

OVERCOMING LAZINESS

FIVE EXCUSES OF DEVELOPERS/SYSADMIN & HOW TO OVERCOME THEM

How to overcome the Five Excuses of developers



Overcoming Laziness

A collaborative effort

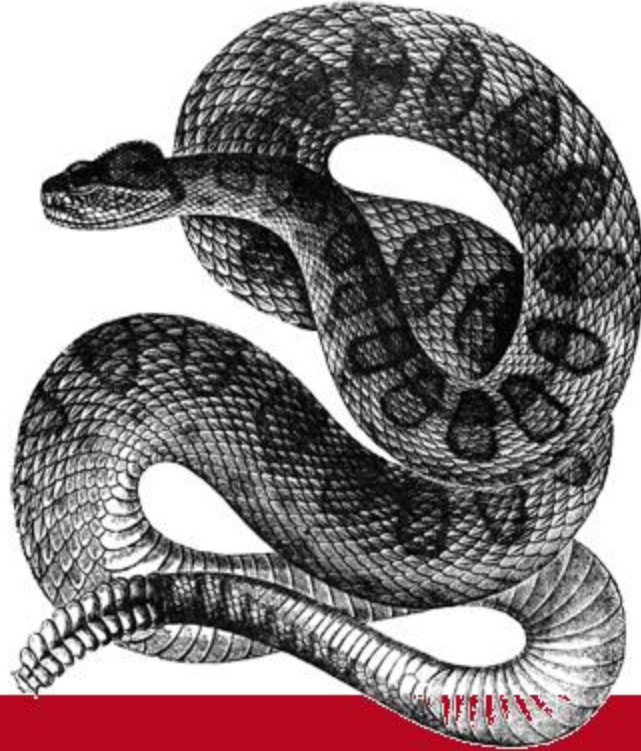
O RLY?

Joseph Z

whoami

- Current: Application Security Tester, E-commerce company
- Security Testing under Big 4 for clients like banks & pharma (2 years)
- Security Testing under a system integrator for clients like Govt (2 years)
- Programming for military (2 years)
- Twitter: @josephzengSG

