ATTACK DEFENSE

by PentesterAcademy

Name	Vulnerable Apache III
URL	https://www.attackdefense.com/challengedetails?cid=199
Type	Infrastructure Attacks : Apache

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.

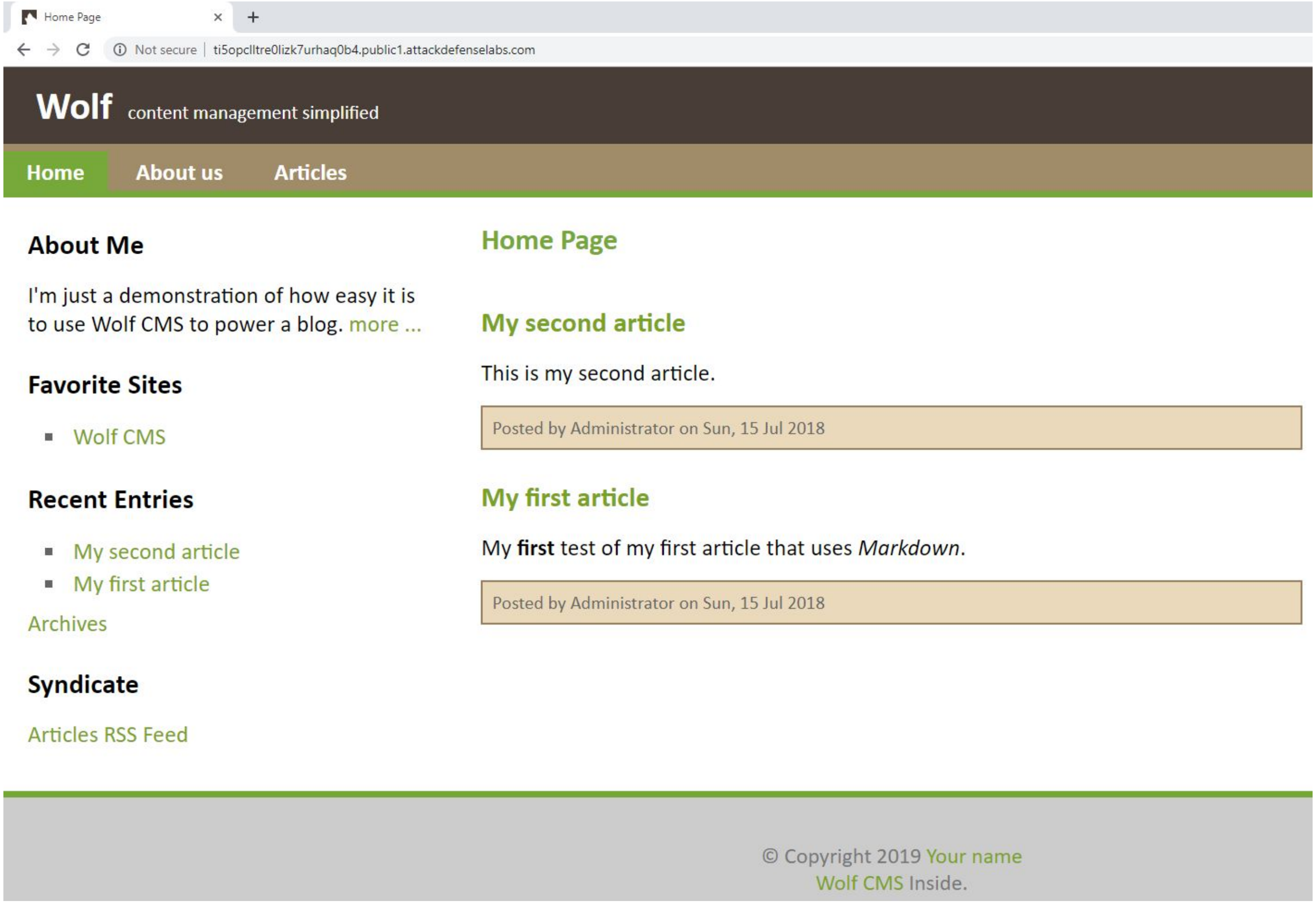
The target server is hosting a web app. The web app is not vulnerable but the directory listing enabled on the server. And, that can lead to sensitive information leakage.

