Securing Access to Internet Voting with the OWASP ModSecurity Core Rule Set

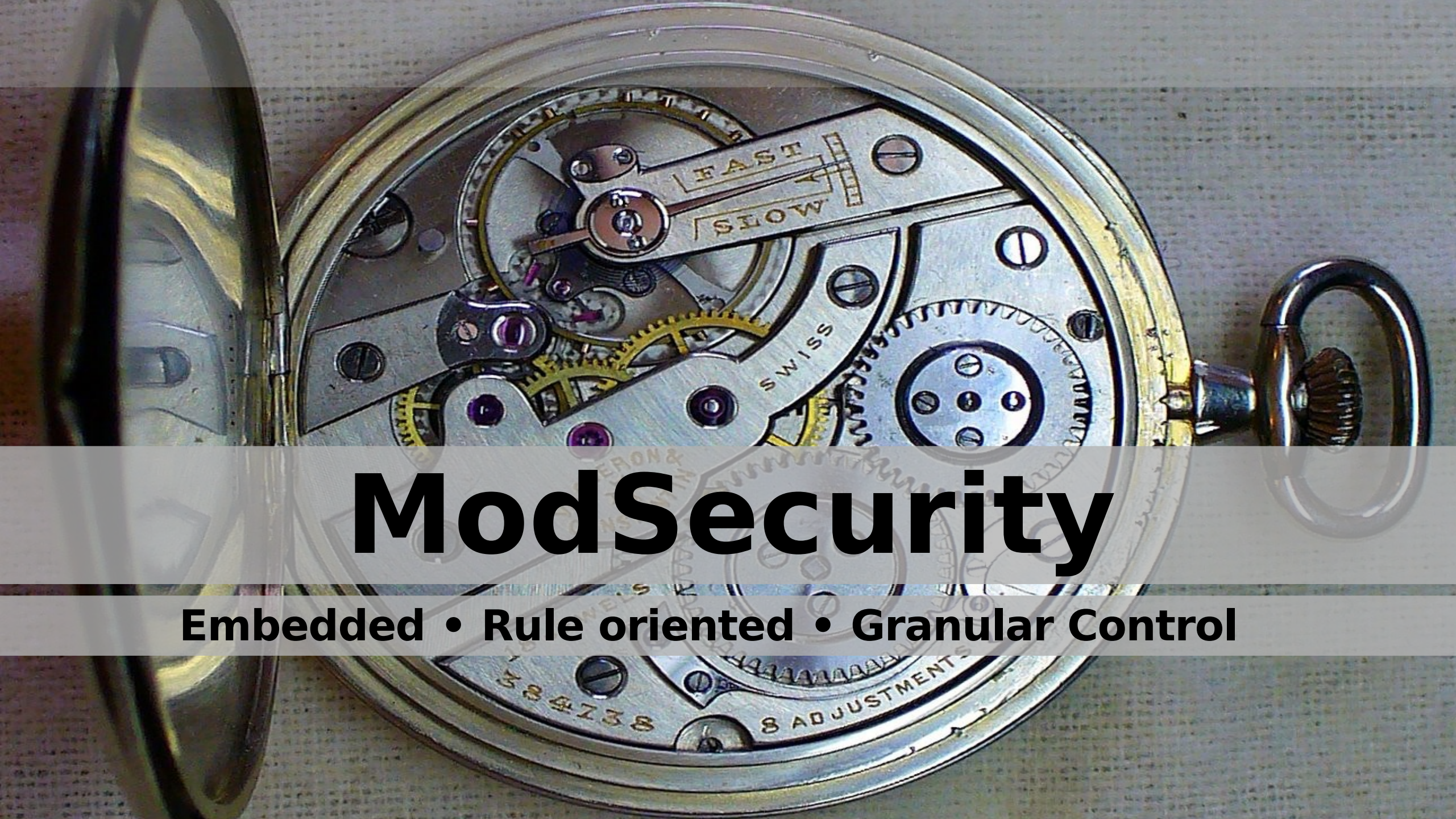
Christian Folini / @ChrFolini

Plan for Today

- Intro to the OWASP ModSecurity Core Rule Set
- History of Internet Voting in Switzerland
- Applying ModSec & CRS for maximum security