How to avoid doing anything after a security test



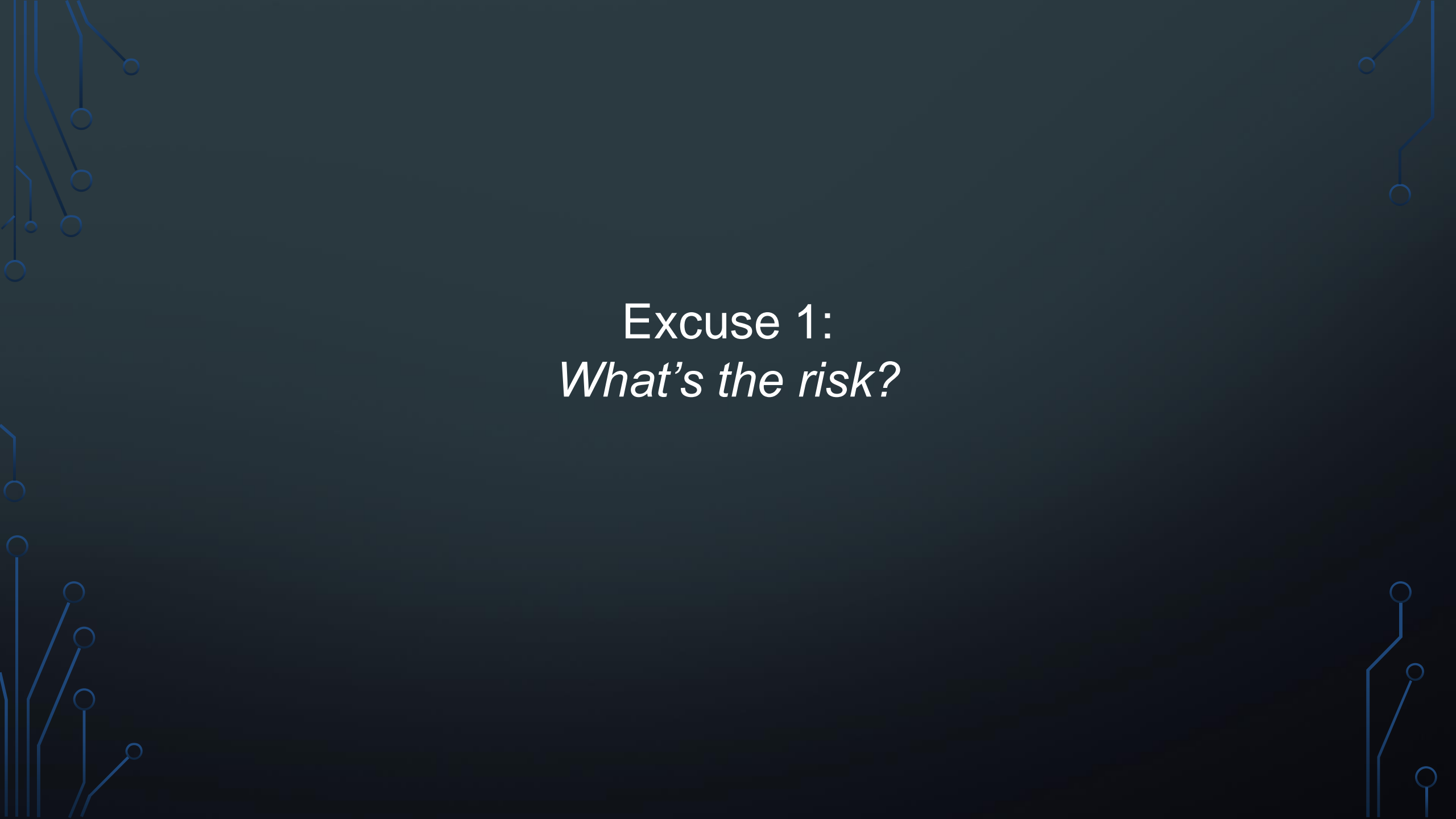
Excuses for developers

O RLY?

Project Manager

An abstract graphic of a circuit board pattern in a light blue color, consisting of various lines and circular nodes, is positioned on the left side of the slide.

As a security tester,
how do I get developers/sysadmins to fix the
issue?

The background is a dark blue gradient. In the corners, there are decorative elements resembling circuit board traces or neural network connections. These consist of thin, light blue lines that branch out and terminate in small circles, creating a symmetrical, abstract pattern in each corner.

Excuse 1:
What's the risk?

[1] What's the risk?

- Risk to business? Best practices?
- Trust - “Just must do it”

[1] What's the risk?

Reporting - which is most effective?


1. Long explanation of the vulnerability and business impact
2. Specific ways to fix the problem

[illegible]

[1] What's the risk?

Reporting – effective examples

- SQL Injection (technically, by test) vs proposed code changes (where & what)
- Different wording - "SQL injection" vs "prepared statements not used"

The background is a dark blue gradient. In the corners, there are decorative elements resembling circuit board traces or neural network connections. These consist of thin, light blue lines that branch out and terminate in small circles, creating a symmetrical, abstract pattern in each corner.

