

Web Hosting & Security 1 - Nov 7

Local Hosting vs. Cloud Hosting

Local Host

It is possible to save an HTML file on your computer and view it in your browser. In this case, your computer acts as a **local host** for the files. When files are hosted locally (on your computer), outsiders who are not on your computer will not be able to view those files.

Cloud Host

When files are hosted (saved) on the cloud, it means the files have been saved on an outside server (not your computer) that is accessible using the internet.

Setting up local host

Follow the instructions in the lesson to set up localhost on your computer. If it doesn't work for you, try the alternate activity. Either way, these files will only be visible to you.

Setting up cloud host

Shared Hosting

For small businesses and/or websites with limited traffic
Less expensive but share resources and security

Dedicated Hosting

Your site is the only one on that server. You are not sharing bandwidth/server resources/memory with other websites. Website runs faster and handles more traffic. Improved, around-the-clock, technical support from the hosting provider.

VPS Hosting (Virtual Private Server)

Ideal for projects that are in between (smaller) shared hosting and (larger) dedicated hosting. Your website is on a shared server BUT a specific quantity of resources, bandwidth and memory are dedicated to your website.

FTP: File Transfer Protocol

Great for moving files between local host and cloud host.
Many free FTP programs. My go to is Filezilla

cPanel

Easy-to-use website management platform offering a wide variety of features including a file manager, database access, virus scanner, PHP version manager and more. It is accessed through your web browser using login credentials provided to you by your web hosting provider. Always request cPanel access to your hosting environment as cPanel tools are tremendously helpful for web development.

Common Security Attacks

Cross site scripting (XSS)

Injection attack

For example, if you have a contact form on your website, if the form submission contains malicious code, that code risks being injected through the contact form. In this way, an attacker may be able to access sensitive/private information or execute malicious code on the server.

SQL injection

The code in the files communicates with the database using MySQL statements. SQL injection is also a type of injection attack that injects malicious code directly into the website database.

Directory traversal

HTTP attack wherein the attacker exploits vulnerabilities to gain access to directories and files outside of the website's root folder. If successful, the attacker can not only view sensitive files, they may also be able to execute commands on the server.

DDoS (Distributed Denial of Service)

Requires the coordination of several computer systems to attack a given target

A large-scale denial of service attack can have important social impacts and constitutes one of the major digital threats of our time.