

 OWASP GLOBAL **AppSec**

VIE'26
NNA JUN
25-26

25

years
of open source security

OWASP GLOBAL AppSec

ViE'26
NNA JUN
25-26

25

years
of open source security

When Museums Get Hacked: OWASP Top 10 Lessons from Heists

José Carlos Chavez @ Okta

José Carlos Chávez

Security Software Engineer @ **Auth0/Okta**

- Open Source contributor and maintainer for 10+ years
- OWASP Coraza WAF co-leader
- Loving father of 2
- Mathematician in quarantine





What is the OWASP Top 10?

and why is it important?



One of the oldest
projects of OWASP
and the appsec
community



Awareness
document for
developers and
web application
security



Most critical
security risks for
web applications



It is updated every
4 years depending
on current
changes and data.
**Last update was
in Nov 2025**

A10: Mishandling of Exceptional Conditions

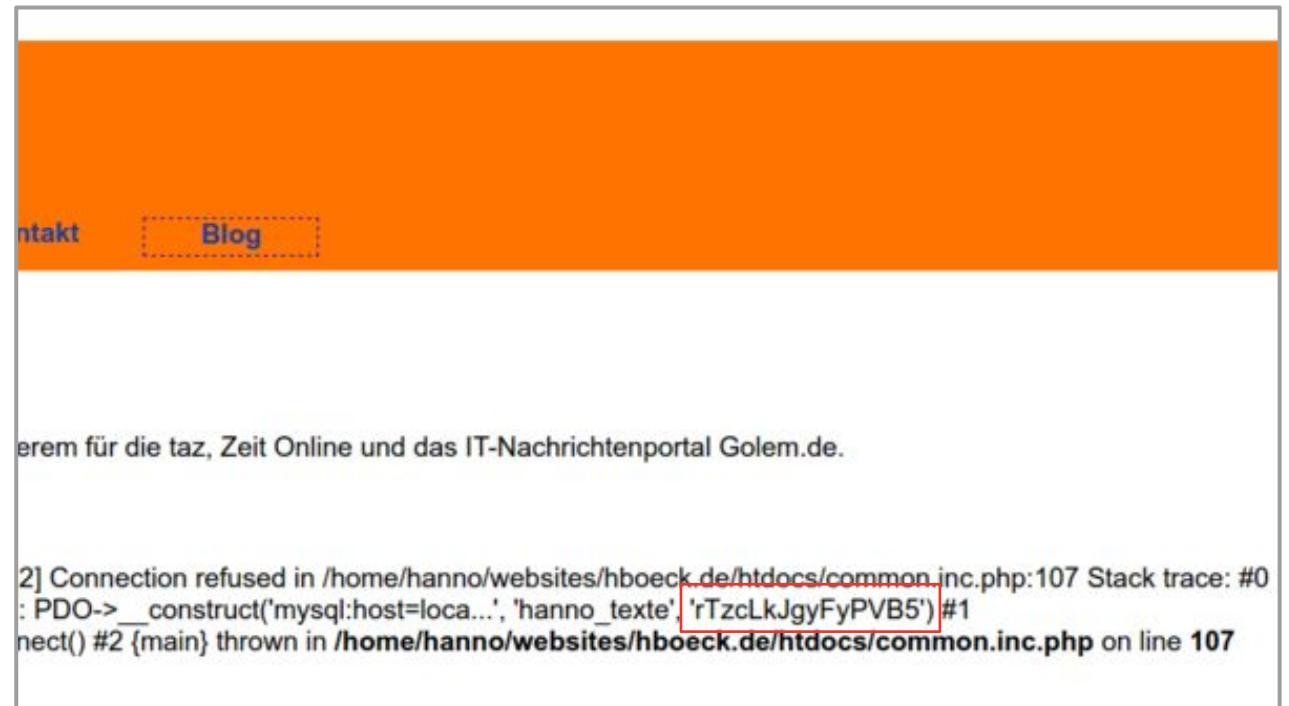


A10: Mishandling of Exceptional Conditions



Attacker

0x101 🍌



A10: Mishandling of Exceptional Conditions

Prevention



Handle every error at the point it occurs



Constrain the blast radius before an exception happens



Establish a global exception handler as the last line of defence

A09: Security Logging and Alerting Failures

☰ **CNN World** Africa Americas Asia Australia China Europe India Middle East More ▾

• Watch Listen 🔍

No security cameras covered Louvre balcony where thieves entered, c

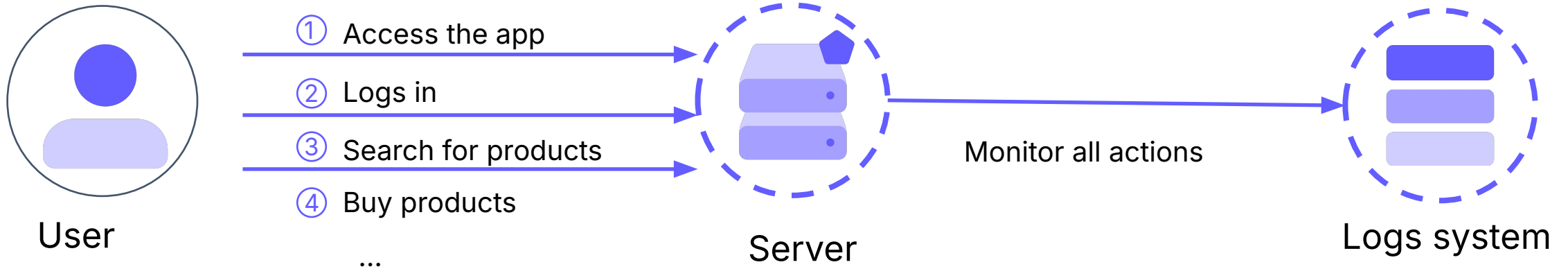
UPDATED OCT 23, 2025 ▾

By Pierre P Bairin, Catherine Nicholls, and  Hilary Whiteman

She said all alarms had functioned during the burglary, but admitted that security cameras did not adequately cover the thieves' point of entry. "The only camera installed is directed westward and therefore did not cover the balcony involved in the break-in," she said.



A09: Security Logging and Alerting Failures



①	Jun 10 06:06:23	GET /app 200	INFO User 1 access the application
②	Jun 10 06:07:03	POST /login 200	INFO User 1 logs in the application
	Jun 10 06:07:06	GET /app 302	DEBUG User redirect to application
③	Jun 10 06:07:23	GET /item?id=23 200	INFO User 1 list product 23
	Jun 10 06:07:43	GET /stock?d=23 200	DEBUG User see stock of product 23
	Jun 10 06:10:23	POST /buy?id=23 200	INFO User 1 buys product id 23
④	Jun 10 06:10:33	GET /purchase?id=3 302	INFO User 1 confirmed purchase 3

