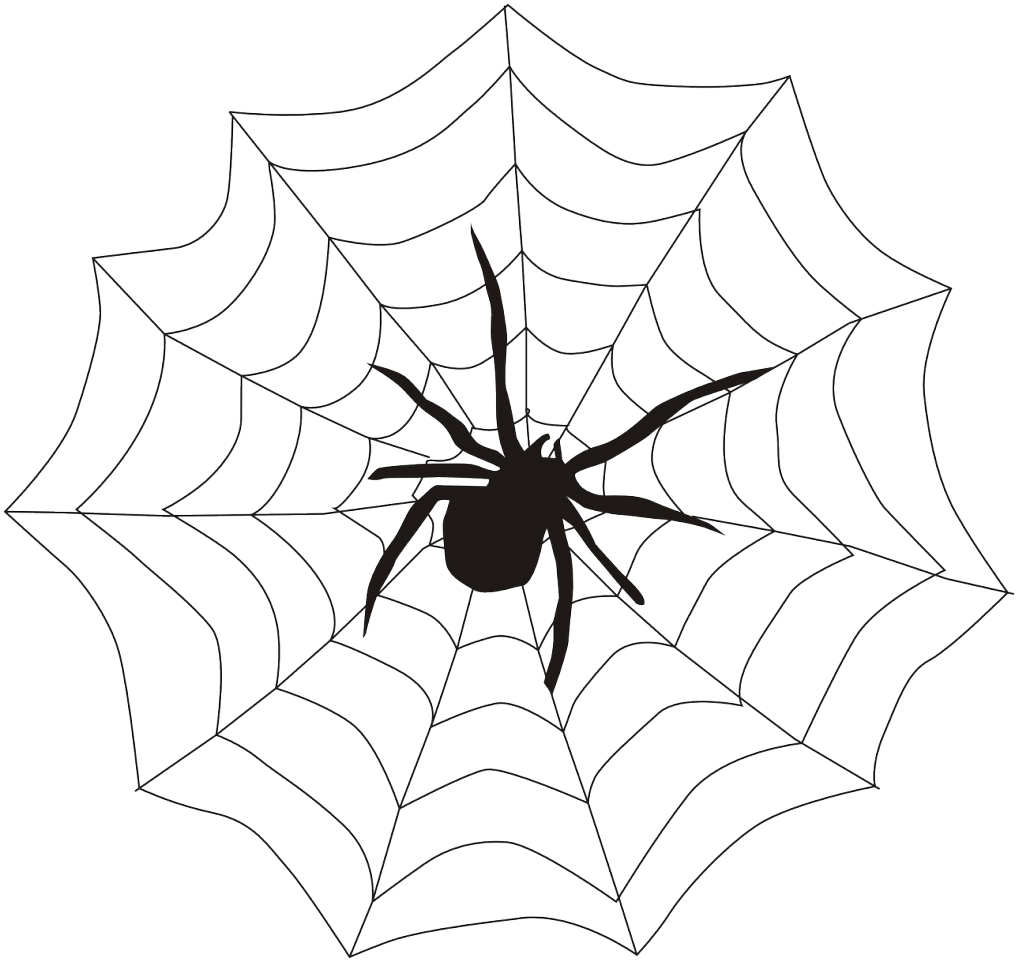
HackerFrogs Afterschool OverTheWire Natas: Part 1

