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

```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

My Workstation

OFFLINE

Start Instance

∞ / 1 spawns left