A09: Security Logging and Alerting Failures

Prevention



Make sure all security-relevant events are recorded



Make logs actionable, not just archival

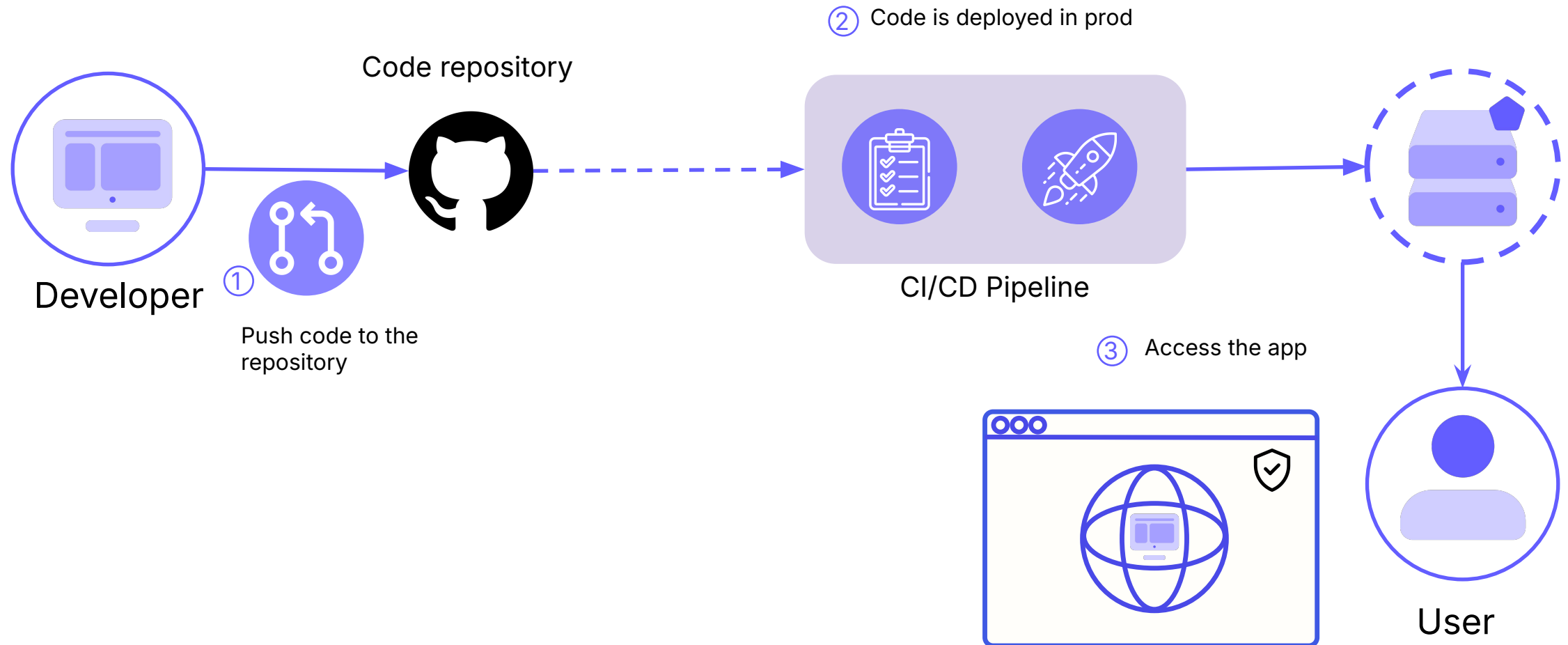


Verify that logs are immutable, reliable, and cannot be manipulated

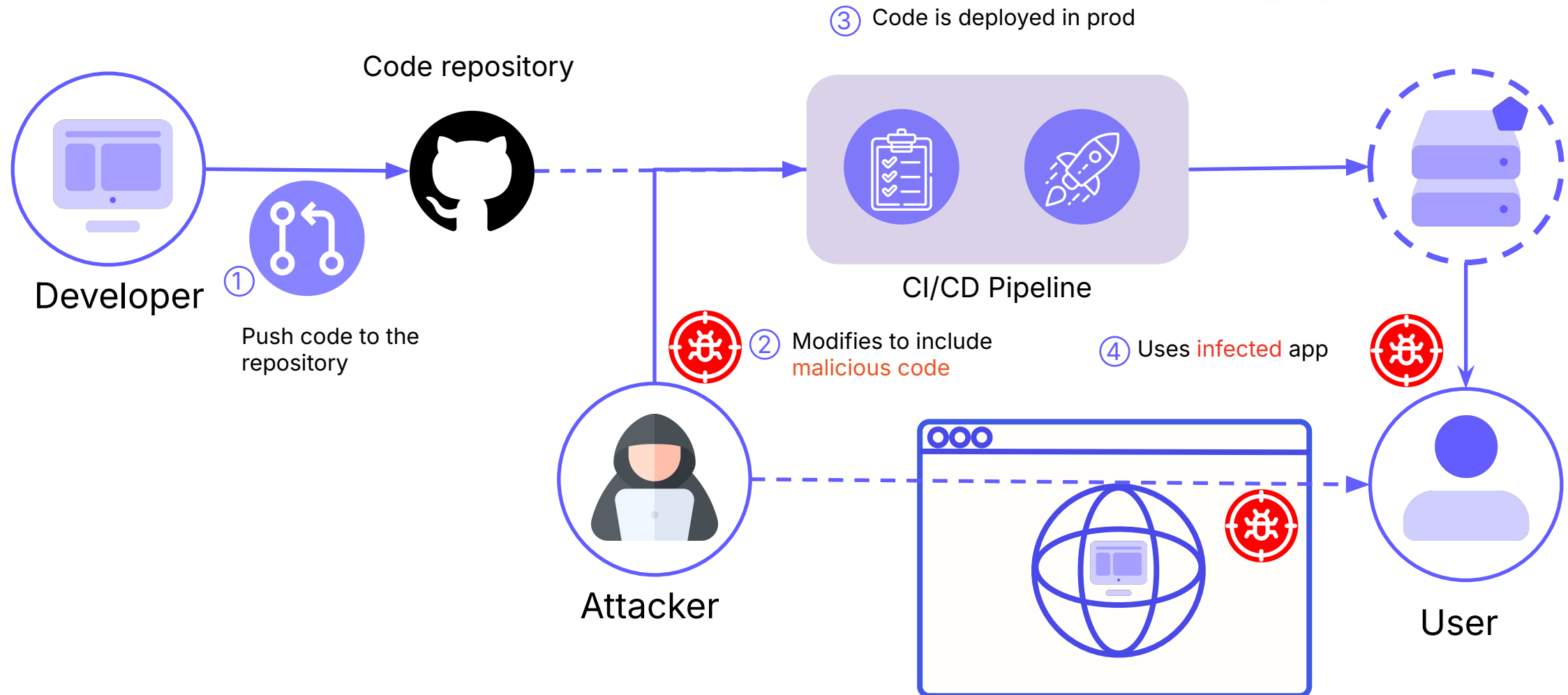
A08: Software and Data Integrity Failures



