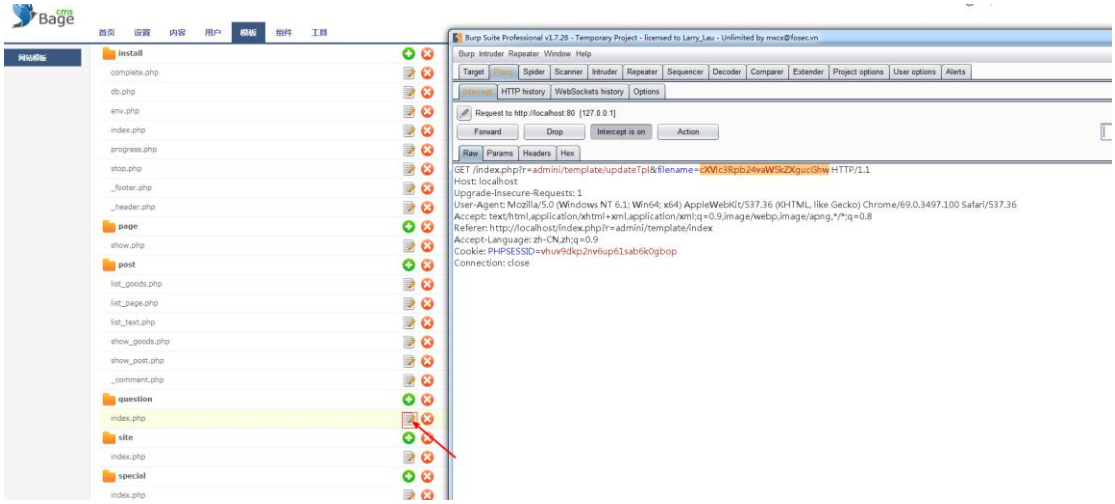
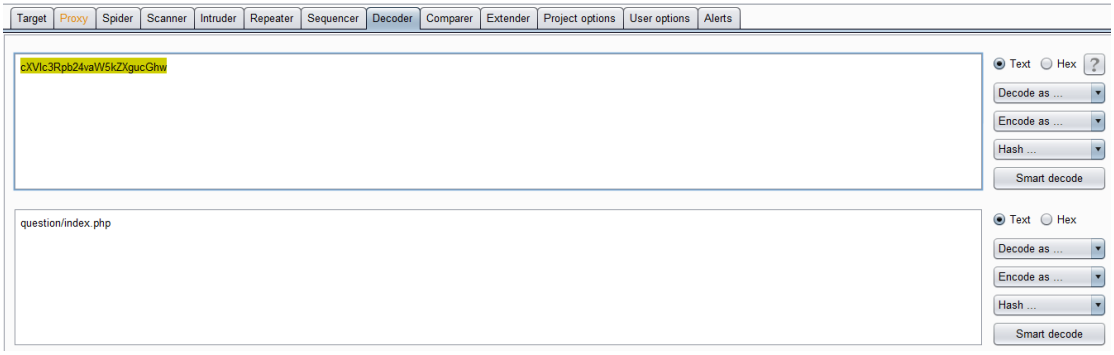
任意文件读取

漏洞入口文件\protected\modules\admini\controllers\TemplateController.php 的 95-117 行

```
95      /**
96       * 编辑
97       *
98       * @param $id
99       */
100     public function actionUpdateTpl( $filename ) {
101         parent::_acl();
102         parent::_configParams(array('action'=>'allowTplOperate', 'val'=>'Y', 'message'=>'不允许创建或编辑模板，请在 protected/config/params.php 中配置 allowTplOperate 为 Y'));
103         $filename = CHtml::encode(trim( $this->_gets->getParam( 'filename' )));
104         $content = trim( $this->_gets->getParam( 'content' ) );
105         if ( isset( $_POST['content'] ) ) {
106             $fileputcontent = file_put_contents(  $this->_themePath.DS.'views'.DS.XUtils::b64decode( $filename ), $content );
107             if ( $fileputcontent == true ) {
108                 AdminLogger::_create( array( 'catalog'=>'update', 'intro'=>'编辑模板' ) );
109                 $this->redirect( array ( 'index' ) );
110             }
111         }
112         $data['filename'] = XUtils::b64decode( $filename );
113         $data['content'] = htmlspecialchars( file_get_contents(  $this->_themePath.DS.'views'.DS.XUtils::b64decode( $filename ) ) );
114         $this->render( 'update', $data );
115
116     }
117
```

不进入 if 判断，$filename 的值经过 base64 编码以后，通过 file_get_contents 函数读入，将读取到的文件内容经过 htmlspecialchars 函数处理。



