

## Forum:[Hack Forums](#)

Thread: [Local File Inclusion \( Sensitive File Disclosures \)](#)

**Money-** - June 9, 2019, 8:31 am

What kind of common files I can read on a website that is hosted on a windows server? Lets say XAMPP ? Instead of Linux.

I want to know the common sensitive files which can be read by LFI vulnerability.  
I know I can do a reverse shell connection and gain full access etc and so on.

This is just an assignment which I will demo and present using windows server instead of a linux.  
So I just want to know what are the possible post-exploitations for LFI on a windows server instead of using shells and other tools etc.. looking more of a manual way.

**f1re\_w1re** - June 9, 2019, 6:10 pm

(Jun 9, 2019 08:31 AM)Money- Wrote: [\[CITE\]](#) What kind of common files I can read on a website that is hosted on a windows server? Lets say XAMPP ? Instead of Linux.

I want to know the common sensitive files which can be read by LFI vulnerability.  
I know I can do a reverse shell connection and gain full access etc and so on.

This is just an assignment which I will demo and present using windows server instead of a linux.  
So I just want to know what are the possible post-exploitations for LFI on a windows server instead of using shells and other tools etc.. looking more of a manual way.

You can try the inclusion of the following files for Windows servers:

c:\windows\system32/drivers/etc/hosts  
c:\WINDOWS\system32\eula.txt  
c:\boot.ini  
c:\WINDOWS\win.ini  
c:\WINNT\win.ini  
c:\WINDOWS\Repair\SAM  
c:\WINDOWS\php.ini  
c:\WINNT\php.ini  
c:\Program Files\Apache Group\Apache\conf\httpd.conf  
c:\Program Files\Apache Group\Apache2\conf\httpd.conf  
c:\Program Files\xampp\apache\conf\httpd.conf  
c:\php\php.ini  
c:\php5\php.ini  
c:\php4\php.ini  
c:\apache\php\php.ini  
c:\xampp\apache\bin\php.ini  
c:\home2\bin\stable\apache\php.ini  
c:\home\bin\stable\apache\php.ini

You can find more common paths if you check online. I am not sure what you mean by "post-exploitation for LFI" when post-exploitation implies that you already have access to the server through some vulnerability.

Hope the above paths help.