Safety Belts

Baseline / 1st Line of Defense



ModSecurity

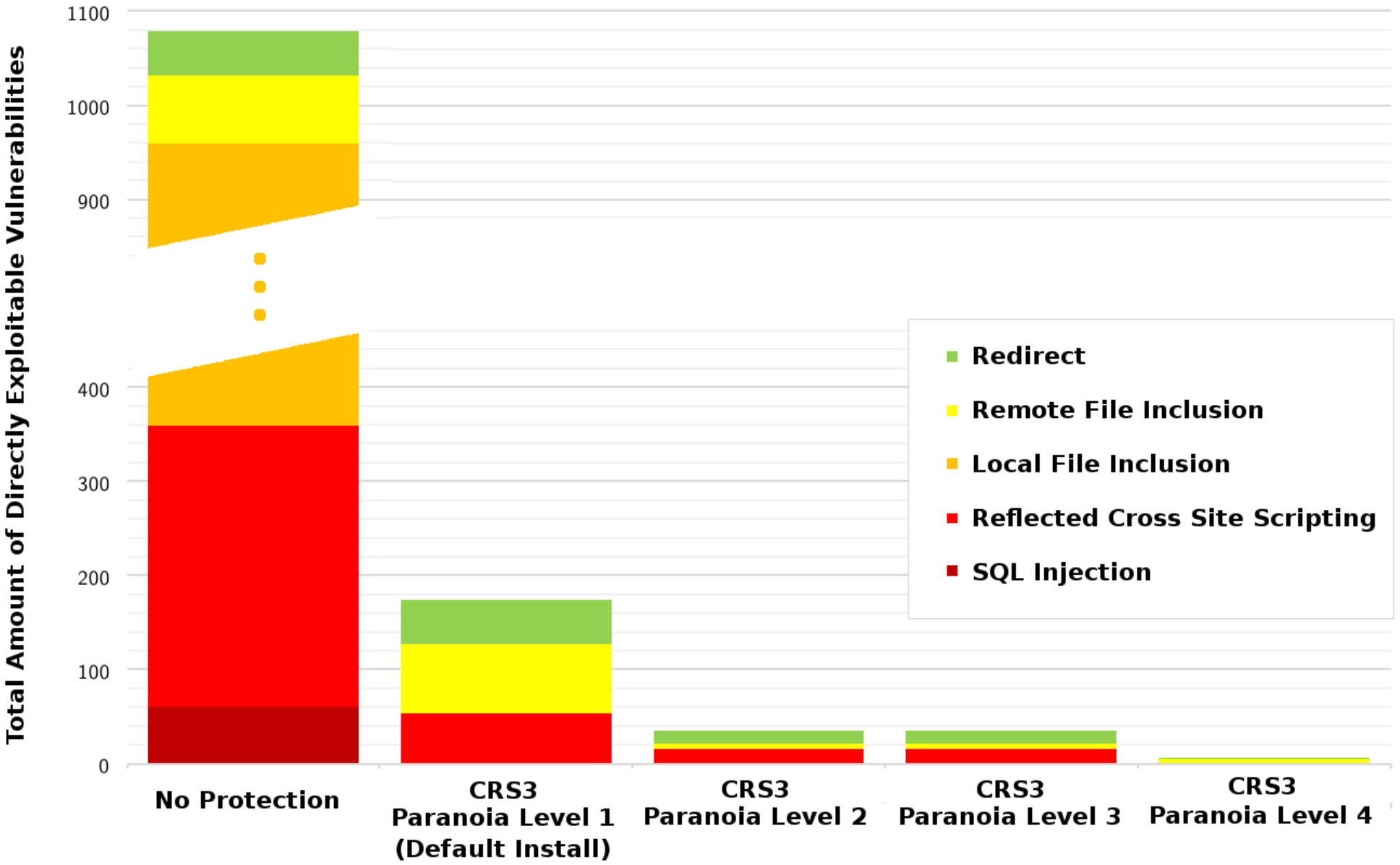
Embedded • Rule oriented • Granular Control

CRS

OWASP ModSecurity Core Rule Set

THE 1ST LINE OF DEFENSE

Burp vs. OWASP ModSecurity Core Rule Set 3.0



CRS3
Default Install

Redir.:	0%
RFI:	0%
LFI:	**-100%**
XSS:	**-82%**
SQLi:	**-100%**

Research based on
4.5M Burp requests.