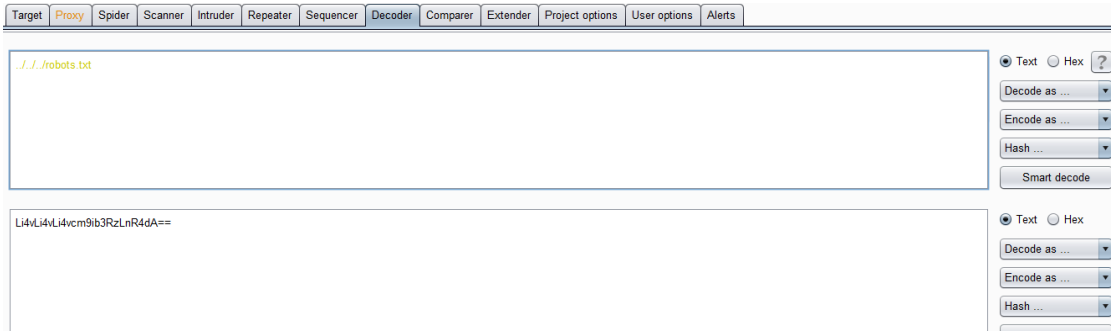


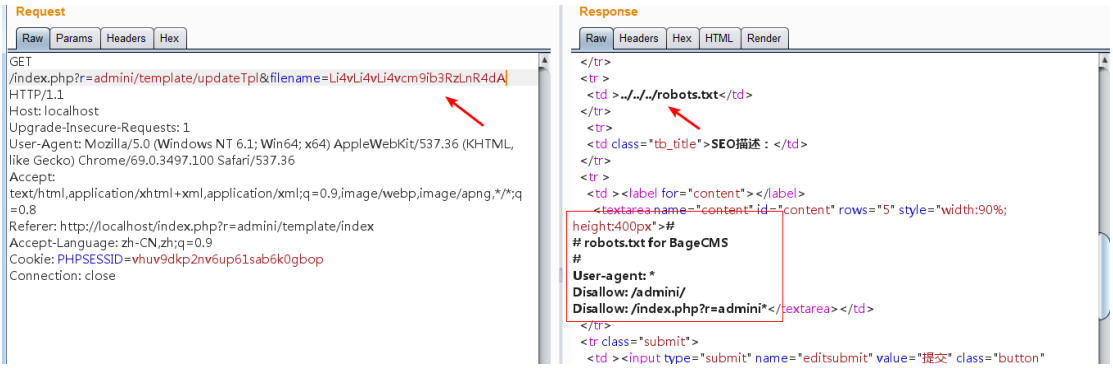
把 filename 的值换为我们想读取的文件内容的 base64 编码，即可读取任意文件，需要注意的是，默认读取\themes\default\views 文件夹下的内容，可以从下面代码中看出来：

```
$data['filename'] = XUtils::b64decode( $filename );
$data['content'] = htmlspecialchars( file_get_contents(  $this->_themePath.DS.'views'.DS.XUtils::b64decode( $filename ) ) );
$this->render( 'update', $data );
```

因为没有任何限制，我们可以使用../来跳转到我们想读取的目录，以读取根目录下的 robots.txt 文件为例：

先将路径 base64 编码，将编码值替换原请求包中的 filename 值：





创建任意文件 GETSHELL

漏洞入口文件\protected\modules\admini\controllers\TemplateController.php 的 95-166 行进入漏洞代码的 if 判断中：

```php
    /**
     * 编辑
     *
     * @param $id
     */
    public function actionUpdateTpl( $filename ) {
        parent::_acl();
        parent::_configParams(array('action'=>'allowTplOperate', 'val'=>'Y', 'message'=>'不允许创建或编辑模板，请在 protected/config/params.php 中配置 allowTplOperate 为 Y'));
        $filename = CHtml::encode(trim( $this->_gets->getParam( 'filename' )));
        $content = trim( $this->_gets->getParam( 'content' ) );
        if ( isset( $_POST['content'] ) ) {
            $fileputcontent = file_put_contents(  $this->_themePath.DS.'views'.DS.XUtils::b64decode( $filename ), $content );
            if ( $fileputcontent == true ) {
                AdminLogger::_create( array( 'catalog'=>'update', 'intro'=>'编辑模板' ) );
                $this->redirect( array ( 'index' ) );
            }
        }
        $data['filename'] = XUtils::b64decode( $filename );
        $data['content'] = htmlspecialchars( file_get_contents(  $this->_themePath.DS.'views'.DS.XUtils::b64decode( $filename ) ) );
        $this->render( 'update', $data );

    }
```

用户 post 的内容未经任何处理直接通过 file_get_contents 读入文件：