Somebody set up us the bomb

Allon Mureinik

Senior Manager, Seeker Interactive Application Security Testing (IAST)

Synopsys, Inc.

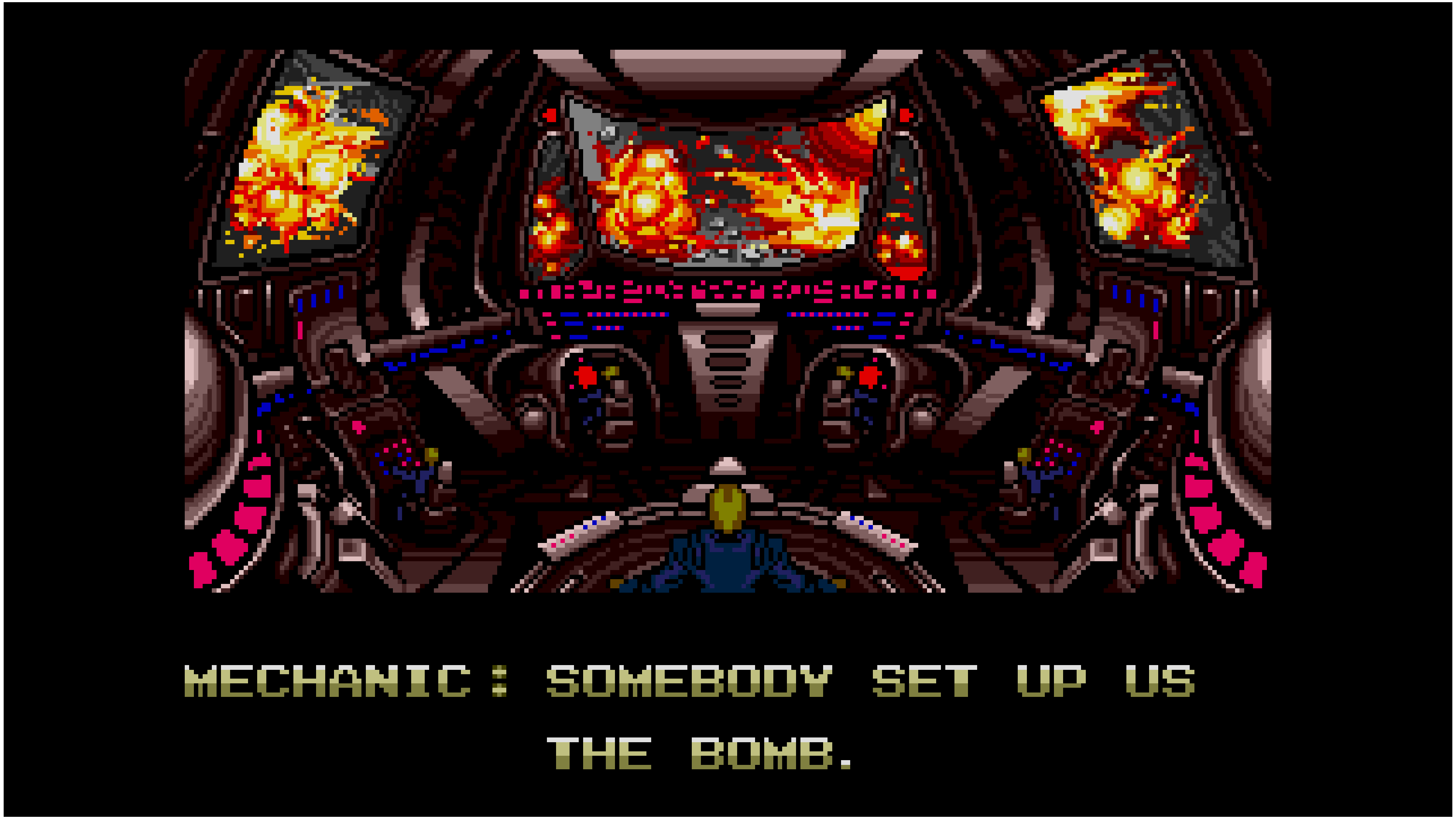
allon.mureinik@synopsys.com / @mureinik / https://www.linkedin.com/in/mureinik/

FOSDEM 2022

To answer the question you may be asking…

https://www.miramax.com/movie/pulp-fiction/

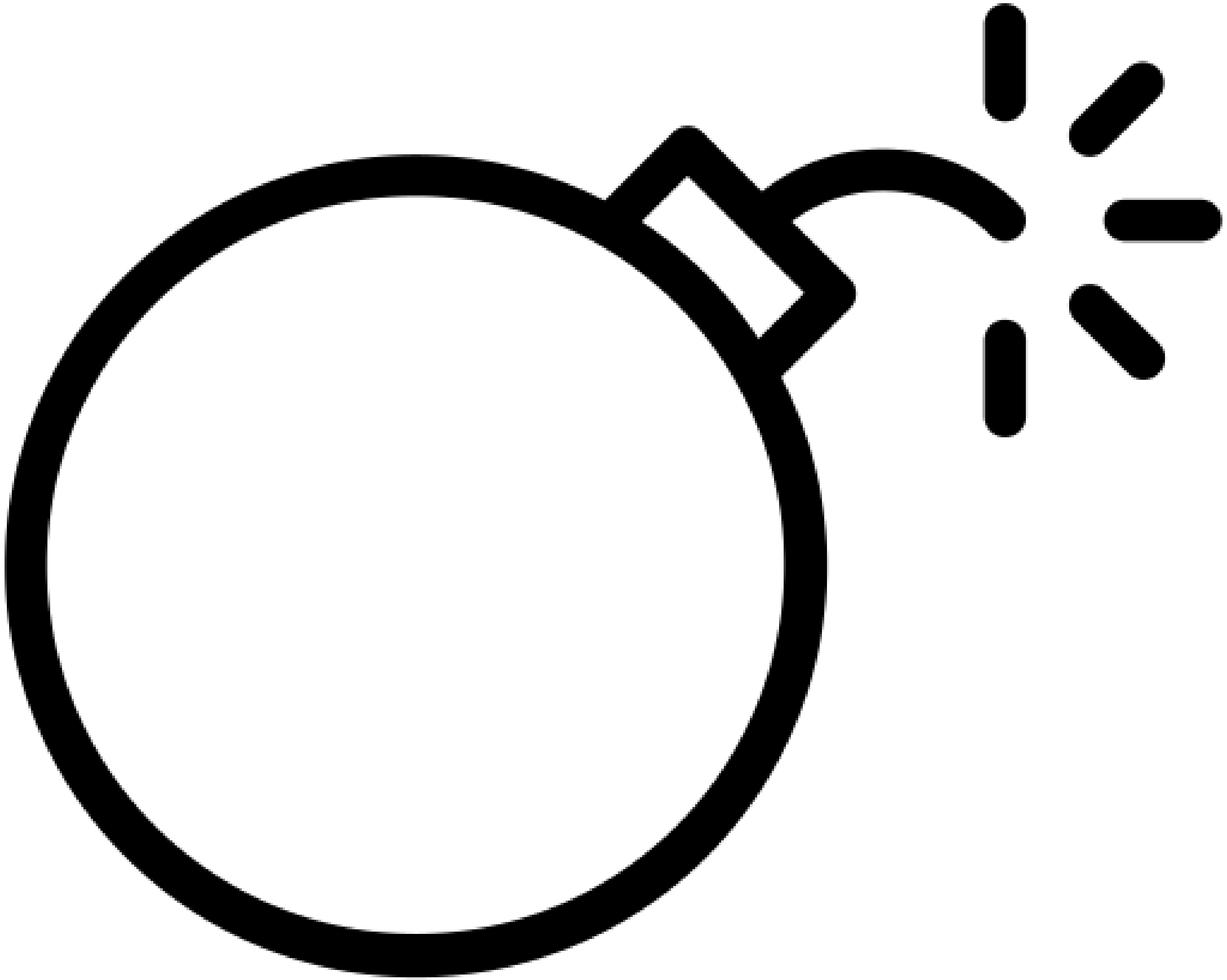
I do.



