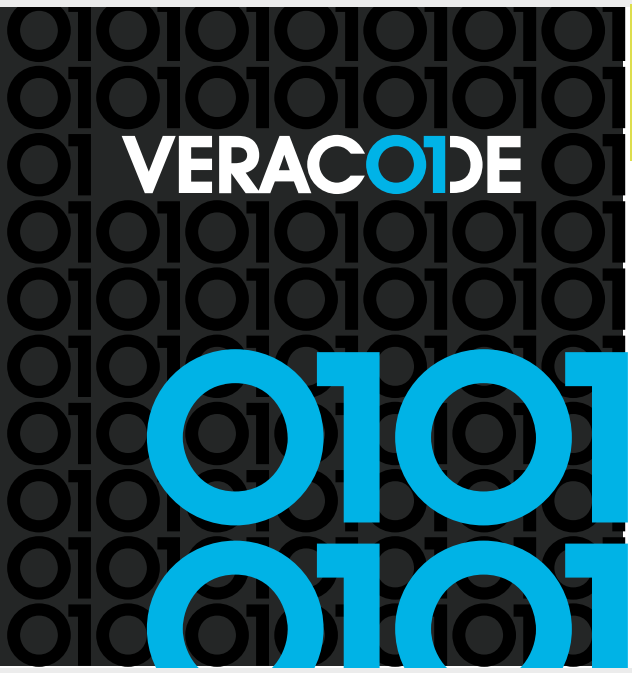
Sandboxing .NET Assemblies for fun, profit and, of course Security!

Niels Tanis

NDC { Sydney }



Cover Slide Option wi
title/intro line, mai
cover title, subhead
date, please delete
subhead, title, etc.
not needed, please le
justify all text

Who am I?

- Niels Tanis
- Principal Security Researcher @ Veracode
  - Background .NET Development, Pentesting/ethical hacking, and software security consultancy
  - ISC^2 CSSLP
  - Research on static analysis for .NET apps

Slide with larger he
when there is not a n
be text heavy.

The content text slide
bullets as preview, ho
you do not need to
bullets. Text is prese
Trebuchet size 14,
bullets may be remo
not needed.

Agenda

- Introduction
- The security risks of third party libraries
- Sandboxing techniques
- Let's create a sandbox!
- Conclusion
- QA

Slide with larger he
when there is not a n
be text heavy.

The content text slide
bullets as preview, ho
you do not need to
bullets. Text is prese
Trebuchet size 14,
bullets may be remo
not needed.

Third Party Libraries

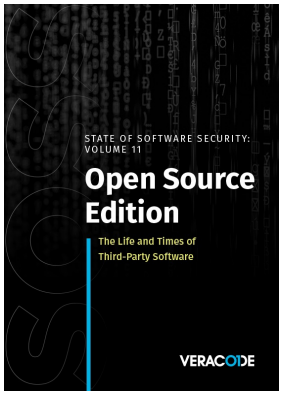
- Big chunk (80%+) of our apps consists of 3rd party libraries
- Efficient in time, why reinvent the wheel?
- How actively is it maintained?
- What do they do for security?

Slide with larger he
when there is not a n
be text heavy.

The content text slide
bullets as preview, ho
you do not need to
bullets. Text is prese
Trebuchet size 14,
bullets may be remo
not needed.

State Of Software Security v11 2021

”Despite this dynamic landscape, 79 percent of the time, developers never update third-party libraries after including them in a codebase.”

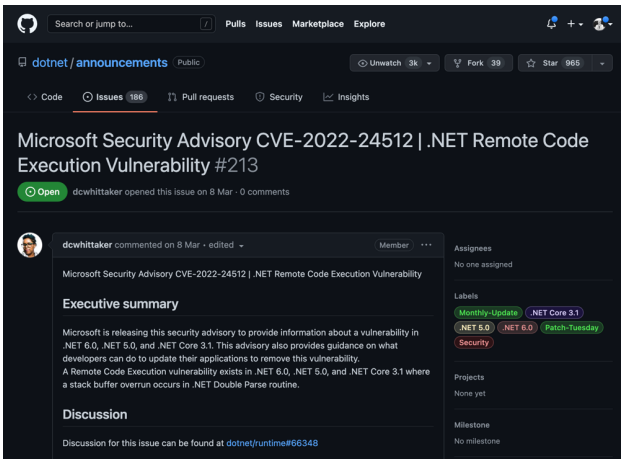


Slide with larger he
when there is not a n
be text heavy.

