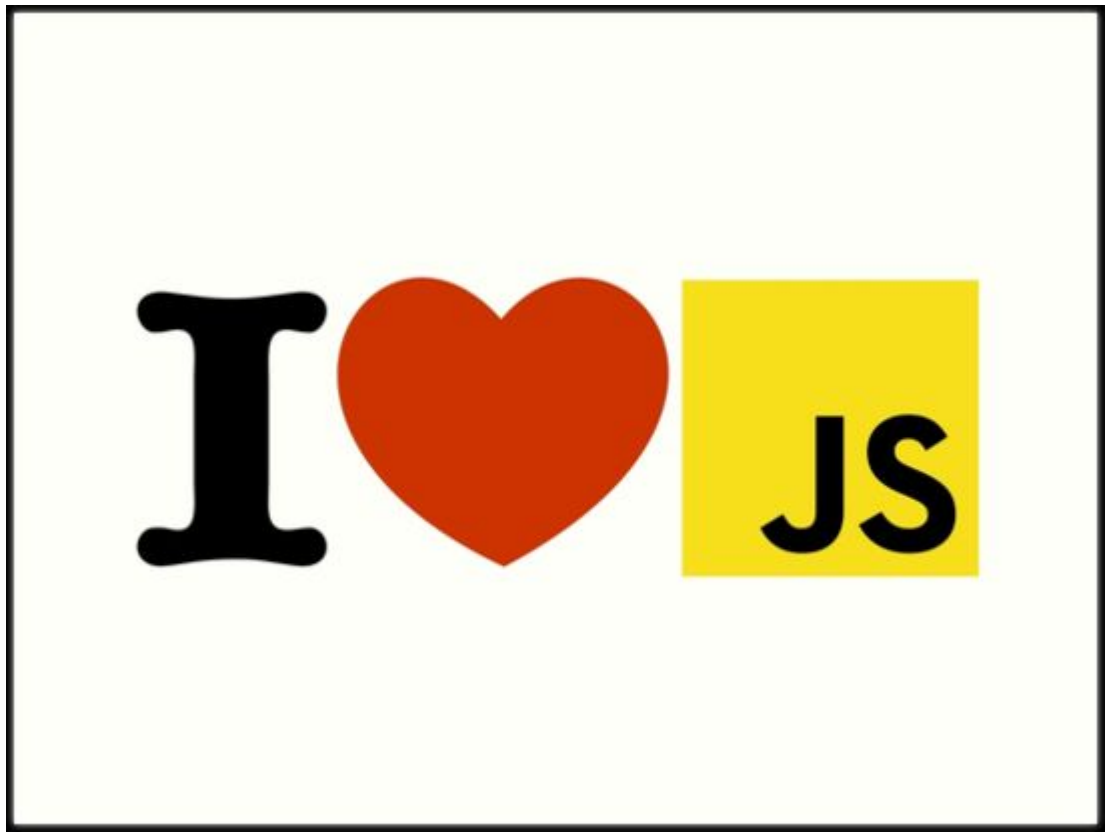
OWASP FOR DUMMIES

Lucian Petri


ionic
TS
JS


RO
PARDO


I
JS

Hacking

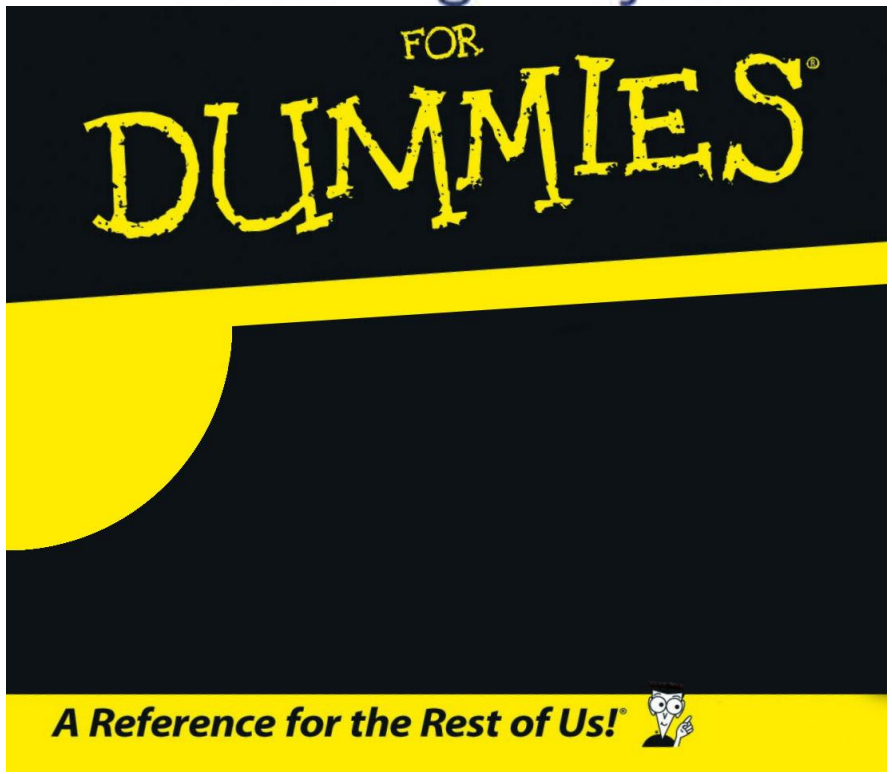
(Shhh…)