A08: Software and Data Integrity Failures



A08: Software and Data Integrity Failures



A08: Software and Data Integrity Failures

Prevention



Use mechanisms such as hash functions to ensure data integrity

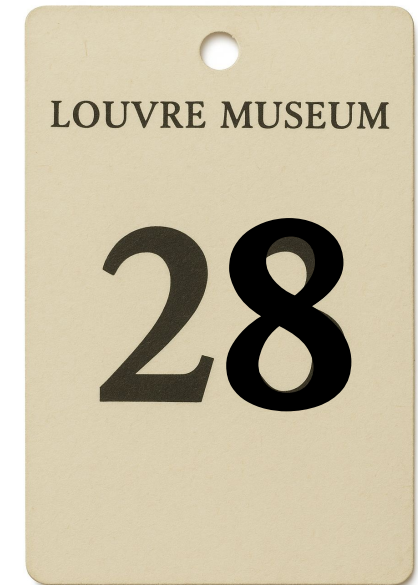


Build an internal inventory of components/software/libraries

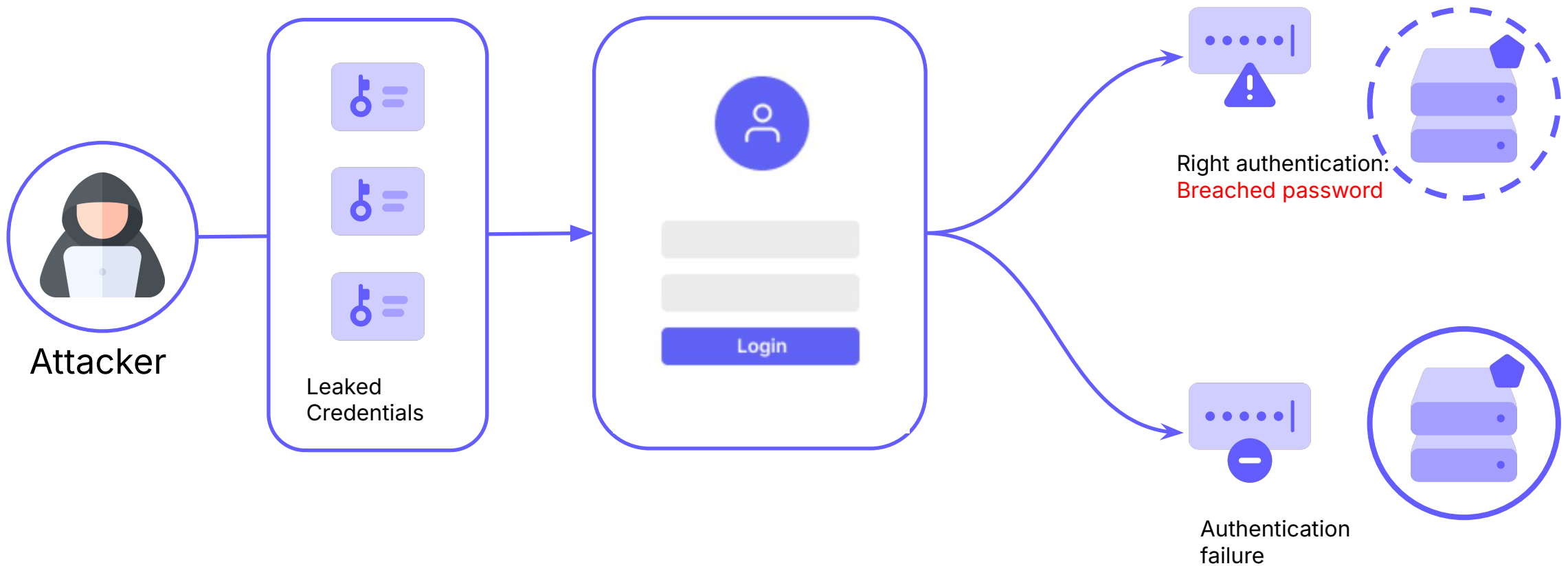


Check and verify that those libraries/software are reliable and secure

A07: Authentication Failures

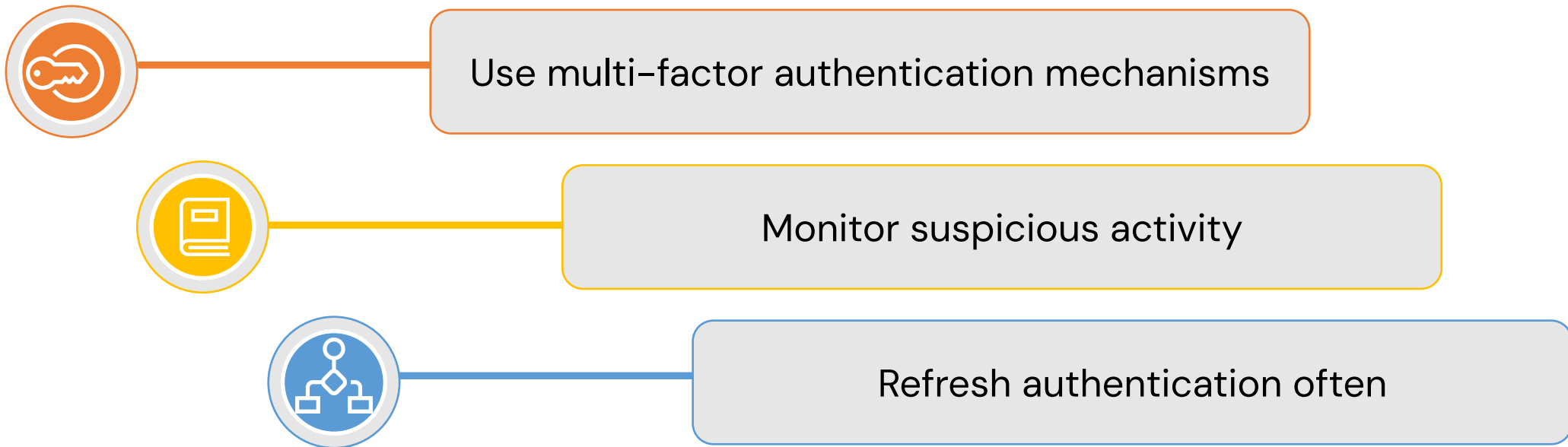


A07: Authentication Failures



A07: Authentication Failures

Prevention



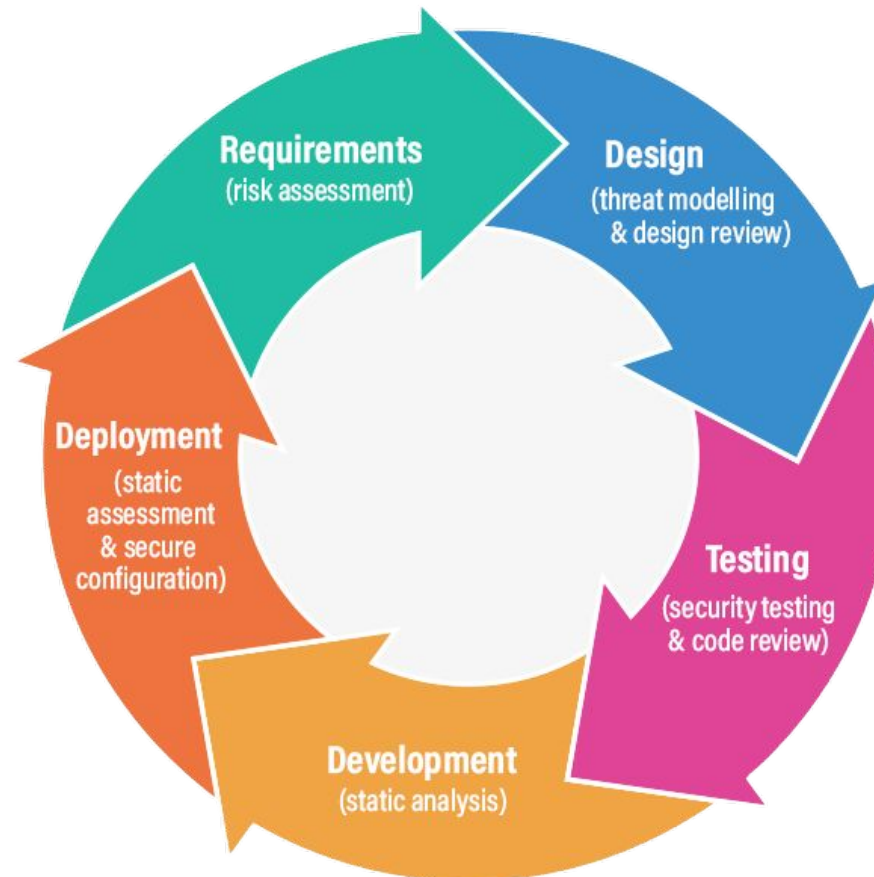
A06: Insecure Design



Des Cars said Wednesday the security system inside the Apollo Gallery “worked perfectly” – but that it was designed several years ago to protect against the greatest risks of that time. For example, the high-security display cases that housed the jewels were designed to withstand bullets.