Objective: Your objective is to login into the webapp as 'admin' user and retrieve the flag!

Solution:

Step 1: Inspect the web application.

URL: http://ti5opclltre0lizk7urhaq0b4.public1.attackdefenselabs.com


Home Page
Not secure | ti5opclltre0lizk7urhaq0b4.public1.attackdefenselabs.com

Wolf content management simplified

About Me

I'm just a demonstration of how easy it is to use Wolf CMS to power a blog. more ...

Favorite Sites

- Wolf CMS

Recent Entries

- My second article
- My first article

Archives

Syndicate

Articles RSS Feed

Home Page

My second article

This is my second article.

Posted by Administrator on Sun, 15 Jul 2018

My first article

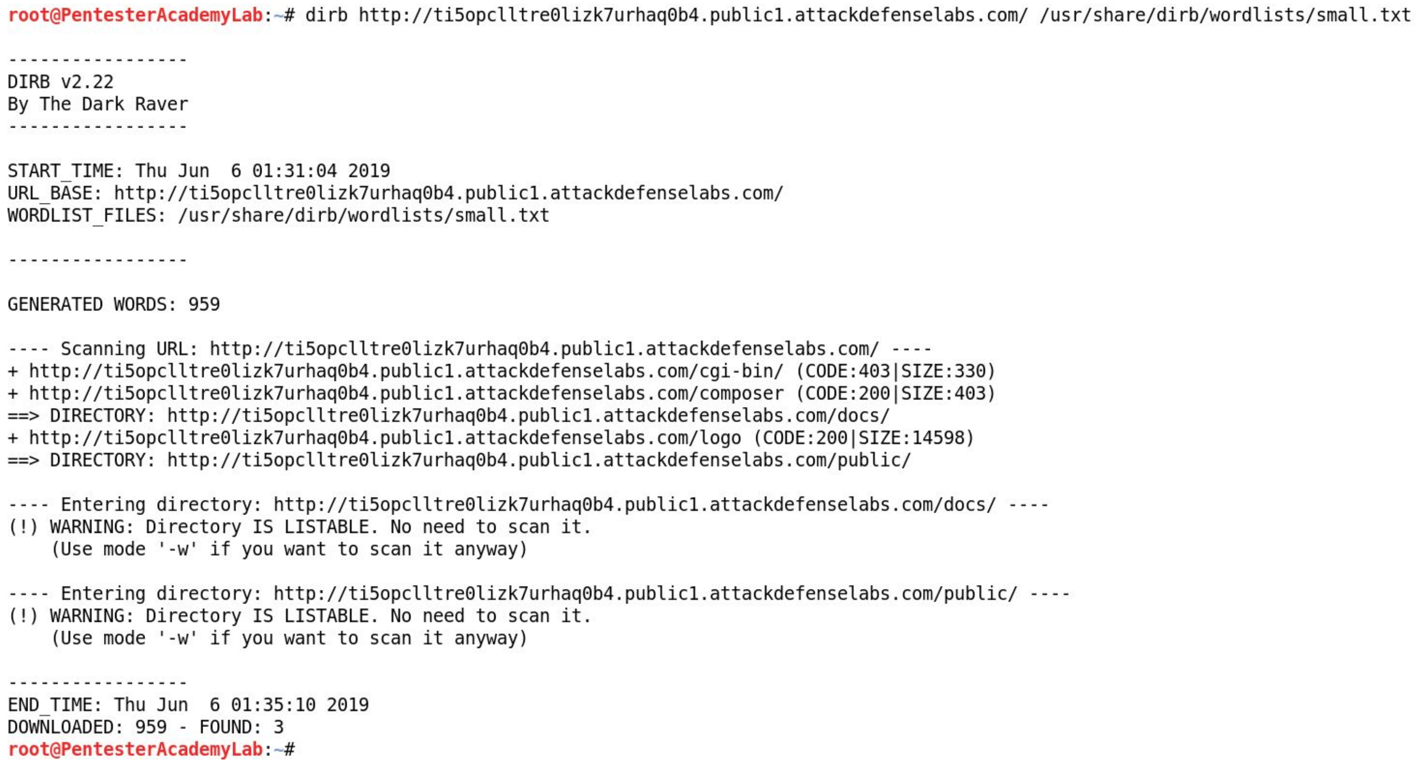
My **first** test of my first article that uses *Markdown*.

