RingZer0 Team Online CTF
(ringzer0ctf.com)

Web

Looking for password file

Detailed Write-up

By

The_Green_Hat_9833

ACoDevTech team leader

Committed

Montreal, July 24th 2019

CONTENTS

CHALLENGE

The challenge is simply like Figure 1 and Figure 2:

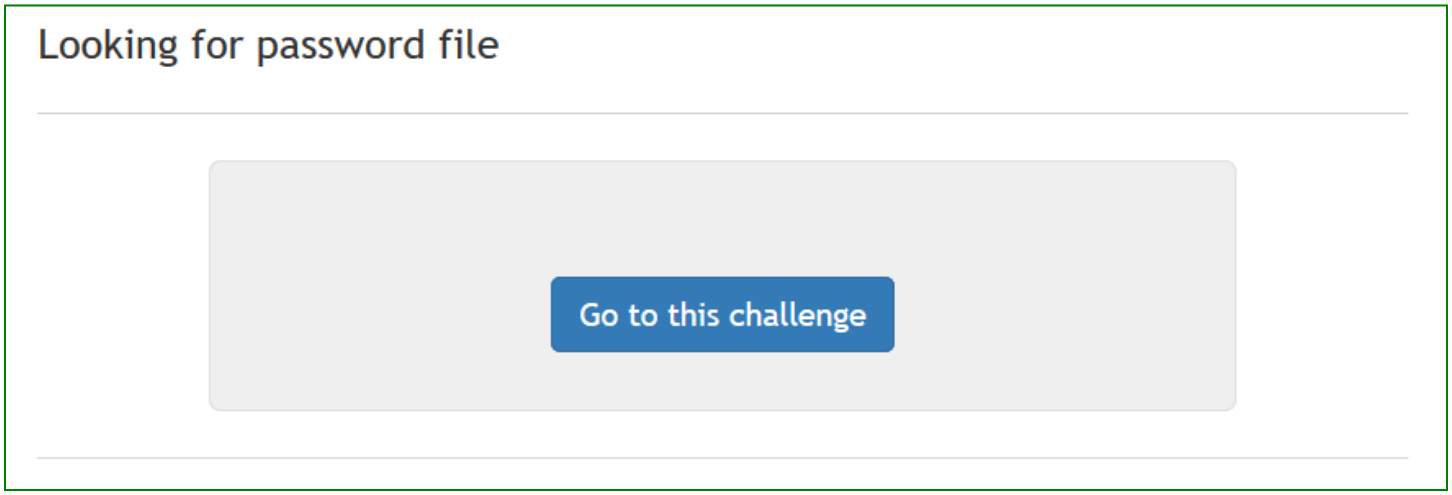

Figure 1 - Challenge first page

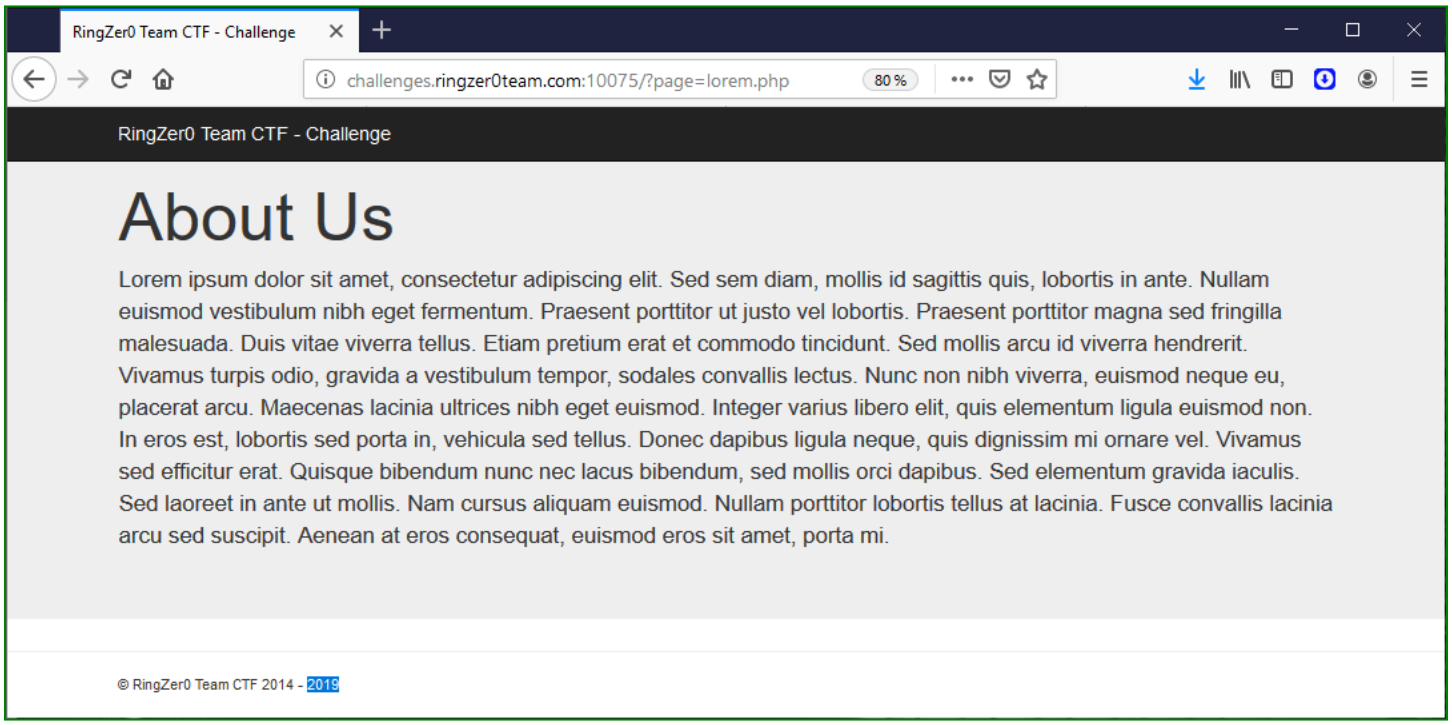

Figure 2 - Challenge second page

TOOLS

Softwares

Firefox 68.0.1 (64 bits)

ANALYZE, EXPLORATION AND RESEARCH

Text show in the page

Step

There is text written in a language resembling Latin. Searching for "Lorem ipsum dolor sit amet, consectetur adipiscing elit" in the Google search engine, we find that it could be random text used to prepare / present layouts. It would therefore contain nothing intelligible. However, someone might have been able to hide a message in it.

Intermediate conclusion / hypothesis

Being in the web and not cryptography or steganography challenges, I did not push further my analysis of the text.

Code HTML of the page

Step

With the Inspect Element feature of Firefox, I looked at the HTML code of the page in the Inspector tab. I did not find anything interesting at first sight.

Intermediate conclusion / hypothesis

There is nothing interesting in the HTML code of the page at this moment.

URL of the page

Step

The URL of the page is :

http://challenges.ringzer0team.com:10075/?page=lorem.php

This URL seems to indicate that we are currently viewing the lorem.php page. I tried to join other pages by manually changing the URL as presented into Table 1.

Table 1 - URL essayés

URL
http://challenges.ringzer0team.com:10075/?page=password.php
http://challenges.ringzer0team.com:10075/?page=robots.php
http://challenges.ringzer0team.com:10075/?page=help.php
http://challenges.ringzer0team.com:10075/?page=*

For each URL entered manually, I received an error message (see Figure 3) from the server informing me that it could not find the file (password.php, robots.php, help.php and *). In addition, this same message tells me that it may be possible to include the path where the file I want to display.