The content text slide
bullets as preview, ho
you do not need to
bullets. Text is prese
Trebuchet size 14,
bullets may be remo
not needed.

https://info.veracode.com/fy22-state-of-software-security-v11-open-source-edition.html

Vulnerabilities in libraries



Slide with larger he
when there is not a n
be text heavy.
The content text slide
bullets as preview, ho
you do not need to
bullets. Text is prese
Trebuchet size 14,
bullets may be remo
not needed.

https://github.com/dotnet/announcements/issues/213

Vulnerabilities in libraries

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

Alerts and Tips Resources Industrial Control Systems

National Cyber Awareness System > Current Activity > Malware Discovered in Popular NPM Package, ua-parser-js

Malware Discovered in Popular NPM Package, ua-parser-js

Original release date: October 22, 2021

Print Tweet Send Share

Versions of a popular NPM package named `ua-parser-js` was found to contain malicious code. `ua-parser-js` is used in apps and websites to discover the type of device or browser a person is using from User-Agent data. A computer or device with the affected software installed or running could allow a remote attacker to obtain sensitive information or take control of the system.

CISA urges users and administers using compromised ua-parser-js versions 0.7.29, 0.8.0, and 1.0.0 to update to the respective patched versions: 0.7.30, 0.8.1, 1.0.1

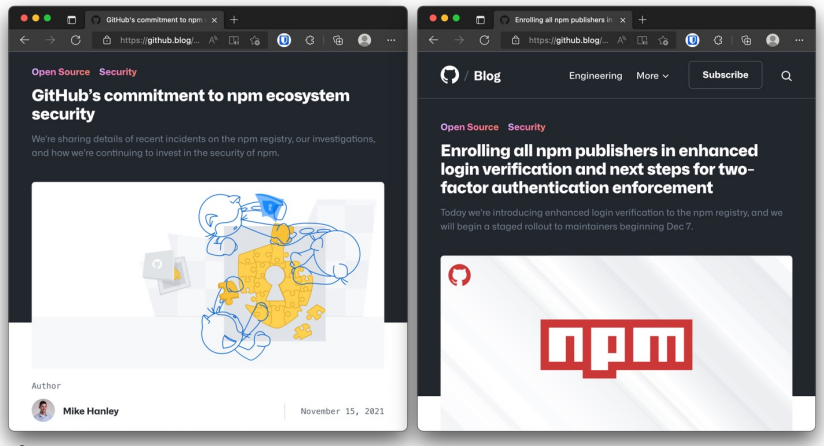
For more information, see Embedded malware in ua-parser-js.

Slide with larger he
when there is not a n
be text heavy.

The content text slide
bullets as preview, ho
you do not need to
bullets. Text is prese
Trebuchet size 14,
bullets may be remo
not needed.

https://us-cert.cisa.gov/ncas/current-activity/2021/10/22/malware-discovered-popular-npm-package-ua-parser-js
https://portswigger.net/daily-swig/popular-npm-package-ua-parser-js-poisoned-with-cryptomining-password-stealing-malware

Vulnerabilities in libraries



Slide with larger he
when there is not a n
be text heavy.
The content text slide
bullets as preview, ho
you do not need to
bullets. Text is prese
Trebuchet size 14,
bullets may be remo
not needed.

https://github.blog/2021-11-15-githubs-commitment-to-npm-ecosystem-security/
https://github.blog/2021-12-07-enrolling-npm-publishers-enhanced-login-verification-two-factor-authentication-enforcement/

Vulnerabilities in libraries

Slide with larger he
when there is not a n
be text heavy.

The content text slide
bullets as preview, ho
you do not need to
bullets. Text is prese
Trebuchet size 14,
bullets may be remo
not needed.

Third-party code comes with some baggage

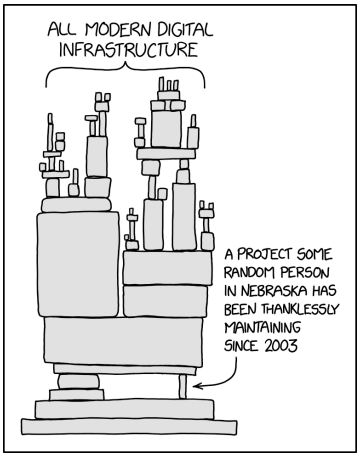
Recognizing risks introduced by statically linked third-party libraries

Introduction

Developing software solutions is a complex task requiring a lot of time and resources. In order to accelerate time to market and reduce the cost, software developers create smaller pieces of functional code which can be reused across

https://blog.secure.software/third-party-code-comes-with-some-baggage

XKDC - Dependency



https://xkcd.com/2347/

Slide with larger he
when there is not a n
be text heavy.

The content text slide
bullets as preview, ho
you do not need to
bullets. Text is prese
Trebuchet size 14,
bullets may be remo
not needed.

Sandboxing .NET Assemblies

- Is there a way we can do a better job?
- A way for us to reduce the security risks?
- Keep in mind it's not a matter of how it's more when!

Slide with larger he
when there is not a n
be text heavy.

The content text slide
bullets as preview, ho
you do not need to
bullets. Text is prese
Trebuchet size 14,
bullets may be remo
not needed.

Sandboxing .NET Assemblies

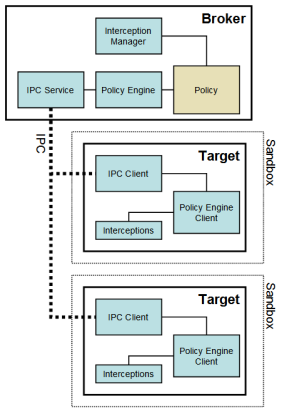
- We want to use the library without modification
- Can we maybe create a controlled (restricted) sandbox?
- A sandbox with limited capabilities?

Slide with larger he
when there is not a n
be text heavy.

The content text slide
bullets as preview, ho
you do not need to
bullets. Text is prese
Trebuchet size 14,
bullets may be remo
not needed.

Browser Sandbox

- Chromium Sandbox
- No direct system access
- Each OS related call is done via IPC
- FireFox Sandbox
  - Containers & Site Isolation
  - RLBox



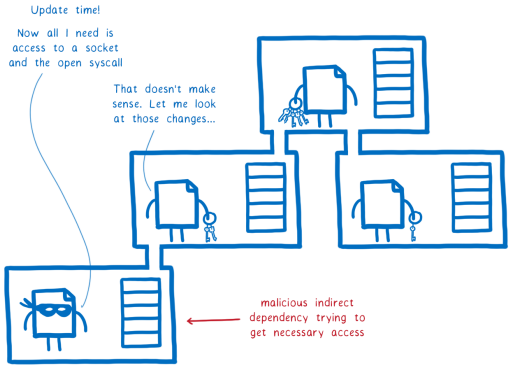
Slide with larger he
when there is not a n
be text heavy.
The content text slide
bullets as preview, ho
you do not need to
bullets. Text is prese
Trebuchet size 14,
bullets may be remo
not needed.

https://chromium.googlesource.com/chromium/src/+/refs/heads/main/docs/design/sandbox.md
https://hacks.mozilla.org/2021/05/introducing-firefox-new-site-isolation-security-architecture/

WebAssembly Nanoprocess

- Lineair memory model
- WASM module isolation

- Declaritive permissions
- Interface types
- WASI for BCL calls



NDC { Sydney }

@nielstanis

Slide with larger he
when there is not a n
be text heavy.
The content text slide
bullets as preview, ho
you do not need to
bullets. Text is prese
Trebuchet size 14,
bullets may be remo
not needed.

https://hacks.mozilla.org/2019/11/announcing-the-bytecode-alliance/

Code Access Security

Slide with larger he
when there is not a n
be text heavy.
The content text slide
bullets as preview, ho
you do not need to
bullets. Text is prese
Trebuchet size 14,
bullets may be remo
not needed.

