安全-Pass02之白名单MIME绕过（upload-labs）

原创

小狐狸FM 于 2021-07-20 17:21:45 发布 512 收藏 1

分类专栏： 安全 # 靶场学习 文章标签： php shell ctf 文件上传漏洞

本文链接：https://blog.csdn.net/smallfox233/article/details/118937945

安全 同时被 2 个专栏收录

91 篇文章 9 订阅

订阅专栏

靶场学习

24 篇文章 1 订阅

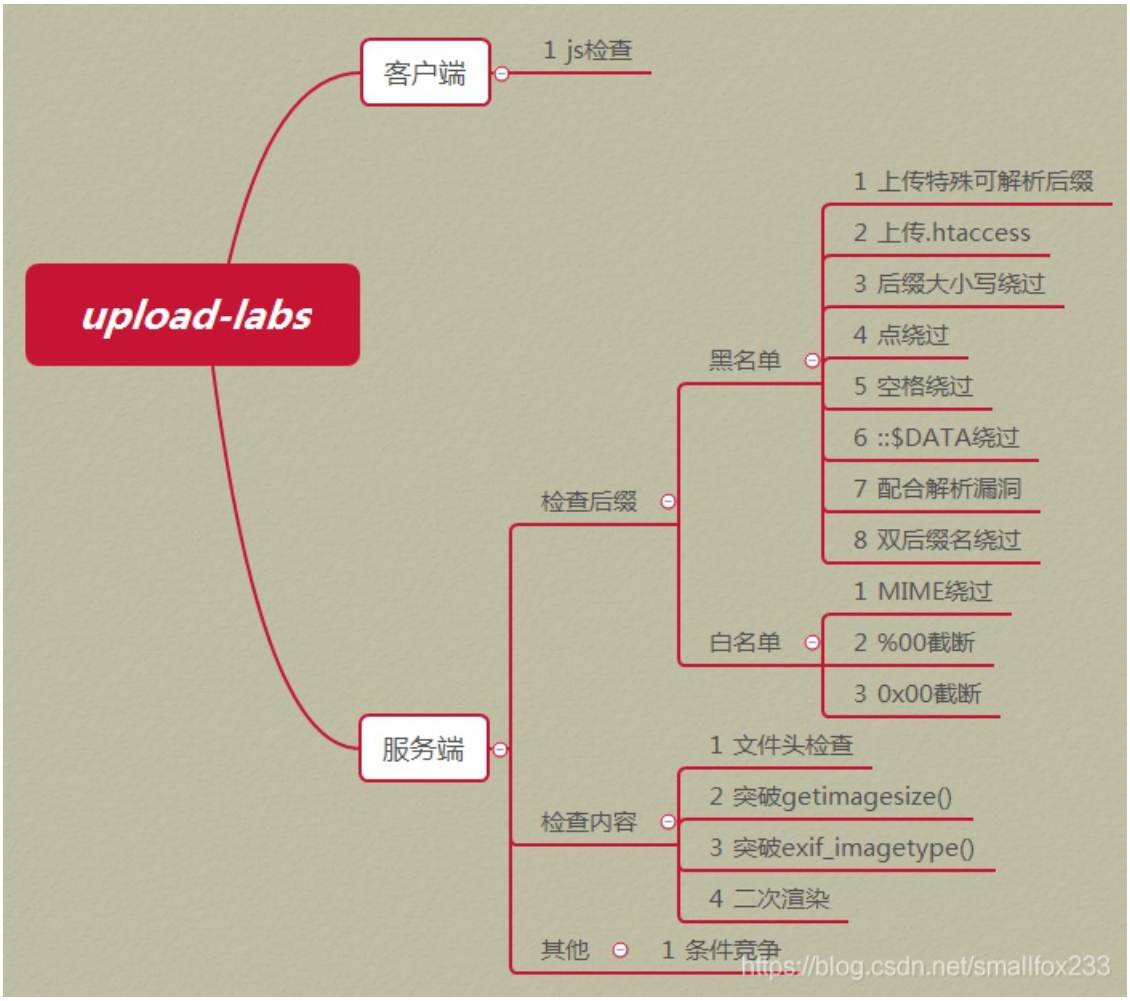
订阅专栏

文章目录

- 前言
  - 相关介绍
  - 其他介绍
- 一、题目
- 二、WriteUp
  - [1]. 函数介绍
  - [2]. 源码审计
    - (1). 变量判断
    - (2). 路径判断
    - (3). MIME类型判断
    - (4). 文件存储路径设置
    - (5). 移动临时文件
  - [3]. MIME绕过