Class:
Web App Hacking

Workshop Number:
AS-WEB-01

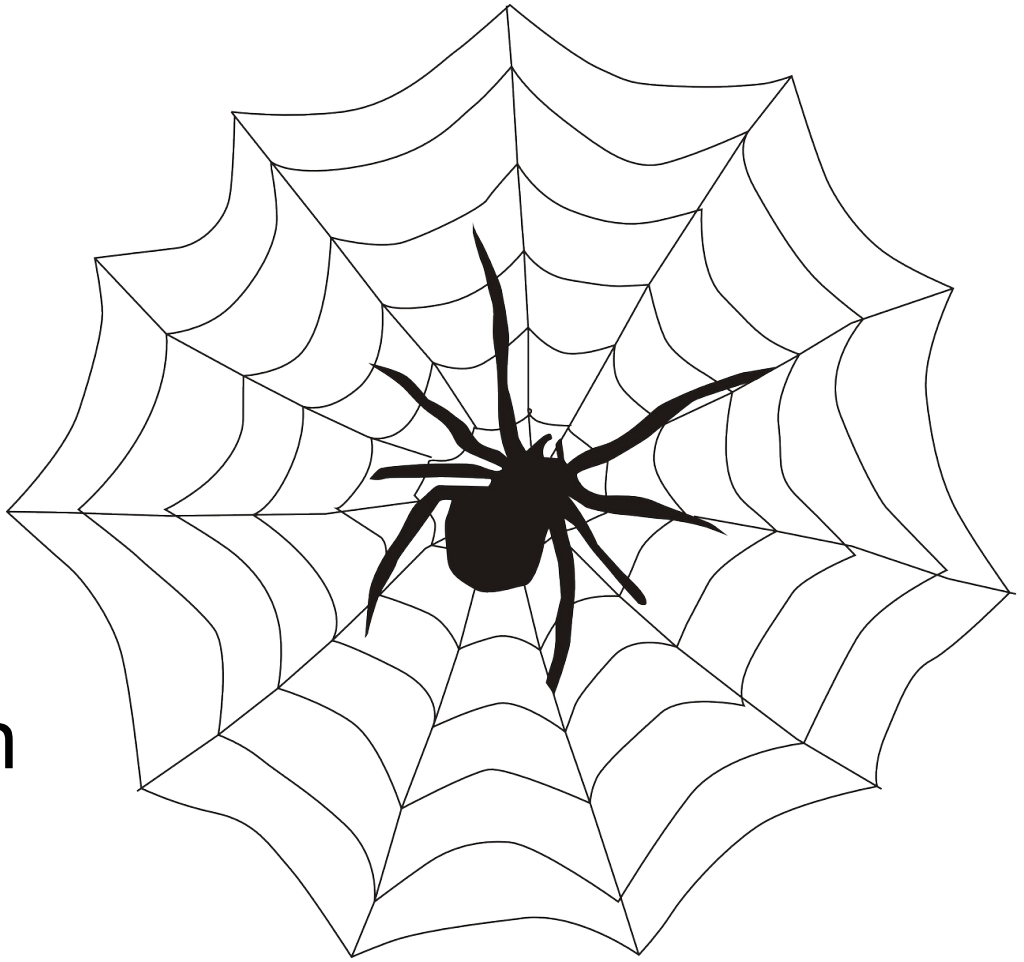
Document Version:
1.2

Special Requirements:
None



Web App Hacking

This is the first workshop in our intro to web app hacking course. Before we start, let's introduce the learning materials we'll be working through in the course.



Natas CTF

The CTF game we will be playing to learn basic web app hacking skills is called Natas, which is hosted on the OverTheWire CTF network. The OverTheWire network hosts several different CTF games.

Natas CTF

The Natas CTF game is made up of many levels of increasing difficulty. The initial levels (0-3) cover the target web app hacking techniques for this workshop.

Natas CTF

To learn about the Natas CTF rules, let's navigate to the following URL:

https://overthewire.org/wargames/natas/

P-0 HTTP Source Code

```
<html>
<head>
<!-- This stuff in the header has nothing to do with the level -->
<link rel="stylesheet" type="text/css"
href="http://natas.labs.overthewire.org/css/level.css">
<link rel="stylesheet" href="http://natas.labs.overthewire.org/css/jquery-ui.css" />
<link rel="stylesheet" href="http://natas.labs.overthewire.org/css/wechall.css" />
<script src="http://natas.labs.overthewire.org/js/jquery-1.9.1.js"></script>
<script src="http://natas.labs.overthewire.org/js/jquery-ui.js"></script>
<script src=http://natas.labs.overthewire.org/js/wechall-data.js></script><script
```

Web browsers render out webpages based on the HTTP code provided by the web server. Every web browser allows us to view a web page's HTTP source code.

P-0 HTTP Source Code

```
<h1>natas2</h1>
<div id="content">
There is nothing on this page
<img src="files/pixel.png">
</div>
</body></html>
```

For web app testing, this allows us to find interesting directories, developer comments, and more

P-1 Lateral Problem Solving

“When hackers encounter a locked door, they look for an open window.”

We can look at web app security in terms of checking which doors and windows are locked, and which can be opened.

P-1 Lateral Problem Solving

This is where the security tester's most powerful weapon, “research”, comes into play. Two common research tools used these days are ChatGTP and the Google search engine.

