Swiss Cybervoting Pit(falls)

Jannis Kirschner

Me

- Independent Security Researcher
- CTF Player

Views are my own and not
related to my employer

@ xorkiwi

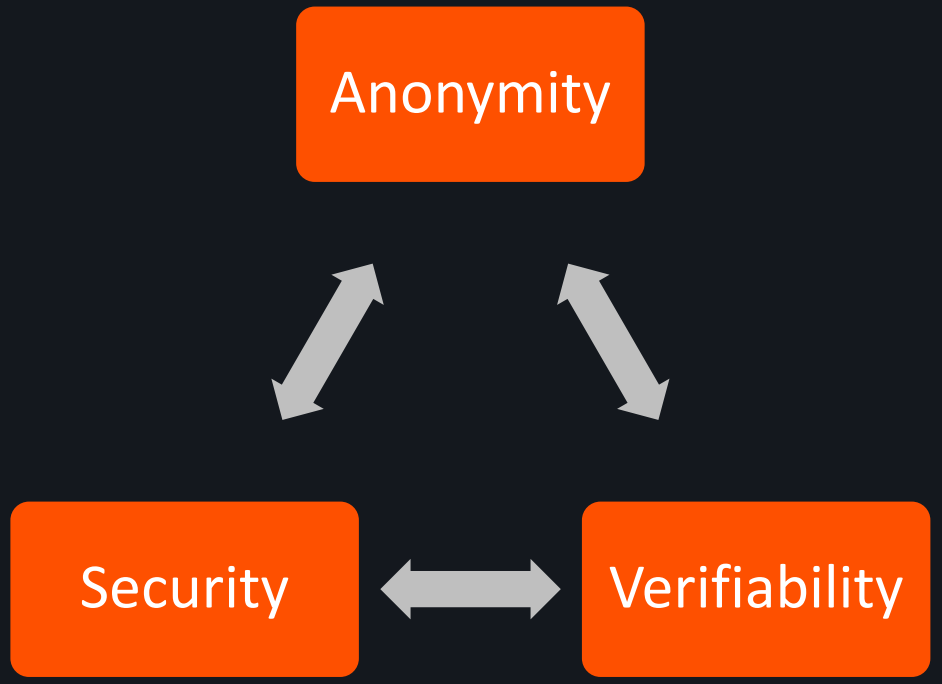
/in/janniskirschner

Why Evoting

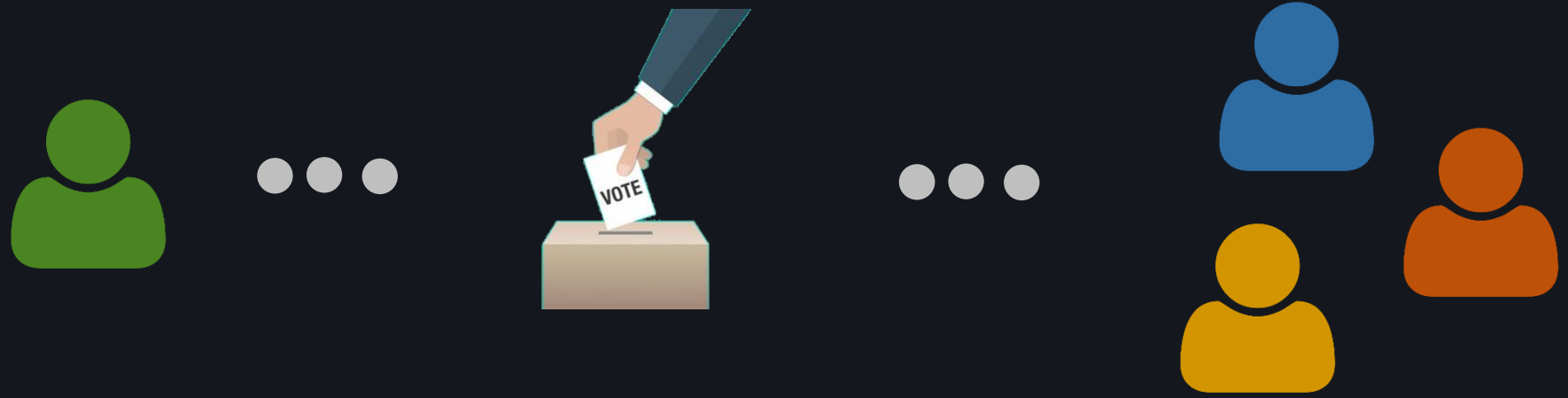
+ Comfortable for expats
+ Should attract young voters
+ More accessible

