HackerFrogs Afterschool Network Hacking – Session 8

Class:
Network Hacking

Workshop Number:
AS-NET-08

Document Version:
1.75

Special Requirements:
Registered account
at tryhackme.com

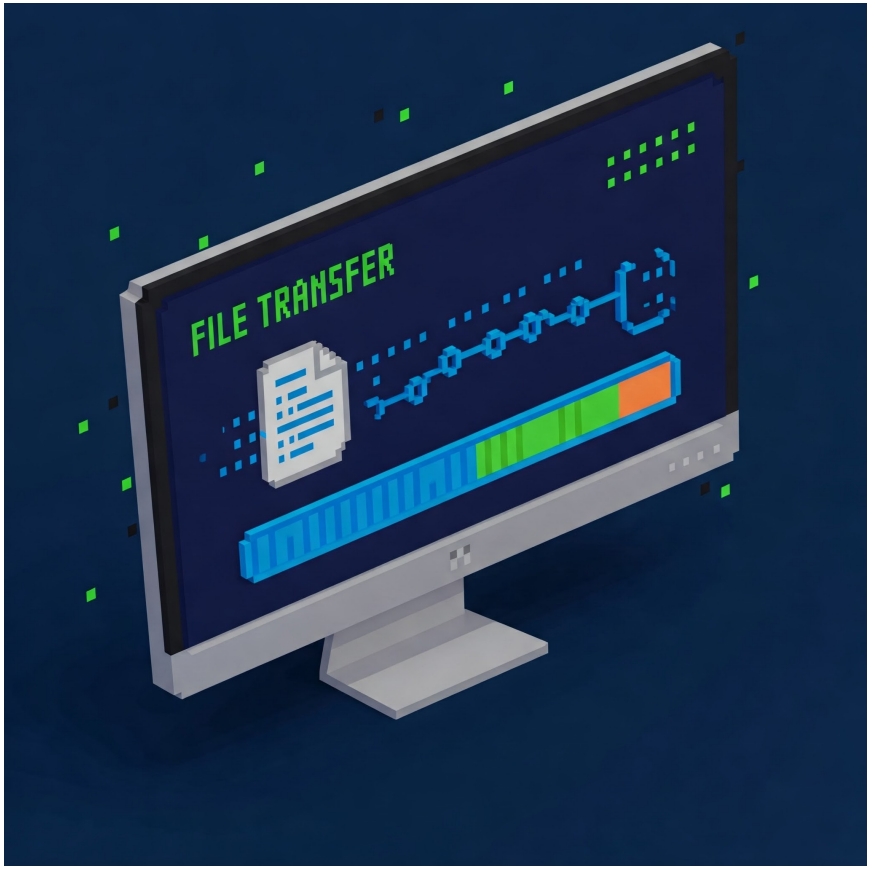
Welcome to HackerFrogs Afterschool!

This is the eighth session for network hacking!

Let's go over the concepts we covered in the previous session!

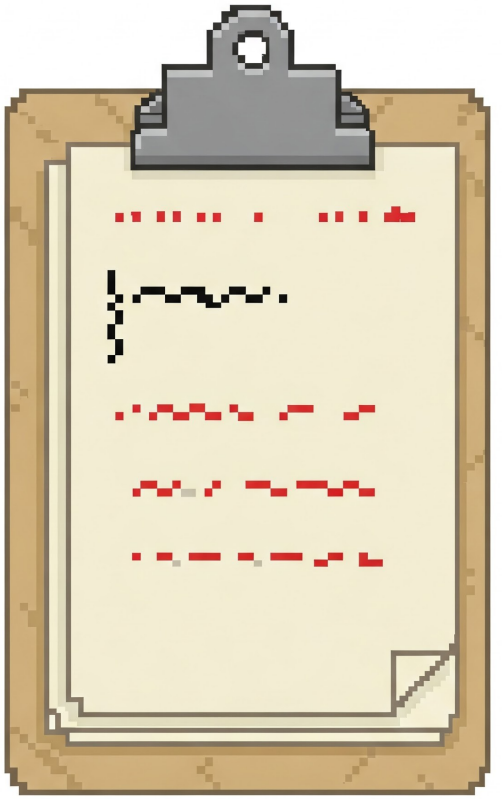
What are File Transfers?

File transfers are an essential operation of computer networking, and we learned a few different methods for file transfer



Transferring Small Files by Clipboard and Base64

The clipboard and Base64 method of file transfer is safe and convenient for small files, but it's not practical for larger files



Transferring Files via Python HTTP and Wget

In controlled networks, hosting files using the Python HTTP module and downloading with Wget is convenient, but it's not recommended for real-world scenarios, since it sends data unencrypted

Transferring Files via Scp (SSH)

If we have SSH on both devices and a set of credentials, the Scp program is an ideal file transfer solution, since it sends files over and encrypted protocol

This Session's Topics

- What are File Upload Attacks?

- Uploading via Web Page

- Uploading via Web Page /w Filter Bypass

What are File Upload Attacks?

File Upload Attacks are a type of web app hack where malicious files can be uploaded to a web server and then accessed on the web app, executing the code within the uploaded malicious files

What are File Upload Attacks?

