Introduction

1 Overview

The report documents the findings of penetration testing of Inclusion box that was performed on the Tryhackme platform.

The objective was to find the flag and a report that documents the main findings, the vulnerabilities that were found, and the methods that were used. The report will also include screenshots that document processes, a conclusion, and suggested fixes that the client must perform to secure the web application.

2 Scope

The “Inclusion box” specified that the testing will occur only on the given box, located in room “Inclusion”.

Social Engineering is not included within the scope.

3 Out of Scope

The client specified that no external resource testing will be permitted, including JS codes that hold certain URLs that are not part of the domain.

4 Summary

At first, the website had to be investigated to collect all the flags. Once the first vulnerability on the website was found, more information about the perspective of the website programmer was obtained, which yielded additional findings.

Detailed Findings

Local File Inclusion (LFI) – User and Root Flag

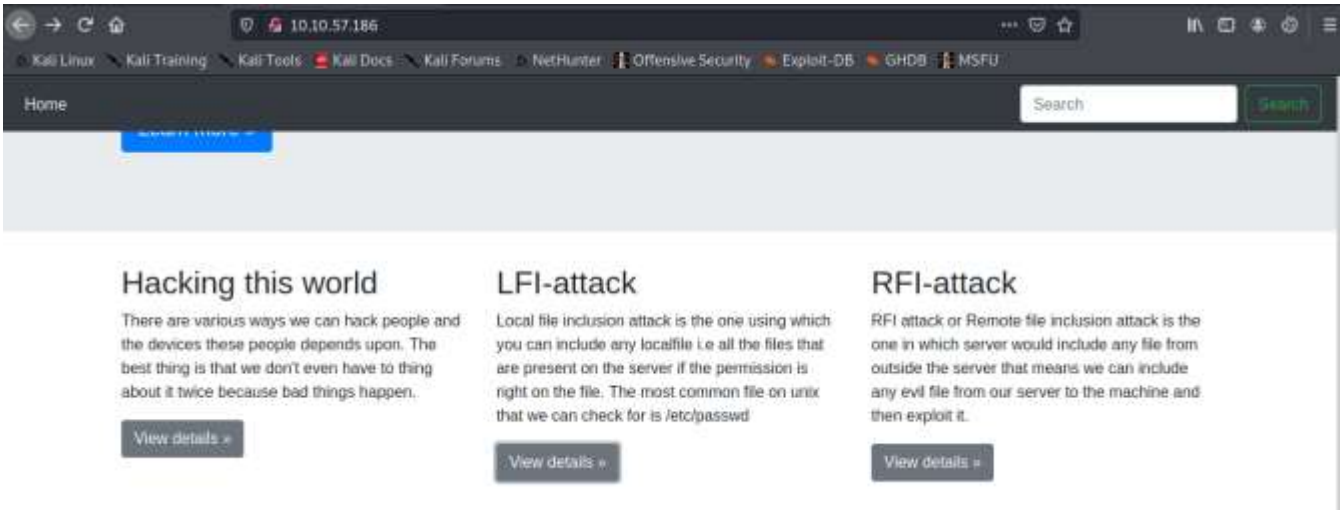
User Flag - 60989655118397345799

Root Flag - 42964104845495153909

Proof of concept (with HD screenshots) –

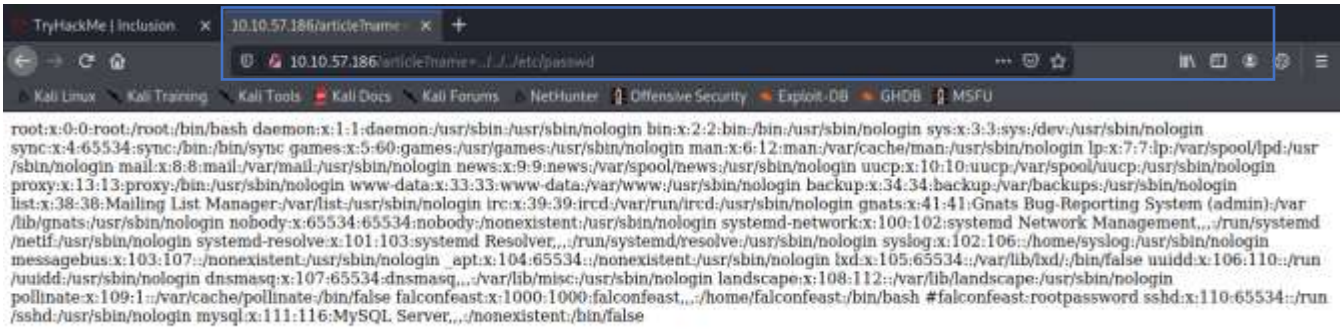
Reconnaissance:

Looking at the website index page a find out a directory “/article” which takes a parameter “name” so, let’s try on that parameter if we can have LFI or RFI.



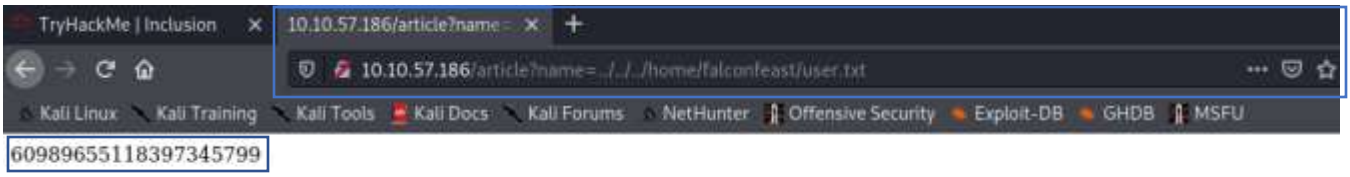
Exploits:

Command: name=../../../etc/password



Trying LFI on the “name” parameter and we get successful. As we tried to get passwd file we got a user “falconfeast” and also, it’s password as “rootpassword”. Let’s try if we can get user flag from this.

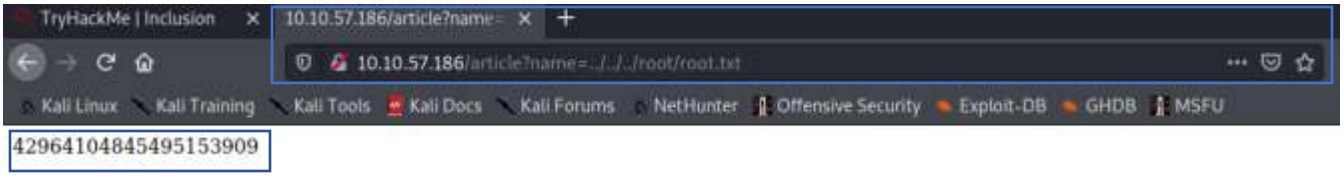
Command: ../../../home/falconfeast/user.txt



User Flag: **60989655118397345799**

We successfully got the User flag and now let’s go for the root flag as well.

Command: ../../../root/root.txt



Root Flag: **42964104845495153909**