Numbers by Tuomo Makkonen

TEST CASE GROUP	TEST CASE COUNT	AWS WAF AMAZON MANAGED	AWS WAF FORTINET MANAGED	AZURE WAF (CRS)	BARRACUDA WAF-AS-A-SERVICE	ALIBABA CLOUD WAF	GCP CLOUD ARMOR (CRS)	CLOUDFLARE WAF (CRS)
COMMAND EXECUTION	896	4 %	10 %	71 %	26 %	48 %	73 %	23 %
SERVER-SIDE INCLUDES (SSI) INJECTION	156	1 %	38 %	100 %	50 %	47 %	99 %	2 %
SQL INJECTION	1300	20 %	47 %	97 %	19 %	92%	99 %	74 %
PATH TRAVERSAL	9042	45 %	31 %	83 %	2 %	86 %	91 %	99 %
MALFORMED XML DOCUMENTS	134	37 %	39 %	96 %	16 %	61 %	97 %	67 %
CROSS SITE SCRIPTING (XSS)	294	23 %	34 %	71 %	65 %	58 %	85 %	58 %
		TESTED ON FEBRUARY 19th				TESTED ON MARCH 31st		

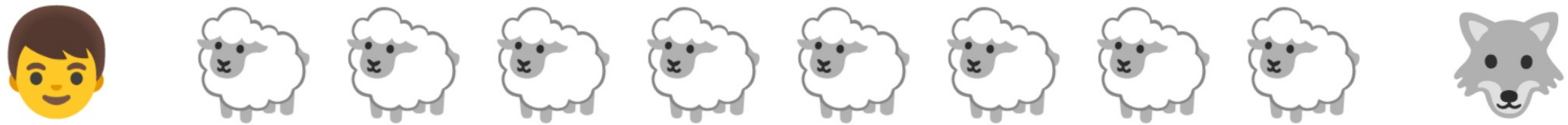
FRAKTAL

https://blog.fraktal.fi/cloud-waf-comparison-part-2-e6e2d25f558c

Why Open Source Beats Commercial!

Why Open Source Beats Commercial!

Why Open Source Beats Commercial!



Why Open Source Beats Commercial!

Why Open Source Beats Commercial!

Why Open Source Beats Commercial!

true positive

false positive

Why Open Source Beats Commercial!

🔔 **true positive**

🔔 **false positive**

$$$ 

false negative

Paranoia Levels

Paranoia Level 1: Minimal number of false positives

Baseline protection

Paranoia Level 2: More rules, some false positives

Real data in the service

Paranoia Level 3: Specialized rules, more false positives

Online banking level security

Paranoia Level 4: Crazy rules, many false positives

Nuclear power plant level security

Paranoia Levels

Paranoia Level 1: Minimal number of false positives

Baseline protection

Paranoia Level 2: More rules, some false positives

Real data in the service

Paranoia Level 3: Specialized rules, more false positives

Online banking level security

Paranoia Level 4: Crazy rules, many false positives

Internet Voting level security

False Positives (FPs)

- FPs are expected from PL2
- FPs are fought with rule exclusions
- Rule exclusion tutorials at netnea.com
- Rule exclusion software c-rex.netnea.com
- Attend one of my courses via netnea.com