MECHANIC : SOMEBODY SET UP US THE BOMB.

https://en.wikipedia.org/wiki/Zero_Wing

Let’s talk about bombs



https://thenounproject.com/icon/bomb-4494642/

Sounds serious, let’s have a laugh

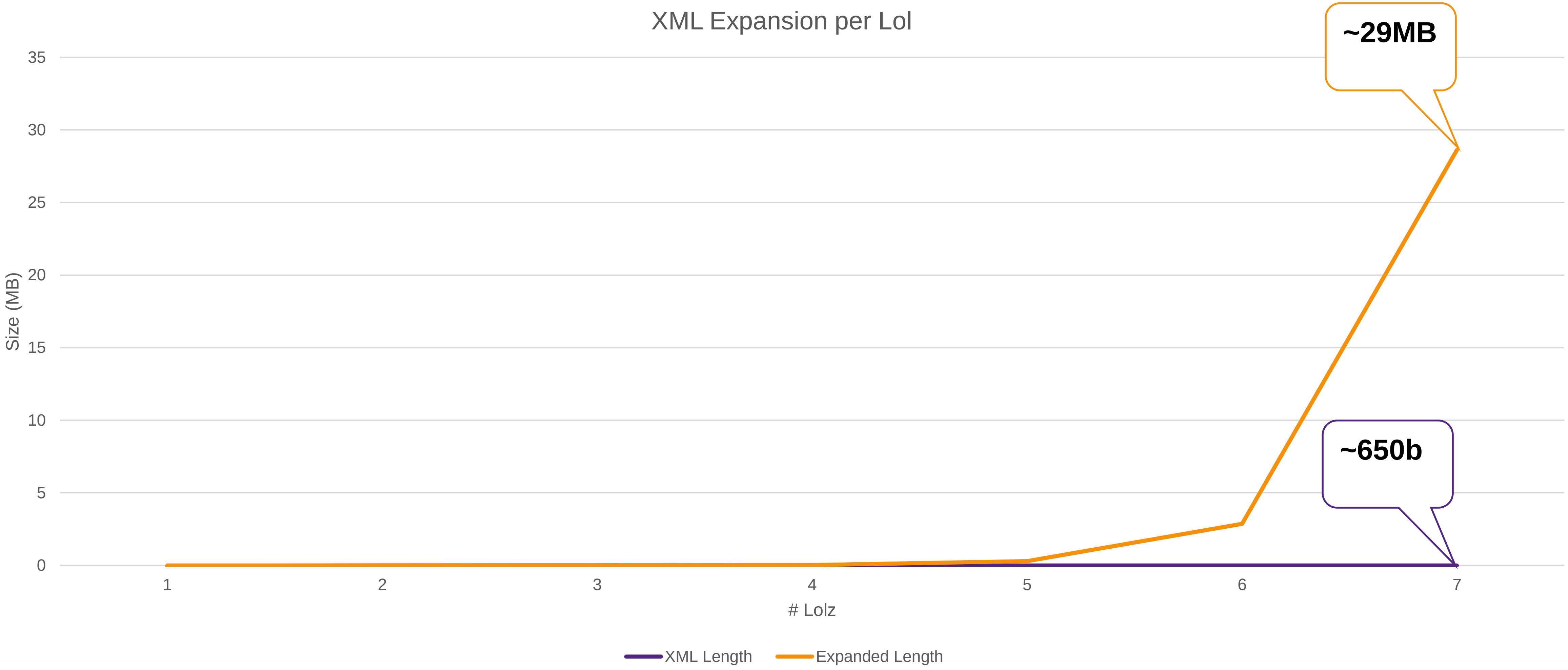
https://thenounproject.com/icon/joker-3976603/

Or a billion laughs

```
<?xml version="1.0"?>
<!DOCTYPE lolz [
    <!ENTITY lol0 "lol">
    <!ELEMENT lolz (#PCDATA)>
    <!ENTITY lol1 "&lol0;&lol0;&lol0;&lol0;&lol0;&lol0;&lol0;&lol0;&lol0;&lol0;">
    <!ENTITY lol2 "&lol1;&lol1;&lol1;&lol1;&lol1;&lol1;&lol1;&lol1;&lol1;&lol1;">
    <!ENTITY lol3 "&lol2;&lol2;&lol2;&lol2;&lol2;&lol2;&lol2;&lol2;&lol2;&lol2;">
    <!ENTITY lol4 "&lol3;&lol3;&lol3;&lol3;&lol3;&lol3;&lol3;&lol3;&lol3;&lol3;">
    <!ENTITY lol5 "&lol4;&lol4;&lol4;&lol4;&lol4;&lol4;&lol4;&lol4;&lol4;&lol4;">
    <!ENTITY lol6 "&lol5;&lol5;&lol5;&lol5;&lol5;&lol5;&lol5;&lol5;&lol5;&lol5;">
    <!ENTITY lol7 "&lol6;&lol6;&lol6;&lol6;&lol6;&lol6;&lol6;&lol6;&lol6;&lol6;">
    <!ENTITY lol8 "&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;">
    <!ENTITY lol9 "&lol8;&lol8;&lol8;&lol8;&lol8;&lol8;&lol8;&lol8;&lol8;&lol8;">
    ]>
<lolz>&lol9;</lolz>
```

https://en.wikipedia.org/wiki/Billion_laughs_attack

How bad is it?