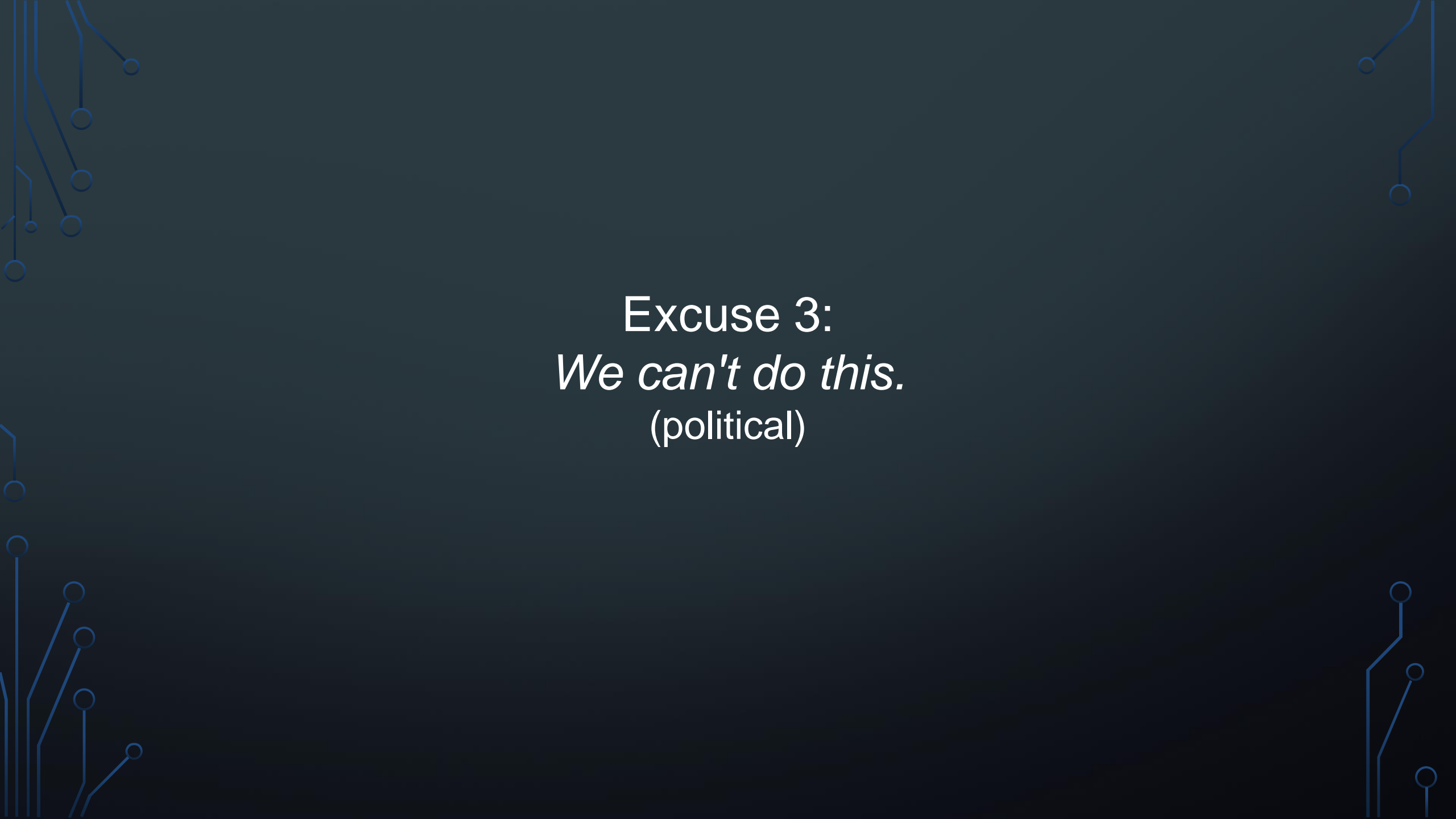
Excuse 2:
We can't do this.
(Technical)

[2] We can't do this (Technical)

- Legacy code / dependencies
- “Appliances”

[2] We can't do this (Technical)

- First, make sure that your “fix” really can work. e.g. Set up a virtual machine to test out your fix.
- Research their reason thoroughly. Is there another alternative?
- Document (and show that you will document) their responses. Test all assertions (e.g. there is no SSL version of an external resource)

The background is a dark blue gradient. In the corners, there are decorative elements resembling circuit board traces or neural network connections. These consist of thin, light blue lines that branch out and terminate in small circles, creating a symmetrical, abstract pattern in each corner.