P-1 Lateral Problem Solving

ChatGPT

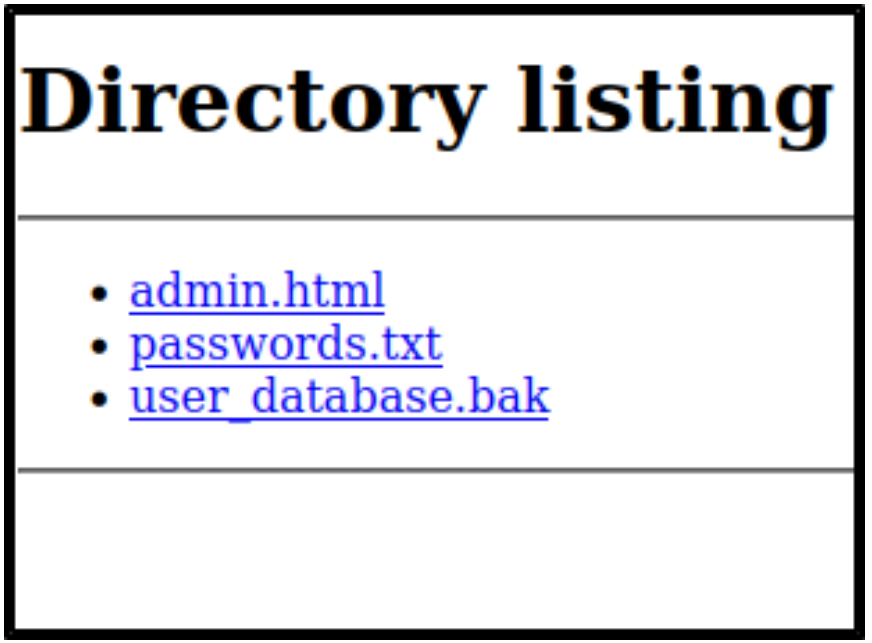
If right-clicking is disabled in your web browser, there are still several alternative methods to view the source code of an HTTP page:

1. Keyboard Shortcuts:
   - For Windows: Press Ctrl+U to view the page source.
   - For Mac: Press Command+Option+U.

So once the obstacle to a problem is discovered, we can research a way to overcome the obstacle, or a method of bypassing it.

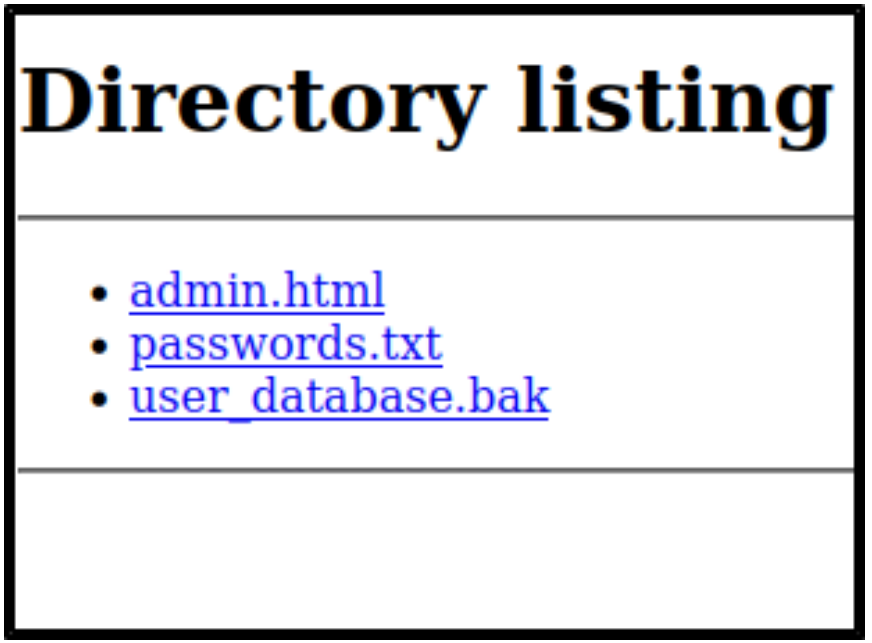
P-2 Directory Indexing

Directory indexing is a insecure setting on websites that allows users to see the file contents of web directories. Although it is quite rare to encounter this issue on modern websites, it is still very common to find it on older websites.



