Understanding File Inclusion Vulnerabilities

If the attacker doesn't have a URL for hosting the HTML file remotely, they would generally need a different method to introduce the HTML content onto the vulnerable server. Here are a few potential ways this could happen:

1. **Local File Inclusion (LFI):**

If the site has a Local File Inclusion (LFI) vulnerability, the attacker might be able to include files that are already present on the server. If the attacker can find a way to upload their HTML file or if the server allows reading from arbitrary files, they could exploit LFI to display the HTML file. This is similar to RFI, but it involves files stored locally on the server instead of remotely.

2. **File Upload Vulnerabilities:**

If the site allows file uploads, an attacker could upload an HTML file (or even a malicious script disguised as an HTML file). Once uploaded, they might be able to access it directly via the file system or via the web server, depending on how the site handles file uploads. This could give the attacker a way to serve their HTML content.

3. **Exploiting Other Input Fields:**

In some cases, an attacker might be able to inject HTML content directly into form fields or other input areas that are displayed back to the user. This would require the site to improperly validate or sanitize input. This is a type of **Cross-Site Scripting (XSS)** attack, where the attacker injects their own HTML code into the page, which gets displayed for other users.

4. **Using Web Shells (Advanced):**

If the attacker can upload a web shell (a file that allows them to control the server), they could use that shell to upload or modify files, including their HTML page. This is a more advanced attack, often requiring a vulnerability like RFI, LFI, or a weak file upload system. Once they have a shell, they can upload any file they want to the server.

To summarize:

- **Without a URL**, an attacker would likely need to exploit a **Local File Inclusion (LFI)** vulnerability or some form of **file upload vulnerability**.
- If the server allows uploading or reading files from arbitrary locations, the attacker might be able to inject or serve their own HTML file.
- If the vulnerability is in user input handling, **XSS** could also be used to inject HTML directly into a page.