- Evidence based model
- Code from different origins have different sets of rights
- Stack-walks that protect against luring attacks

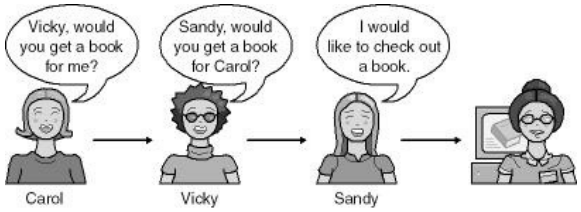
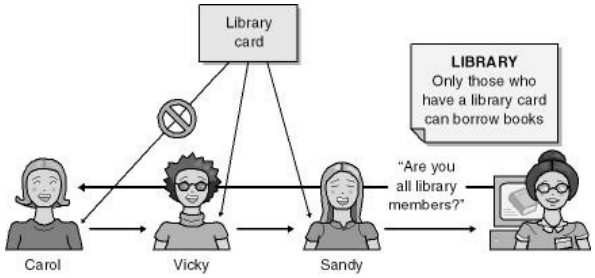


Figure 18-1; Writing Secure Code 2nd Edition

Code Access Security

- Evidence library card
- Policy → Librarian only allows members



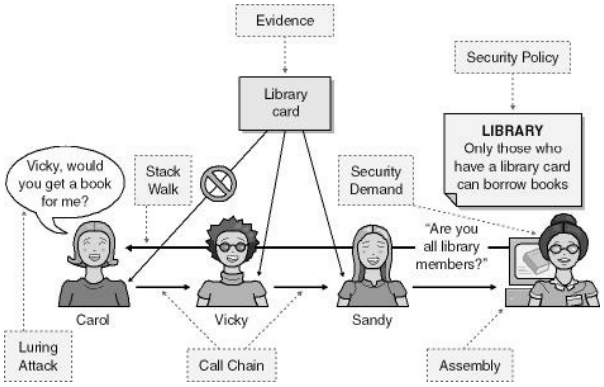
Slide with larger he when there is not a n be text heavy.

The content text slide bullets as preview, ho you do not need to bullets. Text is prese Trebuchet size 14, bullets may be remo not needed.

Figure 18-2; Writing Secure Code 2nd Edition

Code Access Security

- Stack walk



Slide with larger he when there is not a n be text heavy.

The content text slide bullets as preview, ho you do not need to bullets. Text is prese Trebuchet size 14, bullets may be remo not needed.

Figure 18-2; Writing Secure Code 2nd Edition

Code Access Security

Slide with larger he
when there is not a n
be text heavy.
The content text slide
bullets as preview, ho
you do not need to
bullets. Text is prese
Trebuchet size 14,
bullets may be remo
not needed.

- Most practical example, ASP.NET Medium Trust
- CAS is deprecated since .NET Framework 4
- Too complex in administering and use?
- Too early?

https://docs.microsoft.com/en-us/previous-versions/dotnet/framework/code-access-security/code-access-security-basics
https://docs.microsoft.com/en-us/previous-versions/dotnet/framework/code-access-security/code-access-security-policy-compatibility-and-migration

Demo time!

NDC { Sydney }

@nielstanis

Image: C# logo https://docs.microsoft.com/en-us/dotnet/csharp/

DocumentProcessor Package

- Use package as is!
  - Disclaimer: always comply with library license!
  - Not allowed to reverse engineer/decompile
- We do want to change behaviour:
  - Opening documents directly from URL – SSRF
  - Writing files to any arbitrary directory – Path Traversal
- There are *several* ways to *fix* this!

Slide with larger he
when there is not a n
be text heavy.

The content text slide
bullets as preview, ho
you do not need to
bullets. Text is prese
Trebuchet size 14,
bullets may be remo
not needed.

AssemblyLoadContext

Slide with larger he
when there is not a n
be text heavy.
The content text slide
bullets as preview, ho
you do not need to
bullets. Text is prese
Trebuchet size 14,
bullets may be remo
not needed.

