利用报错函数 Updatexml 和 extractvalue 带回回显流量分析

一、updatexml()函数

使用前提：

在 mysql 高版本中(大于 5.1 版本)中添加了对 XML 文档进行查询和修改的函数，updatexml(),extracvalue()

而显示错误则需要在开发程序中采用 print_r mysql_error()函数，将 mysql 错误信息输出。

Updatexml 函数本身介绍

作用：改变文档中符合条件的节点,使用不同的 xml 标记匹配和替换 xml 块的函数。

updatexml(XML_document,XPath_string,new_value);

XML_document:String 格式，为 XML 文档对象的名称，文中为 Doc

XPath_string:Xpath 格式的字符串，代表路径。

new_value:String 格式，替换查找到的符合条件的数据。

Payload 内容:

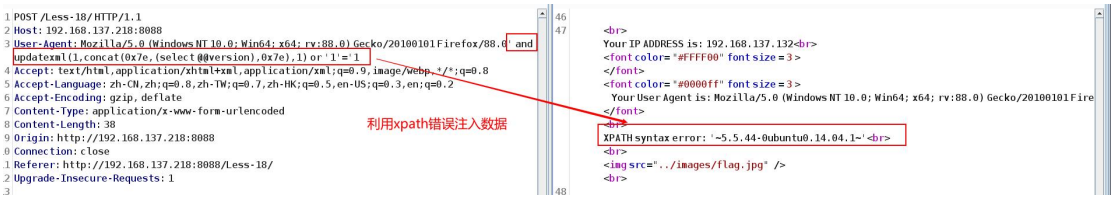
updatexml(xml_document,xpath_string,new_value):

第一个参数:XML 文档对象名称。

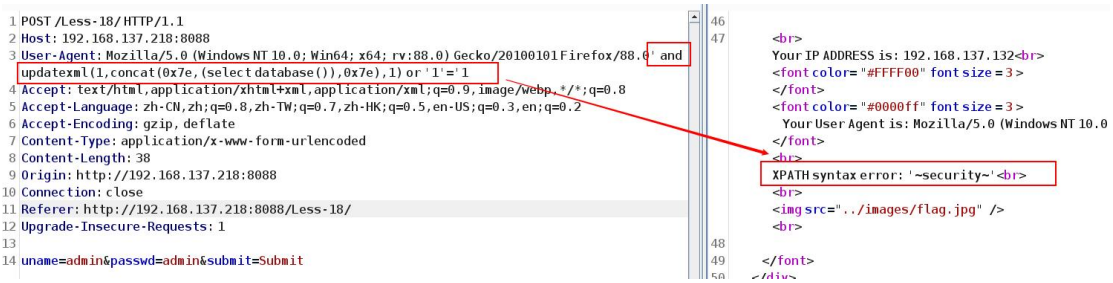
第二个参数:XPath 字符串。

第三个参数:替换查找到的符合条件的数据。

' and updatexml(1,concat(0x7e,(select @@version),0x7e),1) or '1'='1

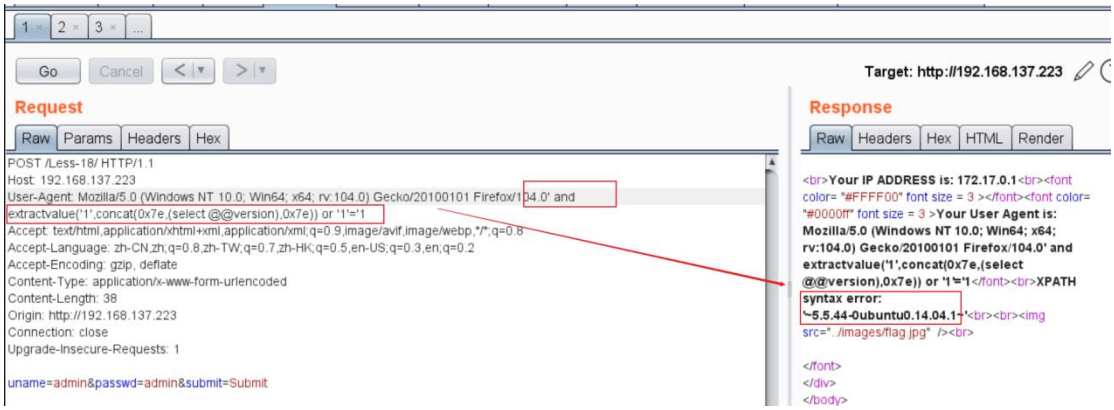


获得数据库名



二、另外一种报错函数注入 extractvalue 的利用

extractvalue 函数的基本格式为：ExtractValue(xml_frag, xpath_expr)
extractvalue 函数接收两个字符串参数，一个属 xml 标记片段和 xpath 表达式 xpath expr（xml 是一种可扩展标记语言，使用标签来操作，html 就是一种常见的标记型语言，xml 主要用来存储数据，体现在作配置文件，或者充当小型数据库，在网络中传输数据，类似与 HTML 语言中的 div 标签；）（xpath expr 也称为定位器，也就是路径查询，因为咱们主要是为了学习 sql 注入，所有函数的原理不用太纠结，只要大概了解一下就行了）其实简单点来说，第一个参数就是为了上传一个 xml 文档，第二个参数就是用 xpath 路径法查找路径，而 extractvalue 报错注入 就是通过再函数中写如不符合语法格式的 xpath 达到报错的目的，并且通过拼接 sql 注入语句从而通过报错查询并显示我们想要查询的内容；
例如:
' and extractvalue('1',concat(0x7e,(select @@version),0x7e)) or '1'='1



三、流量特征

流量关键字
Undatexml
extractvalue
Concat
And
Or
敏感信息函数 version database()等