- Security risks on scale
- Very expensive to maintain
- System must be trusted

Evoting is hard



Offline vs Online



Not new

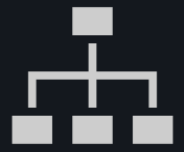
- Many cantons already have e-voting
- Extreme costs already caused stops
- Landscape consists of Scytl’s securevote and Geneva’s chvote

Source Code Publication

- Required to sign NDA
- Open Code != Open Source

Codebase

250‘000 LOC

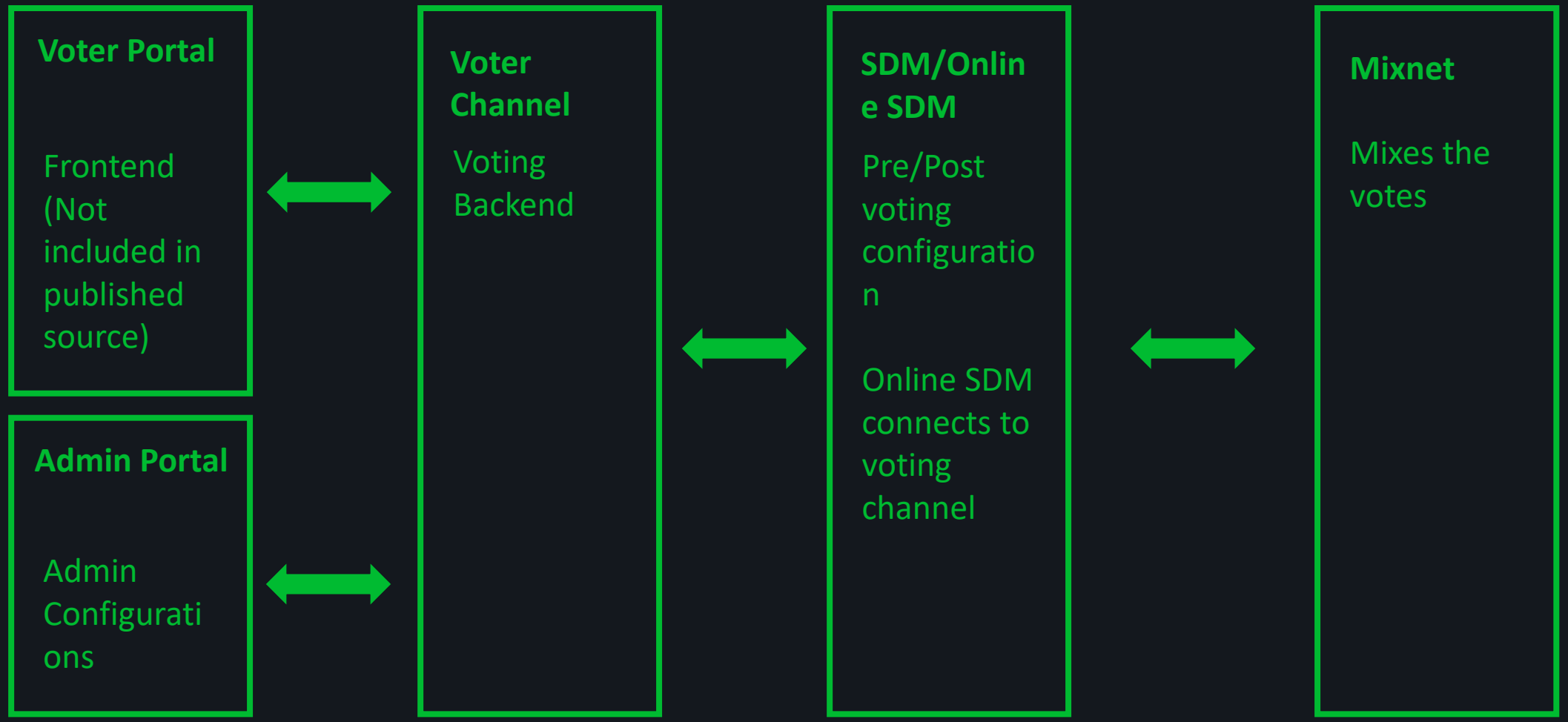


5 Components

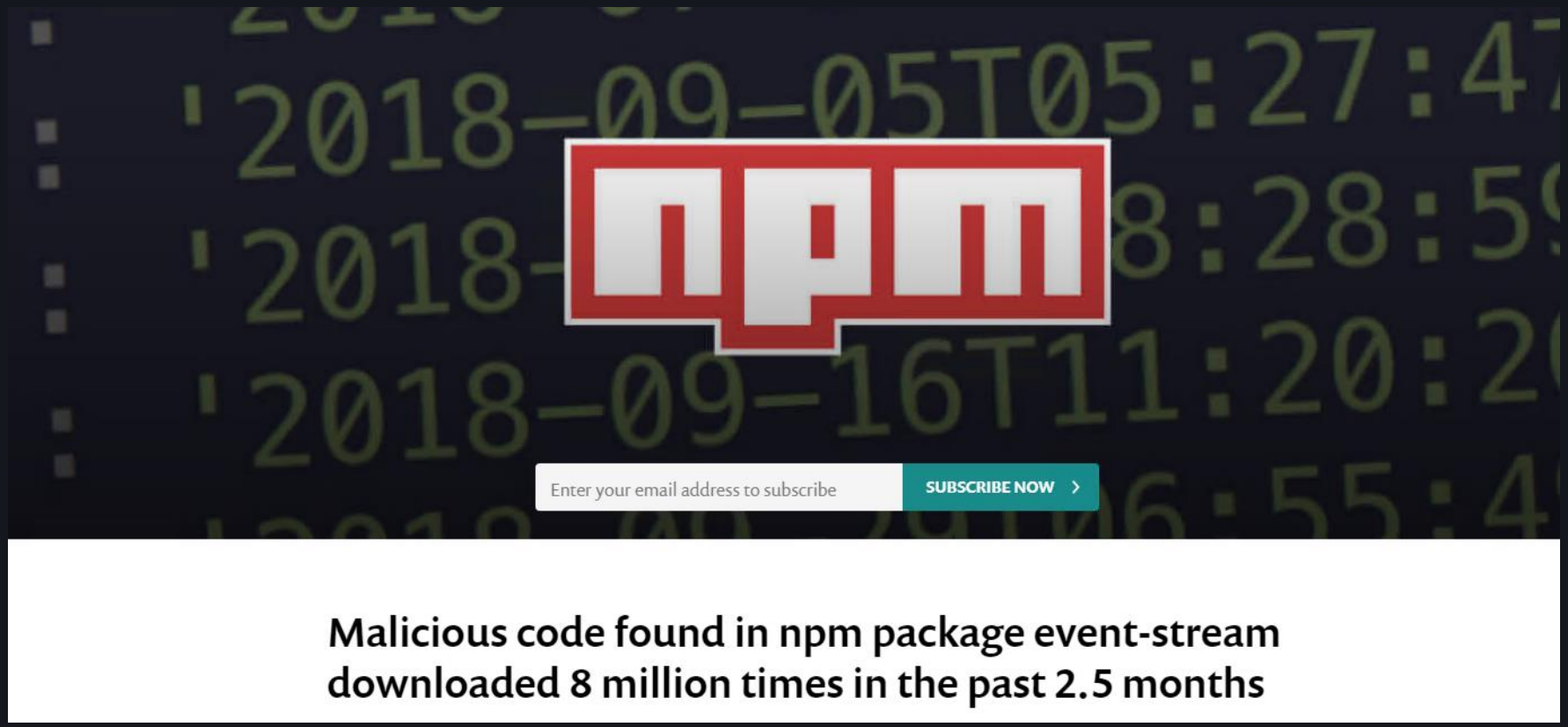
300 External Dependencies

55MB

Architecture