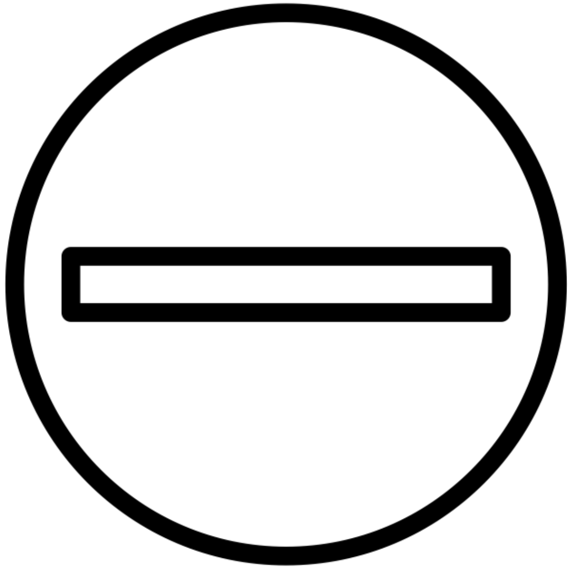


https://github.com/mureinik/somebody-set-up-us-the-bomb

What can I do?

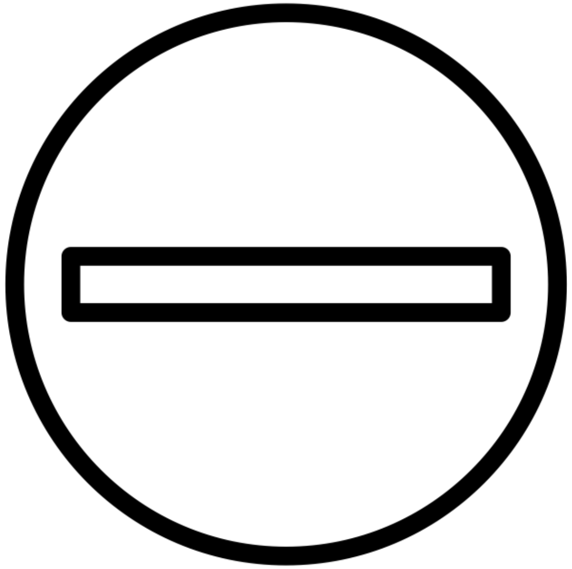
What can I do?

- Don’t use XML
  - If you can…



https://thenounproject.com/term/no-entry/980838

What can I do?

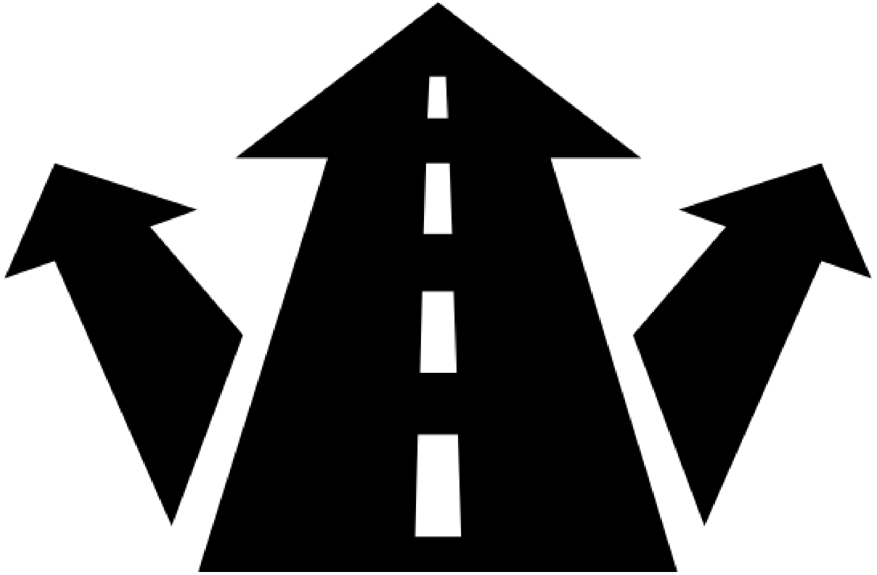


- Don’t use XML
  - If you can…
- Don’t allow tainted input in your XML
  - If you can…

https://thenounproject.com/term/no-entry/980838

What can I do?