Excuse 3:
We can't do this.
(political)

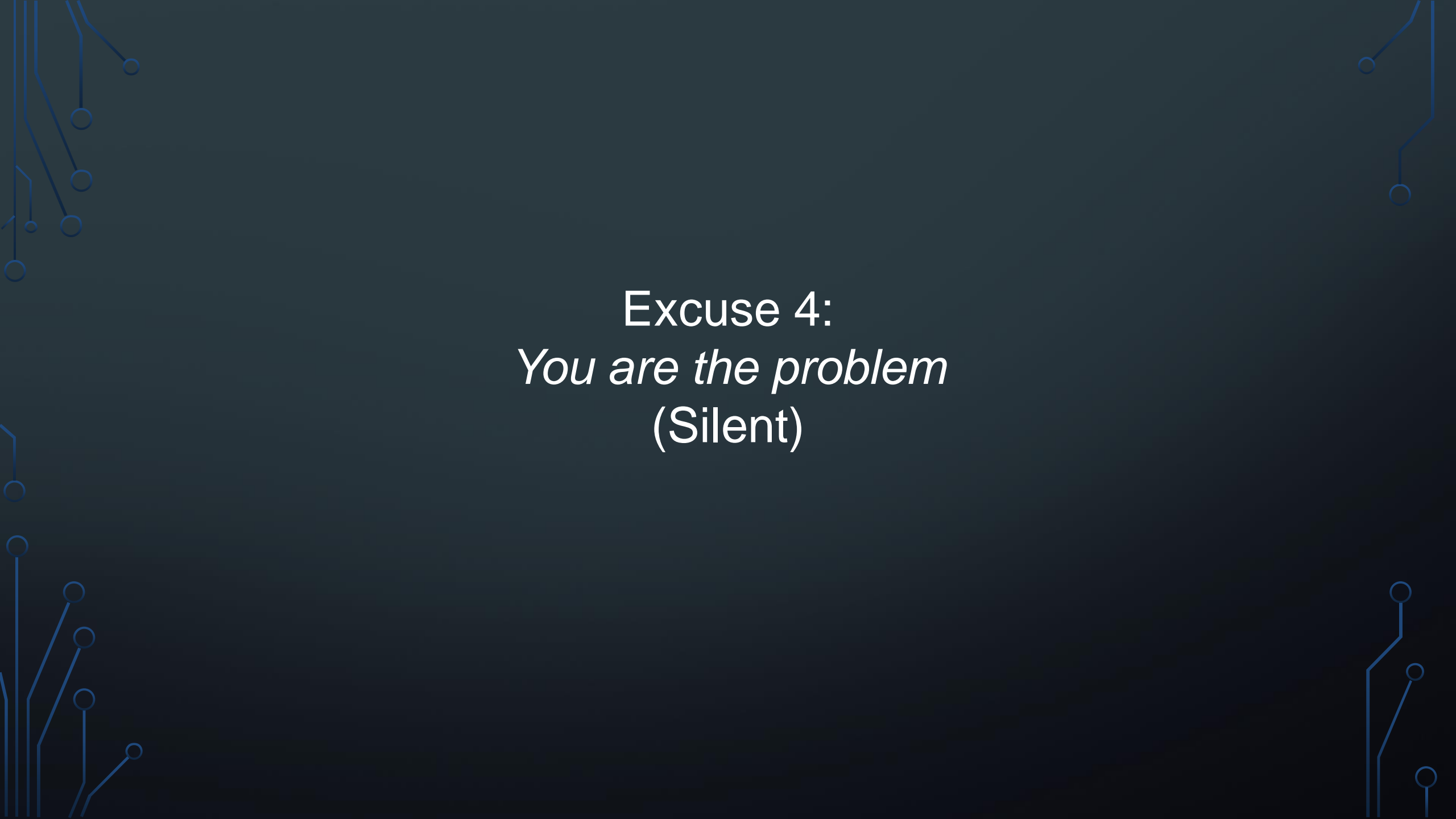
[3] We can't do this (political)

- "Your boss has approved this"
- "Need C-level approval"
- "This is out of scope"

[3] We can't do this (political)

- Check their assertions thoroughly.
- Document (and show that you will document) their responses.
- Be open and transparent! → Claims collapse on checking with the relevant parties (e.g. client, your boss)




The background is a dark blue gradient. In the corners, there are decorative elements resembling circuit board traces or neural network connections. These consist of thin, light blue lines that branch out and terminate in small circles, creating a symmetrical, abstract pattern in each corner.

