积分竞猜网php源码_贵州省网络安全知识竞赛个人赛Writeup

原创

LeoShaoQiang 于 2021-01-13 07:15:45 发布 84 收藏

首先拖到D盾扫描

可以很明显的看出来确实就是两个后门

0x01 Index.php#一句话木马后门

0x02 About.php#文件包含漏洞

都可以很直观的看出来非常明显的漏洞,第一个直接就是eval一句话后门，第二个就是非常简单的文件包含；

第一个漏洞的利用代码即为：system(base64_decode("Y2F0IGZsYWcq"));

Y2F0IGZsYWcq是cat flag*进行base64编码以后的。

第二个漏洞攻击可以通过伪协议中的input写入webshell

about.php?f=php://input

post数据为：<?php fputs(fopen("shell.php","w"),'<?php eval($_POST["cmd"];?>');?>

0x03 challege.php#任意文件读取

这里在41行的时候有一个判断，如果其中一个满足那么就会exit。所以我们不能让她exit，否则不能执行readfile

40行的函数使用的有点问题，应该是parse_url，多了一个n，提供代码给我的这位师傅应该是没有修改过代码的。所以这里应该是比赛方的一个瑕疵。

我们当作parse_url来做

Parse_url函数是拿来解析url的，如下所示：

所以在看41行的代码就很简单了

我们直接让$parts['host']不为空并且等于localhost即可

0x04 SQL注入#message.php

因为我这里没有数据库环境就不多演示如何get数据了。

如果要修复，直接对$_GET['id']进行操作即可。

0x05 SQL注入#logcheck.php

0x06 SQL注入#login.php

0x07 upload.php#任意文件上传

上传成功：/images/15681026431.php

登陆后flag:(因为我这儿仅有源码，所以没显示出正确的flag，比赛环境里在这里应该是可以看到flag的)

0x08 sql注入 #search.php

小结：

打开index.php就可以很明显的看到eval以及undefined index：123这里其实就基本可以猜得到，123这个参数是后门了。所以可以很快通过这个后门直接getshell拿到权限；

上面的注入均没有进行任何过滤，直接通过sqlmap就可以很简单的跑出来；

拿到权限以后，可以对代码进行审计，迅速修复漏洞不让对手入侵下这个网站；

或者利用脚本轮训删除images目录下的文件；

针对个人赛，入侵公共靶机的话，如果是可以修改代码那么就破坏功能点，如果不能修改代码那就可以预先准备好一些小脚本，例如轮训删除images目录下的所有文件。尽可能的达到自己入侵下的靶机就不要给别人入侵的机会；