Local File Intrusion has other names like
Path traversal, Directory Traversam, Dot-Dot-Slasm, Directory Climbing, Back Tracking
There are two directories like root directory and web document root directory.
Root directory is the first one in file systems "/" and other is web documentary, like when ever we started a webserver there'll be a default directory for linux we have var/www/html(explain this terms interms of working)
Consider we have a link while accessing it first it reaches /var/www/html and then the actual path in the url like in url, we have domain,path,variable…
example: www.example.com/index.php?file=green
As we are talking about web document directory it goes to /var/www/html and there'll be an page available named as index.php.
Lets understand another example <img src="/images"?filename=2/png> its an image tag
in the src its saying that there'll be an images directory in web documentory root go access them
->127.0.0.1/dvwa/vulnerabilities/file?page=file.php(in variable place malicious activity can happen)
Vulnerable Code:

```
<?php
   $file = $GET['Page']
//in above line we are not checking anything like blindly trusting that it'll be secure here's the problem…
    ………………….
```

How can we test that vulnerability exists

Backtracking
Climbing
Traverse

BruteForce
Files in CWD

Go Forward Explore

Most important one is Backtracking/Climbing/Traverse by this at the we must reach a file directly from OS. If we found permissions like reading then we can explore.

Lets understand the file structure

/

```
var                              etc                              bin
www          -          passwd          shadow          -
html         -
```

DVWA(In this folder it may have multiple files/folders we can brute force)

I have a doubt like where we should type like unless you are in that system you cant type commands what if we are not in the system like we have to type in url as webserver is running??? Like go back to / from /var/ww/ html/dvwa and then go to /etc/passwd like how we can do if we ddont have command line access but we know that webserver is running on directly web?
The answer is as we are intercepting using burpsuite we can send it to repeater and we can see the request and response right
in the request we can change it as
→GET /dvwa/vulnerabilities/fi/?page=../../../../../../etc/passwd HTTP/1.1

Okay lets find where to look for
cat folder content dir include document action page mod deatil filename conf file show download doc path view.

Lets understand how to perform LFI in post method

We have to take a look on request header and in body the name of the file like name , id like find out the extensions.

Lets understand how we can find in cookies
consider a web code like below

```
Get /vuln.php HTTP/1.0
Host:______________
Cookie:Design=new.php
```

```
<?php
 $file = old.php
   if(is_set($_cookie['DECISION']]
       $file = $_cookie['DECISION']]
    include($file)
?>
```

If we open above website we can see through get request and then a cookie is assigned 'new.php'   and in code we can see that there's a file named old.php like we are checking is_set cookie is set/assigned or not if yes then store it in afile. As here we are not checking the cookie vakid or not blindly trusting and storing what if malicious.

Bypass Mechanisms
Whenever we are requesting a file from the server to read then it'll perform checks for permission or not we can by pass them by
null character, dot truncation, encoding

Null Character:
For example high level languages like pyhton,php cant talk directly with hardware to identify where the username has ended so it passess to OS to hardware so here in OS it uses some API's OS_APZ like translates it to hardware languages and they uses languages like c as it is a procedural language.
consider an example www.example.com/pages?page=1
(we'll add like)
www.example.com/pages?page=/etc/passwd %00
when it reaches c language it looks for null character like ->%00 and it stops and executes command /etc/passwd

Dot Truncation
In php files when the size limit exceeds 4096 bytes the all the data after it will be trucated

Encoding
As we perform using … and /// it'll get identified and gets removed as if we encode them as for example . as %2e and / as %2f and \ as %2c and we can double encode it and also we can encode it as 16 bit Unicode soo all this will help in bypassing.
 can u please explain how these types and other types of this will help in byass ..//..// and …../…../ and ..,/..,/..,/ like this combinations