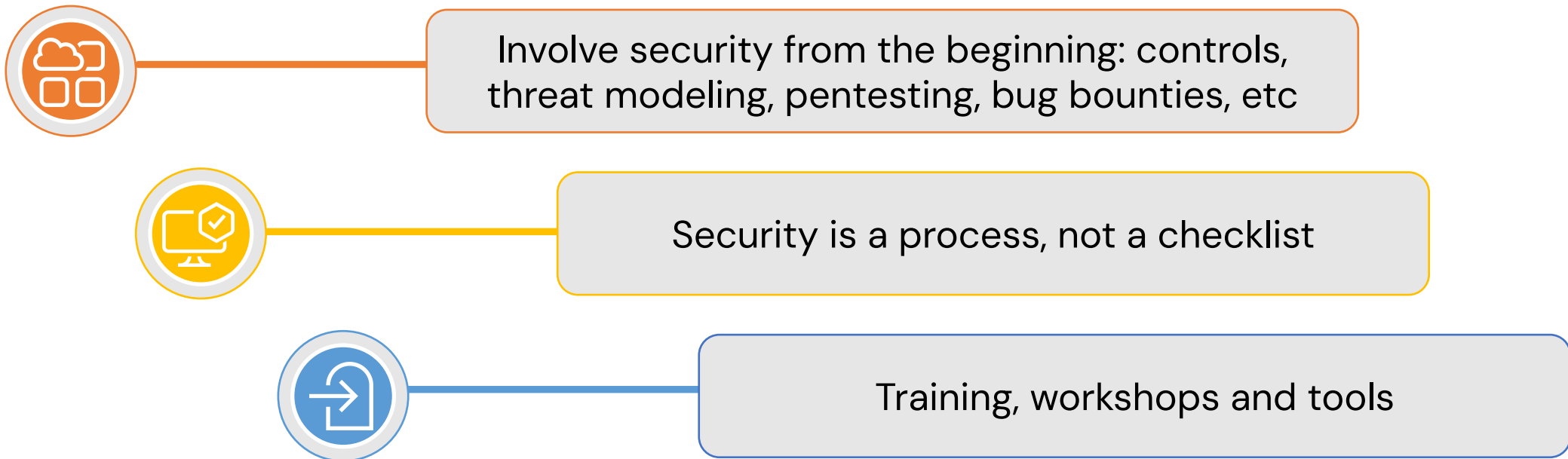
“At the time, this was the dominant modus operandi for this type of attack, for precious objects, jewelry, attacks in jewelry stores,” des Cars said. “That’s what the Louvre is protecting itself against.”

A06: Insecure Design



A06: Insecure Design

Prevention



A05: Injection



FAMOUS PICTURE VANISHES.

“LA JOCONDE” STOLEN FROM
THE PARIS LOUVRE.

TWO ARRESTS.

PARIS POLICE HUNT FOR
MAN IN A BLOUSE.

“La Joconde,” one of the most famous pictures in the world, and Leonardo da Vinci’s masterpiece, vanished from the Louvre on Monday, and not a trace of its whereabouts has been found.

Paris has been thrown into a ferment of excitement over the disappearance of this priceless art treasure, and the entire detective force is being employed to solve the mystery. Every inch of the Louvre has been searched without success, though the frame and protecting glass were found hidden away in a dark corner.

The picture is so well known that any attempt on the part of the thief to dispose of it would mean instant detection. Meanwhile, the negligence of the officials concerned is the subject of general censure.

Interest is centred on two men arrested near Bordeaux, and on the hunt in Paris for a man who was seen at the Louvre at the spot where the frame of the picture was found.

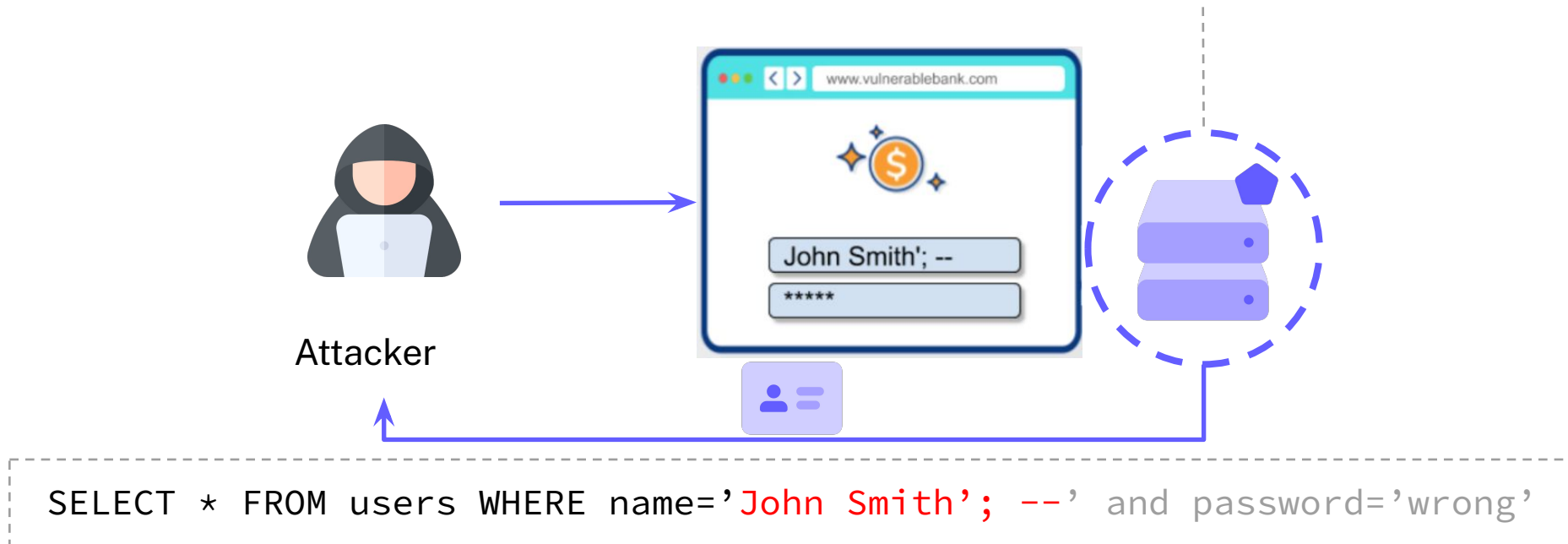
LATEST CLUES.

The latest development in the search for the great picture is the arrest near Bordeaux of two men on suspicion of being concerned in the theft. They are Erhardt

THE LOUVRE’S LOST TREASURE.



A05: Injection



A05: Injection

Prevention



Sanitize and validate input data: never trust the client



Deal with structured messages vs raw data



Multiple layers of protection

A04: Cryptographic Failures



Enigma code machine stolen in Bletchley raid

By Michael Smith

AN ENIGMA cipher machine that formed the centre-piece of the Bletchley Park museum commemorating the work of Britain's wartime code-breakers has been stolen.

The machine, valued at £100,000, is very rare because it came from the Abwehr, Germany's military intelligence. It was stolen from a glass cabinet overnight on Friday or early on Saturday, which was an open day at the site in Milton Keynes, Bucks.

Thames Valley police said the thieves may have had their attention drawn to the value of the machine by a recent visit to Bletchley Park by Mick Jagger and the actress Kate Winslet. They were gathering material for



Missing: a cipher machine

the new film *Enigma*, based on Robert Harris's book about the code-breakers' attempts to break the Nazi cipher.