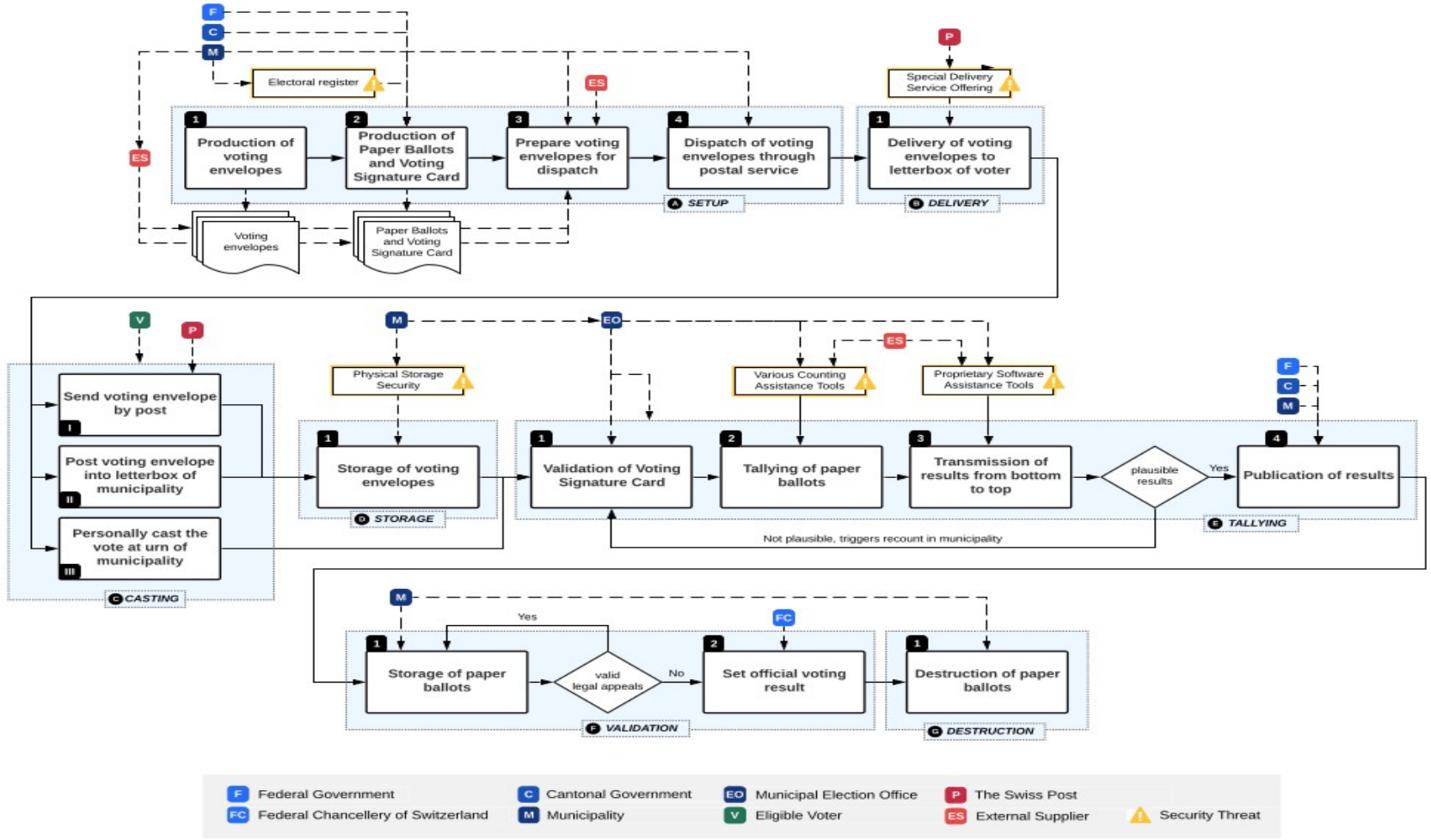
Summary OWASP Core Rule Set

- 1st Line of Defense against web application attacks
- Generic set of deny-rules for WAFs
- Blocks >80% of web application attacks by default
- Paranoia Levels can push this in the >95% region
- Granular control over the behavior of the WAF down to the parameter level

Voting in Switzerland

Photo: Gian Ehrensberger

Process Around Swiss Mail-in Ballots



Killer / Stiller : The Swiss Postal Voting Process and its System and Security Analysis

Typical Swiss Election Ballot

KANTON AARGAU

Wahl von 7 Mitgliedern des Grossen Rats vom 18. Oktober 2020

Bezirk Muri

Wahlzettel-Nr.