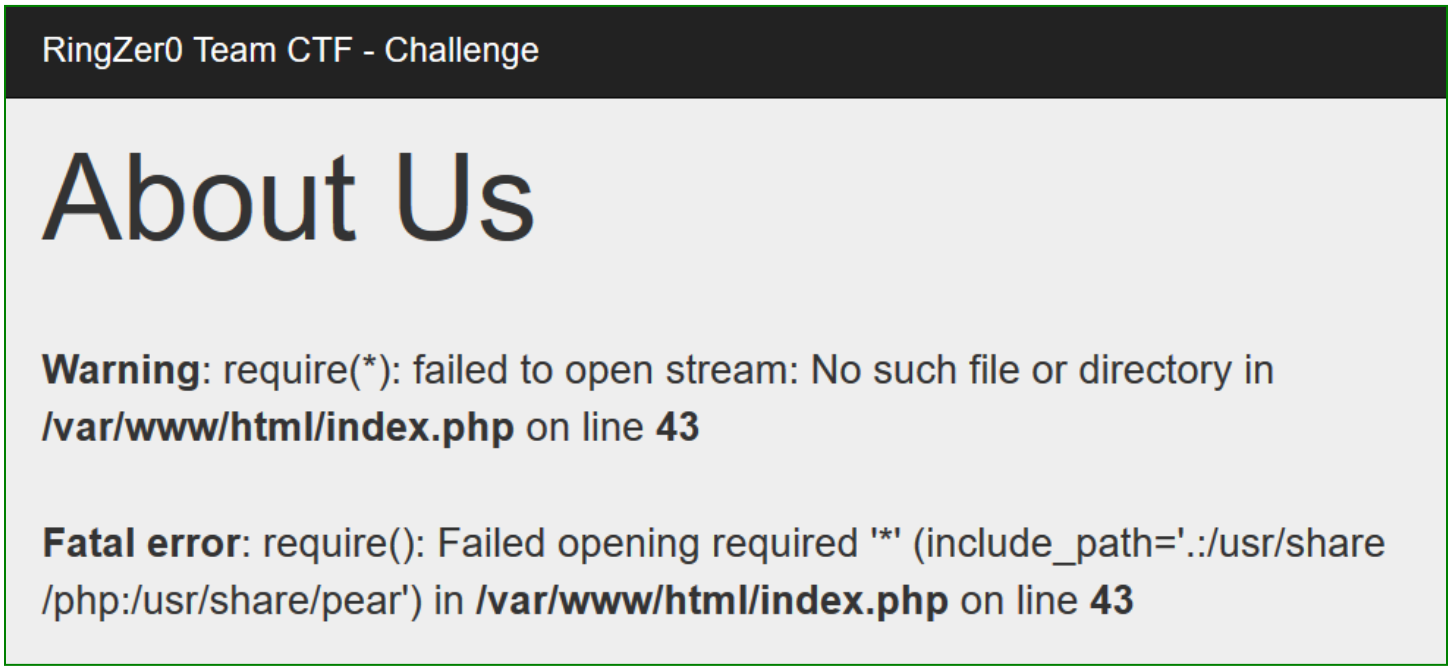

Figure 3 - Message after entering wrong URL

Intermediate conclusion / hypothesis

It is probably possible to display a file or a web page by modifying the URL. However, at this stage, I do not know what to look for as file name nor in what path it could be. Depending on the message, we would be in the directory /var/www/html/.

Informations on server

Step

With the Inspect Element feature of Firefox, I looked to find information about the server used. In the Network tab, I found in the Headers that it would be a Apache/2.4.7 (Ubuntu) server (see Figure 4).

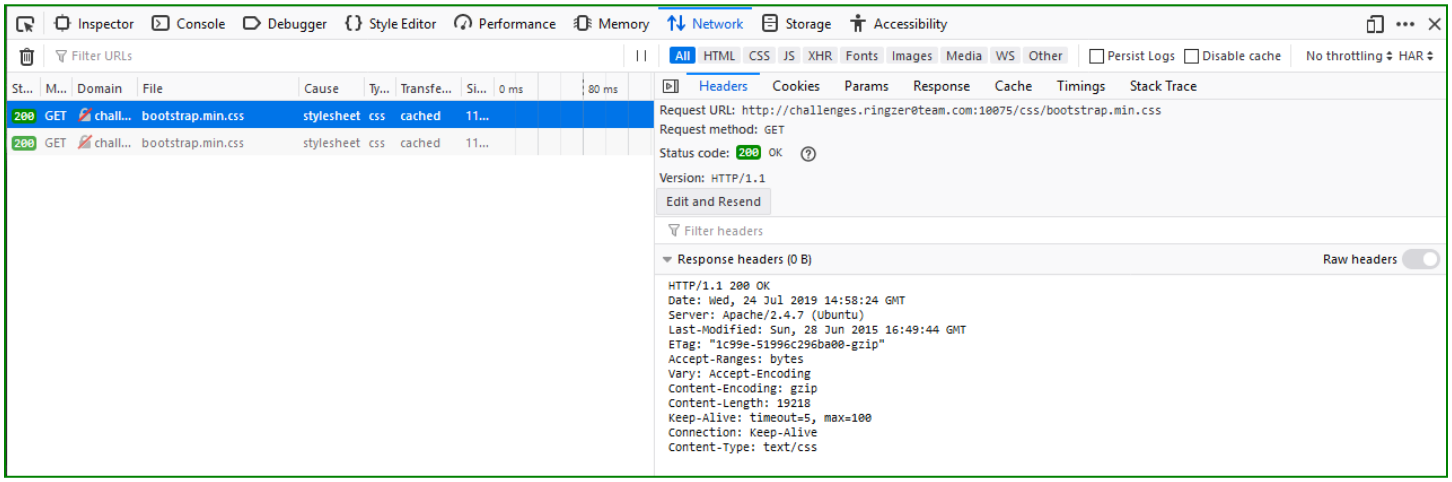

Figure 4 – Firefox – Inspect Element – Network - Headers

Intermediate conclusion / hypothesis

It looks like it's a Apache/2.4.7 (Ubuntu) server.

Find the password file

Step

In the Google search engine, I searched for "Ubunto /var/ password file". I got, that the password file would be passwd and was in /etc. I manually entered the following URL:

http://challenges.ringzer0team.com:10075/?page=/etc/passwd

The server responded by sending the contents of the passwd file as shown in Figure 5.