Christine Large, a Bletchley Park Trust director, said: "This is a devastating theft and has cast a dark cloud over Bletchley Park. It is a

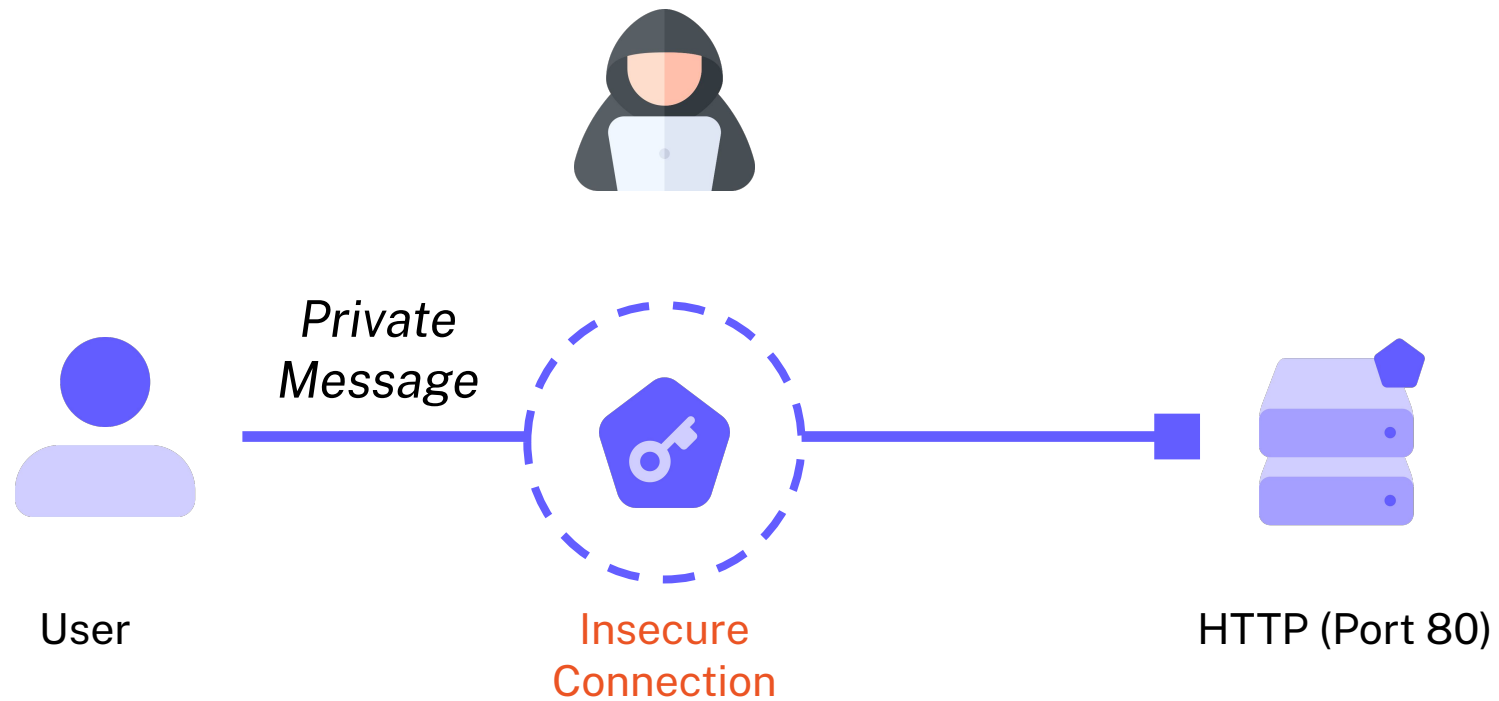
unique piece of history and we are just hoping for its safe return."

She said the house was protected by 24-hour security guards and comprehensive alarm systems, but security would be improved immediately.

The site, once top secret and known as Station X, was home to teams of mathematicians, linguists and chess champions selected for their potential ability to break German, Japanese and Italian codes and ciphers. By the end of the war 10,000 people were working there.

The machine, similar in appearance to a typewriter, had been developed by a German engineer. Its electrical circuits changed each time a key was struck, leading Berlin to believe that the code was unbreakable.

