Feifeicms V4.0.181010  Background Read/delete arbitrary files (in windows)

After login Background

Find in database backup

We can download and delete the backup files.



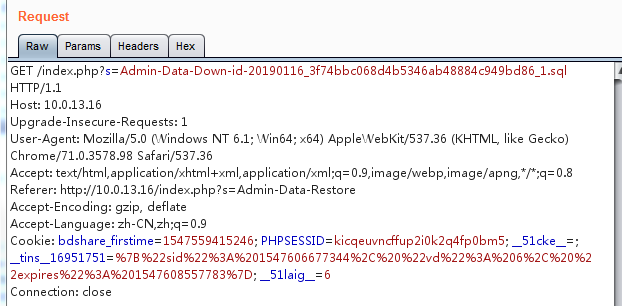
So read the source ,find /Lib/Lib/Action/Admin/DataAction.class.php

We can see “readfile($filepath);”、”unlink:”

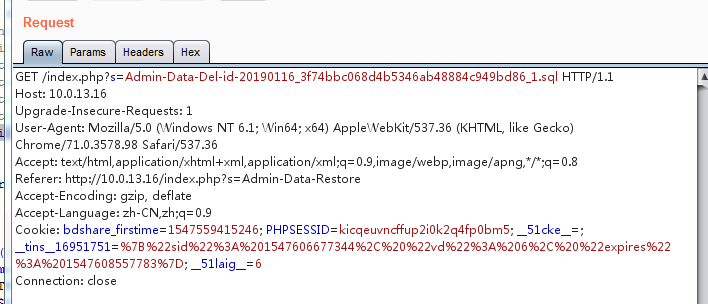


So test it:

Download file:



Delete file:

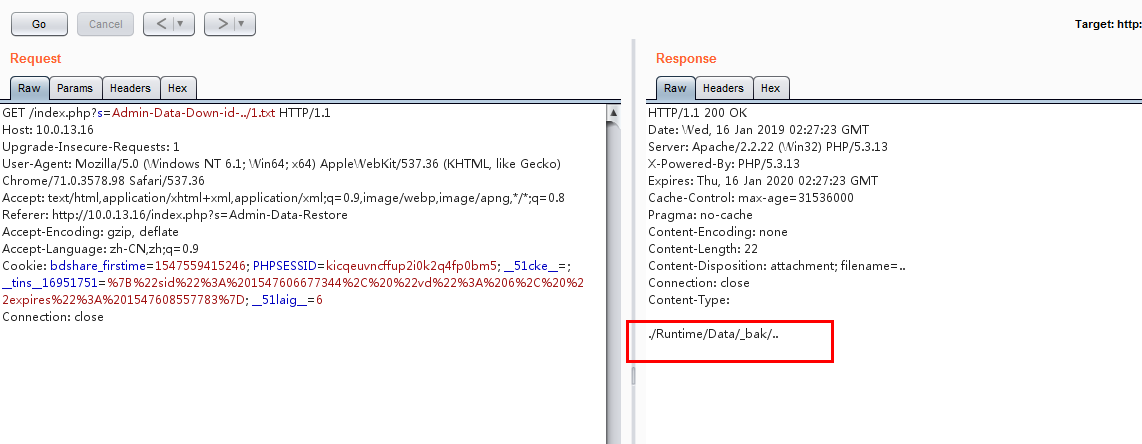


The url it’s mean

admin ——》 Data——》Down/Del——》id。

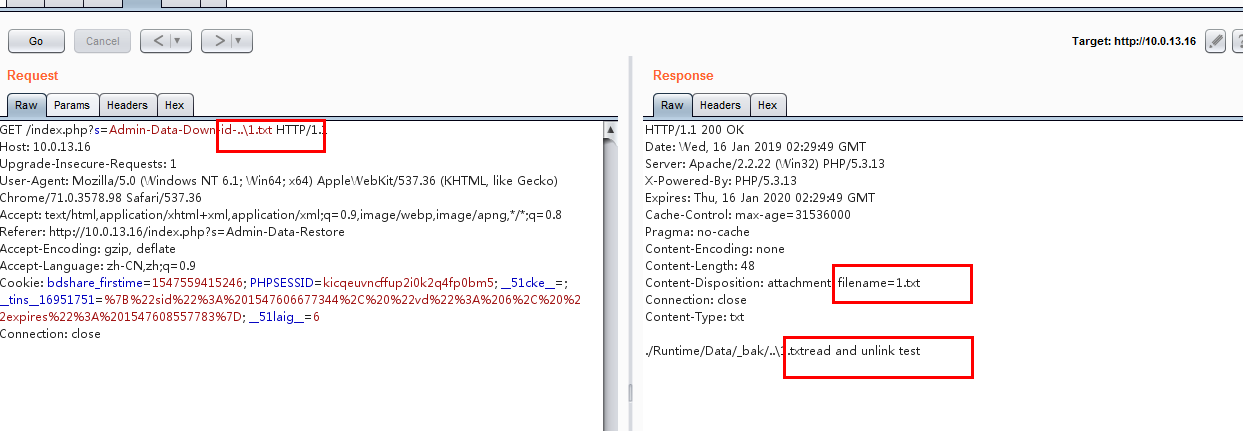
The id parameter will be received

However, it is filtered “/” ,so “../” fail

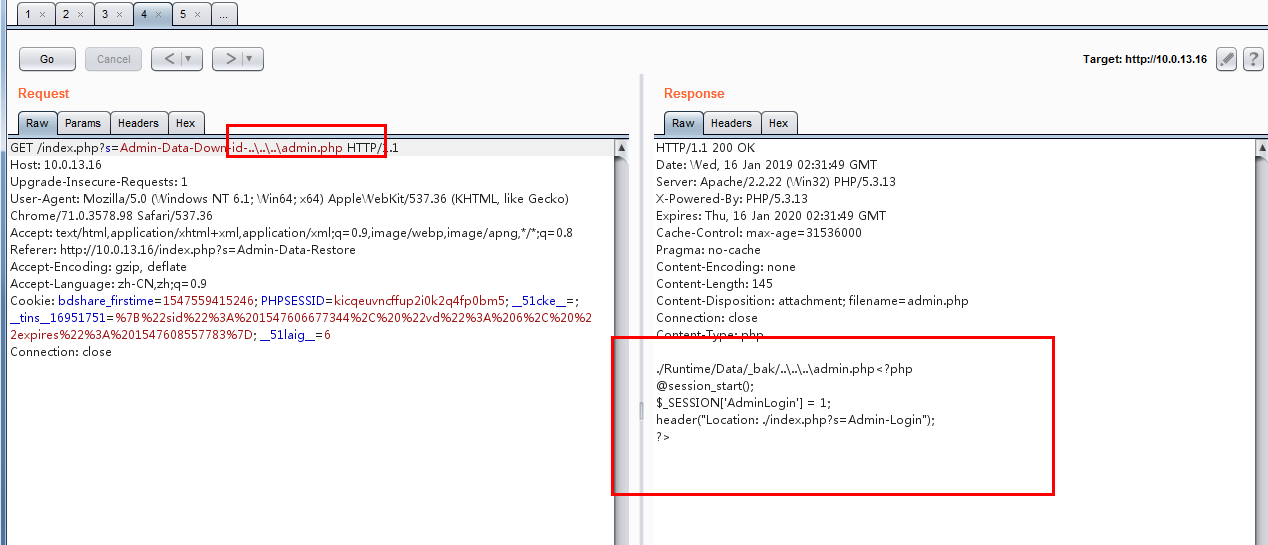


But In a windows environment “..\” Can also read files through the directory.

So it’s success：



Read admin.php:



Delete “1.txt”:

