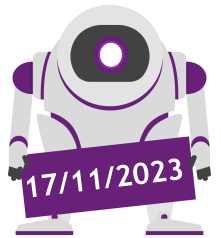
2023

Secure Development for Muggles

Raúl Piracés Alastuey
Diego Rodríguez Varela



Sponsors

NTT DATA

encamina
PIENSA EN COLORES

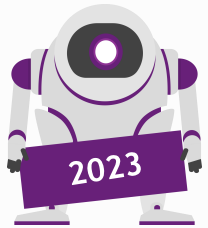
plain concepts

intelequia

Verne
TECHNOLOGY GROUP

TOKIOTA

ilitia



#netcoreconf

Agenda

01 **The State of Security Today**

02 **Most Common Security Errors**

03 **Tips & Tooling**

Main Objective

Reducing significantly the **attack surface** of our applications with the right **mindset**, **tips**, **tooling** and a **minimal effort**...

The State of Security Today

110,294

(up 22.3% on 2021)

Citizens and companies

Source: INCIBE

The State of Security Today

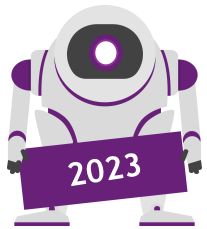
Security numbers

- 91.8% orgs compromised
- 85% of applications with security issues
- A 1:100 relation for security team vs developers
- Allocate 11.9% of IT budget to security

Impact

- Ransomware attacks cost $750,000 average
- GDPR fines issued in Spain are almost €15M (€59M acc.)
- 15.128 complaints in 2022 and raising (AEPD)

Sources: CyberEdge Group (CDR Report), Sophos State of Ransomware Report, Hiscox Report, enforcementtracker.com, GitHub, Verizon



The State of Security Today

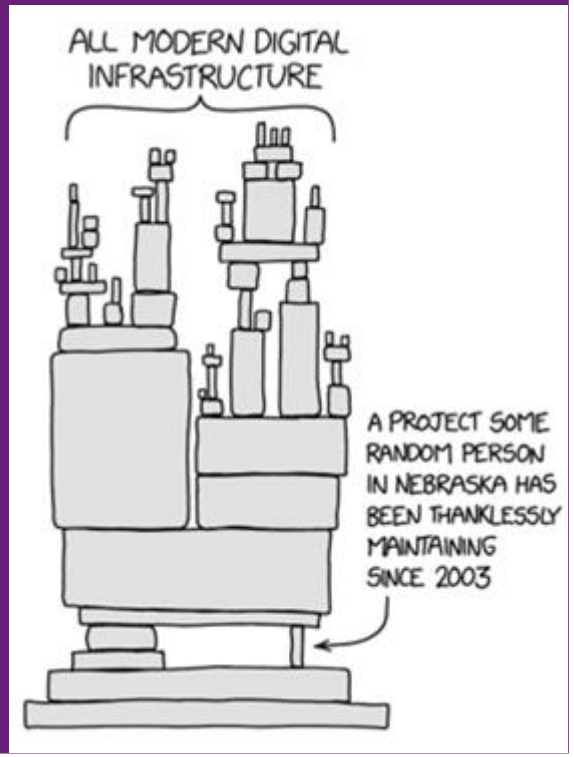
"The internet Relies on People Working for Free…"

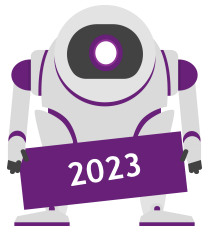
cURL
- 1 main developer (recent CVEs)

OpenSSL
- Heartbleed vulnerability

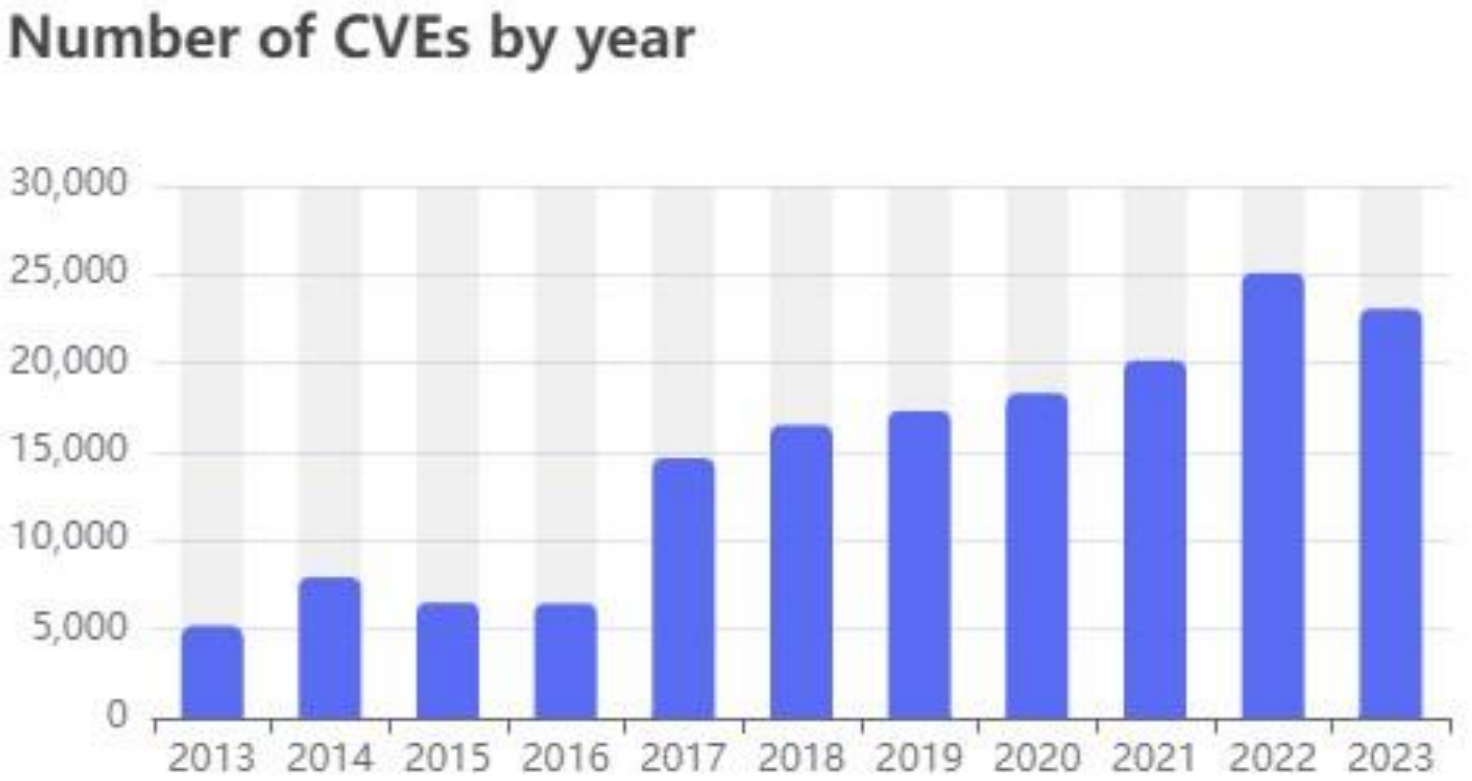
Log4j
- Log4Shell vulnerability

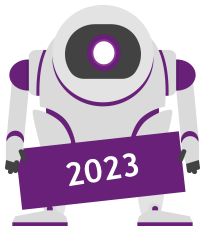
faker.js, colors.js, core.js, left-pad…



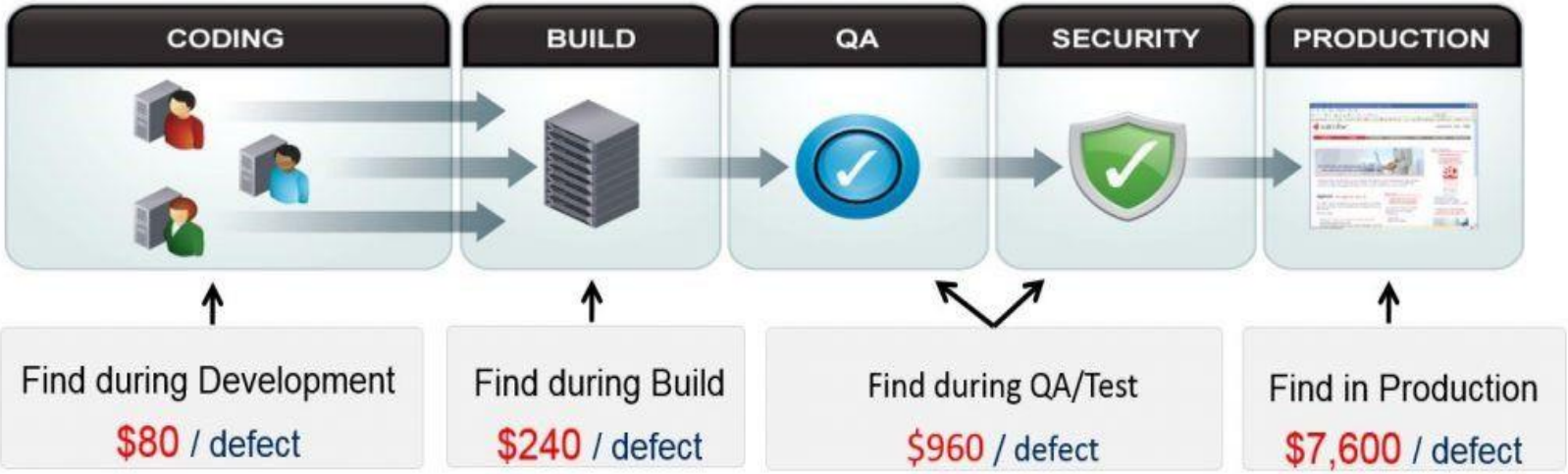


More lines of code == More potential vulns.

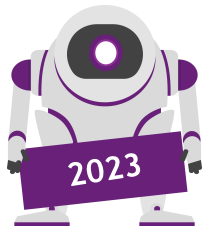




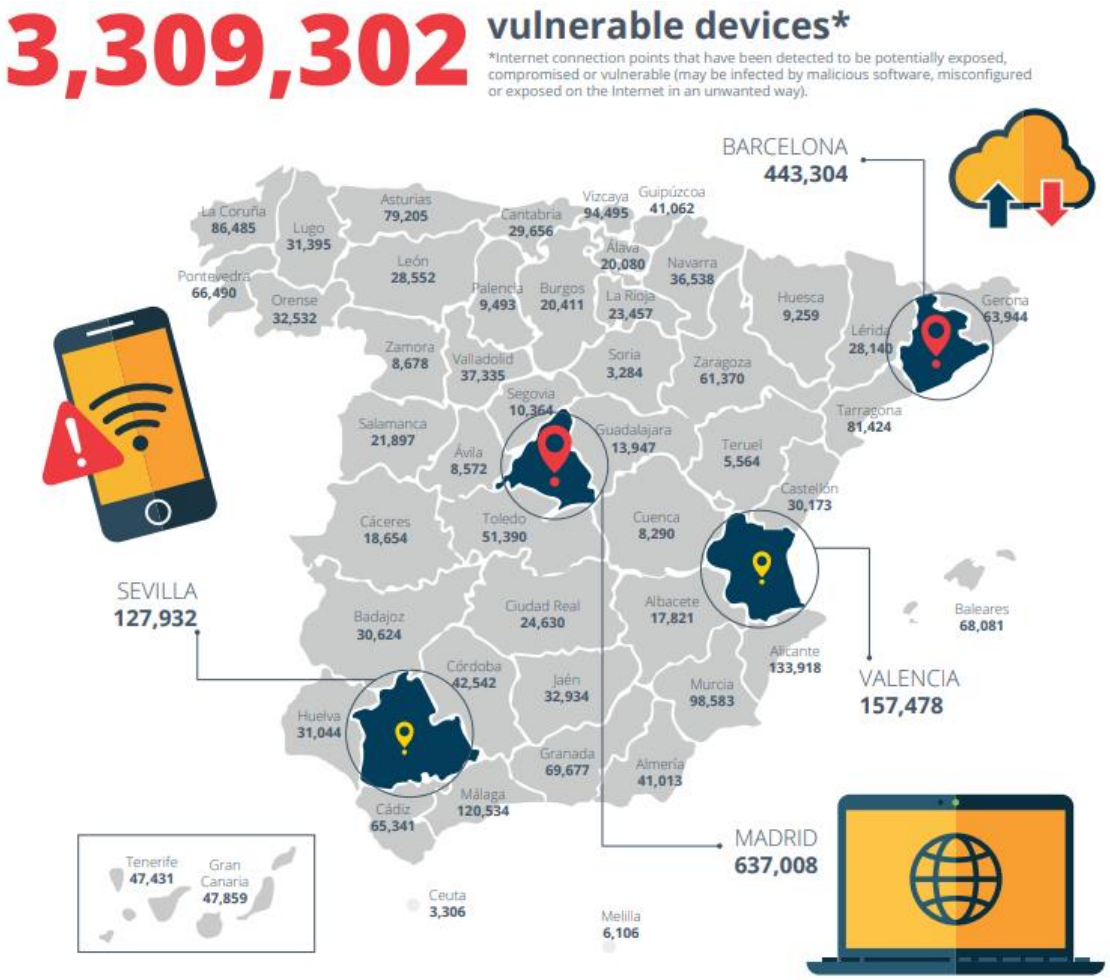
Everyone wants to shift left security…



Source: IBM (2010)



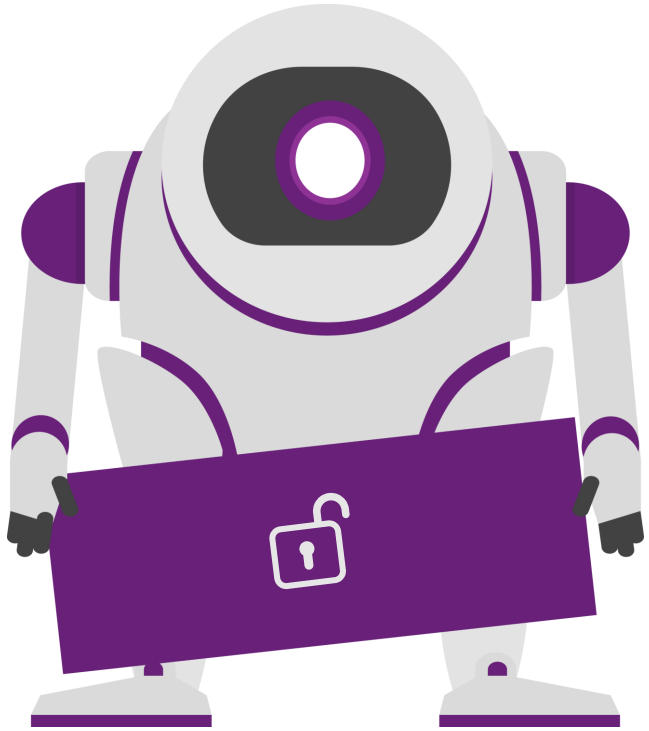
Common Errors

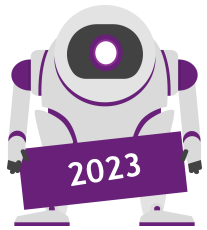


Source: INCIBE

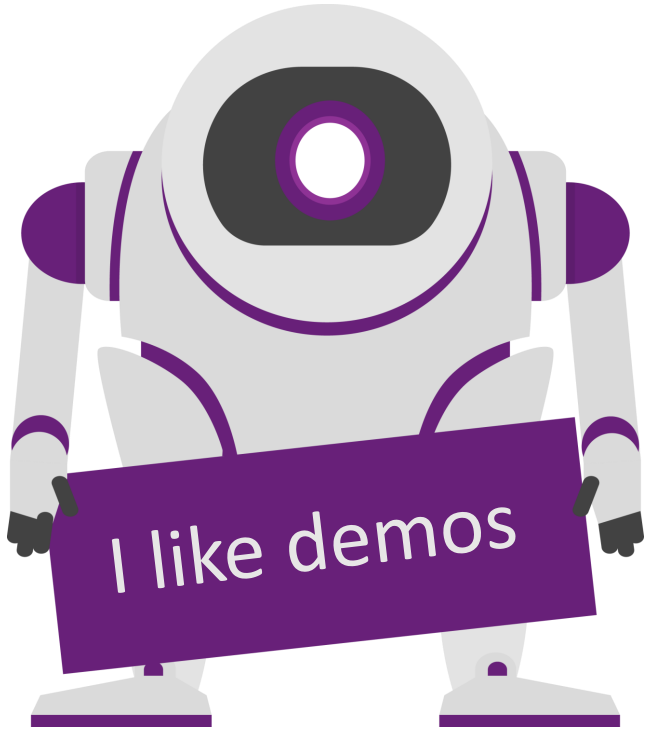
Broken Access Control / Top 1

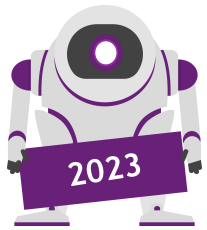
- Sequential Ids (enumeration-based attacks)
- Access to other roles, users... (guards / authorization / inverse proxy)
- Frontend vs Backend validation
  - Authentication
  - Authorization





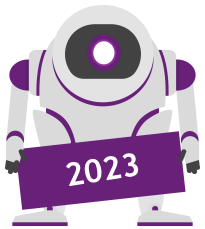
Demo time!



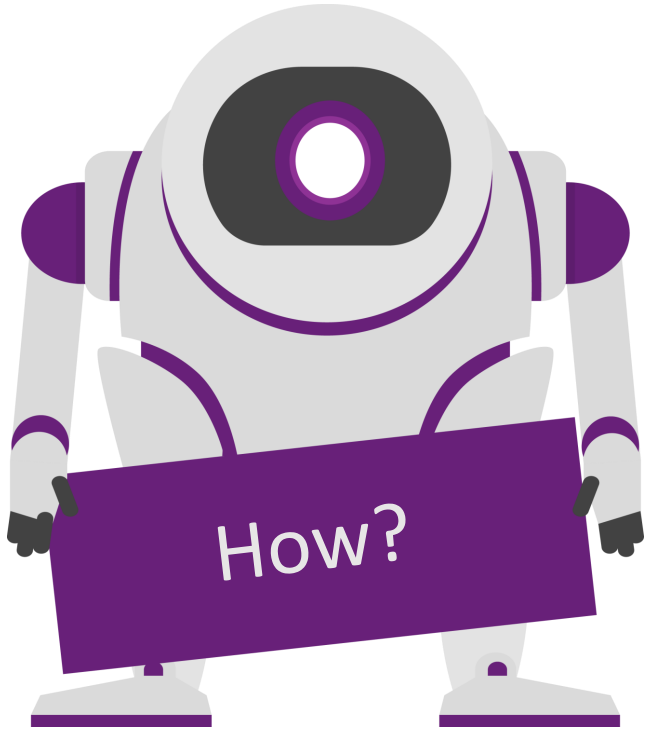


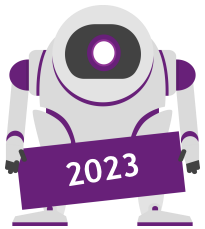
HTTP Headers: CSP, CORS, HSTS

- Frame ancestors (anti-clickjacking, phishing attacks)
- CORS, making sure we respond to legit origins
- HSTS, ensuring connections through HTTPS
- Transition to CSP: CSP Report Only



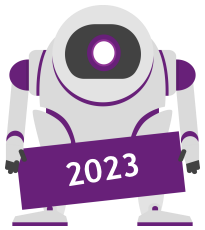
Demo time!





CSRF, SSRF, Injections...

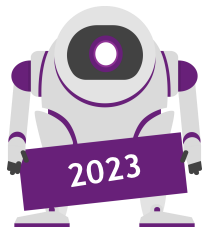
- **Always validate** user input (both in frontend and backend)
- Perform **sanitization**
- **Parse** everything
- Take care with regex...
- Use your framework's support for these kind of security threats



Demo time!


KEEP OUT
OR ENTER.
I'M A SIGN, NOT A COP

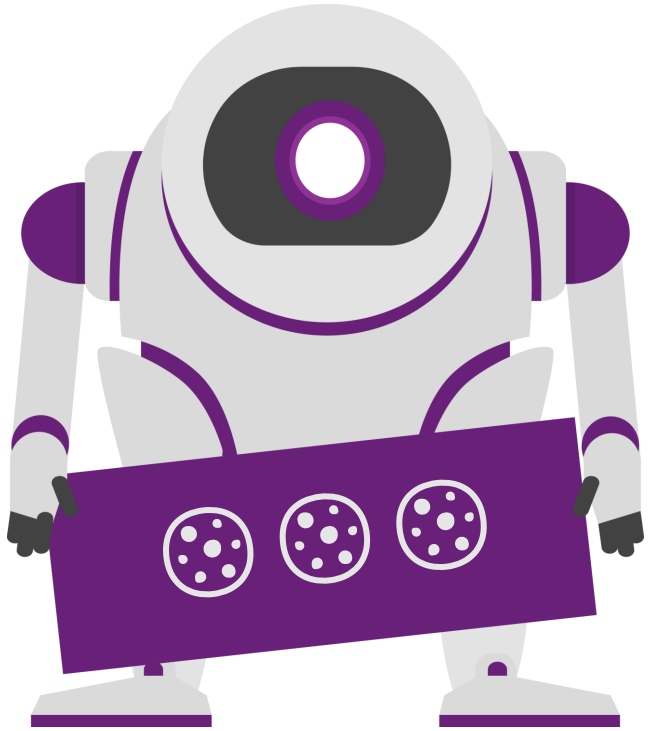

Let's protect ourselves


2023

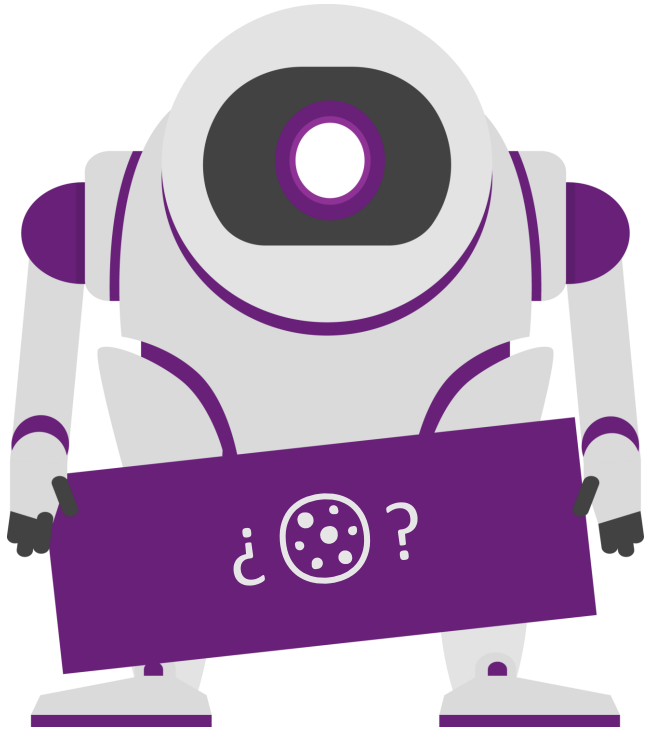
Cookies

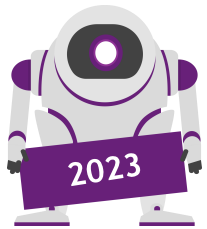
URL http://www.netcoreconf.com/	Same Site	Same Origin
http://www.netcoreconf.com:80	☑	☑
http://netcoreconf.com	☑	✗
http://www.netcoreconf.com:8080	☑	✗
http://test.netcoreconf.com	☑	✗
https://www.netcoreconf.com	✗	✗
http://www.dotnetconfspain.es	✗	✗

- SameSite, Strict or Lax?
- Secure?
- HTTPOnly?
- **Do NOT allow to manage cookies via JavaScript**



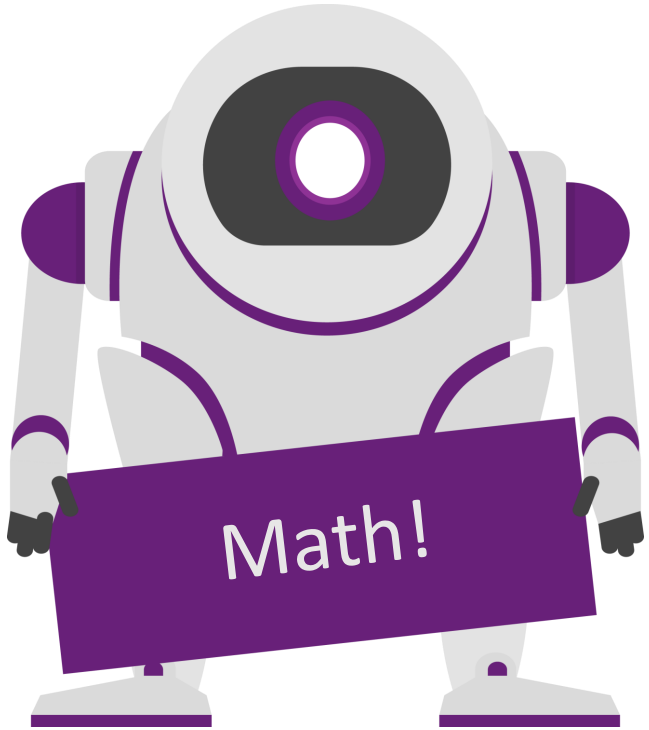
Demo time!



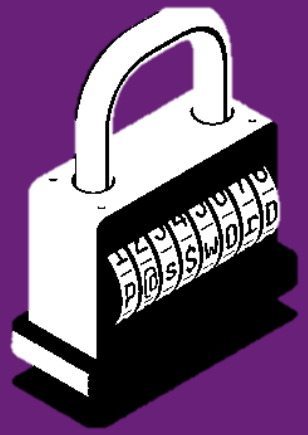


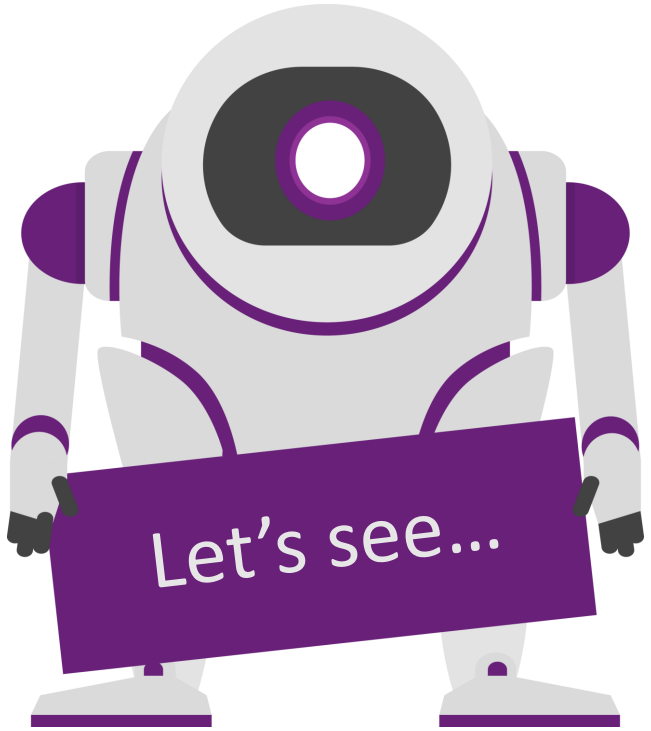
Cryptography bad practices

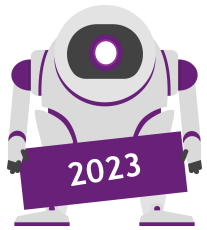
- **Do NOT use custom cryptography solutions…**
- Breaking weak keys in seconds…
- Key strength (How?)
- Salts + pepper
- Verify the certificate chain: SSL Labs, testssl.sh, sslscan, sslyze



Demo time!

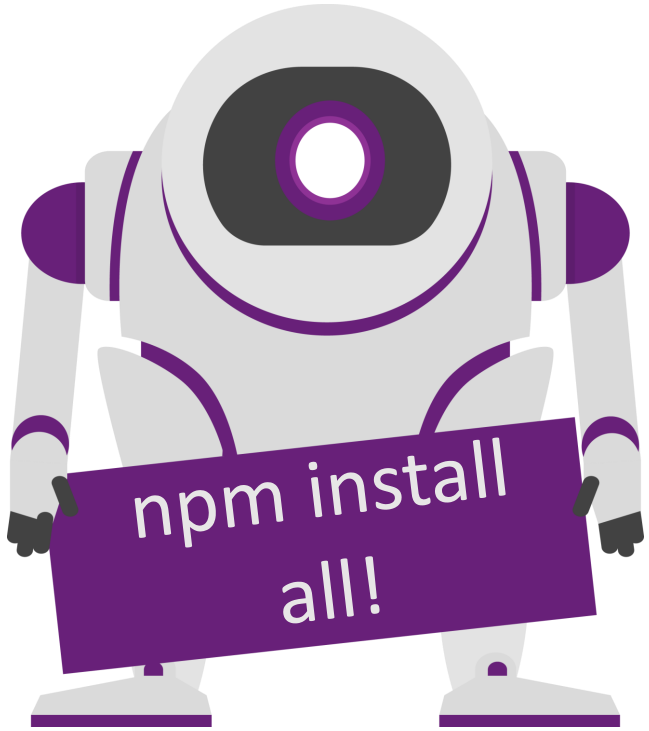


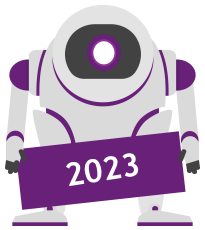




Outdated components

- Keep your dependencies updated!
- Audit the dependencies & keep track of them
- Are your dependencies actively maintained?
- Do they respond to security issues?
- Supply chain security

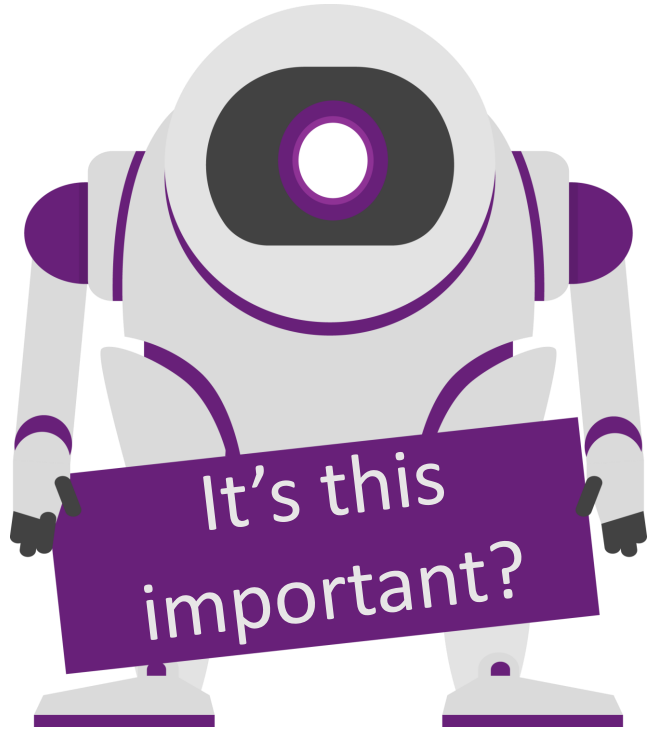


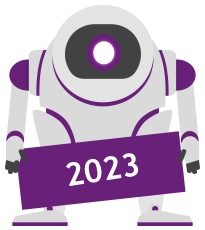


Vulnerabilities report

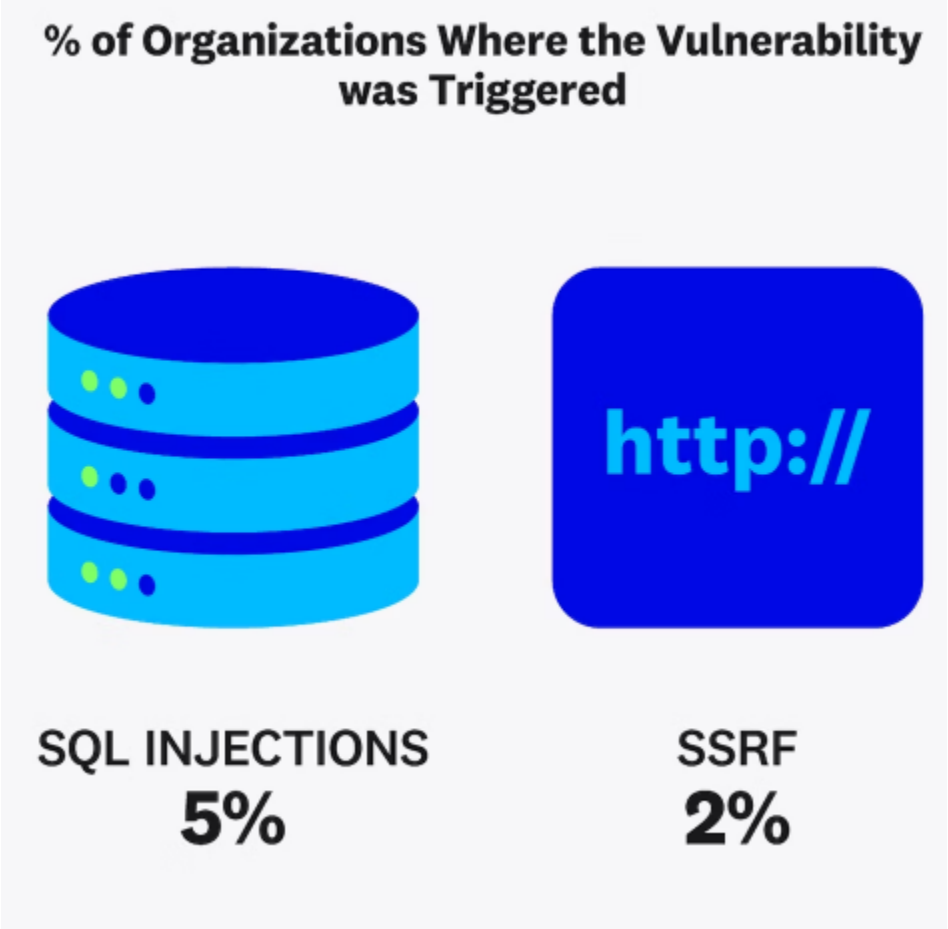
```
36 vulnerabilities (2 low, 11 moderate, 20 high, 3 critical)

To address issues that do not require attention, run:
  npm audit fix

To address all issues (including breaking changes), run:
  npm audit fix --force
```

```
> dotnet list package --vulnerable --include-transitive

The following sources were used:
   https://api.nuget.org/v3/index.json

Project `                    .Host` has the following vulnerable packages
   [net6.0]:
   Top-level Package              Requested   Resolved   Severity   Advisory URL
   > Apache.Avro                  1.10.2      1.10.2     High       https://github.com/advisories/GHSA-868x-rg4c-cjqg
   > Auth0.AuthenticationApi      6.5.3       6.5.3      High       https://github.com/advisories/GHSA-c9cg-q8r2-xvjq
   > Azure.Storage.Blobs          12.9.1      12.9.1     Moderate   https://github.com/advisories/GHSA-64x4-9hc6-r2h6
   > Azure.Storage.Queues         12.9.0      12.9.0     Moderate   https://github.com/advisories/GHSA-64x4-9hc6-r2h6

   Transitive Package                                   Resolved   Severity   Advisory URL

   > Microsoft.AspNetCore.Authentication.JwtBearer      3.1.2      Moderate   https://github.com/advisories/GHSA-q7cg-43mg-qp69
   > NuGet.Common                                       6.3.1      High       https://github.com/advisories/GHSA-6qmf-mmc7-6c2p
   > NuGet.Protocol                                     6.3.1      High       https://github.com/advisories/GHSA-6qmf-mmc7-6c2p
   > System.Security.Cryptography.Pkcs                  6.0.1      High       https://github.com/advisories/GHSA-555c-2p6r-68mm
   > System.Text.RegularExpressions                     4.3.0      High       https://github.com/advisories/GHSA-cmhx-cq75-c4mj
```





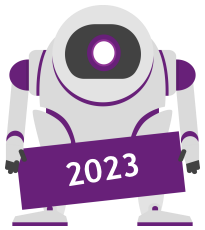
Extra!



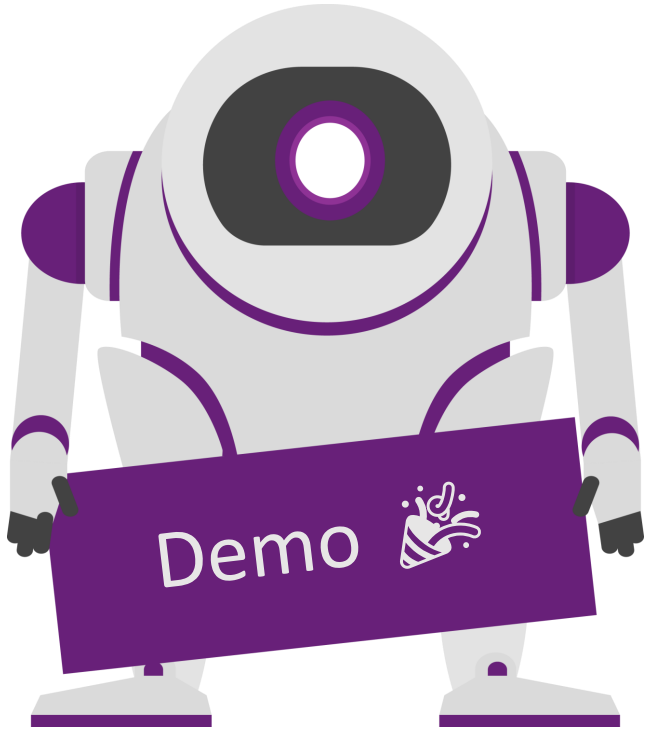
Source: Datadog

Shitf left security

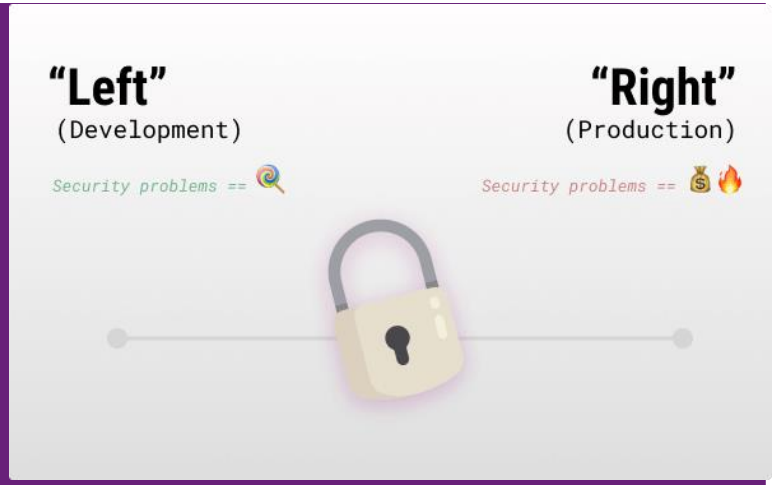
- **Minimum privilege** principle
- Understand/Evaluate your **attack surface**
  - Threat modelling can help
- Test for all cases (authentication/authorization)
- Do **NOT** assume anything
  - Defense in depth
- Review secondary applications, third party code
- Protect resources, variables and secrets
- Do NOT issue commands directly to the operating system



Demo time!



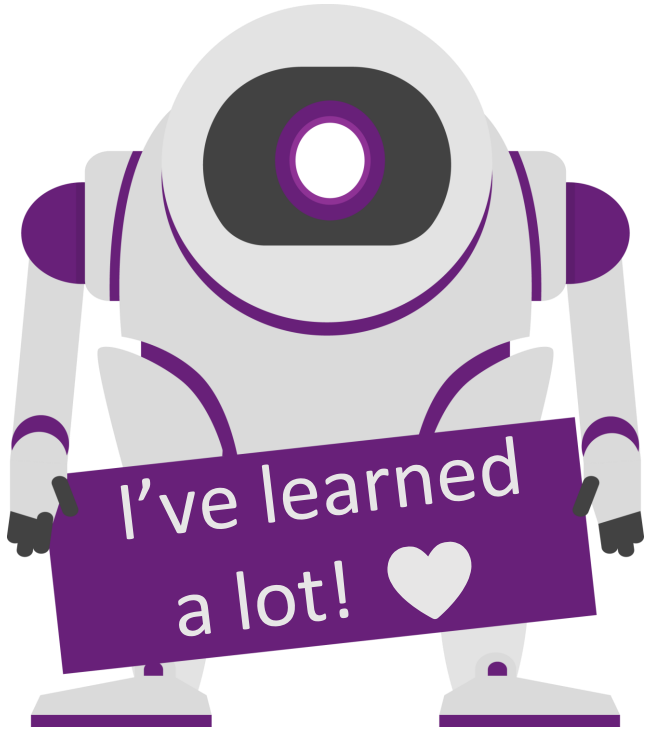
Conclusions

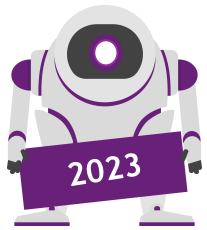


- Current security "performance"
- Most common security problems
- Tips & tools to protect ourselves

Note

- There is no "silver bullet" against attacks
- "Shifting Security Left" is a mindset, not a tool





Sponsors

NTT DATA

encamina
PIENSA EN COLORES

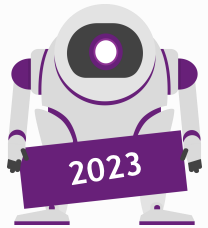
plain concepts

intelequia

Verne
TECHNOLOGY GROUP

TOKIOTA

ilitia



#netcoreconf

More information:
info@netcoreconf.com
@Netcoreconf

Visit on:
netcoreconf.com

@diegorosec

@piraces_