What Your Browser Can Teach You…

…about Software Security

History [edit]

The concept of same-origin policy was introduced by Netscape Navigator 2.02 in 1995,[1] shortly after the introduction of JavaScript in Netscape 2.0.[2][3]

History [edit]

The concept of same-origin policy was introduced by Netscape Navigator 2.02 in 1995,[1] shortly after the introduction of JavaScript in Netscape 2.0.[2][3]

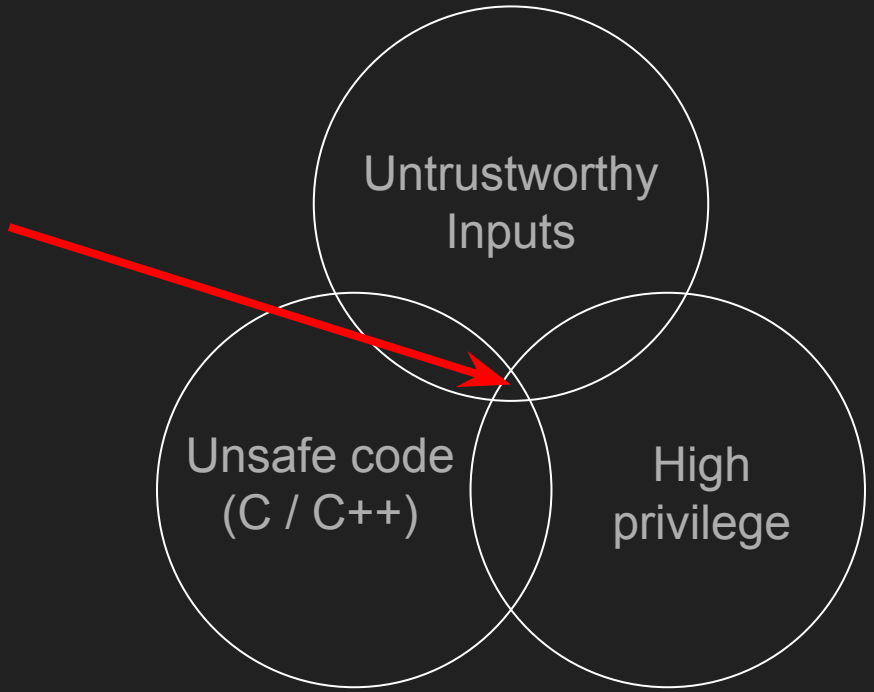
History [edit]

The concept of same-origin policy was introduced by Netscape Navigator 2.02 in 1995,[1] shortly after the introduction of JavaScript in Netscape 2.0.[2][3]

Lesson #1 - Choose Your Boundaries

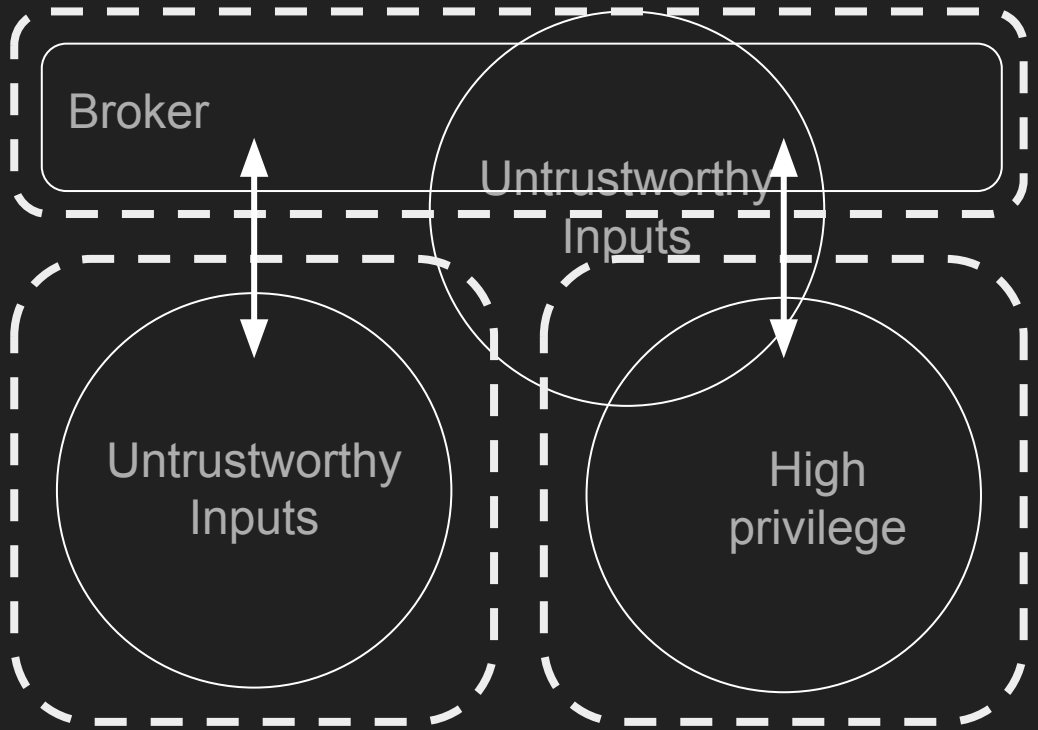
Where are your boundaries?

Doom!
Don’t do this.



https://chromium.googlesource.com/chromium/src/+/master/docs/security/rule-of-2.md

Where are your boundaries?



Where are your boundaries?

Lesson #2 - Align Incentives

Example: Rust in Firefox

Safe systems languages:

- Arguably, the biggest improvement in browser security since sandboxing
- Landed… for **performance** reasons

Aligned incentives:

- Parallel, performant code in C++ is hard
- Secure code in C++ is hard

htt t-in-rust/

The lesson: Align Incentives

Security goals often align with others

Build a culture that encourages identification of these

For example:

- Dependency agility helps security…
- … and speed of change

We’ve Learned…

Think about boundaries

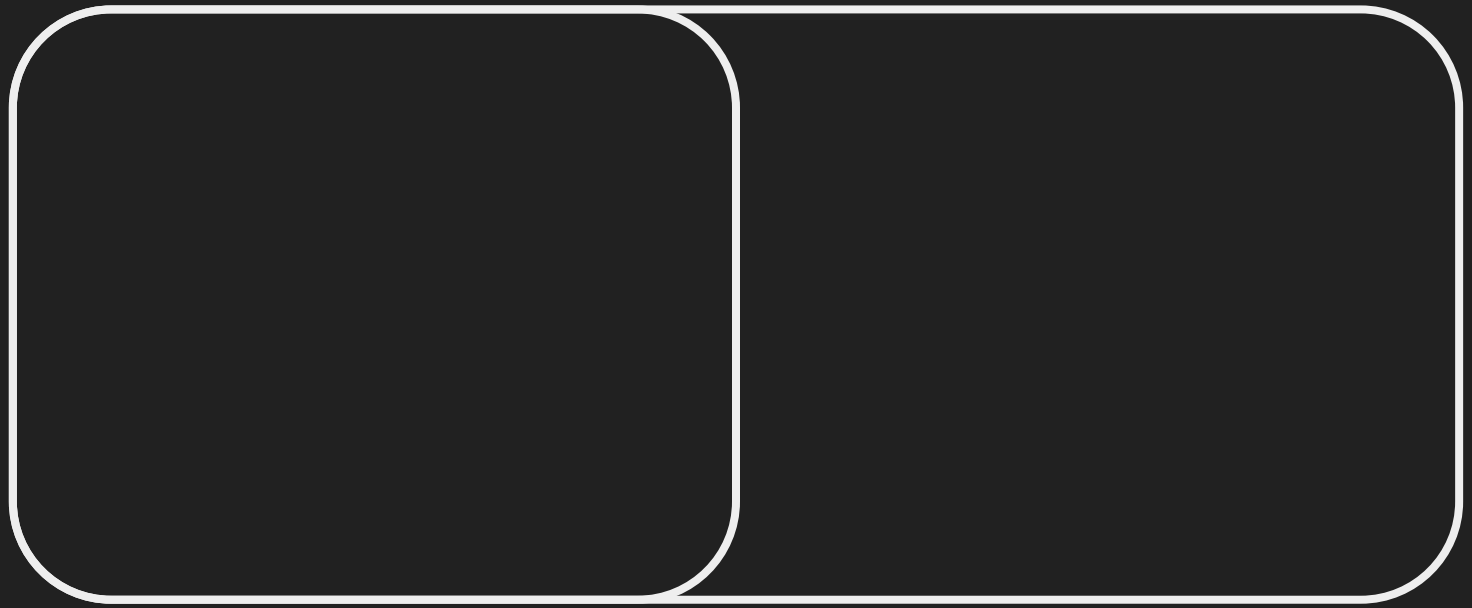
Look for aligned incentives

Finally - remember the horror story?

- difficult beginnings can lead to good outcomes

Thank you!

Threats and Assets Don’t Mix!

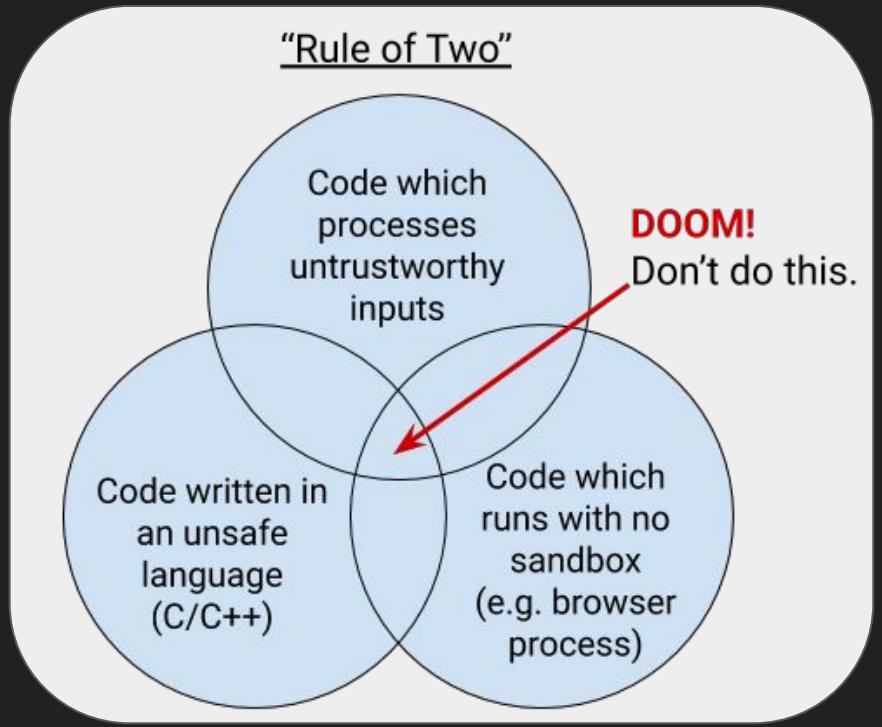


Where are your boundaries?

- Rule of Two - Pick no more of 2 of:
  a. Untrustworthy inputs
  b. Unsafe implementation language*
  c. High privilege

- The browser codebase is C++ (‘b’ is a given!)

- You **must** separate ‘a’ and ‘c’



https://chromium.googlesource.com/chromium/src/+/master/docs/security/rule-of-2.md