Posted by Administrator on Sun, 15 Jul 2018

© Copyright 2019 Your name
Wolf CMS Inside.

Step 2: Enumerate directories present on the target machine using dirb.

Command: dirb http://ti5opclltre0lizk7urhaq0b4.public1.attackdefenselabs.com /usr/share/dirb/wordlists/small.txt

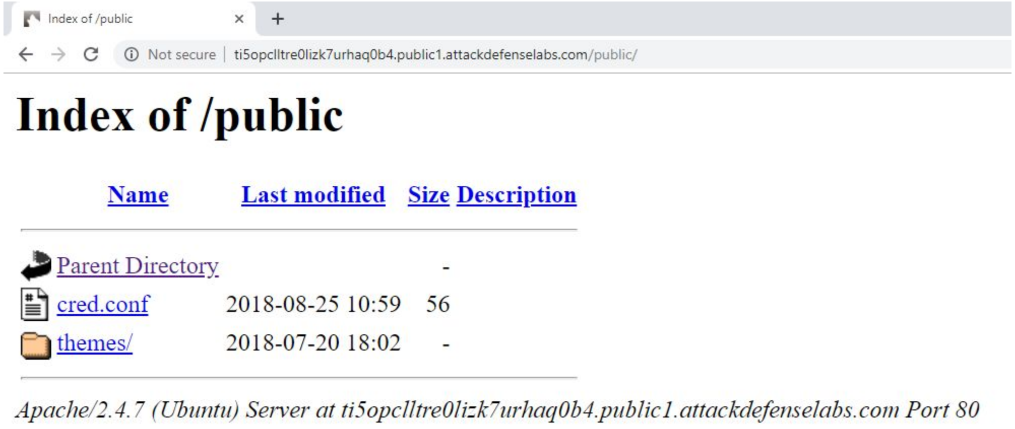


```
root@PentesterAcademyLab:~# dirb http://ti5opclltre0lizk7urhaq0b4.public1.attackdefenselabs.com/ /usr/share/dirb/wordlists/small.txt

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Thu Jun  6 01:31:04 2019
URL_BASE: http://ti5opclltre0lizk7urhaq0b4.public1.attackdefenselabs.com/
WORDLIST_FILES: /usr/share/dirb/wordlists/small.txt

-----------------

GENERATED WORDS: 959

---- Scanning URL: http://ti5opclltre0lizk7urhaq0b4.public1.attackdefenselabs.com/ ----
+ http://ti5opclltre0lizk7urhaq0b4.public1.attackdefenselabs.com/cgi-bin/ (CODE:403|SIZE:330)
+ http://ti5opclltre0lizk7urhaq0b4.public1.attackdefenselabs.com/composer (CODE:200|SIZE:403)
==> DIRECTORY: http://ti5opclltre0lizk7urhaq0b4.public1.attackdefenselabs.com/docs/
+ http://ti5opclltre0lizk7urhaq0b4.public1.attackdefenselabs.com/logo (CODE:200|SIZE:14598)
==> DIRECTORY: http://ti5opclltre0lizk7urhaq0b4.public1.attackdefenselabs.com/public/

---- Entering directory: http://ti5opclltre0lizk7urhaq0b4.public1.attackdefenselabs.com/docs/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://ti5opclltre0lizk7urhaq0b4.public1.attackdefenselabs.com/public/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

-----------------
END_TIME: Thu Jun  6 01:35:10 2019
DOWNLOADED: 959 - FOUND: 3
root@PentesterAcademyLab:~#
```

“public” and “doc” directory are present on the web server.

Step 3: Check the files stored in the “public” directory.

