



# Hiding Secrets & Finding Secrets

How to get hacked with your own credentials

WhatTheStack 2024 Session

Bozidar Spirovski



Attackers only have to get  
it right once

We need to get it right all  
the time

Let's make the effort to get  
it right more



# Software development?

## All about delivery

```
while salary:
```

```
    code()
```

```
    deploy()
```

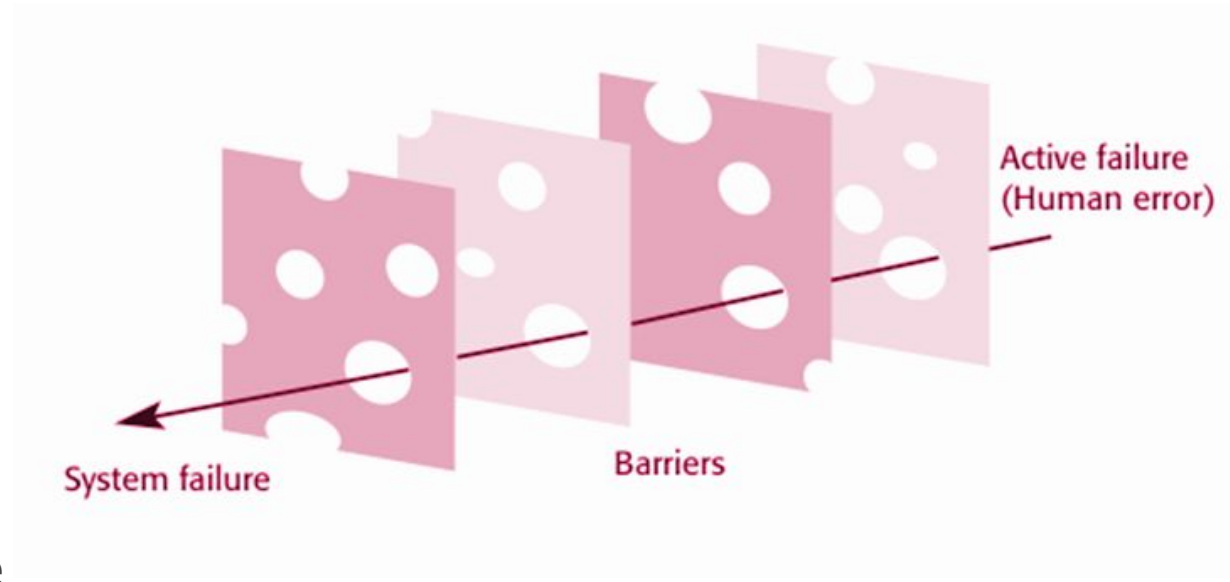
```
    invoice()
```

## OK to make mistakes

- Fix in next sprint
- Code is private

It's how we've always done it

# Hackers are (mostly) not that smart



They don't need to be

- Automation
- Attack at scale
- $\$1 \times 1,000,000 \gg \$1,000,000 \times 1$





```
// ** MySQL settings - You can get this info from your
/** The name of the database for WordPress */
define('DB_NAME', 'solgridt_wp822');

/** MySQL database username */
define('DB_USER', 'solgridt_wp822');

/** MySQL database password */
define('DB_PASSWORD', '@20p8EJS6');

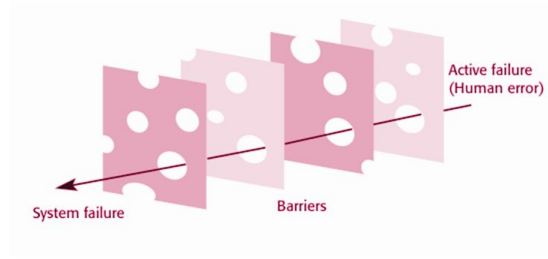
/** MySQL hostname */
define('DB_HOST', 'localhost');

/** Database Charset to use in creating database table */
define('DB_CHARSET', 'utf8');

/** The Database Collate type. Don't change this if in
define('DB_COLLATE', '');
```



But i thought  
he/she is fixing it!