前言

- `php` 即 `Hypertext Preprocessor` 超文本预处理器，多用于 `web` 后端
- 在进行代码审计的时候可以使用 `Seay` 进行全局搜索
  目前正在学习代码审计的内容，所以会介绍得更细一些，以便学习了解。
- `MIME` 全称为 `Multipurpose Internet Mail Extensions` 是一种标准，用来表示文档、文件或字节流的性质或格式。
  浏览器通常使用MIME类型来确定如何处理URL，MIME的组成结构为 `类型/子类型`
- 文章是基于自己见解写的，不能保证完全正确，有错误可以在评论指出
  BUUCTF的upload-labs在线靶场和本地的靶场有点差别，如果用文章的方法没法绕过时，注意看一下源码是否一致



相关介绍

PHP 百度百科

PHP: PHP 手册 - Manual

MIME类型 - HTTP | MDN

其他介绍

文件上传绕过思路集合

upload-labs靶场下载

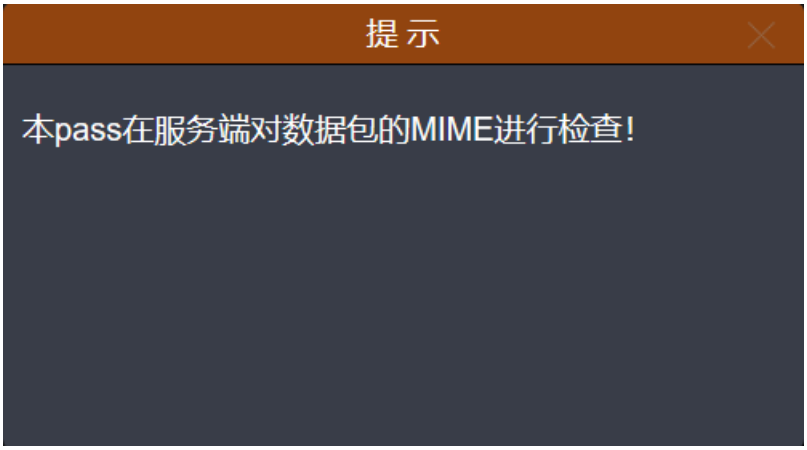
upload-labs在线靶场-BUUCTF

蚁剑AntSword

菜刀Cknife

Seay

一、题目

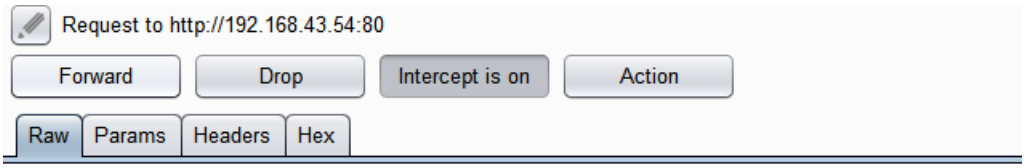


> php 后端代码

```php
$is_upload = false;
$msg = null;
if (isset($_POST['submit'])) {
    if (file_exists(UPLOAD_PATH)) {
        if (($_FILES['upload_file']['type'] == 'image/jpeg') || ($_FILES['upload_file']['type'] == 'image/png')
|| ($_FILES['upload_file']['type'] == 'image/gif')) {
            $temp_file = $_FILES['upload_file']['tmp_name'];
            $img_path = UPLOAD_PATH . '/' . $_FILES['upload_file']['name'];
            if (move_uploaded_file($temp_file, $img_path)) {
                $is_upload = true;
            } else {
                $msg = '上传出错！';
            }
        } else {
            $msg = '文件类型不正确，请重新上传！';
        }
    } else {
        $msg = UPLOAD_PATH.'文件夹不存在,请手工创建！';
    }
}
```

二、WriteUp

> 随便上传一个文件，并抓包了解一下其中都含有那些上传的变量参数




```
POST /upload-labs-master/Pass-02/index.php HTTP/1.1
Host: 192.168.43.54
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://192.168.43.54/upload-labs-master/Pass-02/index.php
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: multipart/form-data; boundary=---------------------------179332396611738
Content-Length: 301

-----------------------------179332396611738
Content-Disposition: form-data; name="upload_file"; filename="test2.txt"
Content-Type: text/plain


-----------------------------179332396611738
Content-Disposition: form-data; name="submit"

涓婁紶
-----------------------------179332396611738--
```

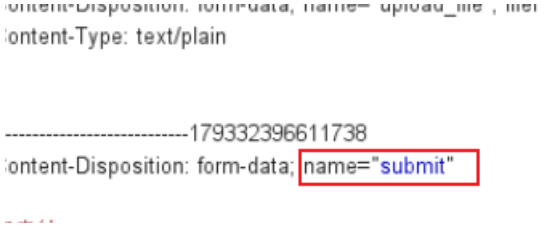
[1]. 函数介绍

PHP函数	介绍
file_exists(路径)	判断指定的文件或目录是否存在，不存在返回true，否则返回false
isset(变量)	如果变量存在且值不为null返回true，否则返回false
move_uploaded_file(文件路径，文件夹路径)	将文件移动到指定文件夹下

