INFORMATION SECURITY

My site was hacked and the attacker got data from the config file [closed]

Asked 9 years, 1 month ago Modified 9 years, 1 month ago Viewed 4k times

0

Closed. This question needs to be more focused. It is not currently accepting answers.

Want to improve this question? Update the question so it focuses on one problem only by editing this post.

Closed 9 years ago.

Improve this question

A few days ago my website was hacked. I found out that the 'hacker' ran queries directly into the database, so he somehow got access to my database credentials.

I'm using laravel 4 and the config file is stored outside the public_html folder into a .env.production.php file and it looks like this:

```
<?php
return array(

'DB_NAME' => 'database_name',
'DB_USER' => 'database_user',
'DB_PASS' => 'my_password',
'DB_SERVER' => 'localhost'); ?>
```

Accessing this file in the browser returns nothing, so how did the attackers got the data? One theory would be that the hosting company got hacked (I'm on shared hosting. They deny that and I have reasons to believe them.

What other possiblities are there? Remote file inclusion? Local file inclusion? I want to know what could cause the data in the config file to be compromised so I know what to check for in my application.

databases configuration

Share Improve this question Follow

asked Jan 5, 2015 at 11:07

blue_is_awesome
1 1 1

1 No matter what you do, if they got your file, or there is a risk, ALWAYS change the details needed to login! even with your admin panel or host. – Lighty Jan 5, 2015 at 11:09

SQL Injection maybe? That way they wouldn't necessarily need to steal your db credentials. Hard to say though without looking at your site & the code – Arlix Jan 5, 2015 at 12:18

2 As Arlix pointed out, without looking at logs this is purely speculation. They could have got the creds from your machine, from sniffing traffic etc – Rory Alsop ♦ Jan 5, 2015 at 12:23

3 Answers

Sorted by: Highest score (default)

1

Your question can not be answered with the given information.

From what we know you might not even been hacked at all. You might start with telling us more about those queries and what do you mean by `directly into the database`. Remote access from other IP address or a query you can't find in your scripts? Those query might be from Laravel or a plugin.

Anyway it's impossible to tell how you got hacked without knowing your logs, PHP scripts and whatever is on this server. Even with root access it might not be possible to tell if the attacked cleaned up or your logging is not covering the attack vector.

First step would be to find the time of the attack and check log files at this time. If you can't find anything check the complete log. If you find something you don't understand google it or ask a question.

If you sure you got hacked, you might want to involve your hoster. They supposed to know there server and might have access to logs and tools you don't know about.

Share Improve this answer Follow

answered Jan 5, 2015 at 14:01

PiTheNumber
5,424 4 22 36

Looks like there are some known vulnerabilities that might have been their starting point. V4 had a CSRF issue in November for example.

0

I agree with the commenter who said that step one is changing your database auth details.

http://blog.laravel.com/csrf-vulnerability-in-laravel-4/

Share Improve this answer Follow

answered Jan 5, 2015 at 12:46

HalfAdd3r
21 2

0

I have a wild guess how the hacker accessed your configuration file. You might have edited it recently; and the PHP temp files during or after edit are remained on the directory where the config file was stored. check if you can access .php~ php# php.save php.swp php.swo

These are the temporary filenames used by the most popular text editors.

Or check what editor is your default editor for PHP files and google what is its temp file extension.

Share Improve this answer Follow

answered Jan 5, 2015 at 21:27

Goli E
915 1 11 20