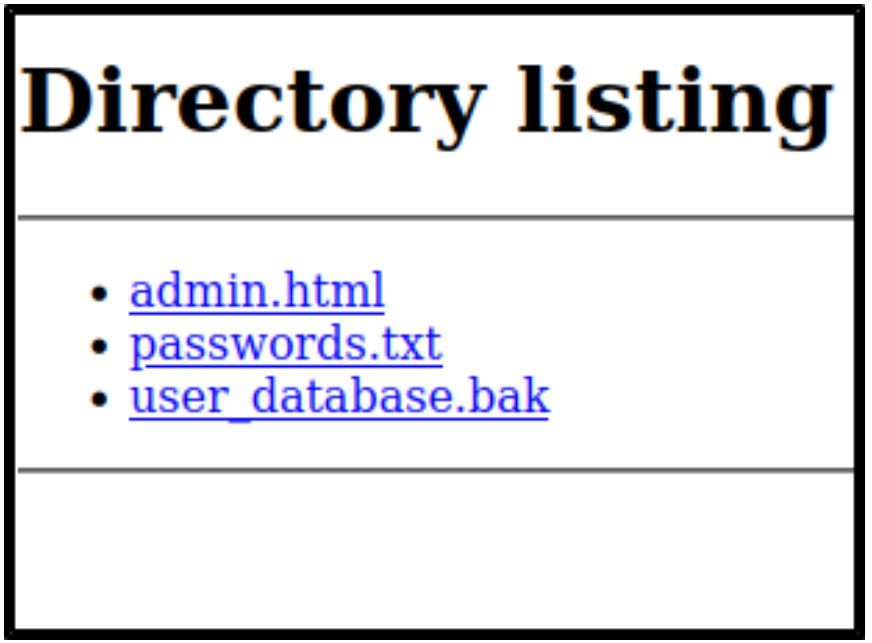
P-2 Directory Indexing

If directory indexing is enabled, and a malicious user is able to discover different directory paths on the website (either through guessing, html source analysis, or “directory busting”),



P-2 Directory Indexing

then sensitive files may be discovered, stolen, or otherwise abused.



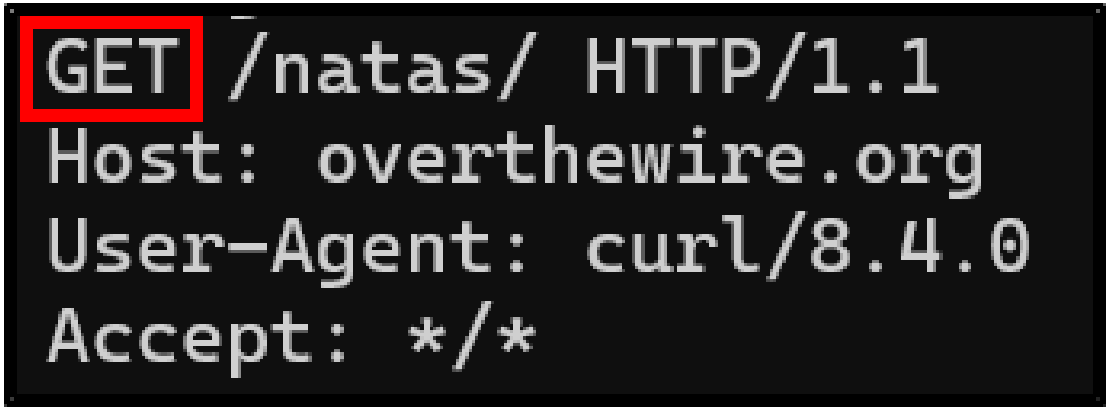
HTTP Requests

HTTP is the backbone of the the internet, and all web browsers receive webpage content by sending **HTTP requests** to web servers.

HTTP Requests

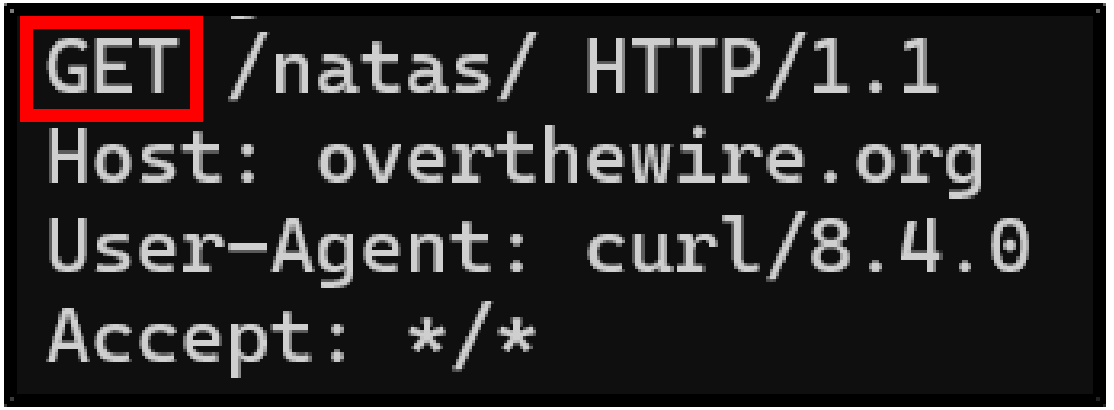
In return, the web servers send the web browser an **HTTP response**, which is rendered by the browser and presented to the user.