A04: Cryptographic Failures



A04: Cryptographic Failures

Prevention



Less is more: store and transfer only what is necessary

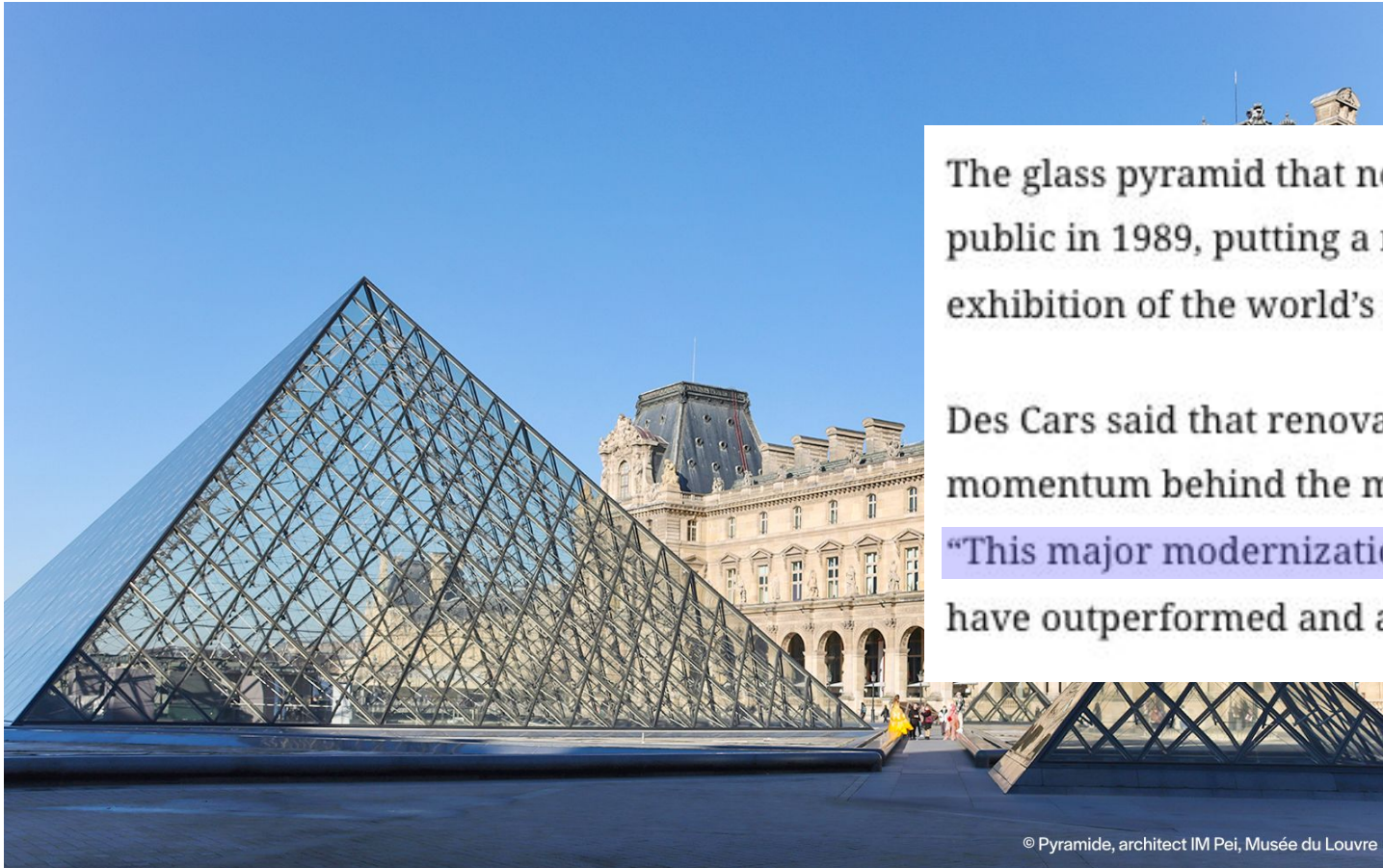


Categorize data to choose an appropriate security level



Use reliable encryption algorithms

A03: Software Supply Chain Failures

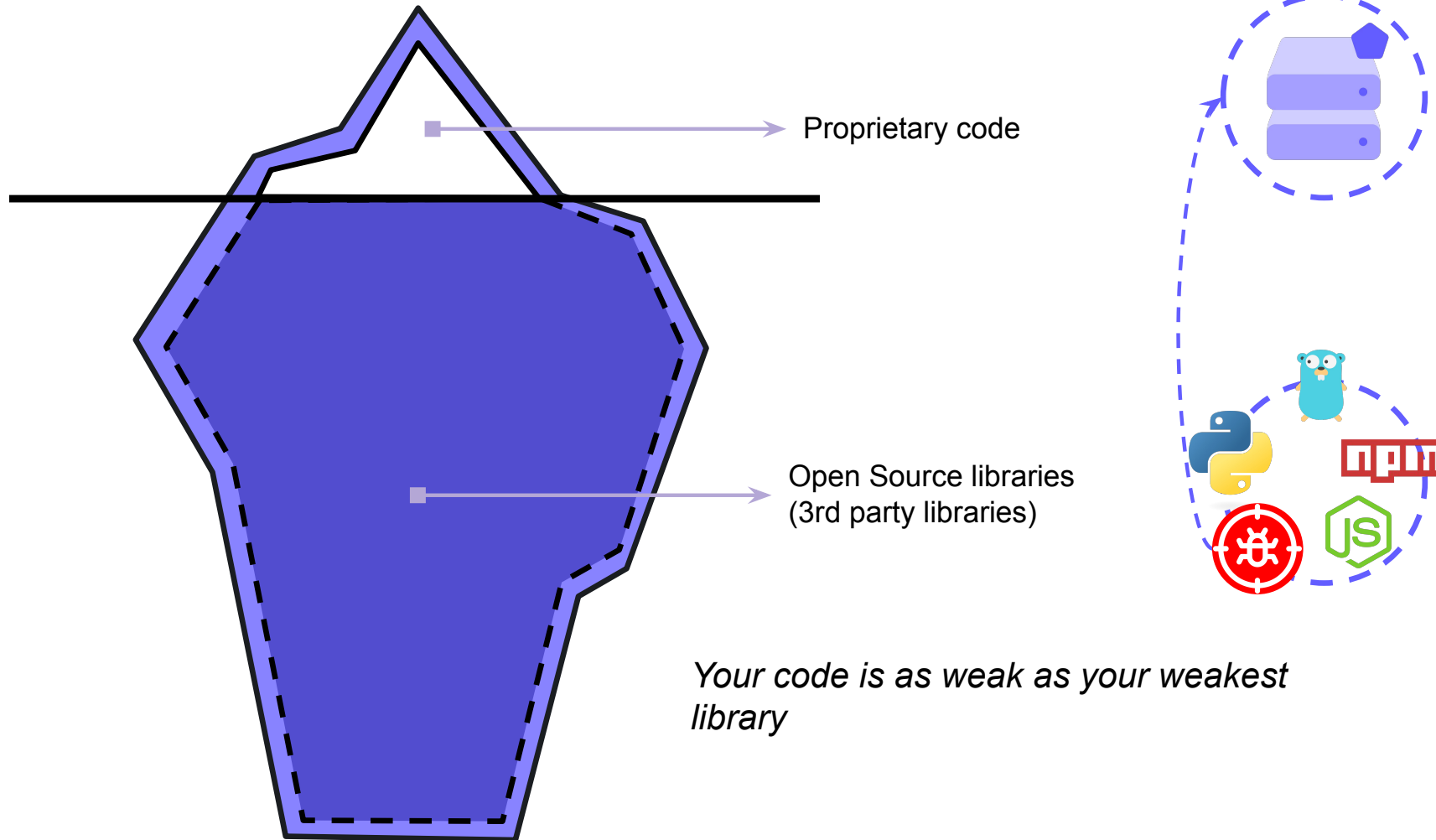


The glass pyramid that now forms the entrance to the museum opened to the public in 1989, putting a modern face on a storied institution known for its exhibition of the world's finest art.

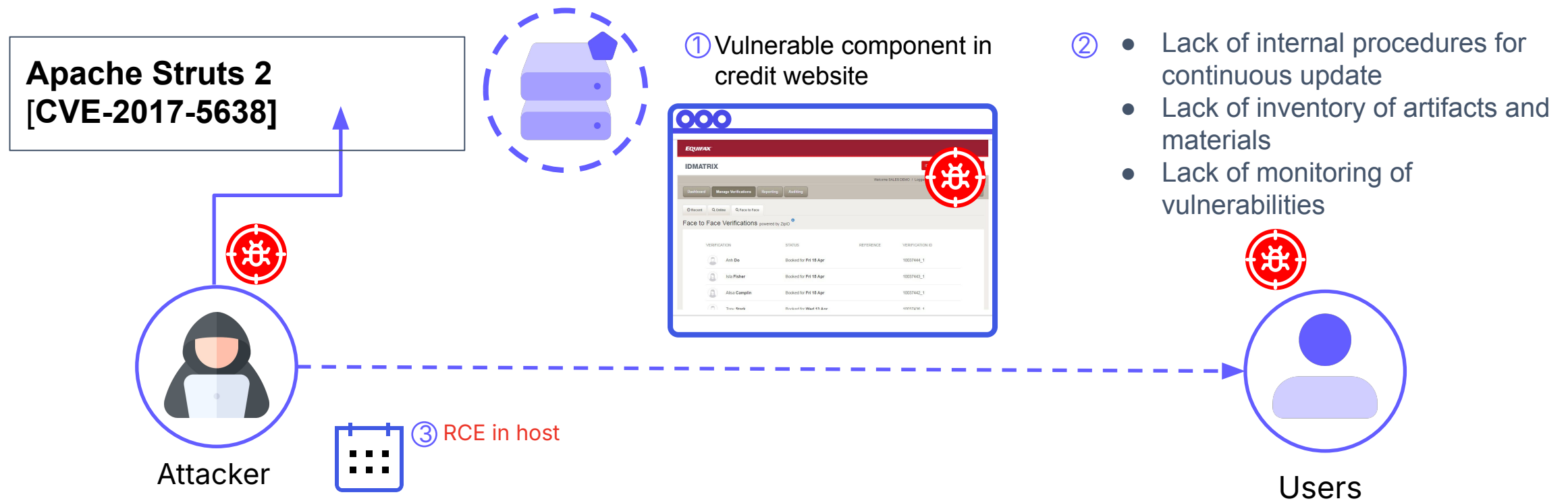
Des Cars said that renovation project may have created an illusion of momentum behind the museum being fully modernized. However, she said: "This major modernization project is now 40 years old, with facilities that have outperformed and are at the end of their tether."

© Pyramide, architect IM Pei, Musée du Louvre

A03: Software Supply Chain Failures



A03: Software Supply Chain Failures



A03: Software Supply Chain Failures

Prevention



Ensure that only the necessary components are used



Evaluate the components, the sources, and verify that they are safe for use



Maintain an up-to-date inventory of components with vulnerability alerts

A02: Security Misconfiguration

Password to Louvre's video surveillance system was 'Louvre', according to employee

At least one of the thieves remains at large, French prosecutors say.