URL: http://ti5opclltre0lizk7urhaq0b4.public1.attackdefenselabs.com/public


Index of /public
Not secure
ti5opclltre0lizk7urhaq0b4.public1.attackdefenselabs.com/public/

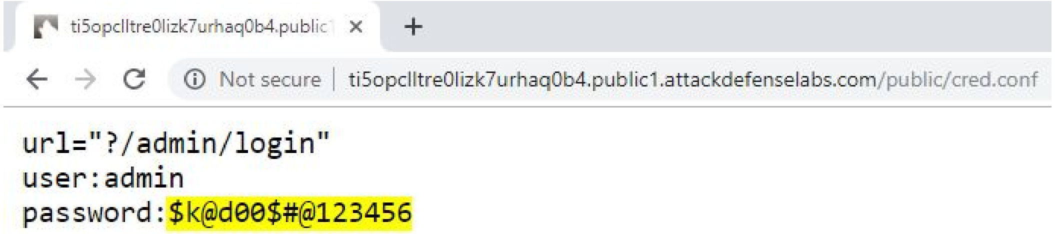
Index of /public

Name	Last modified	Size	Description
Parent Directory		-	
cred.conf	2018-08-25 10:59	56	
themes/	2018-07-20 18:02	-	

Apache/2.4.7 (Ubuntu) Server at ti5opclltre0lizk7urhaq0b4.public1.attackdefenselabs.com Port 80

Step 4: View the contents of file “cred.conf” present in “/public” folder.

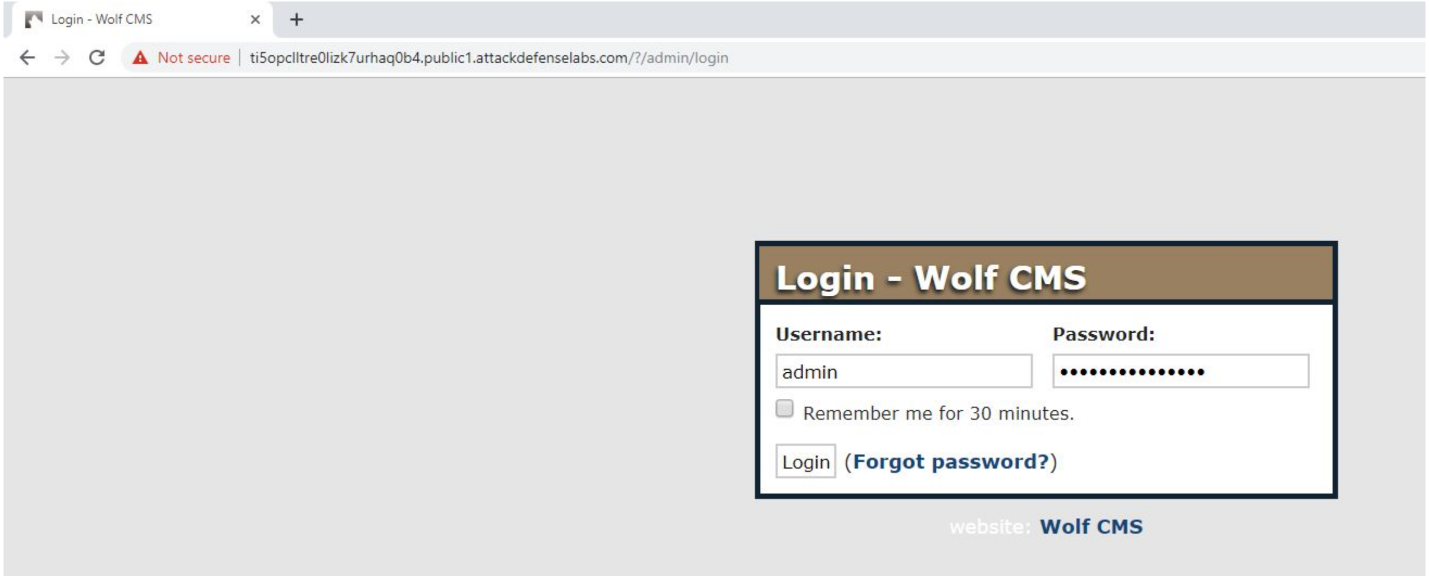
URL: http://ti5opclltre0lizk7urhaq0b4.public1.attackdefenselabs.com/public/cred.conf


ti5opclltre0lizk7urhaq0b4.public1
Not secure
ti5opclltre0lizk7urhaq0b4.public1.attackdefenselabs.com/public/cred.conf

```
url="?/admin/login"
user:admin
password:$k@d00$#@123456
```

Step 5: Login to the web application with the credentials found in previous step.