HTTP Request Methods



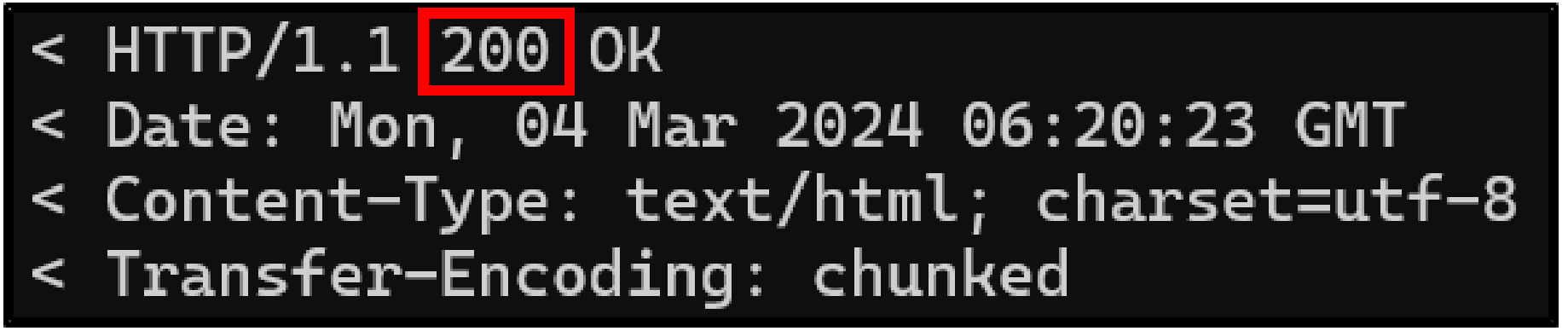
Each HTTP request is made with a specific **HTTP method**, which tells the web server what kind of interaction you want from it.

HTTP Request Methods



The most common HTTP method is the **GET** method, which retrieves the contents of webpages.

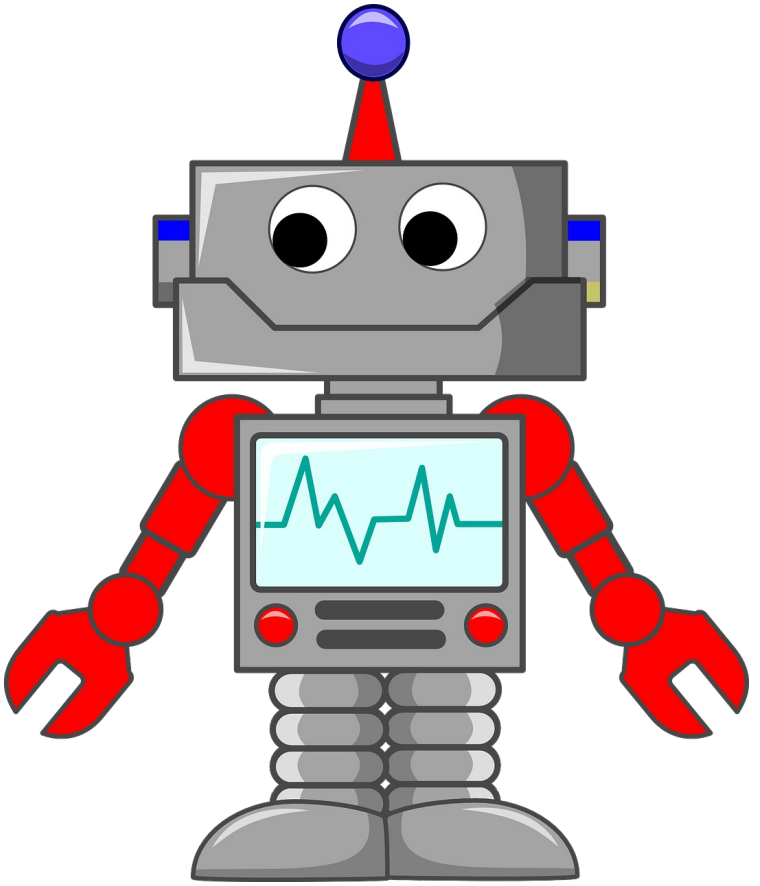
HTTP Response Codes



The web server will always return an HTTP **status code** with its response, in the form of a 3-digit number. Any code in the 2XX range is considered a successful response.

