

# Forum:[Hack Forums](#)

Thread: [SQL Injection in IFRAME?](#)

**8220347** - January 14, 2017, 9:42 am

Hi,

So there is site #1 and site #2

So I was browsing site #1, and noticed that it was utilizing an iframe to allow users on their site to use a basic search engine located on site #2. I was able to find a SQL Injection vulnerability on a parameter on site #1, but that is actually utilized on site #2. I know this sounds confusing, so hear is what the link looks like so you can better understand:

site #1 looks like this, and is using an iframe:

<http://site#1.com/search/site#2/index.php?a=1>

site #2 looks like this:

<http://site#2.com/index.php?a=1>

So my question is, if I have successfully exploited the query "and 1=1" on <http://site#1.com/search/site#2/index.php?a=1>, would I be accessing the Database of site #1 or site #2?

**Maxie** - January 14, 2017, 9:47 am

Probably site 2. Seems very weird though. Are you sure that there is no vulnerability available on site 2?

•^v^-[ bLacKn3x ]-^v^• - January 14, 2017, 9:47 am

You exploit Site#1

Site2 is only in search parameter.

**Gee4rce** - January 14, 2017, 10:29 am

You could use the SQLi to check for database() name, (which may already reveal the name of the site it's connected to),

or you could list all (under the current user you are acting with) accessible databases.

This should already give enough hints to which site the injection belongs, and/or if both sites are maybe connected to the db.

Cheers, Gee.

**8220347** - January 14, 2017, 10:35 am

I have tried to check database names, but site #1 has a strong WAF. I am able to run sqlmap on site #2 though (<http://site#2.com/index.php?a=1>) because it has no WAF, and Im able to access it's databases.

•^v^-[ bLacKn3x ]-^v^• - January 14, 2017, 11:47 am

If you want some help pm me i can try to bypass that .

I do it manually

**Disparity** - January 15, 2017, 1:24 pm

(Jan 14, 2017 11:35 AM)8220347 Wrote: [\[CITE\]](#) I have tried to check database names, but site #1 has a strong WAF. I am able to run sqlmap on site #2 though (<http://site#2.com/index.php?a=1>) because it has no WAF, and I'm able to access its databases.

Site 2 might be the only vulnerable one, it depends. Is it running on a totally separate domain, similar to how on-site google searches work? If you're going to try and beat the WAF you should do it manually, especially if it's giving you errors. As far as site 2 goes, what kind of data are you getting from the db, and what's the db name, or at the very least what does the name reveal?

If you want more help feel free to drop me a PM.