- Only single AppDomain in .NET Core.
- AssemblyLoadContext replaces the isolation mechanisms provided by multiple AppDomain instances in .NET Framework.
- Conceptually, a load context creates a scope for loading, resolving, and potentially unloading a set of assemblies.

https://docs.microsoft.com/en-us/dotnet/api/system.runtime.loader.assemblyloadcontext?view=net-5.0
https://docs.microsoft.com/en-us/dotnet/core/dependency-loading/understanding-assemblyloadcontext

AssemblyLoadContext

- It allows multiple versions of the same assembly to be loaded within a single process.
- It does not provide any security features. All code has full permissions of the process.
- But it does allow us to control what gets loaded!

Slide with larger he
when there is not a n
be text heavy.
The content text slide
bullets as preview, ho
you do not need to
bullets. Text is prese
Trebuchet size 14,
bullets may be remo
not needed.

https://docs.microsoft.com/en-us/dotnet/api/system.runtime.loader.assemblyloadcontext?view=net-5.0
https://docs.microsoft.com/en-us/dotnet/core/dependency-loading/understanding-assemblyloadcontext

AssemblyLoadContext

- Interface project used as shared contract
- Remove DocumentProcessor package from ConsoleApp
  - Add reference to interface project
- Create Library that implements interface
  - Reference interface project and DocumentProcessor Package
  - Self-contained deployment to folder that has all to be loaded by our sandboxed loadcontext

Slide with larger he
when there is not a n
be text heavy.

The content text slide
bullets as preview, ho
you do not need to
bullets. Text is prese
Trebuchet size 14,
bullets may be remo
not needed.

https://docs.microsoft.com/en-us/dotnet/api/system.runtime.loader.assemblyloadcontext?view=net-5.0
https://docs.microsoft.com/en-us/dotnet/core/dependency-loading/understanding-assemblyloadcontext

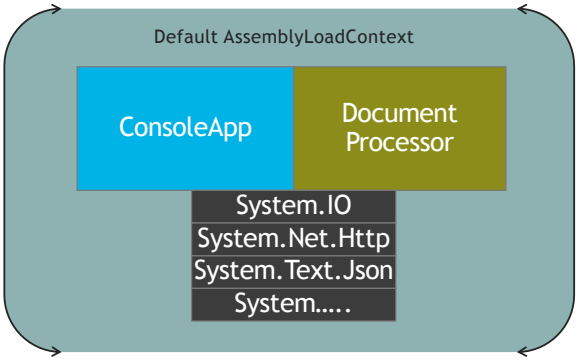
Sandboxing DocumentProcessor

NDC { Sydney }

@nielstanis

Image: C# logo https://docs.microsoft.com/en-us/dotnet/csharp/

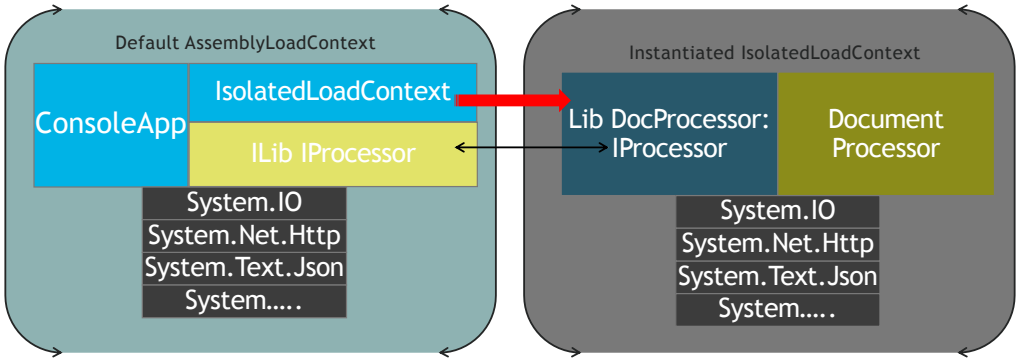
ConsoleApp Start



Slide with larger he
when there is not a n
be text heavy.

The content text slide
bullets as preview, ho
you do not need to
bullets. Text is prese
Trebuchet size 14,
bullets may be remo
not needed.

ConsoleApp & Sandboxed Library



Slide with larger he
when there is not a n
be text heavy.

The content text slide
bullets as preview, ho
you do not need to
bullets. Text is prese
Trebuchet size 14,
bullets may be remo
not needed.

Removing Types?

