

Forum:[Hack Forums](#)

Thread: [\[SQL\] Issues creating remote connection to SQL Database.](#)

Armada - June 16, 2015, 10:48 am

Ok, so long story short, I am trying to do a SQL database dump against a website.

I have located the SQL user/db/pw information, and after a bit of testing found my way past cloudflares protection to the true servers IP#.

However, using the provided credentials, I am hitting an error where the server returns an error back to me directly saying Connectivity to this SQL database from <Whatever my host is> is not allowed.

Now, I am suspecting this has something to do with the fact the webserver's policy seems pretty restrictive.

Example of .htaccess

Code Order deny,allow

Deny from all

Allow from 127.0.0.1

I have tried using IP#'s as close to the originating server's true geographical location, but to no avail.

Any suggestions?

Scy7e - June 16, 2015, 10:50 am

Sounds like they only allow localhost connections and they either work locally or through a SSH tunnel. Not much you can do in that case.

Armada - June 16, 2015, 10:53 am

(Jun 16, 2015 10:50 AM)Scy7e Wrote: [\[CITE\]](#) Sounds like they only allow localhost connections and they either work locally or through a SSH tunnel. Not much you can do in that case.

The SQL server certainly resides on the webserver, all configs point directly to 'localhost' for the SQL server calls.

The issue I seem to have hit here is I ONLY have the SQL DB information.

How can I create queries to the SQL by making it believe I am in fact the localhost and not a remote connection?

Im thinking IP spoofing MIGHT work, but....

Scy7e - June 16, 2015, 11:04 am

(Jun 16, 2015 10:53 AM)Armada Wrote: [\[CITE\]](#) The SQL server certainly resides on the webserver, all configs point directly to 'localhost' for the SQL server calls.

The issue I seem to have hit here is I ONLY have the SQL DB information.

How can I create queries to the SQL by making it believe I am in fact the localhost and not a remote connection?

Im thinking IP spoofing MIGHT work, but....

Eh, IP spoofing won't work. If you can't gain access to the localhost, then you're out of luck.

Armada - June 16, 2015, 11:08 am

(Jun 16, 2015 11:04 AM)Scy7e Wrote: [\[CITE\]](#) Eh, IP spoofing won't work. If you can't gain access to the localhost, then you're out of luck.

That is kind of my thinking, even assuming I managed to convince the server I was its IP#, and it accepted it, any data requested will get sent back to the server and not myself at the remote connection ?

regexks - June 16, 2015, 12:04 pm

You should probably check out MySQL privilege grant tables. Versions of MySQL previous to 5.6.7 still offer privilege limitations to tables based on host.

tendercareAustin - June 17, 2015, 12:01 pm

(Jun 16, 2015 10:50 AM)Scy7e Wrote: [\[CITE\]](#) Sounds like they only allow localhost connections and they either work locally or through a SSH tunnel. Not much you can do in that case. I'd suggest using Filezilla to download the admin folder from the database. This way you can edit the admin.php cos that's where the privilege to connect via web is set. you can reop the admin.php and over write the previous.

I've bn ablt to do similar via webshell so I blv Filezilla can do the magic.

Armada - June 17, 2015, 1:59 pm

(Jun 17, 2015 12:01 PM)tendercareAustin Wrote: [\[CITE\]](#) I'd suggest using Filezilla to download the admin folder from the database. This way you can edit the admin.php cos that's where the privilege to connect via web is set. you can reop the admin.php and over write the previous.

I've bn ablt to do similar via webshell so I blv Filezilla can do the magic.

If I could use Filezilla to connect to anything this would not be a problem whatsoever.

Secondly, what does connecting to the Database have to do with the web servers files whatsoever (admin.php)?

.php files call and reference the SQL database, not directly manipulate it.
So this is less than helpful in any event.

Thirdly, The site does not even have an admin.php file

.....?

WubCannon - June 17, 2015, 2:18 pm

(Jun 17, 2015 01:59 PM)A?mªDa Wrote: [\[CITE\]](#) If I could use Filezilla to connect to anything this would not be a problem whatsoever.

Secondly, what does connecting to the Database have to do with the web servers files whatsoever (admin.php)?

.php files call and reference the SQL database, not directly manipulate it.
So this is less than helpful in any event.

Thirdly, The site does not even have an admin.php file

.....? I have no idea what he is talking about and I dont think he does either. I wouldnt pay any attention to him. most DBMS's will have a setup whereby they will either only allow a single IP, or an IP range or just localhost. These are setup directly in the DBMS and so have no bearing from .htaccess files. If this is the case then you are out of luck. IP spoofing is not an option and neither would getting IP's close to the location.

Best option available would be to do an nmap scan and try to find some vulnerable daemons running on the server, or trying to exploit the access you already have in another way (im assuming you have a LFI or download exploit). Finally you could look at any other sites that may be hosted on the server if its shared hosting. Pop a shell on that site, then upload adminer and use that from the localhost

Armada - June 17, 2015, 2:30 pm

(Jun 17, 2015 02:18 PM)WubCannon Wrote: [\[CITE\]](#) I have no idea what he is talking about and I dont think he does either. I wouldnt pay any attention to him. most DBMS's will have a setup whereby they will either only allow a single IP, or an IP range or just localhost. These are setup directly in the DBMS and so have no bearing from .htaccess files. If this is the case then you are out of luck. IP spoofing is not an option and neither would getting IP's close to the location.

Best option available would be to do an nmap scan and try to find some vulnerable daemons running on the server, or trying to exploit the access you already have in another way (im assuming you have a LFI or download exploit). Finally you could look at any other sites that may be hosted on the server if its shared hosting. Pop a shell on that site, then upload adminer and use that from the localhost

That is pretty much what I have started working towards.

I am aware the .htaccess has little bearing on the SQL service itself, but I noticed the .htaccess i also configured that way, so I figured it was a safe assumption other services would be configured accordingly.

Upon trying to directly connect to the database it returned an error confirming that suspicion.

As for IP# spoofing, I thought about this briefly, but then realized regardless it was a moot concept, even assuming I wa able to craft packets with the host IP# as mine, my queries would never be received. Because derp, the servers going to send it to itself, and not me. ?

Its looking like finding some kind of exploitable entry point is the only option for this sadly. ?