

Forum:[Hack Forums](#)

Thread: [Being a White Hat](#)

device - July 27, 2019, 1:54 pm

Just a thought I had, I stumbled on emails I sent last year to businesses listing vulns in their websites.

I told them what the problem was and they never messaged me back.

Here's an exemple:

"Hi www.*****Team.

You may have noticed extensive activity in your network logs, this was due to scanning for vulnerabilities in your website.

I have used different techniques and have managed to access the SQL database of your website.

I thought I'd inform you about these problems as I am not interested in doing wrong to people.

I haven't tried to list the columns of your SQL tables as that is not my intent.

I suggest you contact a specialist that can help you solve this issue. Updating you MySQL version is a good start, as you seem to be running 5.1.

To show you how easy it is to KNOW if your website is vulnerable to this type of vulnerability all you have to do is the following:

This is a normal link of your website: https://www.*****

This is the same link with another request showing the ERROR CODE: https://www.*****'

See how the only difference is the (') added at the end ?

As you seem to be a popular business in your country I recommend you fix these PHP-MySQL database errors really quick, any hacker with a small understanding of SQL injections could steal all your user information and much more. Here is proof of your database leak:

PASTED DB

Have a good day.

The next day they had it fixed but I never got a message back. At least I helped someone and that's all that counts but it would feel good to at least have a thank you.

That's what I sent them:

"Hey, glad to see you have fixed your website !

Would you mind sending me a certificate saying I have helped in Pen Testing your website? It would really help.

If so please respond to this message.

Have a good day."

frank3nstien - July 27, 2019, 7:11 pm

Yes very true sometimes feel like such a drag after spending efforts and reports to them also an big effort, recently this was happened to me as well it was a well known AV company, they fixed an sql and persistant xss issue in 15 days but never replied me back and i get to know that when i was trying to penetrate again. ?