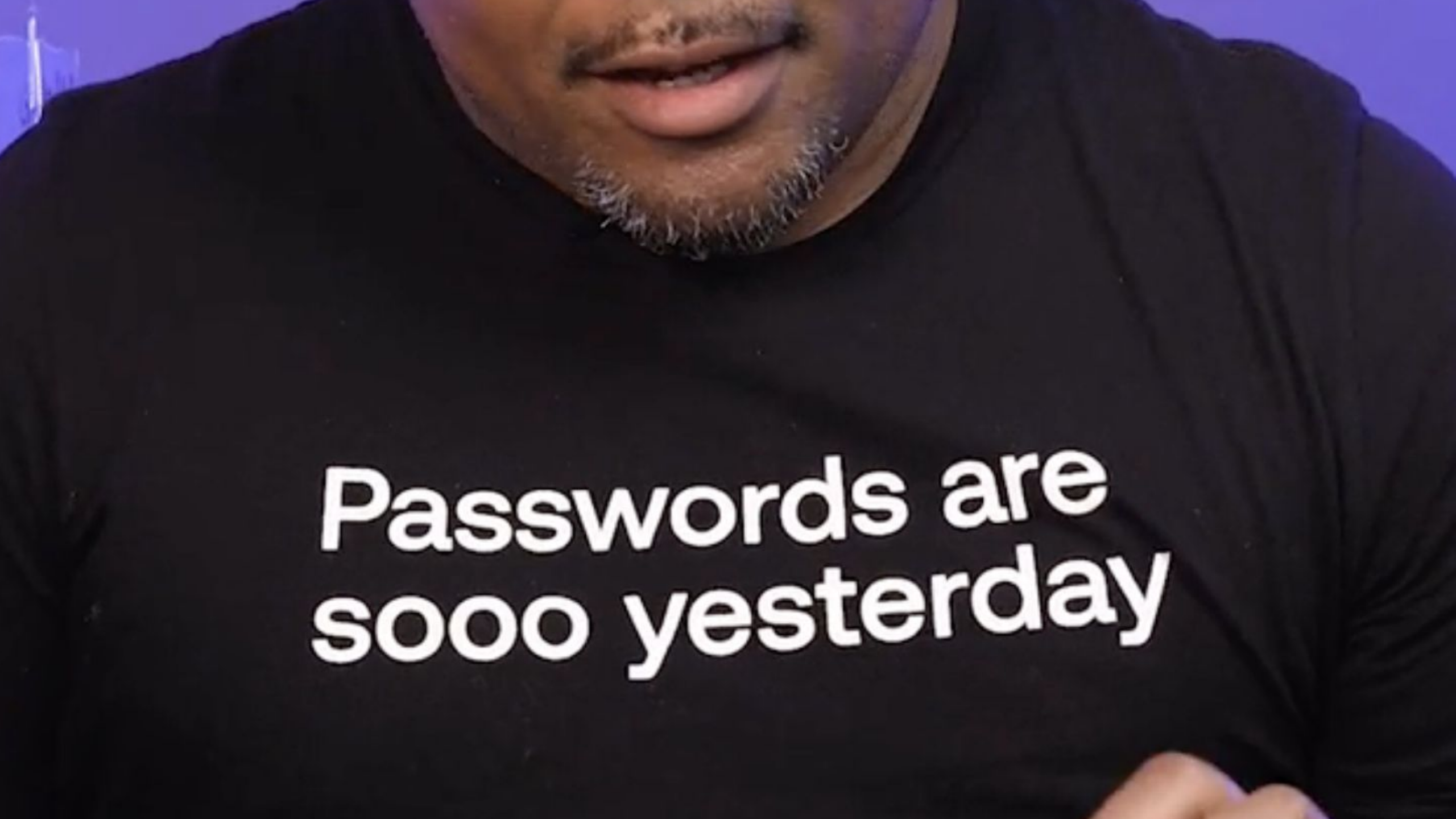
By [Mason Leath](#)

Video by [Lilia Geho](#)

November 6, 2025, 1:38 AM

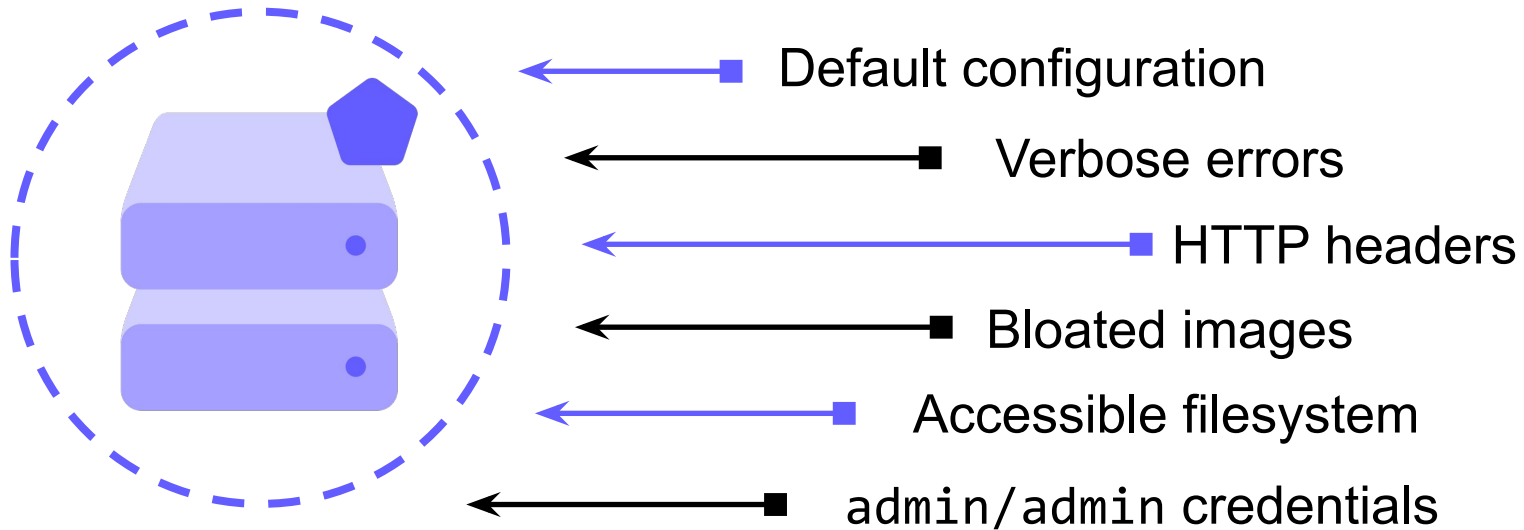


Image Source: ABC News

A close-up shot of a man's face and upper torso. He has a short beard and is wearing a black t-shirt. The text 'Passwords are sooo yesterday' is printed in white on the t-shirt. The background is a solid blue color.