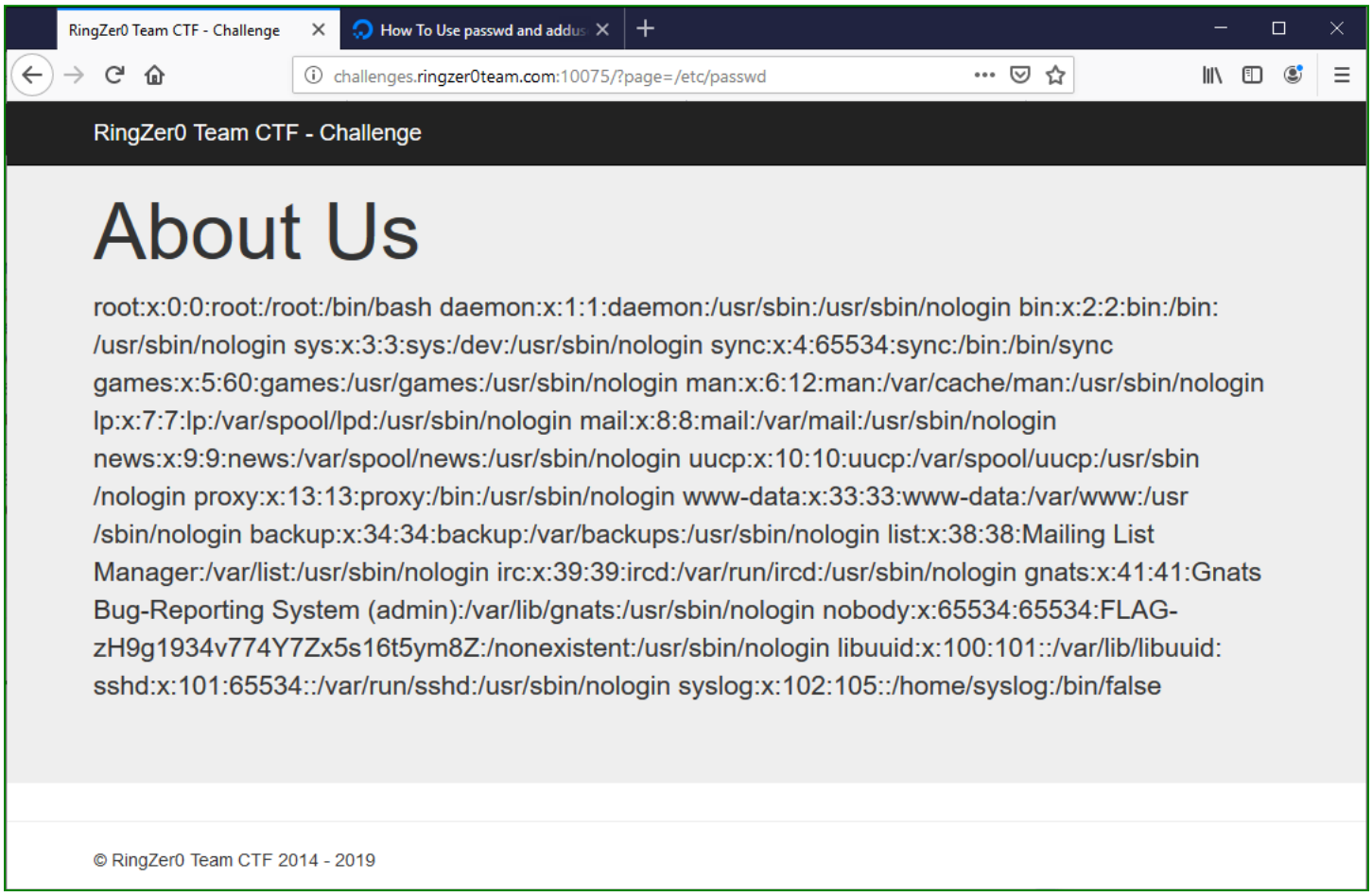

Figure 5 - http://challenges.ringzer0team.com:10075/?page=/etc/passwd

Intermediate conclusion / hypothesis

If we look at the content, we find the Flag!

CONCLUSION AND FLAG

In the end, it is simply a Directory traversal attack.

FLAG-zH9g1934v774Y7Zx5s16t5ym8Z

REFERENCES

Websites

https://en.wikipedia.org/wiki/Lorem_ipsum, July 2019

https://www.digitalocean.com/community/tutorials/how-to-set-up-password-authentication-with-apache-on-ubuntu-16-04, July 2019

https://www.digitalocean.com/community/tutorials/how-to-use-passwd-and-adduser-to-manage-passwords-on-a-linux-vps, July 2019