06	glp – Grünliberale Partei	
06.01	**Budmiger Hans-Peter (Hampi),** 1976, Unternehmer, Gemeindepräsident, Muri	1
~~06.02~~	~~**Langenbacher Knüsel Silvia,** 1966, Unternehmerin, Abtwil~~	
06.01	Budmiger Hans-Peter	2
06.03	**Peyer Samuel,** 1985, BSc in Wirtschaftsinformatik, Unternehmer, Muri	3
~~06.04~~	~~**Masoch Loredana,** 1996, BLaw, Masterstudentin Rechtswissenschaften,~~	
06.05	~~Waltenschwil~~ Stöckli Cornel	4
06.05	**Stöckli Cornel,** 1975, Dr. med., Rheumat. & Innere Med., Integrationskom., Muri	5
~~06.06~~	~~**Chande Sabrina,** 1989, Projektleiterin Elektroplanung, Mitglied GL, Buttwil~~	
04.01	Bucher Ralf, CVP	6
06.07	**Weber Thomas,** 1974, Content Manager, Journalist, Buttwil	7

Vom Wahlbüro auszufüllen →	Kandidatenstimmen:	Zusatzstimmen:	Total:

Typical Swiss Election Ballot

KANTON AARGAU

Wahl von 7 Mitgliedern des Grossen Rats vom 18. Oktober 2020

Bezirk Muri

Wahlzettel-Nr.

06	glp – Grünliberale Partei	
06.01	**Budmiger Hans-Peter (Hampi),** 1976, Unternehmer, Gemeindepräsident, Muri	1
~~06.02~~	~~**Langenbacher Knüsel Silvia,** 1966, Unternehmerin, Abtwil~~	
06.01	Budmiger Hans-Peter	2
06.03	**Peyer Samuel,** 1985, BSc in Wirtschaftsinformatik, Unternehmer, Muri	3
~~06.04~~	~~**Masoch Loredana,** 1996, BLaw, Masterstudentin Rechtswissenschaften, Waltenschwil~~	4
06.05	Stöckli Cornel	
06.05	**Stöckli Cornel,** 1975, Dr. med., Rheumat. & Innere Med., Integrationskom., Muri	5
~~06.06~~	~~**Chande Sabrina,** 1989, Projektleiterin Elektroplanung, Mitglied GL, Buttwil~~	6
04.01	Bucher Ralf, CVP	
06.07	**Weber Thomas,** 1974, Content Manager, Journalist, Buttwil	7

Vom Wahlbüro auszufüllen →	Kandidatenstimmen:	Zusatzstimmen:	Total:

Bonus points for spotting the content manager from Butt-ville.

Key Argument against Internet Voting

"We simply can’t build an Internet voting system that is secure against hacking because of the requirement for a secret ballot."

Bruce Schneier, Online Voting Won’t Save Democracy, The Atlantic, May 2017

Arguments in Favor of Internet Voting

The Swiss Perspective

Arguments in Favor of Internet Voting

The Swiss Perspective

- **Citizens living abroad**

Arguments in Favor of Internet Voting

The Swiss Perspective

- **Citizens living abroad**
- **Visually impaired and quadriplegic voters**

Arguments in Favor of Internet Voting

The Swiss Perspective

- **Citizens living abroad**
- **Visually impaired and quadriplegic voters**
- **Formally invalid ballots**

