

Server-Side Includes Overview

Server-side includes (SSI) is a technology used by web applications to create dynamic content on HTML pages before loading or during the rendering process by evaluating SSI directives. Some SSI directives are:

Code: [html](#)

```
// Date
<!--#echo var="DATE_LOCAL" -->

// Modification date of a file
<!--#flastmod file="index.html" -->

// CGI Program results
<!--#include virtual="/cgi-bin/counter.pl" -->

// Including a footer
<!--#include virtual="/footer.html" -->

// Executing commands
<!--#exec cmd="ls" -->

// Setting variables
<!--#set var="name" value="Rich" -->

// Including virtual files (same directory)
<!--#include virtual="file_to_include.html" -->

// Including files (same directory)
<!--#include file="file_to_include.html" -->

// Print all variables
<!--#printenv -->
```

The use of SSI on a web application can be identified by checking for extensions such as .shtml, .shtm, or .stm. That said, non-default server configurations exist that could allow other extensions (such as .html) to process SSI directives.

We need to submit payloads to the target application, such as the ones mentioned above, through input fields to test for SSI injection. The web server will parse and execute the directives before rendering the page if a vulnerability is present, but be aware that those vulnerabilities can exist in blind format too. Successful SSI injection can lead to extracting sensitive information from local files or even executing commands on the target web server.

[← Previous](#) [Next →](#)

[Mark Complete & Next](#)

Table of Contents

Introduction to Server-Side Attacks	<input checked="" type="checkbox"/>
Abusing Intermediary Applications	
AJP Proxy	<input checked="" type="checkbox"/>
Nginx Reverse Proxy & AJP	<input checked="" type="checkbox"/>
Apache Reverse Proxy & AJP	<input checked="" type="checkbox"/>
Server-Side Request Forgery (SSRF)	
Server-Side Request Forgery (SSRF) Overview	<input checked="" type="checkbox"/>
SSRF Exploitation Example	<input checked="" type="checkbox"/>
Blind SSRF	<input checked="" type="checkbox"/>
Blind SSRF Exploitation Example	<input checked="" type="checkbox"/>
Time-Based SSRF	<input checked="" type="checkbox"/>
Server-Side Includes (SSI) Injection	
Server-Side Includes Overview	<input checked="" type="checkbox"/>
SSI Injection Exploitation Example	<input checked="" type="checkbox"/>
Edge-Side Includes (ESI) Injection	
Edge-Side Includes (ESI)	<input checked="" type="checkbox"/>
Server-Side Template Injections	
Introduction to Template Engines	<input checked="" type="checkbox"/>
SSTI Identification	<input checked="" type="checkbox"/>
SSTI Exploitation Example 1	<input checked="" type="checkbox"/>
SSTI Exploitation Example 2	<input checked="" type="checkbox"/>
SSTI Exploitation Example 3	<input checked="" type="checkbox"/>
Extensible Stylesheet Language Transformations Server-Side Injections	
Attacking XSLT	<input checked="" type="checkbox"/>
Skills Assessment	
Server-Side Attacks - Skills Assessment	<input checked="" type="checkbox"/>

My Workstation

OFFLINE
Start Instance
00 / 1 spawns left

