* **LESSON 2 UPLOADING YOUR WEBSITE FILES**

**Course Overview:**

In this course, we'll delve into the process of uploading your website files to a web server while maintaining a strong focus on cybersecurity. Uploading your website files is a critical step in making your website accessible to users worldwide. However, it also introduces potential security risks if not done securely. Throughout this course, you'll learn how to securely upload your website files, ensuring the confidentiality, integrity, and availability of your website and its data.

* **Learning Objectives:**
* Understand the importance of secure file uploading in maintaining website security.
* Learn how to securely transfer website files to a web server using various protocols.
* Explore best practices for protecting against common security vulnerabilities during the file uploading process.
* Gain hands-on experience in configuring secure file transfer methods and implementing encryption techniques.
* Understand the role of access controls and permissions in securing uploaded website files.

**Course Outline:**

* **Introduction to Uploading Website Files:**
	+ Importance of secure file uploading in website development.
	+ Overview of the file uploading process and associated security considerations.
* **File Transfer Protocols:**
	+ Comparison of file transfer protocols (FTP, SFTP, SCP, HTTP/S).
	+ Understanding the security features and considerations of each protocol.
* **Secure Configuration of File Transfer Clients:**
	+ Configuring FTP/SFTP clients for secure file transfer.
	+ Implementing encryption and authentication mechanisms to protect file transfers.
* **Securing File Upload Forms:**
	+ Best practices for securing file upload forms on websites.
	+ Validating file types, sizes, and content to prevent malicious uploads.
* **Implementing Secure File Permissions:**
	+ Understanding file permissions and ownership on web servers.
	+ Configuring access controls to restrict unauthorized access to uploaded files.
* **Data Encryption During File Transfer:**
	+ Encrypting files during transit using protocols such as HTTPS and SSH.
	+ Implementing SSL/TLS certificates for secure communication.
* **Protecting Against File Manipulation Attacks:**
	+ Mitigating risks of file manipulation attacks (e.g., path traversal, file inclusion).
	+ Applying input validation and sanitization techniques to prevent exploitation.
* **Hands-on Exercises:**
	+ Configuring secure file transfer clients and servers.
	+ Implementing secure file upload forms with input validation.
	+ Setting up access controls and permissions on web servers.
* **Project: Secure Website Deployment:**
	+ Students will apply their knowledge to securely upload a sample website to a web server, ensuring compliance with cybersecurity best practices.
	+ Emphasis on protecting against common security threats and vulnerabilities during the uploading process.
* **Conclusion:**

Uploading your website files is a crucial step in making your website accessible to users, but it must be done securely to protect against potential security risks. This course will equip you with the knowledge and skills to securely upload your website files, ensuring the confidentiality, integrity, and availability of your website and its data. Join us as we explore the intricacies of file uploading from a cybersecurity perspective and learn how to safeguard your website against threats in the digital landscape.