- Self contained set of assemblies, could we not remove types?
- What about trimming that got introduced with .NET 5?
- Maybe we need something more rigorous?

Slide with larger he
when there is not a n
be text heavy.

The content text slide
bullets as preview, ho
you do not need to
bullets. Text is prese
Trebuchet size 14,
bullets may be remo
not needed.

Patching with Harmony2

- A library for patching, replacing and decorating .NET and Mono methods during runtime.
  - Patch at runtime (pre- and postfix)
  - Transpile at compile time (rewrite IL)
- Harmony v2
  - Lib.Harmony on NuGet
  - https://github.com/pardeike/Harmony

Slide with larger he
when there is not a n
be text heavy.
The content text slide
bullets as preview, ho
you do not need to
bullets. Text is prese
Trebuchet size 14,
bullets may be remo
not needed.

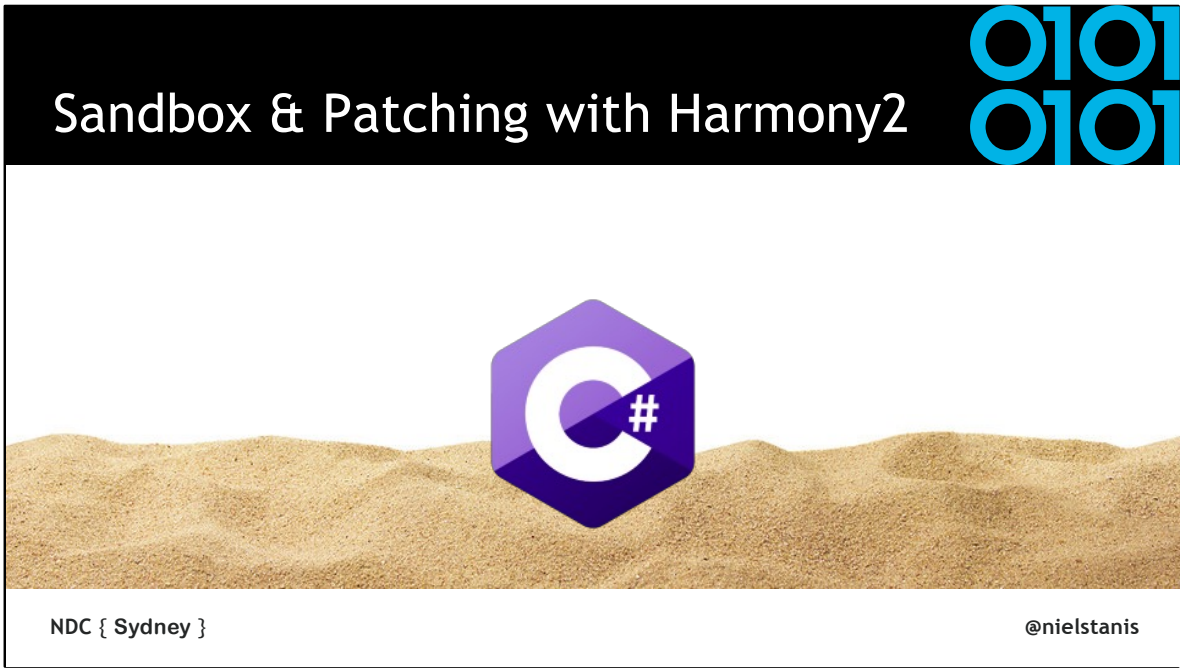
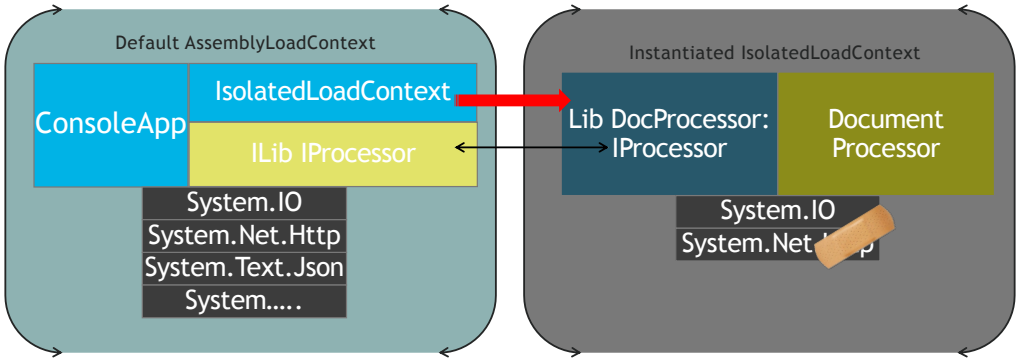


Image: C# logo https://docs.microsoft.com/en-us/dotnet/csharp/

ConsoleApp & Sandboxed Library



Slide with larger he
when there is not a n
be text heavy.

