第三届4.29“安恒杯”网络安全技术大赛初赛wirteup心得-WEB

转载

weixin_34342905 于 2016-04-23 22:16:00 发布 244 收藏
文章标签： php 网络 数据库
原文链接：http://www.cnblogs.com/puluotiya/p/5425850.html

writeup地址：

http://www.easyaq.org/info/infoLink?id=851212685&from=groupmessage&isappinstalled=0

WEB1

解题第一步骤，我发现了username和uid根本就是加密了。。当时就一个劲的想怎么解admin。。原来题目的漏洞在于uid啊，，，我觉得这篇讲的很好，里面的python语句也写得挺好：http://www.tuicool.com/articles/N3iIBzN

总体来讲就是，uid是可以随意更改的，但是必须要求三位，而事实上admin的id<10 所以问题就在怎么登陆个位数的id啦。。 6-- 或者6abc..

WEB2

首先，找到可写目录，这个要慢慢试

然后，写一句话代码，可以先放入数据库，也可以直接写进去

select xxx into outfile ‘var/www/…’

然后菜刀连接，可以去查查目录里面有没有

WEB3

反序列化题，对我来讲是很新的知识点

大致的该题的思路见：http://www.tuicool.com/articles/Bfuayyl

index.php网页有一句这样的话：

```
ini_set('session.serialize_handler', 'php');
```

这个页面下，session的序列化方法是php，查看phpinfo.php发现，session默认的序列方法是php_serialize(php>=5.5.4) 关于他们的区别：

php
键名 ＋ 竖线 ＋ 经过 serialize() 函数反序列处理的值

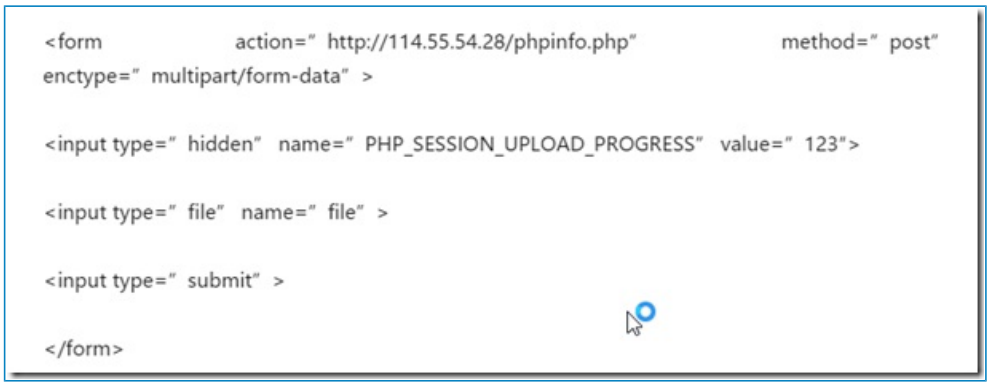
php_binary
键名的长度对应的 ASCII 字符 ＋ 键名 ＋ 经过 serialize() 函数反序列处理的值

php_serialize
(php>=5.5.4)经过 serialize() 函数反序列处理的数组

当两个网页使用不同的序列化函数，bug就产生了

在一般情况下，该攻击的实现需要一个网页去构造序列化参数，然后另一个页面以另一种反序列化方式读取它，导致执行。但是我们这个题目，根本没有session的读取。。

所以，我们要自己创造。。



这是官网上给出的代码，根据phpinfo.php的信息，发现session.upload_progress.enabled是打开的，也就是文件任意上传。然后我们就上传一个文件，然后php就会给我们创建一个session，为了控制上传进度，具体可以看：http://php.net/manual/zh/session.upload-progress.php

问题就剩下，怎么构建漏洞与语句了，官网writeup也是给了（注意标点的中英文）：

用抓包软件修改上传数据包，将filename修改为filename="|O:4:/"foo1/":1:{s:4:/"varr/";O:4:/"foo2/":2:{s:4:/"varr/";s:1:/"1/";s:3:/"obj/";O:4:/"foo3/":1:{s:4:/"varr/";s:30:/"system(/"ls -a /var/www/html/");/";}}}"

访问index.php，列出文件目录，找出flag文件。

再次抓包上传，filename修改为filename="|O:4:/"foo1/":1:{s:4:/"varr/";O:4:/"foo2/":2:{s:4:/"varr/";s:1:/"1/";s:3:/"obj/";O:4:/"foo3/":1:{s:4:/"varr/";s:27:/"system(/"cat flag_xxx.php/");/";}}}"

访问index.php获取flag

转载于:https://www.cnblogs.com/puluotiya/p/5425850.html