The danger of dependencies



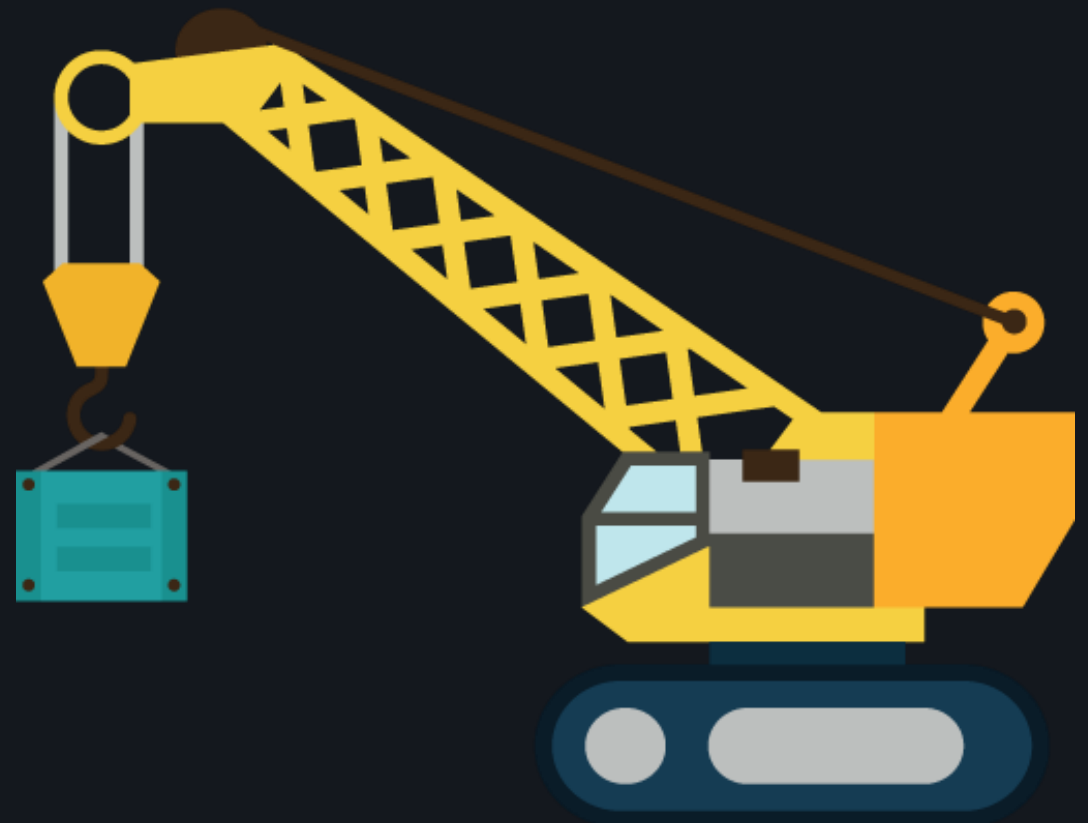
snyk.io

Documentation

- 3 High level documents
- Raml files in code describing various apis
- Security Audits released incompletely

Build

- Not buildable
- Public efford to reconstruct without success



The «Leak»