Excuse 4:
You are the problem
(Silent)

[4] You are the problem

Good documentation

- Anything wrong? Nothing. What questions do you have about the issue?
Nothing.
- There was no debate about the problem, sysadmin reported fixed.
- Deleted finding from report


The background is a dark blue gradient. In the corners, there are decorative elements resembling circuit board traces or neural network connections. These consist of thin, light blue lines that branch out and terminate in small circles, creating a symmetrical, abstract pattern in each corner.



Excuse 5:
We cannot be 100%
(i.e. we cannot fix everything)



[5] We cannot be 100%



TechnologyProductsIndustriesNews

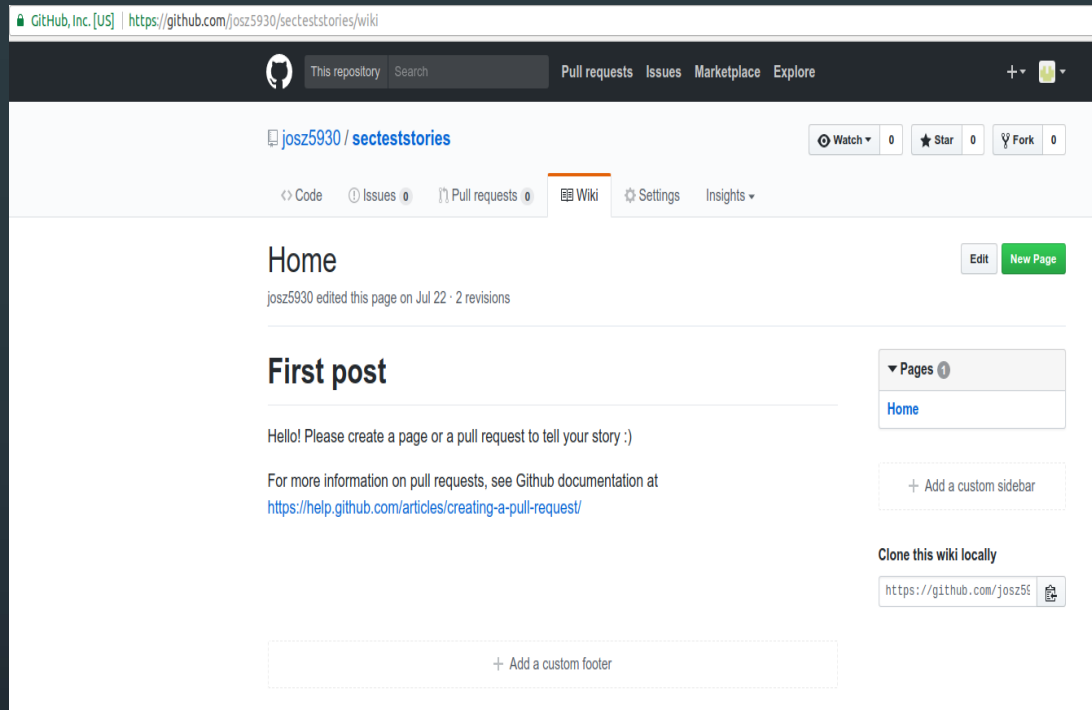
**CNN: A smart fish tank left a casino vulnerable to hackers**
Wednesday July 19, 2017 | Source: News
[Read more](#)



New
 We reviewed your report of HanyingFu WuRen MingTan.
 1 minute ago

Earlier
 You have memories to look back on today.
 4 hours ago

 We reviewed your report of Ciara Ashlie Mila.
 5 hours ago



Visit
wecannotbe100percent.top

No results for #secteststories

The term you entered did not bring up any results. You may have mistyped your term or your [Search setting](#) could be protecting you from some potentially sensitive content.

Tweet @josephzengSG