[2]. 源码审计

(1). 变量判断

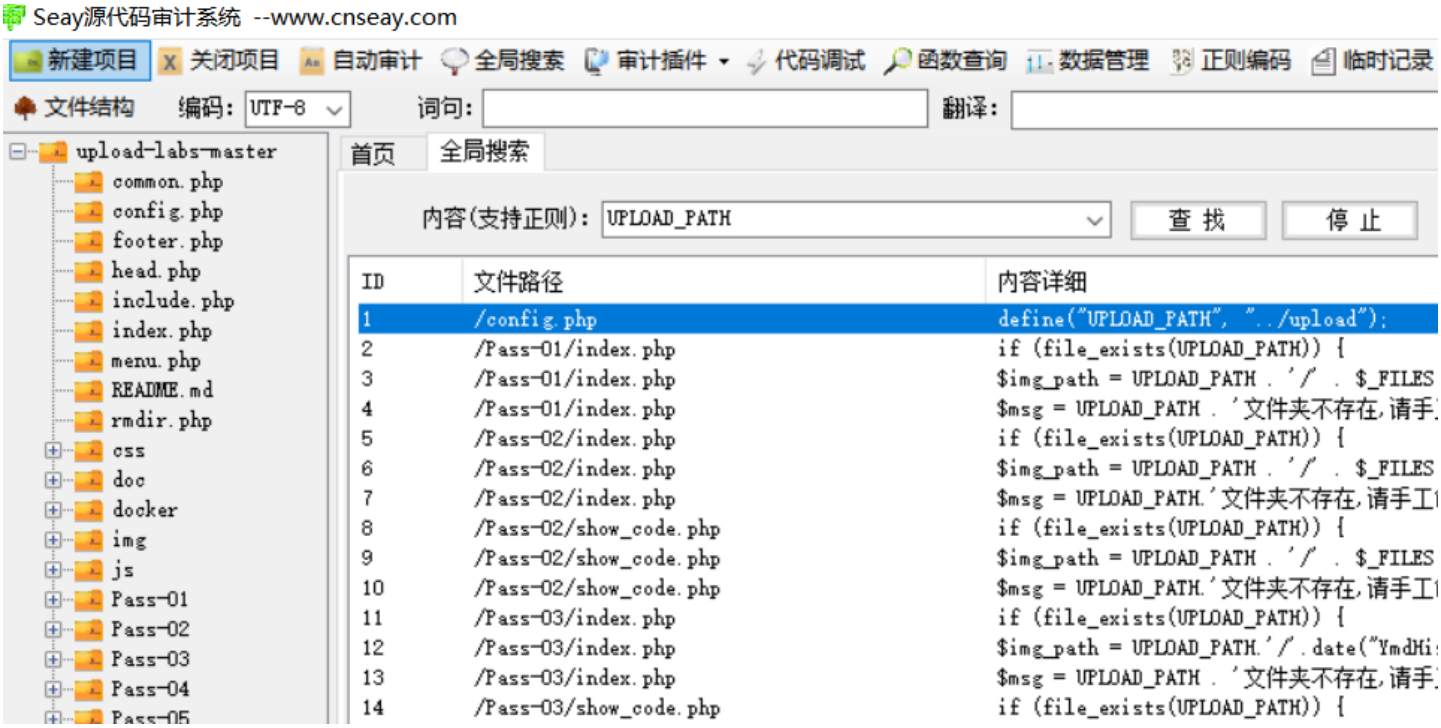
> - 对 `php` 代码进行审计，if语句比较多最好从外往内分析
> - 第一条 `if` 语句只是判断了一下提交的 `post` 请求中 `submit` 参数是否被设置且非空
>   PHP:isset - Manual

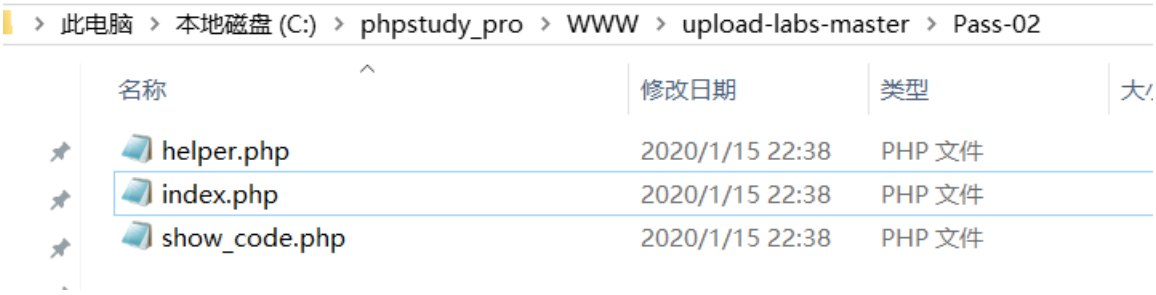



```php
$is_upload = false;
$msg = null;
if (isset($_POST['submit'])) {//第一条if
 //代码
}
```