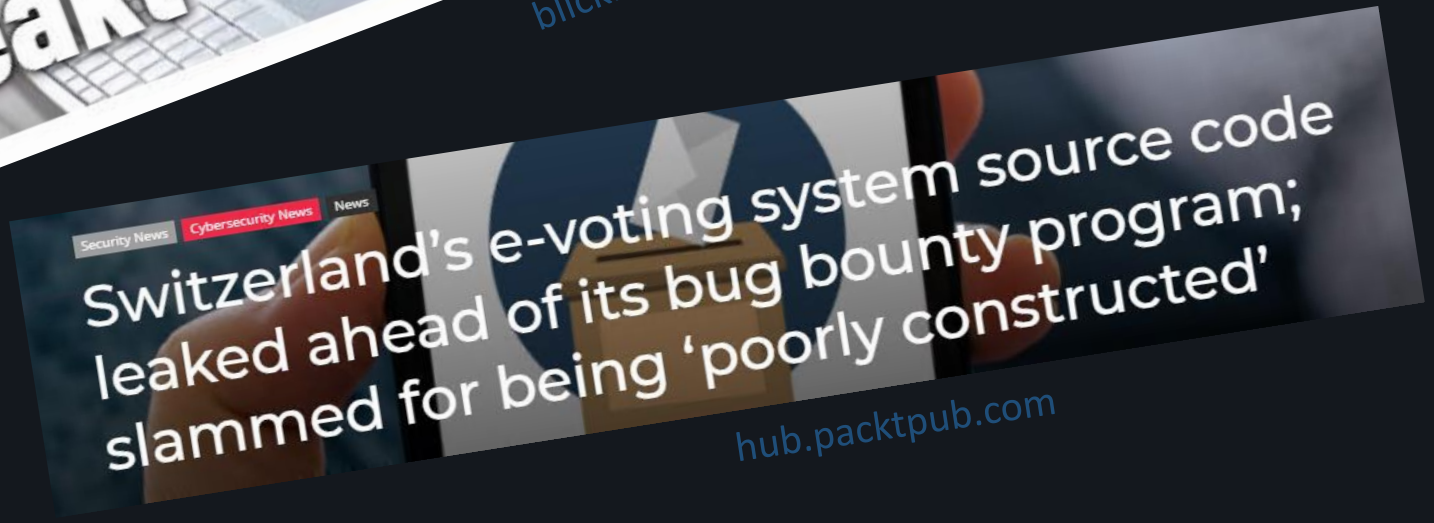
blick.ch

NEWS

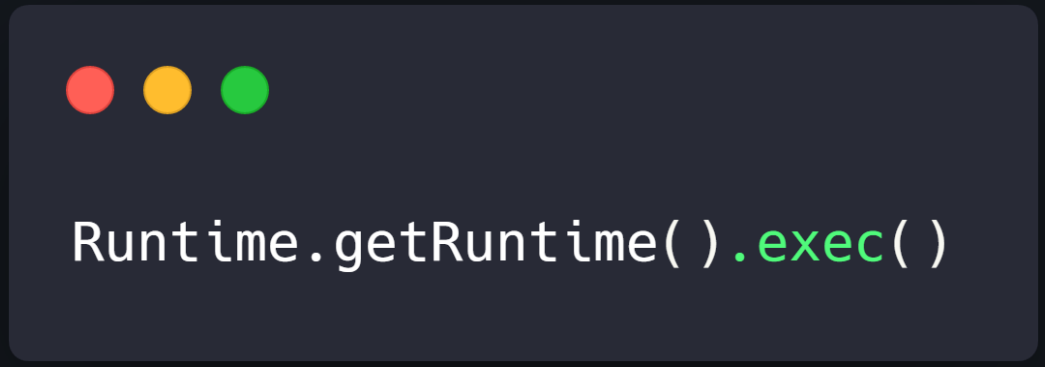
Veröffentlichung auf Gitlab

Update: Post äussert sich zu Quellcode-Leak

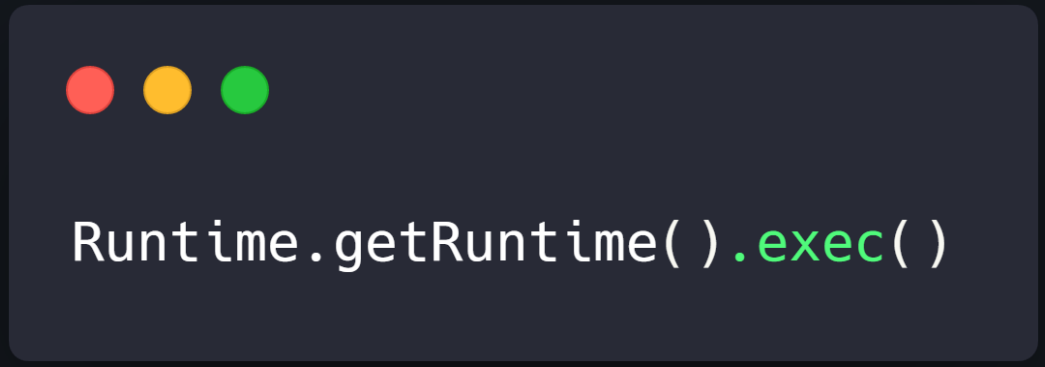
it-markt.ch



hub.packtpub.com


Runtime.getRuntime().exec()

SOM Command Injection



PIT Start

The scope of the PIT includes the public-facing service as well as corresponding e-voting backend of this dedicated instance:

- pit.evoting-test.ch (Voter Access used by voters)
- pit-admin.evoting-test.ch (Admin Access used by Secure Data Manager SDM)

onlinevote-pit.ch

PIT Start

The scope of the PIT includes the public-facing service as well as corresponding e-voting backend of this dedicated instance:

- pit.evoting-test.ch (Voter Access used by voters)
- pit-admin.evoting-test.ch (Admin Access used by Secure Data Manager SDM)

onlinevote-pit.ch

Pit Scope

Pit Scope

250‘000 LOC

Pit Scope

250‘000 LOC

Pit Scope

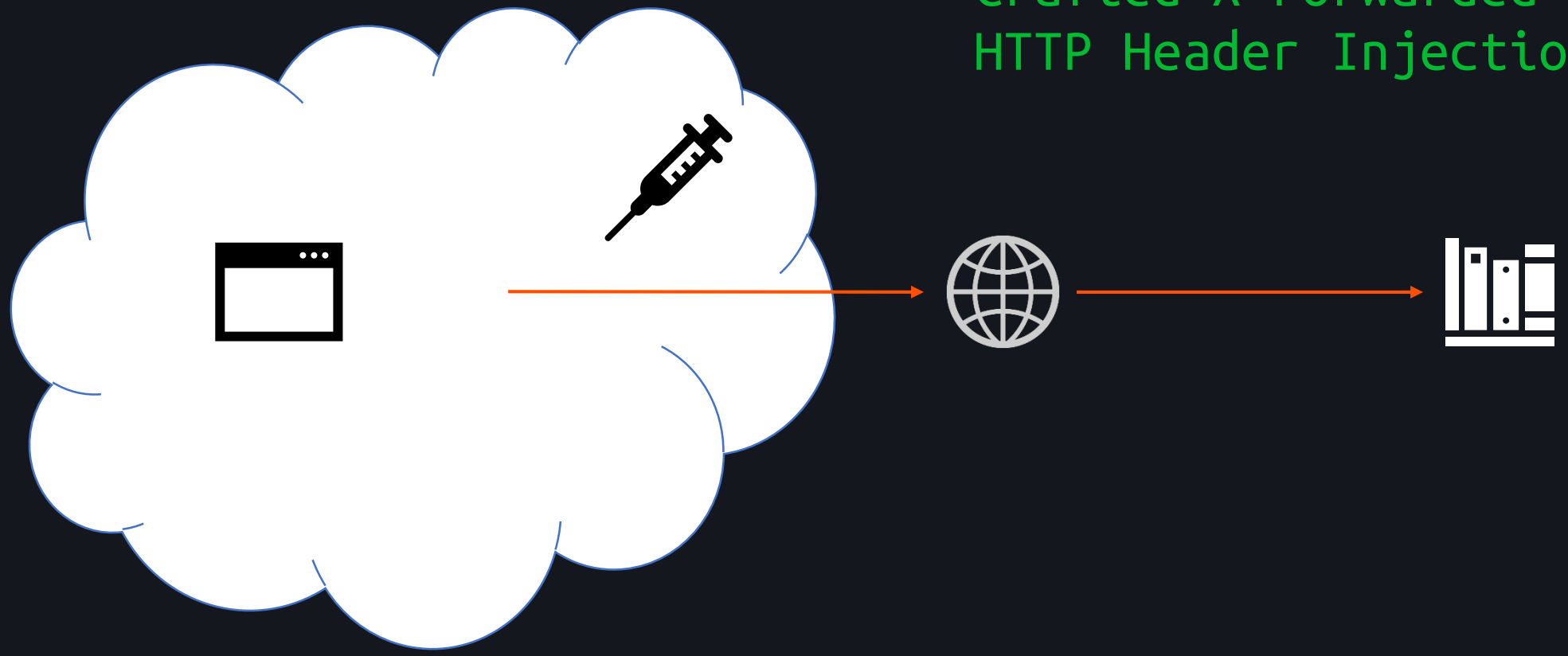
250‘000 LOC

Package	File	Function	Implementation & Client
voting	AuthenticationTokenResource	getAuthenticationToken()	ov-voting-workflow
voting	CastCodeResource	getCastCodeMessage()	ov-voting-workflow
voting	ChoiceCodeResource	getChoiceCodes()	ov-voting-workflow
voting	ConfirmationMessageResource	validateConfirmationMessage()	ov-voting-workflow
voting	CredentialInformationResource	getAuthenticationInformation()	ov-voting-workflow
voting	ExtendedAuthenticationResource	getEncryptedStartVotingKey()	ov-extended-authentication
voting	ExtendedAuthenticationResource	updateExtendedAuthData()	ov-extended-authentication
voting	ReceiptResource	getReceiptByVotingCardId()	ov-voting-workflow
voting	VoteResource	validateVoteAndStore()	ov-voting-workflow

All Available REST Endpoints

Still contained vulnerabilities

Crafted X-Forwarded-For
HTTP Header Injection



Crypto Flaws

- Remember the universal verifiability?...
- ...apperently it‘s broken aswell

Future?

- E-Voting Moratorium in Switzerland?
- Developments made by big corporations
- Lots of interesting research area