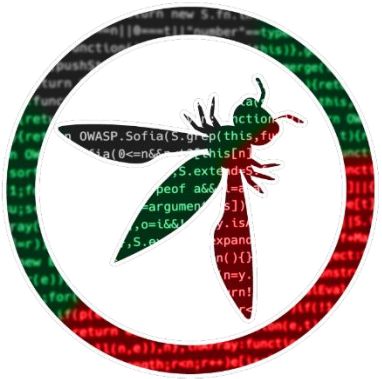


OWASP
SOFIA, BULGARIA

Ivan Ivanov

Introduction

A .NET dev who builds secure systems by day and breaks them (responsibly) by… afternoon

- Senior Principal Software Engineer
  “Reporting, Documents & Tools” @Progress
- Security Champion

- How to fail with .NET reflection?
- Write your own custom (de)serialization!

. . .

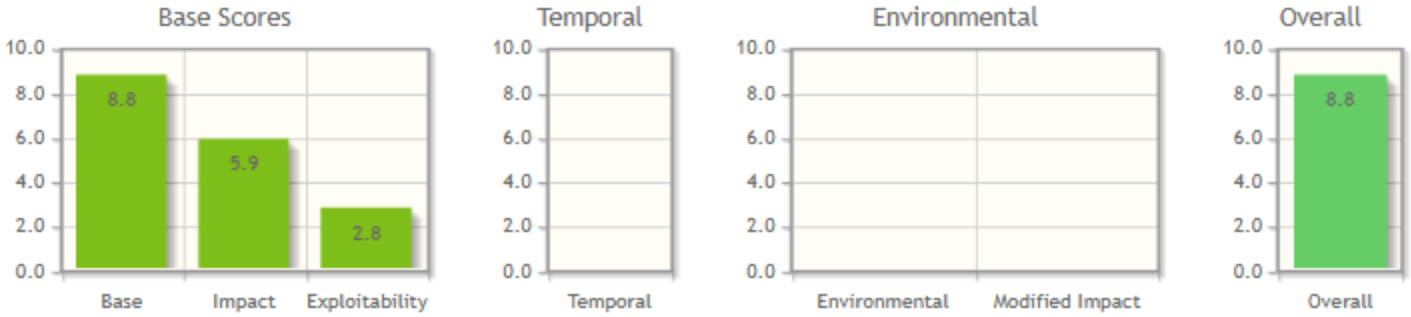

"That's all Folks!"

Common Myths

“Easy, don’t use .NET”

- Reflection

It can’t be that bad…



CVSS Base Score: 8.8
Impact Subscore: 5.9
Exploitability Subscore: 2.8
CVSS Temporal Score: NA
CVSS Environmental Score: NA
Modified Impact Subscore: NA
Overall CVSS Score: 8.8

Show Equations

CVSS v3.1 Vector
AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Base Score Metrics

Exploitability Metrics

Attack Vector (AV)*
Network (AV:N) | Adjacent Network (AV:A) | Local (AV:L) | Physical (AV:P)

Attack Complexity (AC)*
Low (AC:L) | High (AC:H)

Privileges Required (PR)*
None (PR:N) | Low (PR:L) | High (PR:H)

User Interaction (UI)*
None (UI:N) | **Required (UI:R)**

Scope (S)*
Unchanged (S:U) | Changed (S:C)

Impact Metrics

Confidentiality Impact (C)*
None (C:N) | Low (C:L) | **High (C:H)**

Integrity Impact (I)*
None (I:N) | Low (I:L) | **High (I:H)**

Availability Impact (A)*
None (A:N) | Low (A:L) | **High (A:H)**

“But I should be fine, I guess…”

- “I read that MSDN article: Deserialization Risks…, and I use none of these”
- We have custom implementation
- “SAST tool is green”
- We have a block list for all the “bad” types that we know

Marked Safe From

Deserialization attacks

Today

“I can cast it and be safe”