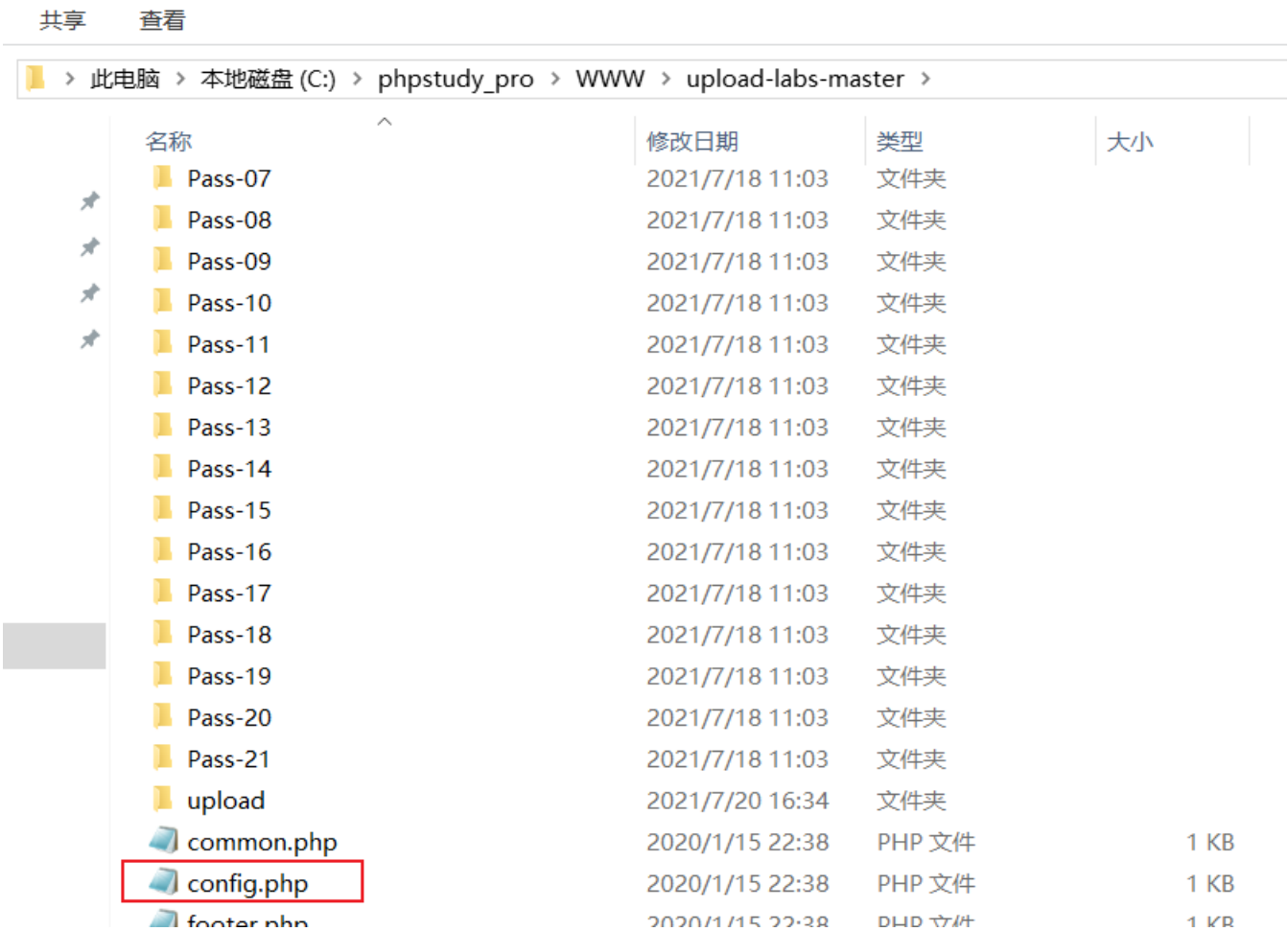
(2). 路径判断

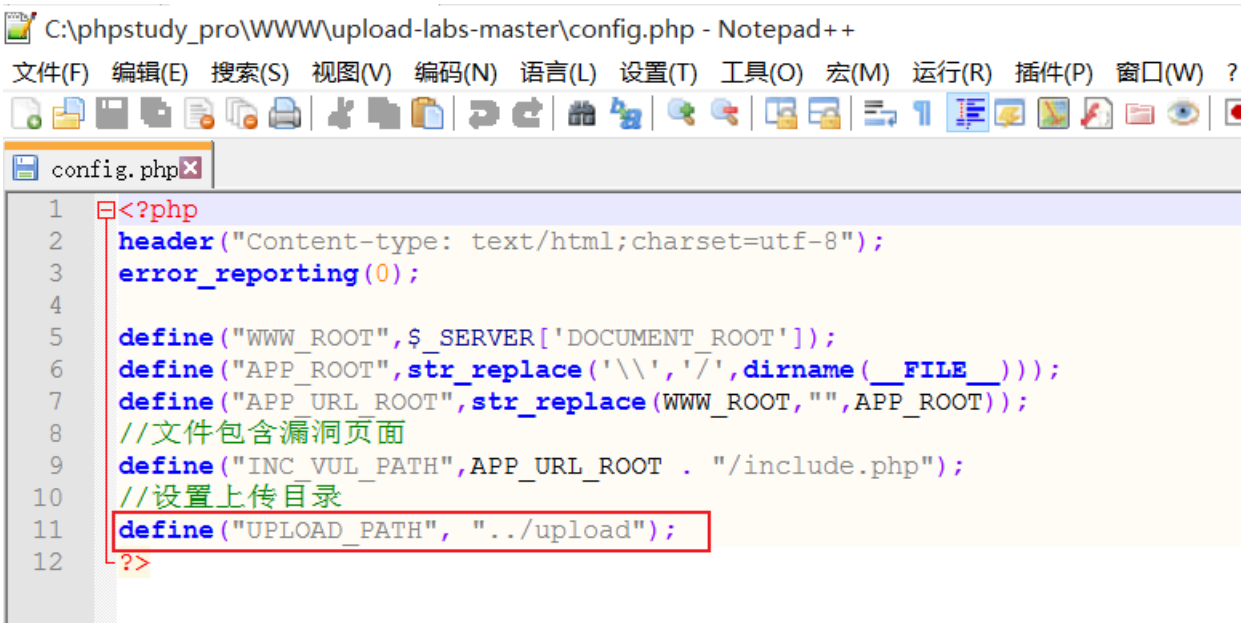
> - 第二条语句判断了一下文件上传的路径存不存在，存在的话就执行里面的代码，不存在就给 `$msg` 设置回显信息
> - 通过 `Seay` 审计的全局搜索功能可以找到 `UPLOAD_PATH` 是在 `config.php` 中被定义的
>   `Pass-02\index.php` 的代码中包含了上一级目录下的 `config.php`
>   然后这个变量就可以在 `Pass-02\index.php` 中直接使用
> - `../` 表示访问上一级的目录，所以 `upload-labs-master\Pass-02\index.php` 包含的是 `upload-labs-master\config.php`
> - 当 `UPLOAD_PATH` 变量在 `upload-labs-master\Pass-02\index.php` 中被调用时，就会设置上传的父文件夹为 `upload-labs-master\upload`


Seay源代码审计系统 --www.cnseay.com
新建项目
关闭项目
自动审计
全局搜索
审计插件
代码调试
函数查询
数据管理
正则编码
临时记录
文件结构
编码: UTF-8
词句:
翻译:
upload-labs-master
common.php
config.php
footer.php
head.php
include.php
index.php
menu.php
README.md
rmdir.php
css
doc
docker
img
js
Pass-01
Pass-02
Pass-03
Pass-04
Pass-05
首页
全局搜索
内容(支持正则): UPLOAD_PATH
查 找
停 止
ID
文件路径
内容详细
1 /config.php define("UPLOAD_PATH", "../upload");
2 /Pass-01/index.php if (file_exists(UPLOAD_PATH)) {
3 /Pass-01/index.php $img_path = UPLOAD_PATH . '/' . $_FILES
