web127

```php
 <?php
error_reporting(0);
include("flag.php");
highlight_file(__FILE__);
$ctf_show = md5($flag);
$url = $_SERVER['QUERY_STRING'];
//特殊字符检测
function waf($url){
    if(preg_match('/\`|\~|\!|\@|\#|\^|\*|\(|\)|\\$|\_|\-|\+|\{|\;|\:|\
[|\]|\}|\'|\"|\<|\,|\>|\.|\\\|\//', $url)){
        return true;
    }else{
        return false;
    }
}
if(waf($url)){
    die("嗯哼？");
}else{
    extract($_GET);
}
if($ctf_show==='ilove36d'){
    echo $flag;
}
```

这里开启了`$_SERVER['QUERY_STRING']`，这里用了一个extract()函数

extract() 函数从数组中将变量导入到当前的符号表，使用数组键名作为变量名，使用数组键值作为变量值

extract

(PHP 4, PHP 5, PHP 7, PHP 8)
extract — 从数组中将变量导入到当前的符号表

说明

```
extract(array &$array, int $flags = EXTR_OVERWRITE, string $prefix = ""): int
```

本函数用来将变量从数组中导入到当前的符号表中。

检查每个键名看是否可以作为一个合法的变量名，同时也检查和符号表中已有的变量名的冲突。

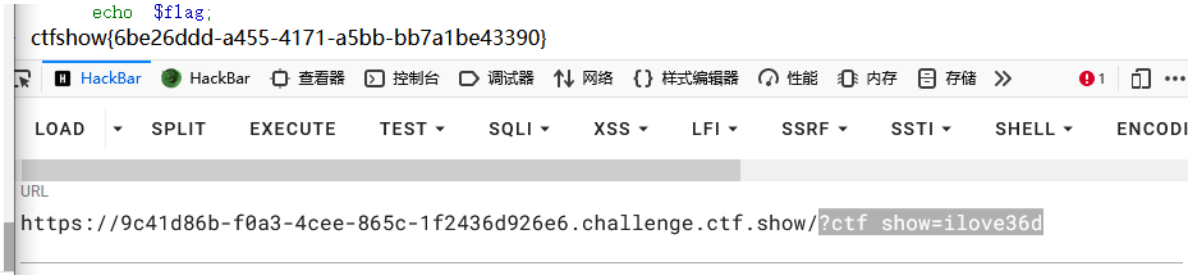
Warning 不要对不可信的数据使用 `extract()`，类似用户输入 （例如 `$_GET`、`$_FILES`）。

举例就是`?a=2`，就会变成`$a=2`，这里`ctf_show`有个`_`需要构造，前面说过php中变量名只有数字字母下划线，被get或者post传入的变量名，如果含有`空格、+、[`则会被转化为`_`，这里空格没有被禁，使用空格

payload

```
?ctf show=ilove36d
```

得到flag



web128

```php
<?php
error_reporting(0);
include("flag.php");
highlight_file(__FILE__);

$f1 = $_GET['f1'];
$f2 = $_GET['f2'];

if(check($f1)){
    var_dump(call_user_func(call_user_func($f1,$f2)));
}else{
    echo "嗯哼？";
}
function check($str){
    return !preg_match('/[0-9]|[a-z]/i', $str);
}
```

还是这个函数`call_user_func`

> 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。

call_user_func() 函数把第一个参数作为回调函数，其余参数都是回调函数的参数

这里对`$f1`进行了正则过滤，不能为数字和字母，这里可以使用gettext拓展，

`_()` 等效于 `gettext()`

```
php
<?php
echo gettext("1");
//输出结果：1

echo _("1");
//输出结果：1
```

因此`call_user_func('_','ctfshownb')`返回的结果为ctfshownb，接下来到第二层`call_user_func`，找了一圈发现`get_defined_vars`函数可以使用

get_defined_vars (void) : array 函数**返回一个包含所有已定义变量列表的多维数组**，这些变量包括环境变量、服务器变量和用户定义的变量。

get_defined_vars

(PHP 4 >= 4.0.4, PHP 5, PHP 7, PHP 8)
get_defined_vars — 返回由所有已定义变量所组成的数组

说明

```
get_defined_vars(): array
```

此函数返回多维数组。包含调用 get_defined_vars() 作用域内所有已定义的变量、环境变量、服务器变量、用户定义变量列表。

参数

此函数没有参数。

构建payload

```
?f1=_&f2=get_defined_vars
```

得到flag