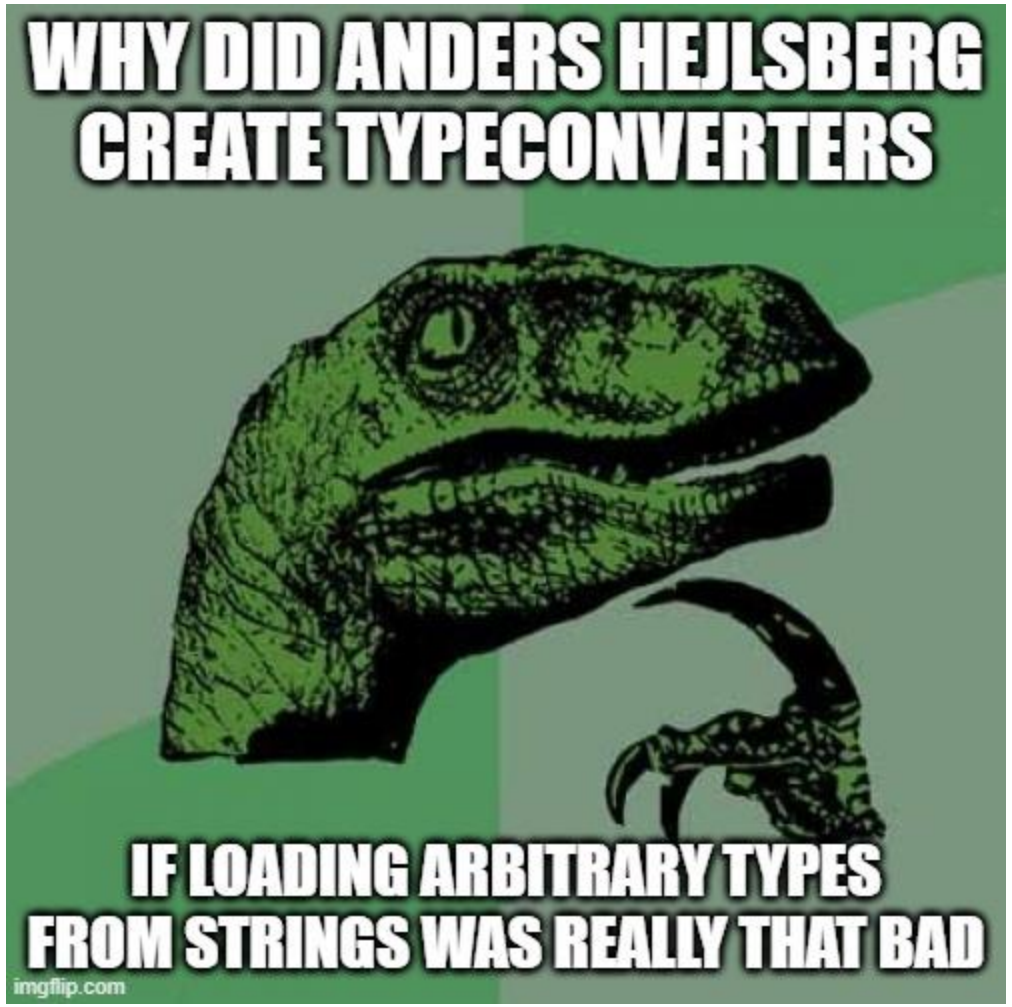
```
var suspectObject = myBinaryFormatter.Deserialize(untrustedData);

//Check below is too late! Execution may have already occurred.
if (suspectObject is SomeDangerousObjectType)
{
    //generate warnings and dispose of suspectObject
}
```

*Unsafe deserialization is the second most evil thing after screenshots of code

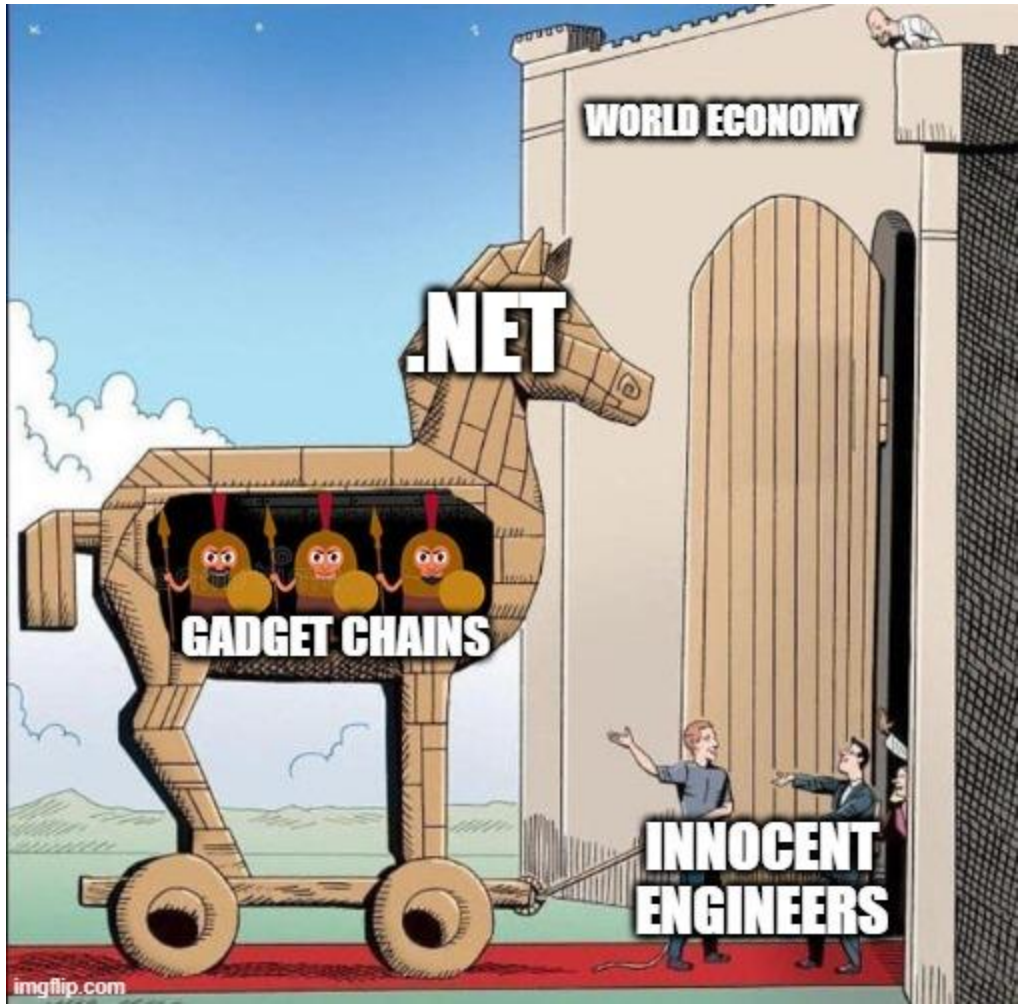
“…I can cast it and be safe”