4 /Pass-01/index.php $msg = UPLOAD_PATH . '文件夹不存在,请手
5 /Pass-02/index.php if (file_exists(UPLOAD_PATH)) {
6 /Pass-02/index.php $img_path = UPLOAD_PATH . '/' . $_FILES
7 /Pass-02/index.php $msg = UPLOAD_PATH.'文件夹不存在,请手工
8 /Pass-02/show_code.php if (file_exists(UPLOAD_PATH)) {
9 /Pass-02/show_code.php $img_path = UPLOAD_PATH . '/' . $_FILES
10 /Pass-02/show_code.php $msg = UPLOAD_PATH.'文件夹不存在,请手工
11 /Pass-03/index.php if (file_exists(UPLOAD_PATH)) {
12 /Pass-03/index.php $img_path = UPLOAD_PATH.'/'.date("YmdHi
13 /Pass-03/index.php $msg = UPLOAD_PATH . '文件夹不存在,请手
14 /Pass-03/show_code.php if (file_exists(UPLOAD_PATH)) {


此电脑 > 本地磁盘 (C:) > phpstudy_pro > WWW > upload-labs-master > Pass-02
名称
修改日期
类型
helper.php 2020/1/15 22:38 PHP 文件
index.php 2020/1/15 22:38 PHP 文件
show_code.php 2020/1/15 22:38 PHP 文件


C:\phpstudy_pro\WWW\upload-labs-master\Pass-02\index.php - Notepad++
文件(F) 编辑(E) 搜索(S) 视图(V) 编码(N) 语言(L) 设置(T) 工具(O) 宏(M) 运行(R)
index.php
1 <?php
2 include '../config.php';
3 include '../head.php';
4 include '../menu.php';

