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:

Code: ssi

```
<!--#name param1="value1" param2="value" -->
```

For instance, the following are some common SSI directives.

printenv

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

Code: ssi

```
<!--#printenv -->
```

config

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:

Code: ssi

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

echo

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_NAME`: the current file's name
- `DOCUMENT_URI`: the current file's URI
- `LAST_MODIFIED`: timestamp of the last modification of the current file
- `DATE_LOCAL`: local server time

Code: ssi

```
<!--#echo var="DOCUMENT_NAME" var="DATE_LOCAL" -->
```

exec

This directive executes the command given in the `cmd` parameter:

Code: ssi

```
<!--#exec cmd="whoami" -->
```

include

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

Code: ssi

```
<!--#include virtual="index.html" -->
```

SSI Injection

SSI injection occurs when an attacker can inject SSI directives into a file that is subsequently served by the web server, resulting in the 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.

Previous Next

Mark Complete & Next

Cheat Sheet

Table of Contents

Introduction

Introduction to Server-side Attacks

SSRF

Introduction to SSRF

Identifying SSRF

Exploiting SSRF

Blind SSRF

Preventing SSRF

SSTI

Template Engines

Introduction to SSTI

Identifying SSTI

Exploiting SSTI - Jinja2

Exploiting SSTI - Twig

SSTI Tools of the Trade & Preventing SSTI

SSI Injection

Introduction to SSI Injection

Exploiting SSI Injection

Preventing SSI Injection

XSLT Injection

Intro to XSLT Injection

Exploiting XSLT Injection

Preventing XSLT Injection

Skills Assessment

Server-Side Attacks - Skills Assessment

My Workstation

OFFLINE

Start Instance

∞ / 1 spawns left