- (Code Demo)



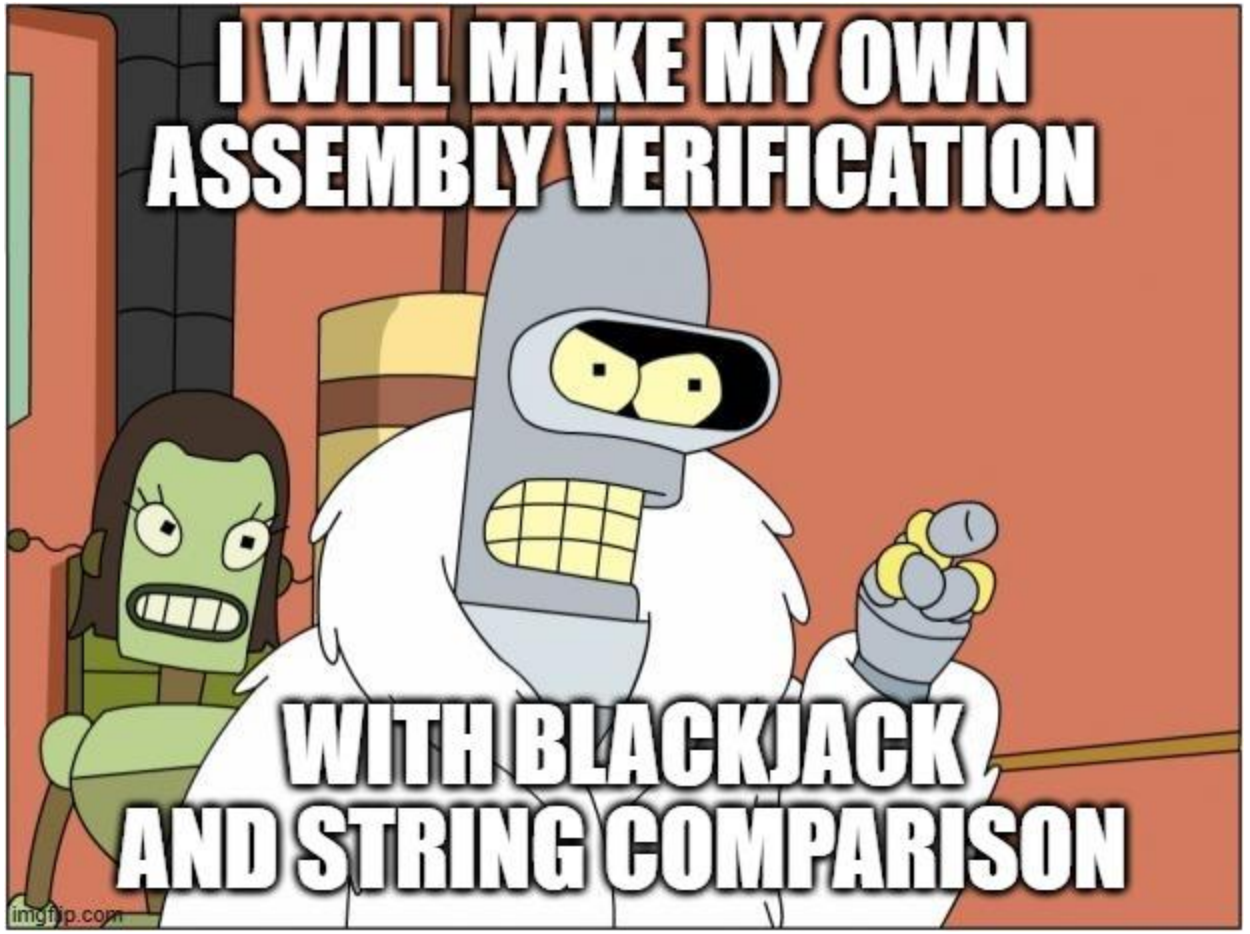
“My AppDomain is my castle”