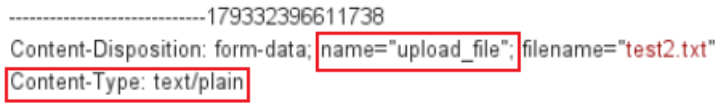

共享
查看
此电脑 › 本地磁盘 (C:) › phpstudy_pro › WWW › upload-labs-master ›
名称
修改日期
类型
大小
Pass-07 2021/7/18 11:03 文件夹
Pass-08 2021/7/18 11:03 文件夹
Pass-09 2021/7/18 11:03 文件夹
Pass-10 2021/7/18 11:03 文件夹
Pass-11 2021/7/18 11:03 文件夹
Pass-12 2021/7/18 11:03 文件夹
Pass-13 2021/7/18 11:03 文件夹
Pass-14 2021/7/18 11:03 文件夹
Pass-15 2021/7/18 11:03 文件夹
Pass-16 2021/7/18 11:03 文件夹
Pass-17 2021/7/18 11:03 文件夹
Pass-18 2021/7/18 11:03 文件夹
Pass-19 2021/7/18 11:03 文件夹
Pass-20 2021/7/18 11:03 文件夹
Pass-21 2021/7/18 11:03 文件夹
upload 2021/7/20 16:34 文件夹
common.php 2020/1/15 22:38 PHP 文件 1 KB
config.php 2020/1/15 22:38 PHP 文件 1 KB


C:\phpstudy_pro\WWW\upload-labs-master\config.php - Notepad++
文件(F) 编辑(E) 搜索(S) 视图(V) 编码(N) 语言(L) 设置(T) 工具(O) 宏(M) 运行(R) 插件(P) 窗口(W) ?
config.php
1 <?php
2 header("Content-type: text/html;charset=utf-8");
3 error_reporting(0);
4
5 define("WWW_ROOT",$_SERVER['DOCUMENT_ROOT']);
6 define("APP_ROOT",str_replace('\\','/',dirname(__FILE__)));
7 define("APP_URL_ROOT",str_replace(WWW_ROOT,"",APP_ROOT));
8 //文件包含漏洞页面
9 define("INC_VUL_PATH",APP_URL_ROOT . "/include.php");
10 //设置上传目录
11 define("UPLOAD_PATH", "../upload");
12 ?>

```php
$is_upload = false;
$msg = null;
if (xxx) {//第一条if语句
    if (file_exists(UPLOAD_PATH)) {//第二条if语句
     //代码
    }else {//第二条if为假时
        $msg = UPLOAD_PATH.'文件夹不存在,请手工创建! ';
    }
}
```

(3). MIME类型判断

- 第三条if语句判断的条件稍微多了点，主要是判断了文件的`Content-Type`参数是否为`image/jpeg`、`image/png`、`image/gif`三者中的一个
- 如果符合就通过此if语句，否则就设置`$msg`的值用于回显错误提示信息




```php
$is_upload = false;
$msg = null;
if (xxx) {//第一条if语句
    if (xxx) {//第二条if语句
        if (($_FILES['upload_file']['type'] == 'image/jpeg')
        || ($_FILES['upload_file']['type'] == 'image/png')
        || ($_FILES['upload_file']['type'] == 'image/gif')) {//第三条if语句
         //代码
        } else {//第三条if为假时
            $msg = '文件类型不正确，请重新上传! ';
        }
    } else {//第二条if为假时
        //代码
    }
}
```

(4). 文件存储路径设置

- 在上传文件的时候，文件都会被存储在一个临时的文件夹下
  我们不需要知道具体路径，只需要通过`tmp_name`参数获取路径即可
- 下方两条语句是先将获取的临时路径存储到`$temp_file`变量内，然后设置上传的路径
- 假设上传的文件名为`test2.txt`，则`$img_path`值为`../upload/test2.txt`

```php
$is_upload = false;
$msg = null;
if (xxx) {//第一条if语句
    if (xxx) {//第二条if语句
        if (xxx) {//第三条if语句
         $temp_file = $_FILES['upload_file']['tmp_name'];
            $img_path = UPLOAD_PATH . '/' . $_FILES['upload_file']['name']
            //代码
        } else {//第三条if为假时
            //代码
        }
    } else {//第二条if为假时
        //代码
    }
}
```

(5). 移动临时文件

> - 第四条if语句会执行 `move_uploaded_file` 函数，将存在临时文件夹内的文件移动到指定的 `upload` 文件夹下，并以原先的文件名存储。
> - 如果移动失败就设置回显语句，成功就设置 `$is_upload` 为真