- Don’t use XML
  - If you can…
- Don’t allow tainted input in your XML
  - If you can…
- Use a simple(r) XML library
  - If you can…
  - E.g., xml-js, xml2js



https://thenounproject.com/term/alternative-route/2902159

What can I do?

- Don’t use XML
  - If you can…
- Don’t allow tainted input in your XML
  - If you can…
- Use a simple(r) XML library
  - If you can…
  - E.g., xml-js, xml2js
- Configure the library not to expand entities
  - If you can…
  - libxmljs based parsers: `{noent: false}` or `{huge: false}`

https://thenounproject.com/icon/configure-1883381/

What can I do?

- Don’t use XML
  - If you can…
- Don’t allow tainted input in your XML
  - If you can…
- Use a simple(r) XML library
  - If you can…
  - E.g., xml-js, xml2js
- Configure the library not to expand entities
  - If you can…
  - libxmljs based parsers: `{noent: false}` or `{huge: false}`
- Sanitize the XML input
  - E.g., xml-escape

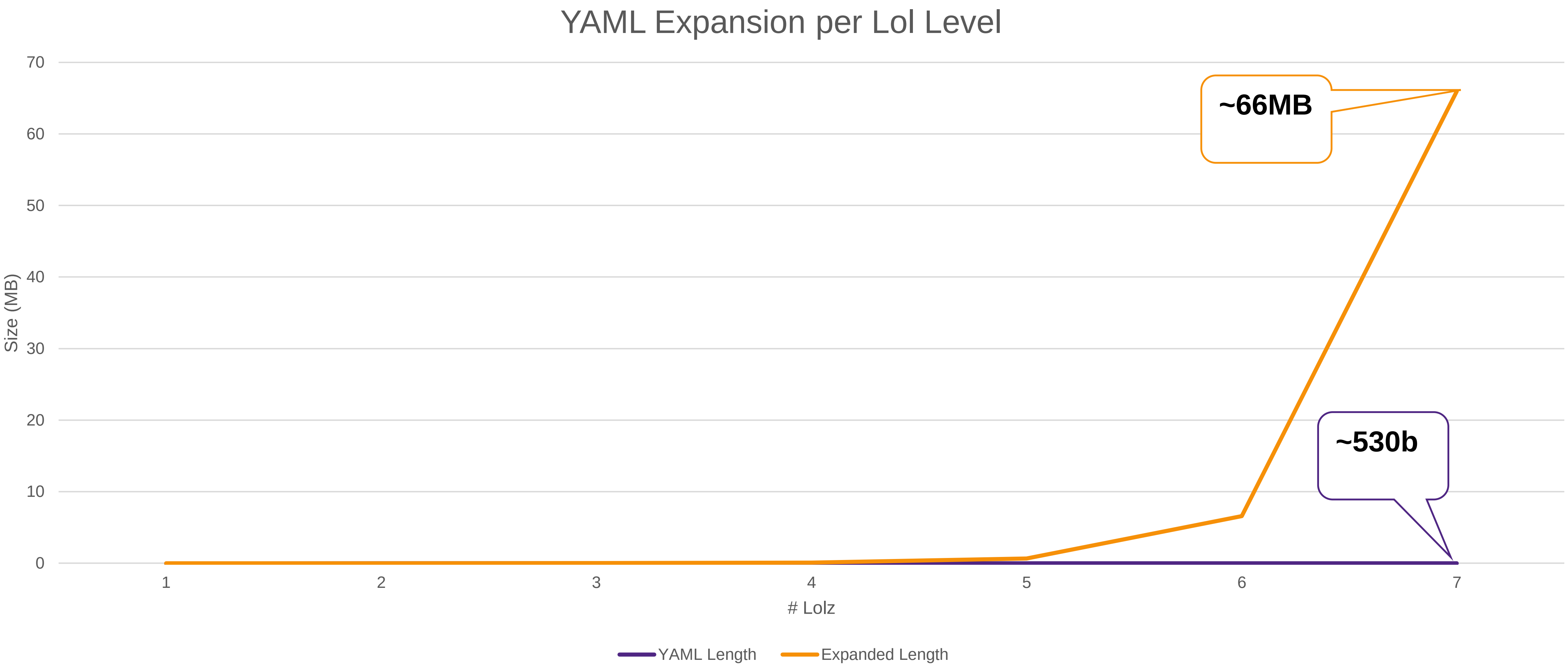
https://thenounproject.com/icon/sanitizer-3470901/