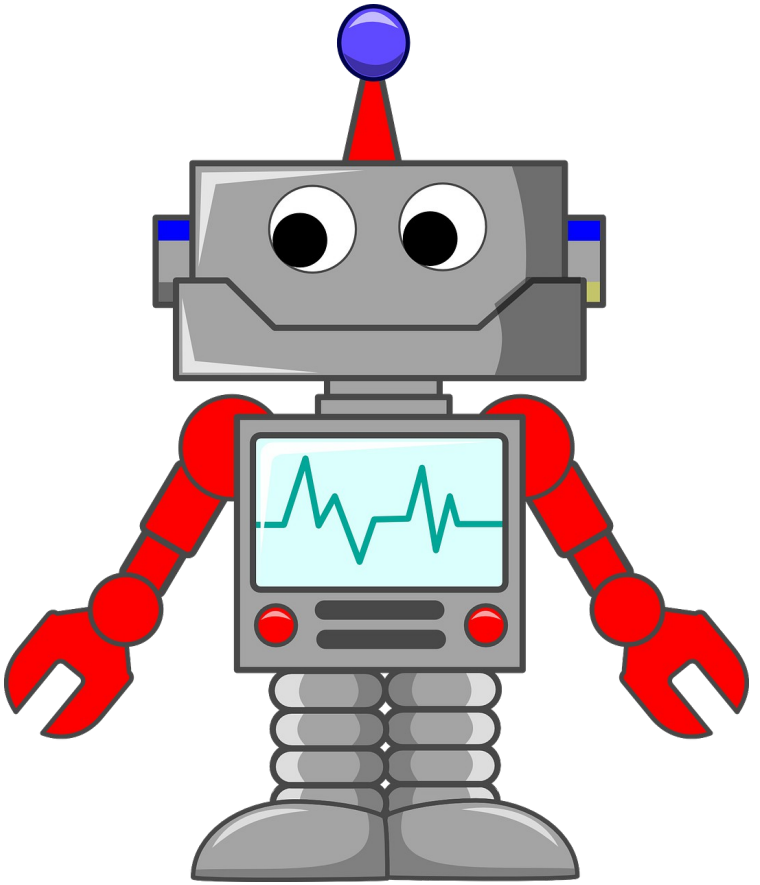
P-3 Robots.txt

Search engines (such as Google, Yahoo, DuckDuckGo, etc) use programs called robots to visit websites and map out their webpages. However, this may cause sensitive areas of websites to appear in search results.



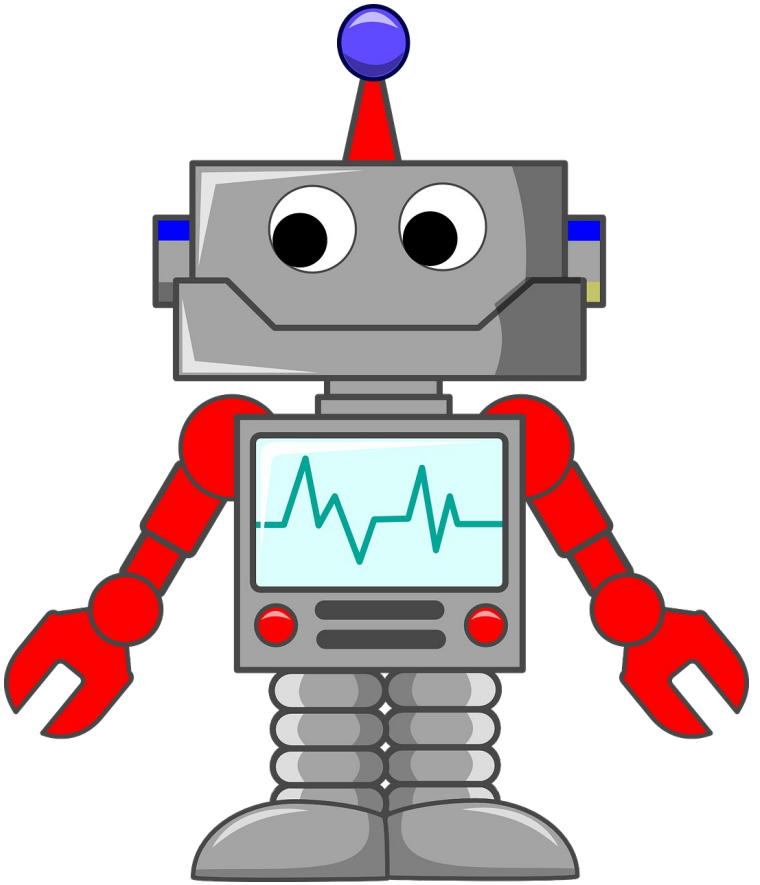
P-3 Robots.txt

In order to prevent this, website administrators can add a file called **robots.txt** to their website, which specifies which directories and / or pages of the website are off-limits to search engine robot programs.