The content text slide
bullets as preview, ho
you do not need to
bullets. Text is prese
Trebuchet size 14,
bullets may be remo
not needed.

Conclusion

- Update libraries; security problems get fixed
- Integrate security into your development lifecycle
- Know what libraries are used, where and what's inside and most important what you'd expect from it.

Slide with larger he
when there is not a n
be text heavy.

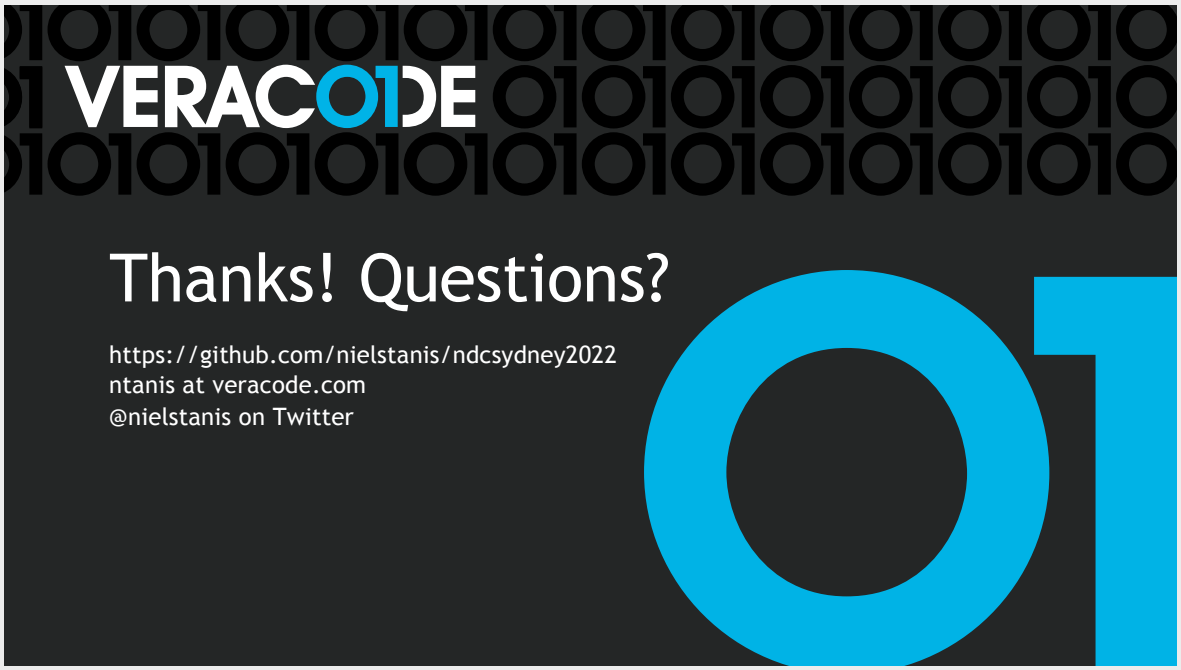
The content text slide
bullets as preview, ho
you do not need to
bullets. Text is prese
Trebuchet size 14,
bullets may be remo
not needed.

Conclusion

Slide with larger he
when there is not a n
be text heavy.

The content text slide
bullets as preview, ho
you do not need to
bullets. Text is prese
Trebuchet size 14,
bullets may be remo
not needed.

- Futures of this Sandbox Concept
  - Easier developer integration (e.g. source generator)
  - Package + good guidance on how this can be used in different application contexts like ASP.NET Core.
  - Basic patches/policy that can be applied on libraries



Closing slide