But I don’t use XML, I use YAML

```yaml
lol0: &lol0 "lol"
lol1: &lol1 [*lol0,*lol0,*lol0,*lol0,*lol0,*lol0,*lol0,*lol0,*lol0]
lol2: &lol2 [*lol1,*lol1,*lol1,*lol1,*lol1,*lol1,*lol1,*lol1,*lol1]
lol3: &lol3 [*lol2,*lol2,*lol2,*lol2,*lol2,*lol2,*lol2,*lol2,*lol2]
lol4: &lol4 [*lol3,*lol3,*lol3,*lol3,*lol3,*lol3,*lol3,*lol3,*lol3]
lol5: &lol5 [*lol4,*lol4,*lol4,*lol4,*lol4,*lol4,*lol4,*lol4,*lol4]
lol6: &lol6 [*lol5,*lol5,*lol5,*lol5,*lol5,*lol5,*lol5,*lol5,*lol5]
lol7: &lol7 [*lol6,*lol6,*lol6,*lol6,*lol6,*lol6,*lol6,*lol6,*lol6]
lol8: &lol8 [*lol7,*lol7,*lol7,*lol7,*lol7,*lol7,*lol7,*lol7,*lol7]
lol9: &lol9 [*lol8,*lol8,*lol8,*lol8,*lol8,*lol8,*lol8,*lol8,*lol8]
```

https://en.wikipedia.org/wiki/Billion_laughs_attack

How bad is it?

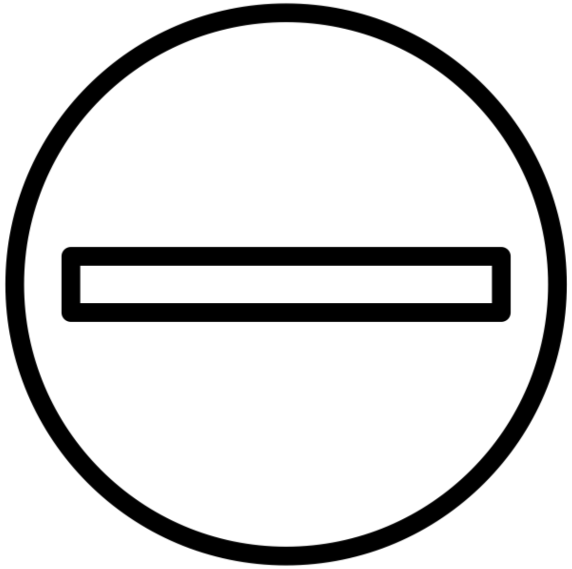


https://github.com/mureinik/somebody-set-up-us-the-bomb

What can I do?

What can I do?

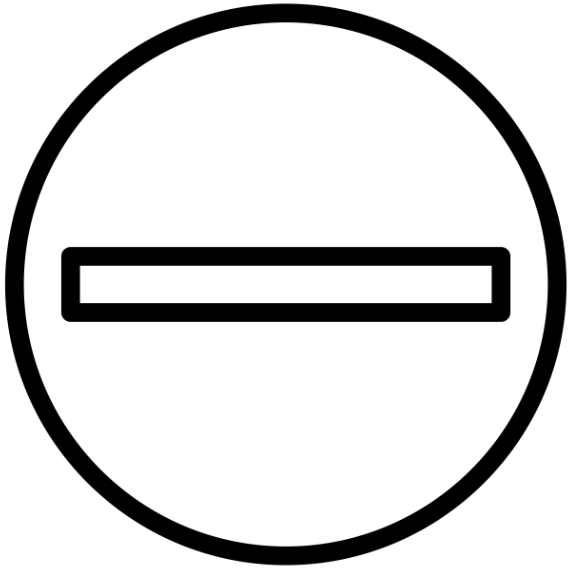
- Don’t use YAML
  - If you can…



https://thenounproject.com/term/no-entry/980838

What can I do?