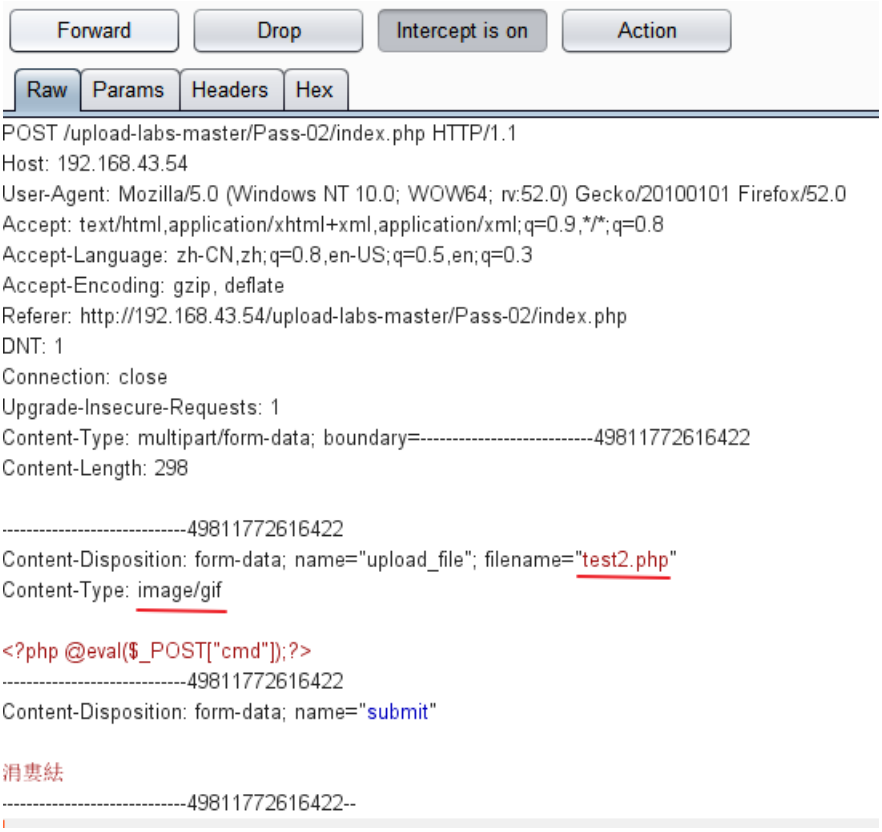
```php
$is_upload = false;
$msg = null;
if (xxx) {//第一条if语句
    if (xxx) {//第二条if语句
        if (xxx) {//第三条if语句
         //代码
            if (move_uploaded_file($temp_file, $img_path)) {//第四条if语句
                $is_upload = true;
            } else {//第四条if为假时
                $msg = '上传出错！';
            }
        } else {//第三条if为假时
            //代码
        }
    } else {//第二条if为假时
        //代码
    }
}
```

[3]. MIME绕过

> - 知道了源码的上传思路后，就比较好绕过了
> 其中比较重要的是第三条if语句，其他的语句没有对文件进行过滤
> - 所以只要 `Content-Type` 的值为 `image/jpeg` 、 `image/png` 、 `image/gif` 其中一个，就可以绕过
> 存在于服务器的文件后缀必须为 `php` ，不然没有办法解析里面的代码
> - 下方的表格来自MIME类型 - HTTP | MDN

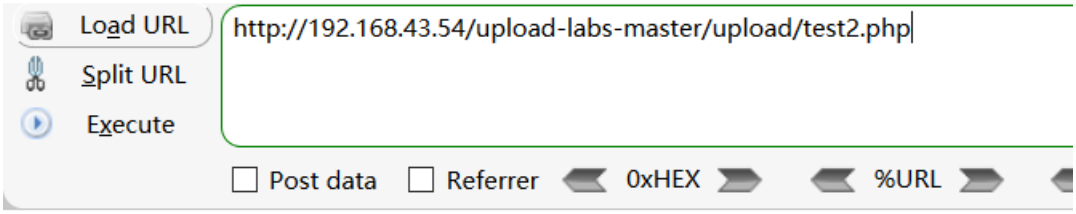
类型	描述	示例
text	表明文件是普通文本，理论上是人类可读	text/plain, text/html, text/css, text/javascript

类型	描述	示例
image	表明是某种图像，不包括视频，但是动态图也使用image类型	image/gif, image/png, image/jpeg, image/bmp, image/webp, image/x-icon, image/vnd.microsoft.icon
audio	表明是某种音频文件	audio/midi, audio/mpeg, audio/webm, audio/ogg, audio/wav
video	表明是某种视频文件	video/webm, video/ogg
application	表明是某种二进制数据	application/octet-stream, application/pkcs12, application/vnd.mspowerpoint, application/xhtml+xml, application/xml, application/pdf