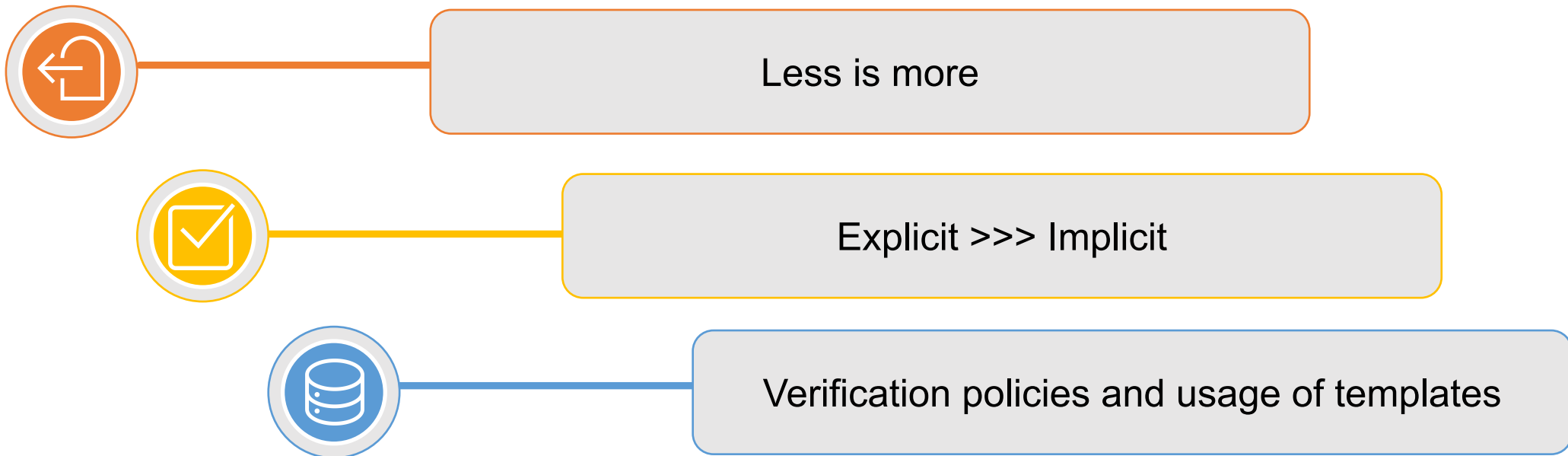
**Passwords are
sooo yesterday**

A02: Security Misconfiguration

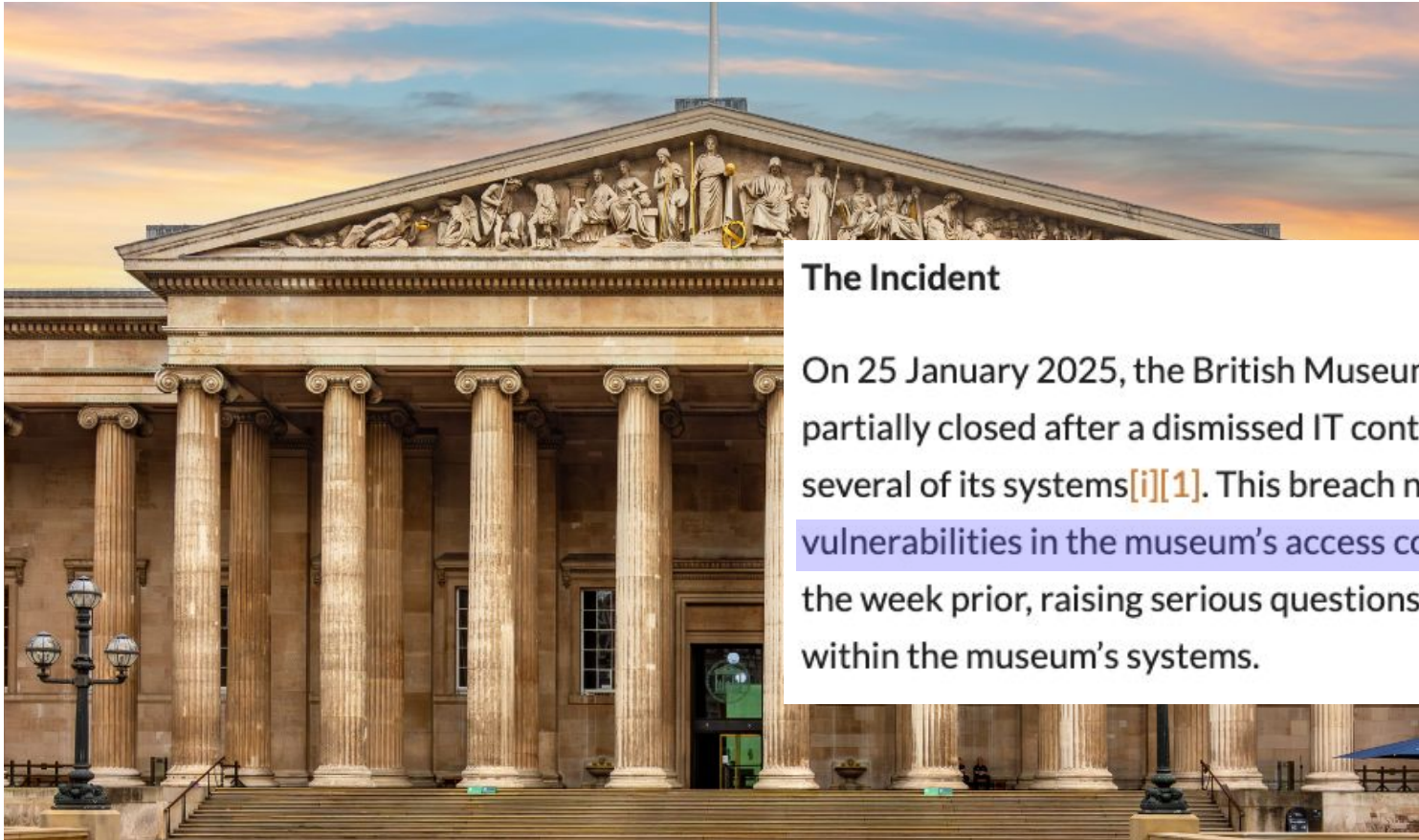


A02: Security Misconfiguration

Prevention



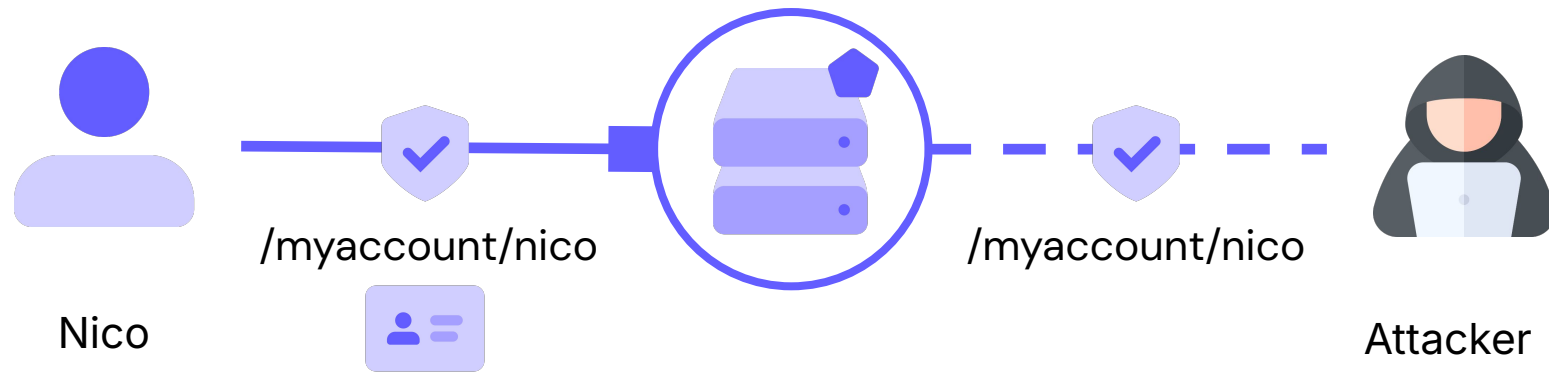
A01: Broken access control



The Incident

On 25 January 2025, the British Museum, one of the UK's most popular tourist attractions, was partially closed after a dismissed IT contractor allegedly broke into the building and shut down several of its systems[i][1]. This breach not only disrupted operations but also exposed vulnerabilities in the museum's access control protocols. Notably, the contractor had been dismissed the week prior, raising serious questions about why they still had physical and technical access within the museum's systems.

A01: Broken access control



A01: Broken access control

Prevention



Less is more: fewer permits, more granular



Contextualized access controls



Have an up-to-date, documented, and visible
permission map

CONCLUSIONS

1. The OWASP Top 10 is a snapshot of reality, not a comprehensive checklist.
2. Vulnerabilities evolve, but root causes remain the same.
3. Security is a continuous journey.



VIENNA'26 JUN
25-26

25 years
of open source security

THANK YOU!