- Don’t use YAML
  - If you can…
- Don’t allow tainted input in your YAML
  - If you can…



https://thenounproject.com/term/no-entry/980838

What can I do?

- Don’t use YAML
  - If you can…
- Don’t allow tainted input in your YAML
  - If you can…
- Use the libraries’ methods for stringifying and not `JSON.stringify`
  - yaml: `strinfigy`
  - js-yaml: `dump`

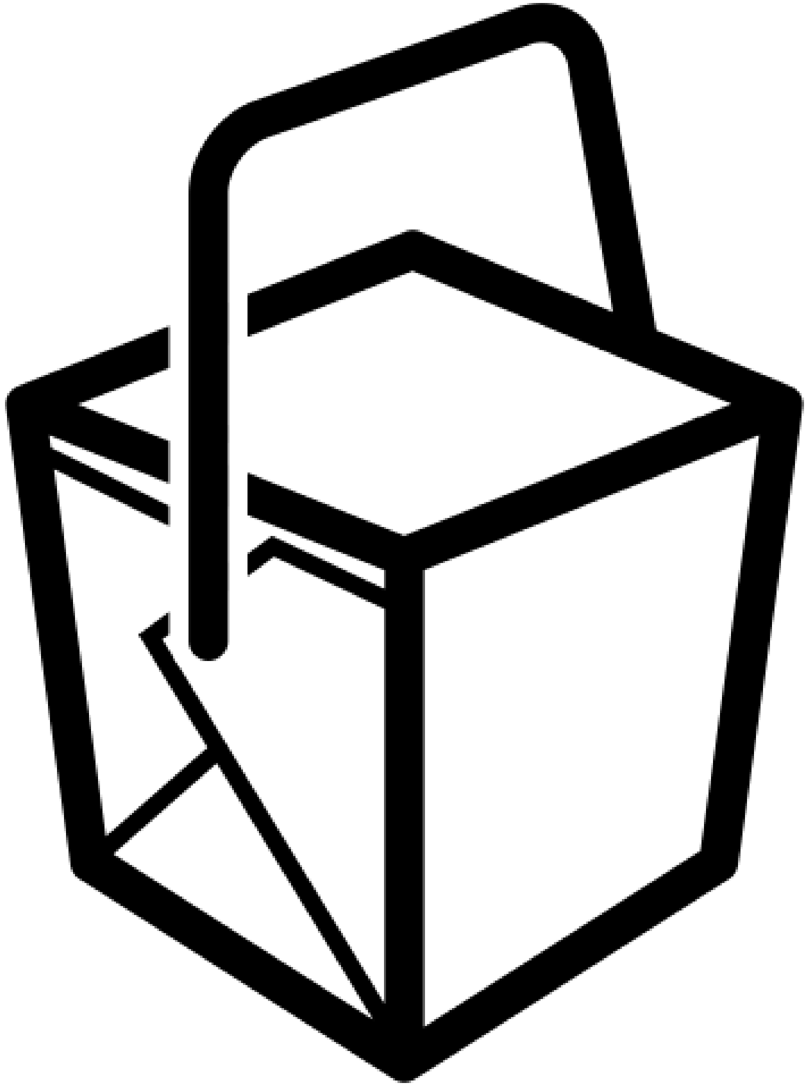
https://thenounproject.com/icon/library-751626/

What can I do?

- Don’t use YAML
  - If you can…
- Don’t allow tainted input in your YAML
  - If you can…
- Use the libraries’ methods for stringifying and not `JSON.stringify`
  - yaml: `stringfigy`
  - js-yaml: `dump`
- Configure the library to prevent or limit entities expansions
  - If you can…
  - yaml: `{maxAliasCount: -1}` or some small number
  - js-yaml: `{noRefs: false}`

https://thenounproject.com/icon/configure-1883381/

Takeaways



https://thenounproject.com/term/takeout/38140

Questions?

https://thenounproject.com/term/questions/1195076/

Thank You

Contact
https://github.com/mureinik/somebody-set-up-us-the-bomb
allon.mureinik@synopsys.com
https://www.linkedin.com/in/mureinik/
@mureinik