Disclaimer

- Limba pe care o voi folosi în prezentare va fi faimoasa Romengleza
- Prezentarea va fi foarte serioasă cu 0 sarcasm și ironie(I’m not lying)
- Nu vă voi arăta live hacking(I’m lying)
- Nici un calculator nu va fi rănit în procesul acestei demonstrări(hope so...)
- Eu nu sunt responsabil pentru orice vei face cu ce ai învățat aici și… blablabla

OWASP

Open Web Application Security Project

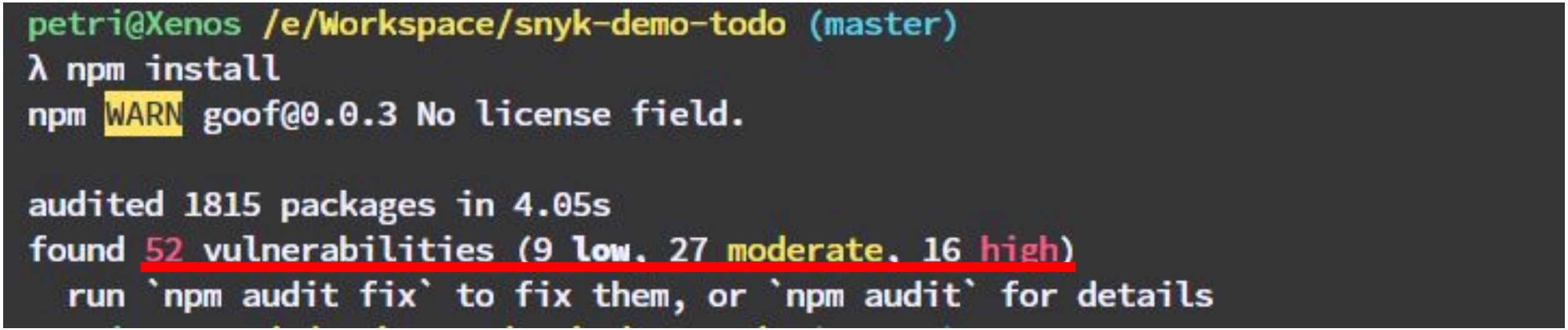


Using Components With Known Vulnerabilities
Insufficient Logging And Monitoring
Security Misconfiguration
Broken Authentication
Sensitive Data Exposure
Broken Access Control
XML External Entities
Cross-Site Scripting
SQL Injection

Javascript won!


Most Pull Requests 2017
GitHub
Javascript
2,300,000
Python
1,000,000
Java
986,000
Ruby
870,000
PHP
559,000
C++
413,000
CSS
335,000
C#
326,000
Go
285,000
C
239,000
Typescript
207,000
Shell
206,000
Swift
107,000
Scala
99,000
Objective-C
66,000


node
JS


petri@Xenos /e/Workspace/snyk-demo-todo (master)
λ npm install
npm WARN goof@0.0.3 No license field.
audited 1815 packages in 4.05s
found 52 vulnerabilities (9 low, 27 moderate, 16 high)
run `npm audit fix` to fix them, or `npm audit` for details

Back in the old days

VS

Today’s days

You could have air tight security

Code is vulnerable? Your fault.

More effort = More readable code

You can never know quickly enough

App vulnerable? Check yo modules!

Frameworks do your job

LET’S START H4CK1NG! <3


That's all Folks!
Q & A Time!

Links for help

- https://github.com/LucianPetri/goof
- http://dreamerslab.com/blog/en/write-a-todo-list-with-express-and-mongodb/
- https://snyk.io/vuln/npm:mongoose:20160116
- https://snyk.io/vuln/npm:st:20140206
- https://snyk.io/vuln/npm:marked:20150520