User: admin
Password: $k@d00$#@123456
URL: http://ti5opclltre0lizk7urhaq0b4.public1.attackdefenselabs.com/?/admin/login



Login - Wolf CMS

Not secure | ti5opclltre0lizk7urhaq0b4.public1.attackdefenselabs.com/?/admin/login

Login - Wolf CMS

Username: admin

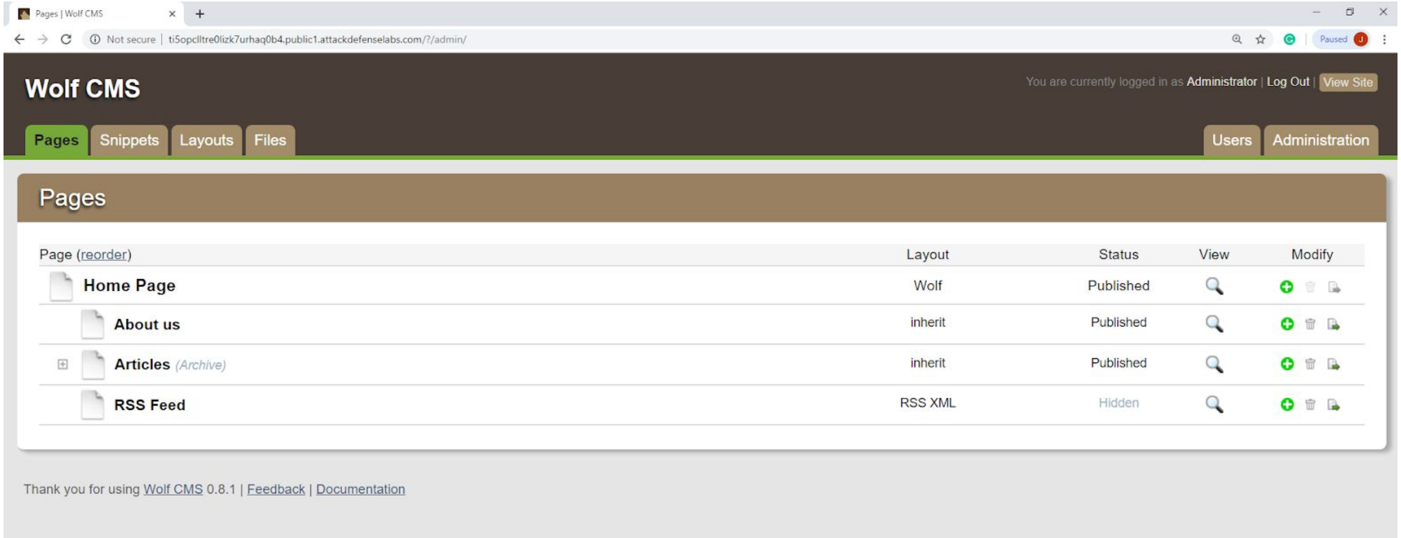
Password: •••••••••••••••

□ Remember me for 30 minutes.

Login (Forgot password?)

website: Wolf CMS

Dashboard:



Pages | Wolf CMS

Not secure | ti5opclltre0lizk7urhaq0b4.public1.attackdefenselabs.com/?/admin/

Wolf CMS

You are currently logged in as Administrator | Log Out | View Site

Pages

Page (reorder)	Layout	Status	View	Modify
Home Page	Wolf	Published		
About us	inherit	Published		
⊞ Articles *(Archive)*	inherit	Published		
RSS Feed	RSS XML	Hidden		

Thank you for using Wolf CMS 0.8.1 | Feedback | Documentation

Admin Password: $k@d00$#@123456

References:

1. Apache httpd (https://httpd.apache.org/)
2. Wolf CMS (https://github.com/wolfcms/wolfcms)
3. dirb (https://tools.kali.org/web-applications/dirb)