

Page 13 / Introduction to SSI Injection

# **Introduction to SSI Injection**

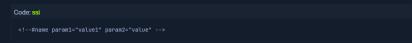
Server-Side Includes (SSI) is a technology web applications use to create dynamic content on HTML pages. SSI is supported by many popular web servers such as Apache and IIS. The use of SSI can often be inferred from the file extension. Typical file extensions include .shtml, .shtm, and .stm. However, web servers can be configured to support SSI directives in arbitrary file extensions. As such, we cannot conclusively conclude whether SSI is used only from the file extension.

### **SSI Directives**

SSI utilizes directives to add dynamically generated content to a static HTML page. These directives consist of the following components:

- name: the directive's name
- parameter name: one or more parameters
- value: one or more parameter values

An SSI directive has the following syntax:



For instance, the following are some common SSI directives.

This directive prints environment variables. It does not take any variables.

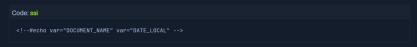
```
Code: ssi
```

This directive changes the SSI configuration by specifying corresponding parameters. For instance, it can be used to change the error message using the errmsg parameter:

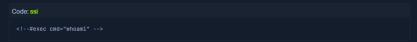
```
<!--#config errmsg="Error!" -->
```

This directive prints the value of any variable given in the var parameter. Multiple variables can be printed by specifying multiple var parameters. For instance, the following variables are supported:

- DOCUMENT\_URI: the current file's URI
- LAST\_MODIFIED: timestamp of the last modification of the current file

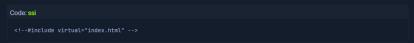


## exec



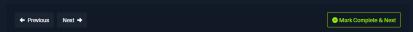
### include

This directive includes the file specified in the virtual parameter, it only allows for the inclusion of files in the web root directory.



## **SSI Injection**

execution of the injected SSI directives. This scenario can occur in a variety of circumstances. For instance, when the web application contains a vulnerable file upload vulnerability that enables an attacker to upload a file containing malicious SSI directives into the web root directory. Additionally, attackers might be able to inject SSI directives if a web application writes user input to a file in the web root directory.







		POWEIED BY THACKTHEBOX