- (Code Demo)



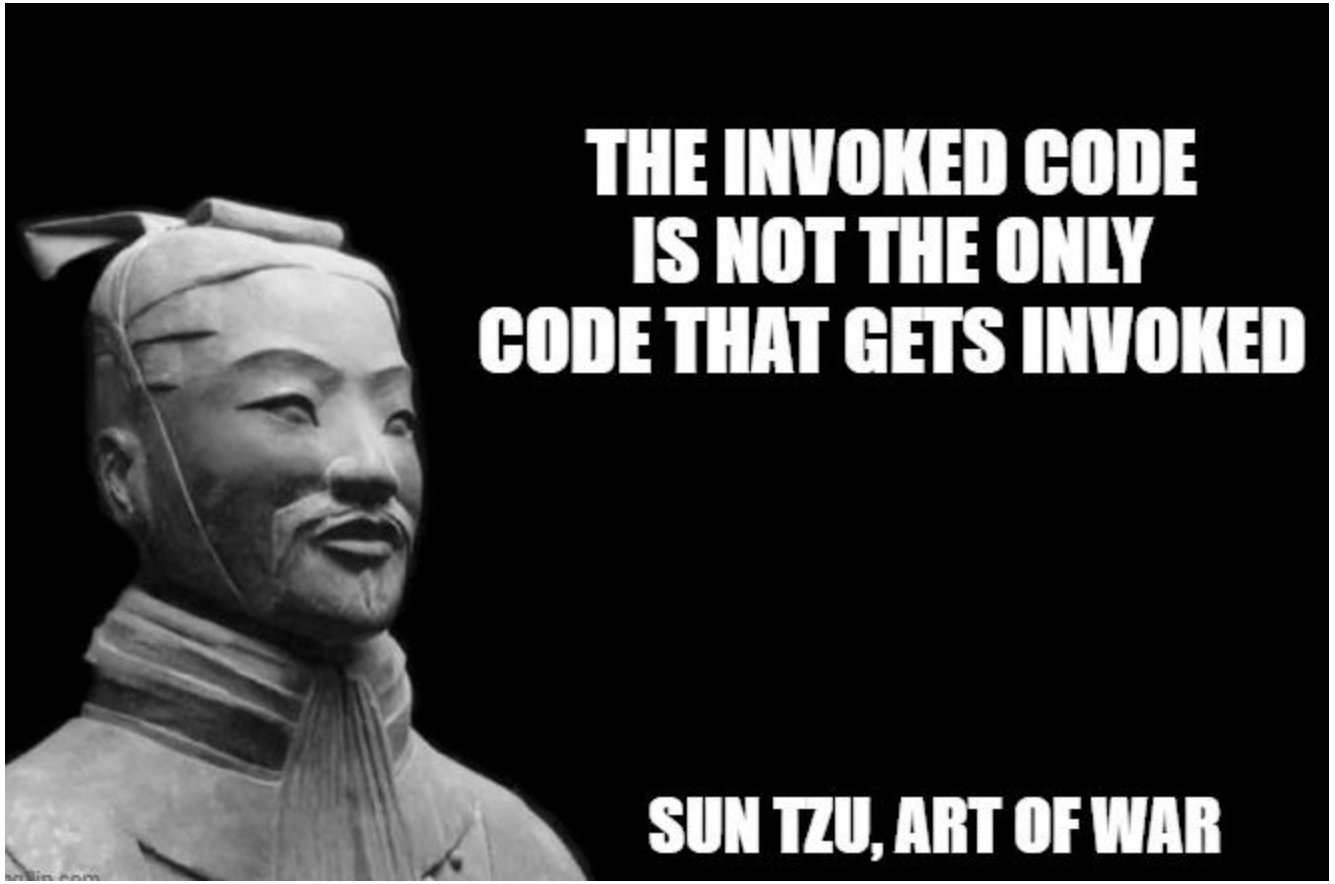
“I will write my own assembly verification”

- (Code Demo)



“I read the invoked code. Trust me, bro!”

- (Code Demo)



Placeholder, one of the demo cases should be revamped as it was too specific to reporting context

OK, Now What?

Allowlist vs Denylist

Allowlists:

- Align with “Secure by default” principle
- Require less maintenance
- Are more beginner friendly to new developers on the team

Rule Enforcement

- Code Analysis and Roslyn Analyzers
  - Write your own
  - Use a 3rd party one

Demo

Q&A