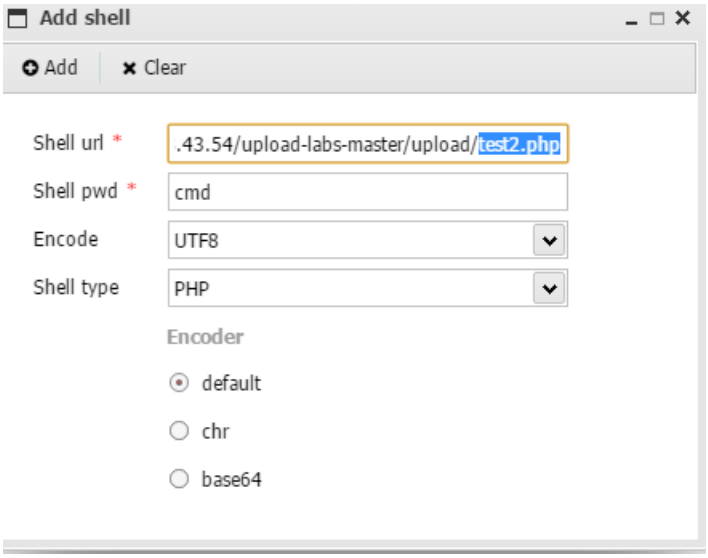


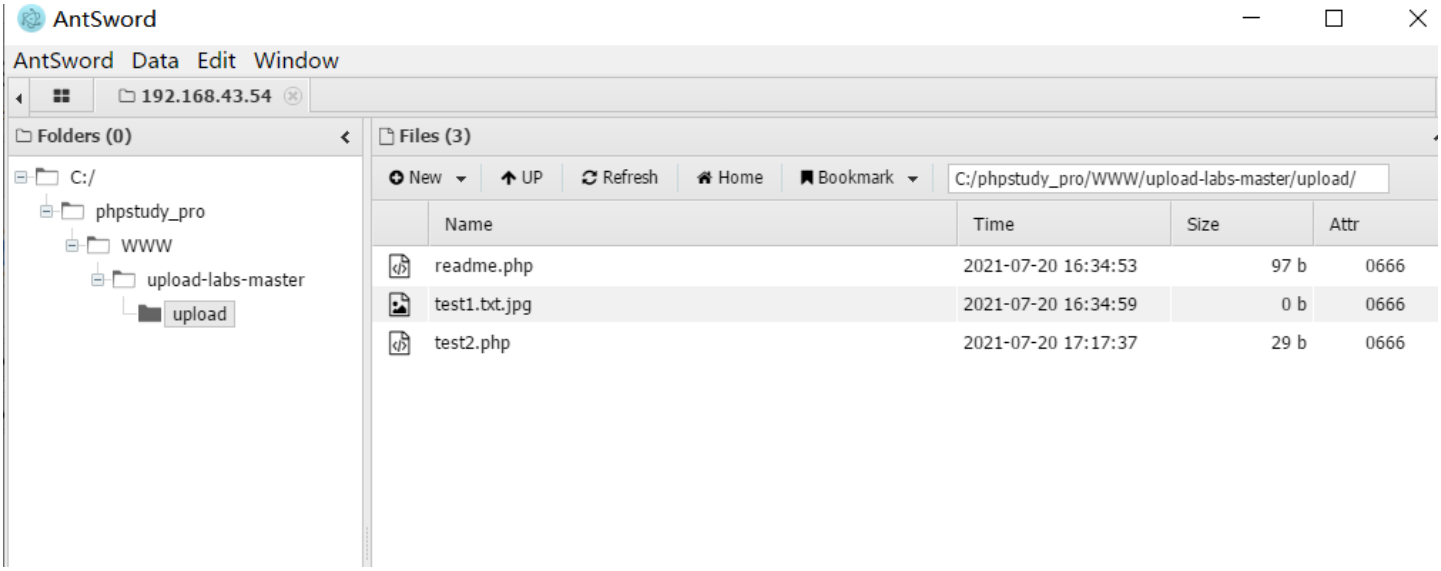
> 上传成功后，右键查看图片的url并访问
> 没有报错，就说明成功解析了这个php文件


任务
上传一个 webshell 到服务器。
上传区
请选择要上传的图片：
浏览...
未选择文件。
上传


Load URL
Split URL
Execute
http://192.168.43.54/upload-labs-master/upload/test2.php
Post data
Referrer
0xHEX
%URL

使用蚁剑进行连接


Add shell
Add
Clear
Shell url *
.43.54/upload-labs-master/upload/test2.php
Shell pwd *
cmd
Encode
UTF8
Shell type
PHP
Encoder
default
chr
base64


AntSword
AntSword Data Edit Window
192.168.43.54
Folders (0)
C:/
phpstudy_pro
WWW
upload-labs-master
upload
Files (3)
New
UP
Refresh
Home
Bookmark
C:/phpstudy_pro/WWW/upload-labs-master/upload/
Name
Time
Size
Attr
readme.php
2021-07-20 16:34:53
97 b
0666
test1.txt.jpg
2021-07-20 16:34:59
0 b
0666
test2.php
2021-07-20 17:17:37
29 b
0666