# /usr/bin/whoami

- CISO of Blue dot and Sourcico
- Trying to get people to do the right thing for better part of two decades
- Terrified of people chasing deadlines and being pressured into MVPs
- Many mistakes, incidents and a lot of stress
- 1/2 of Dev-vs-CISO

Email: [b.spirovski@beyondmachines.net](mailto:b.spirovski@beyondmachines.net)

Youtube: <https://www.youtube.com/@spirovskib>

LinkedIn:

<https://www.linkedin.com/in/spirovskibozidar/>



/root/lawyer



**All examples, concepts, and code in this session are for educational purposes only**

Use this knowledge to improve security on platforms you work with.

Do not use any information or techniques from this training for illegal or harmful purposes.

We are not responsible for any misuse of the content provided.





Looking for  
secrets?

Good hunting





# Simple mistakes in code go a long way

Let's write some code and commit...

and

...make a mistake (we'll fix it in the next sprint)

- Hacked Employee
- Leaked SSH keys
- Blog posts and presentations
- Logs
- Let's make this open source!

New commit doesn't help. Github doesn't forget anything.



# But my code is private!

On Tue, Feb 20, 2024 at 8:47 PM Github <[notifications@github.com](mailto:notifications@github.com)> wrote:

Hello,

We have an exciting opportunity for you! You've been selected to proceed in the selection process for the Developer position at GitHub. Congratulations on your achievement!

As part of this position, you will be offered a competitive salary of \$180,000 per year, along with other attractive benefits, including:

- Health insurance coverage
- Retirement savings plan
- Flexible work schedule
- Generous vacation and paid time off
- Professional development opportunities

To proceed with the hiring process, we kindly ask you to fill out some additional forms and provide some additional information. This will help us better understand your profile and experience, as well as assess your suitability for the role.







Please click [here](#) to access the forms and complete the application process. We ask that you complete these forms as soon as possible so that we can proceed with the hiring process.

**Important:** You have 24 hours to complete the application process.

If you have any questions or need further information, please don't hesitate to contact us.

Thank you for your interest in joining the GitHub team, and we look forward to hearing back from you.

Best regards,  
GitHub Recruitment Team

	<b>Delete repositories</b> Ability to delete any adminable repository	▼
	<b>Gists</b> Read and write access	▼
	<b>Organizations and teams</b> Read-only access	▼
	<b>Repositories</b> Public and private	▼
	<b>Personal user data</b> Full access	▼
	<b>Discussions</b> Write, update, and react to Team discussions.	▼



# Containers anyone?



Every solution needs a problem

- **Solution:** keys in the Docker image ENV
- **Problem:** The curse of

```
COPY . /app
```



# Nobody will see this in production

Source code included in the  
build/deployment

Visible/browsable/indexed

Very vulnerable to fuzzing and forced  
browsing



# What about our AWS key?

Let's go back to AWS!

- Reconnaissance starts immediately (matter of minutes)

AWS/Google helps out - but works ONLY for their keys.





Attackers only have to get  
it right once

We need to get it right all  
the time

Let's make the effort to get  
it right more

# How to be better?

Pre-commit hooks\* + gitleaks on your repos

*.dockerignore* and *.gitignore* are your friends

Use roles where possible!

Secrets ONLY in vaults / parameter stores

Want to read more scary stories?

<https://securitycafe.ro/2024/05/08/aws-cloudquarry-digging-for-secrets-in-public-amis/>

\*<https://github.com/dev-vs-ciso/wts24-secrets>







**I OVERTHINK, THEREFORE**



**I OVERAM**

imgflip.com

# A question?

The first thing that  
comes to mind!

# Thank you



Email: [b.spirovski@beyondmachines.net](mailto:b.spirovski@beyondmachines.net)

Youtube:

<https://www.youtube.com/@spirovskib>

Linked In:

<https://www.linkedin.com/in/spirovskibozidar/>