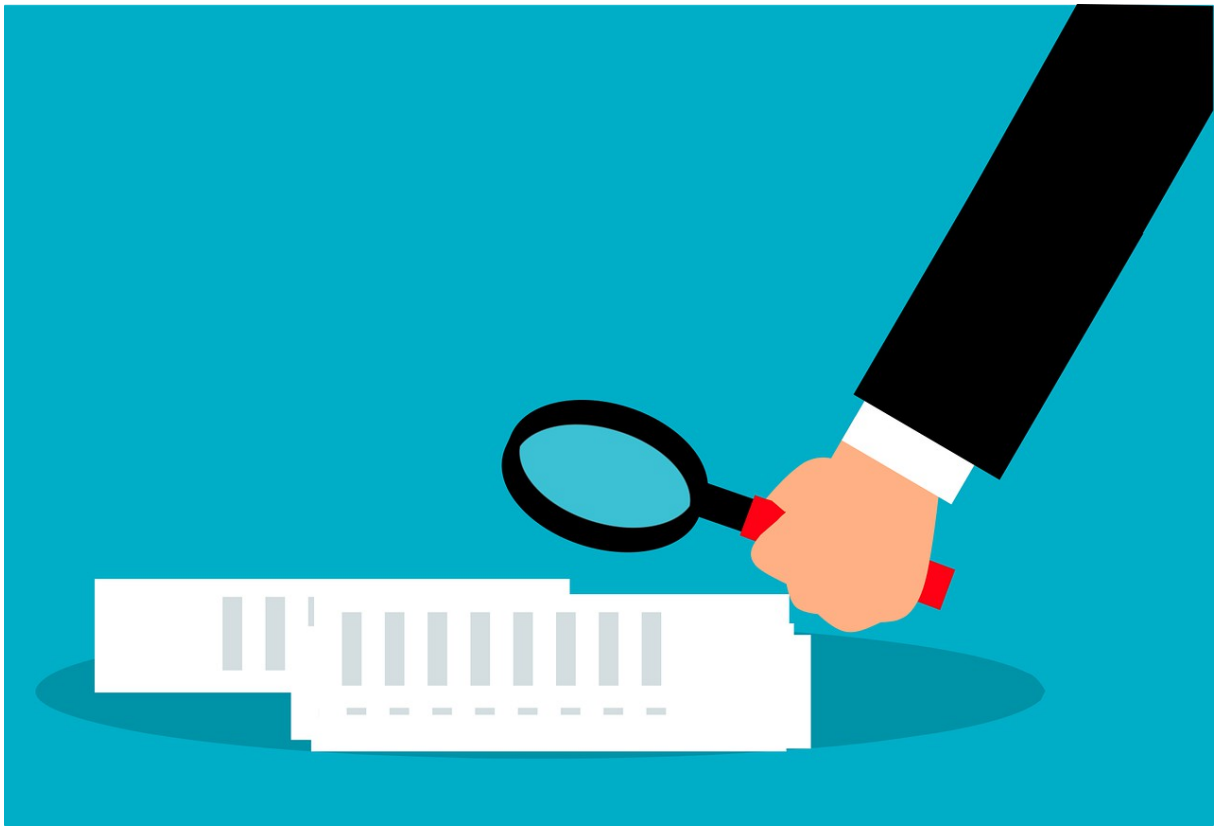


P-3 Robots.txt

Unfortunately, if malicious users know how to find the **robots.txt** file, the contents of the file could potentially lead them to sensitive areas of the website.