In order to perform a file upload attack, there are three conditions that must be met

1) There must be a way to upload files to a web-accessible location, via web app, or another service (e.g., FTP, SMB)

2) The upload location must be known to us

3) The app must be able to execute code: e.g., PHP or ASP

Accessing TryHackMe

Let's access this TryHackMe room to learn about file upload attacks:

https://tryhackme.com/room/dvwa

File Upload Condition

The app lets us upload files, and a lot of apps only let you upload files of a certain type, but this app allows any file type to be uploaded, aka unrestricted file upload

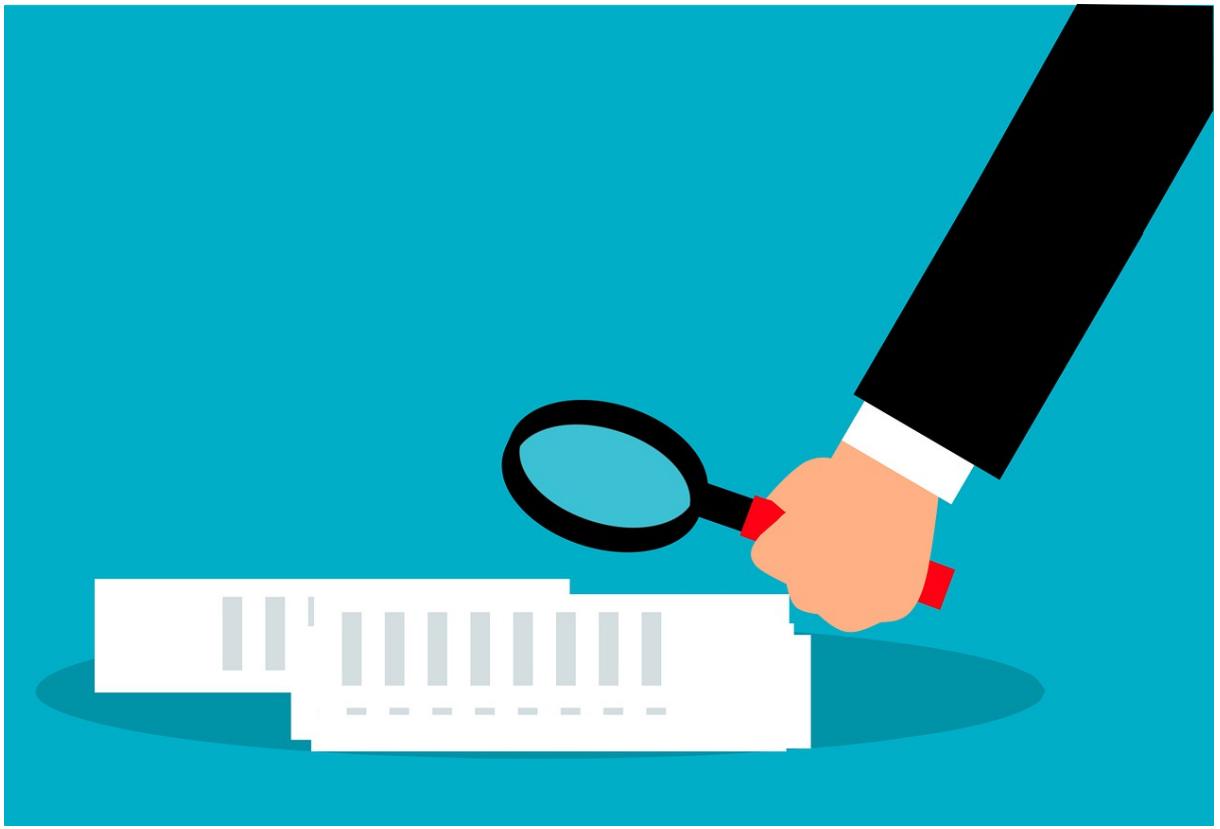
Code Execution Condition

File upload attacks will not work unless the web app executes code in files. PHP is a classic example, and web apps that host PHP files is a good indicator that an app is vulnerable

Known Upload Location Condition

The last condition of file upload attack is the ability to access the malicious file you upload to the application. This app explicitly lets us know where uploaded files are located in the app

Summary



Let's review the network hacking concepts we learned in this workshop:

What are File Upload Attacks?

File Upload Attacks are a type of web app hack where malicious files can be uploaded to a web server and then accessed on the web app, executing the code within the uploaded malicious files

File Upload Condition

The app lets us upload files, and a lot of apps only let you upload files of a certain type, but this app allows any file type to be uploaded, aka unrestricted file upload

Code Execution Condition

File upload attacks will not work unless the web app executes code in files. PHP is a classic example, and web apps that host PHP files is a good indicator that an app is vulnerable

Known Upload Location Condition

The last condition of file upload attack is the ability to access the malicious file you upload to the application. This app explicitly lets us know where uploaded files are located in the app

What's Next?

In the next HackerFrogs Afterschool Network Hacking workshop, we'll be learning how escalate privileges on Linux servers!