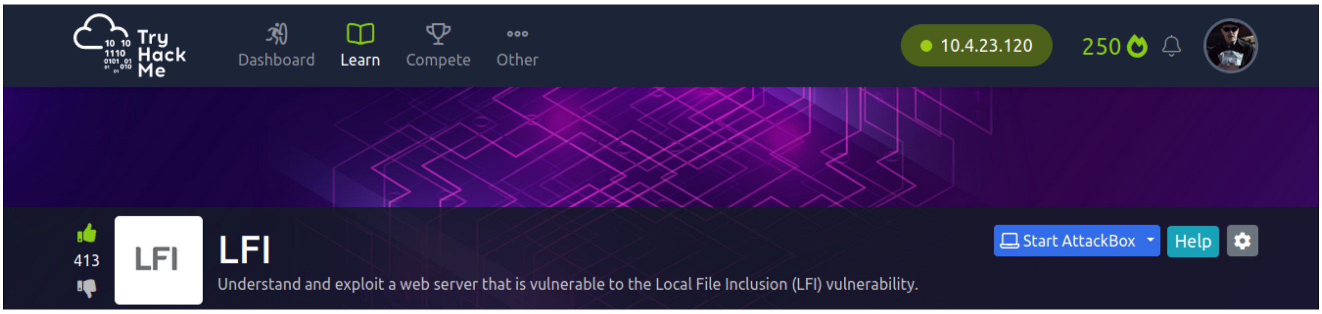
Try Hack Me
Dashboard
Learn
Compete
Other
10.4.23.120
250
413
LFI
LFI
Understand and exploit a web server that is vulnerable to the Local File Inclusion (LFI) vulnerability.
Start AttackBox
Help

TryHackMe LFI

Saikat Karmakar | Jul 25 : 2021

LFI

Local File Inclusion (LFI) is the vulnerability that is mostly found in web servers. This vulnerability is exploited when a user input contains a certain path to the file which might be present on the server and will be included in the output. This kind of vulnerability can be used to read files containing sensitive and confidential data from the vulnerable system.

The main cause of this type of Vulnerability is improper sanitization of the user's input. Sanitization here means that whatever user input should be checked and it should be made sure that only the expected values are passed and nothing suspicious is given in input. It is a type of Vulnerability commonly found in PHP based websites but isn't restricted to them.

To test for LFI what we need is a parameter on any URL or any other input fields like request body etc. For example, if the website is tryhackme.com then a parameter in the URL can look like `https://tryhackme.com/?file=robots.txt`. Here `file` is the name of the parameter and `robots.txt` is the value that we are passing (*include the file robots.txt)*.

Importance of Arbitrary file reading

A lot of the time LFI can lead to accessing (without the proper permissions) important and classified data. An attacker can use LFI to read files from your system which can give away sensitive information such as passwords/SSH keys; enumerated data can be further used to compromise the system.

https://www.cyberciti.biz/faq/understanding-etcpasswd-file-format/