Summary



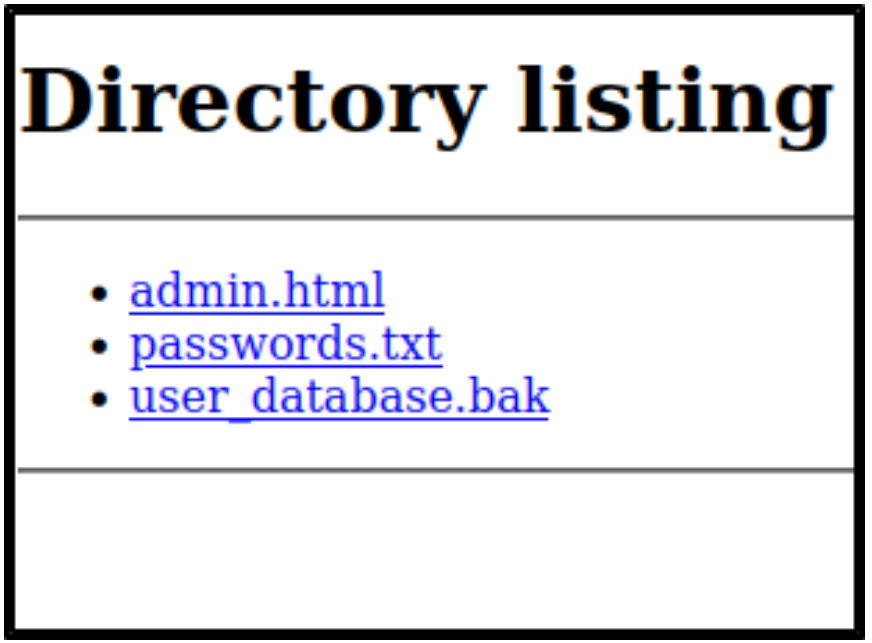
Let's review the web exploitation concepts we learned in today's workshop:

Lateral Problem Solving

The most important skill to develop in cybersecurity is researching: Google and ChatGPT are two powerful research tools, use them wisely!

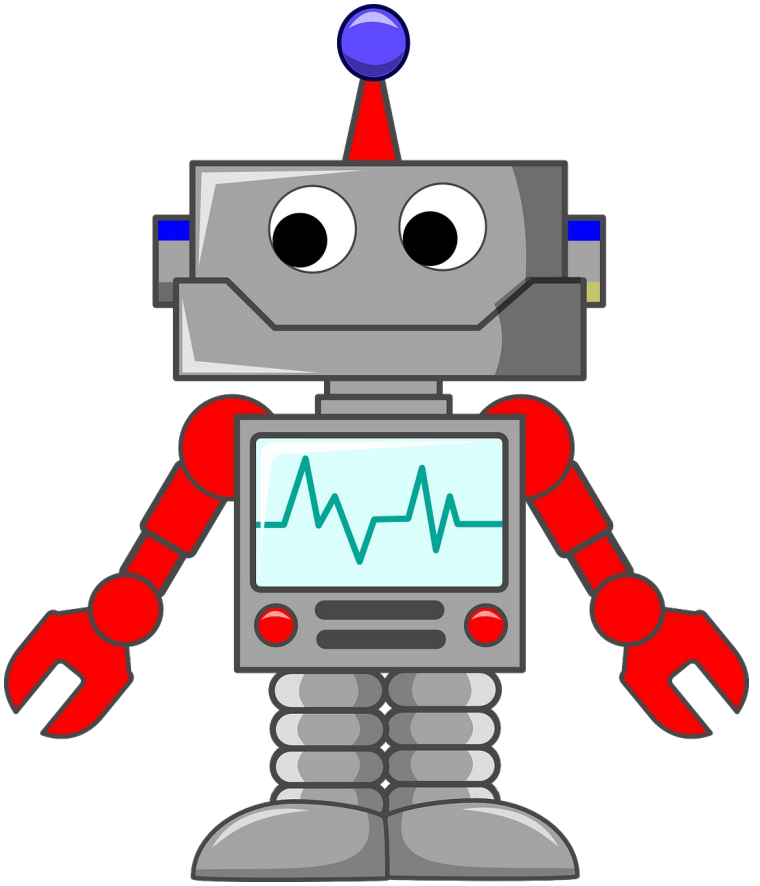
Directory Indexing

Directory indexing is a vulnerability on websites that allows users to see the file contents of web directories, which can lead to sensitive data exposed to arbitrary website visitors.



Robots.txt

Robots.txt is a special file included on certain websites that indicate which files on the site can / cannot be indexed by search engines. It can be abused to point malicious users to sensitive parts of the website.



What's Next?

In the next HackerFrogs Afterschool web exploitation workshop, we'll continue learning web exploitation skills with Natas CTF.

Extra Credit

Looking for more study material on this workshop's topics?

See this video's description for links to supplemental documents and exercises!

Until Next Time, HackerFrogs!