Arguments in Favor of Internet Voting

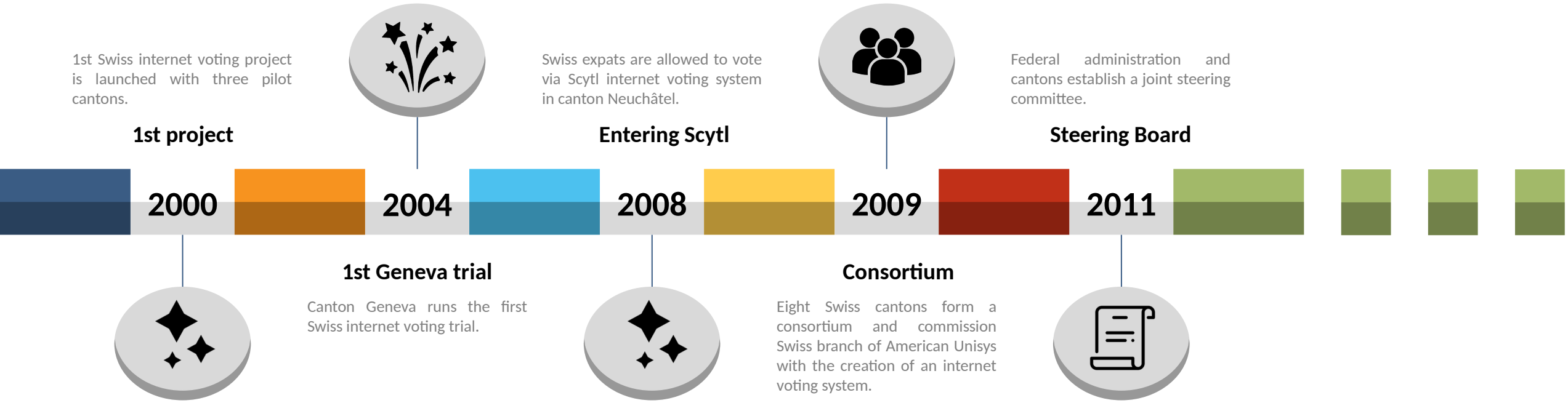
The Swiss Perspective

- **Citizens living abroad**
- **Visually impaired and quadriplegic voters**
- **Formally invalid ballots**
- **Security issues of physical voting**

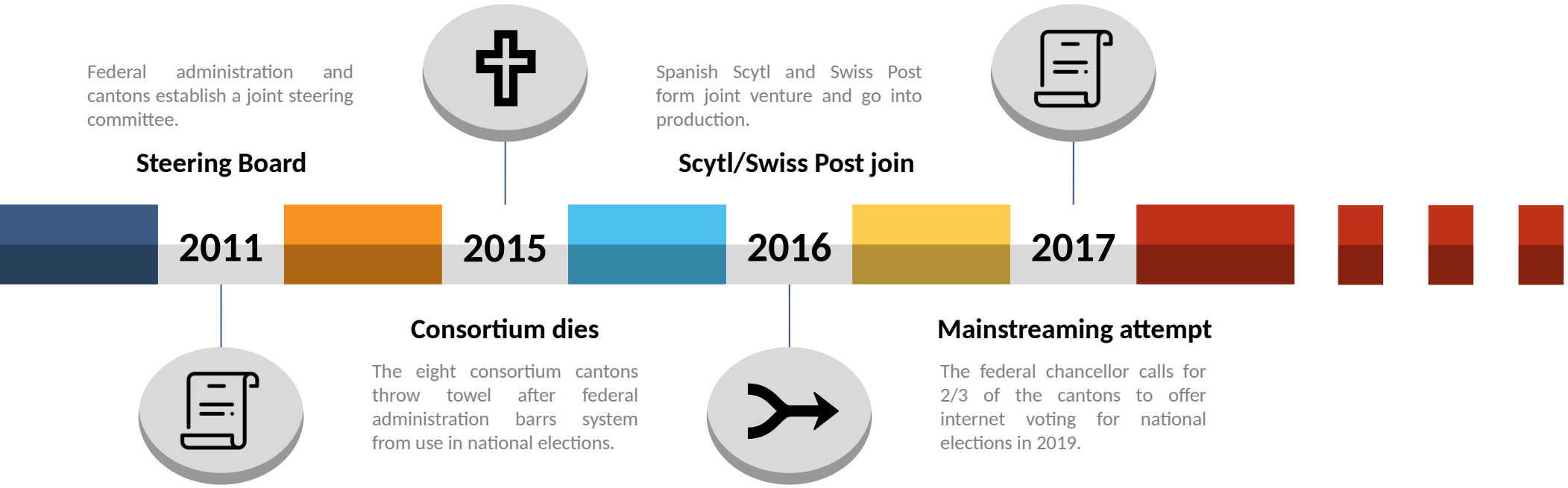
The Cantons of Switzerland

Graphic: Wikipedia

Timeline Internet Voting in Switzerland



Timeline Internet Voting in Switzerland

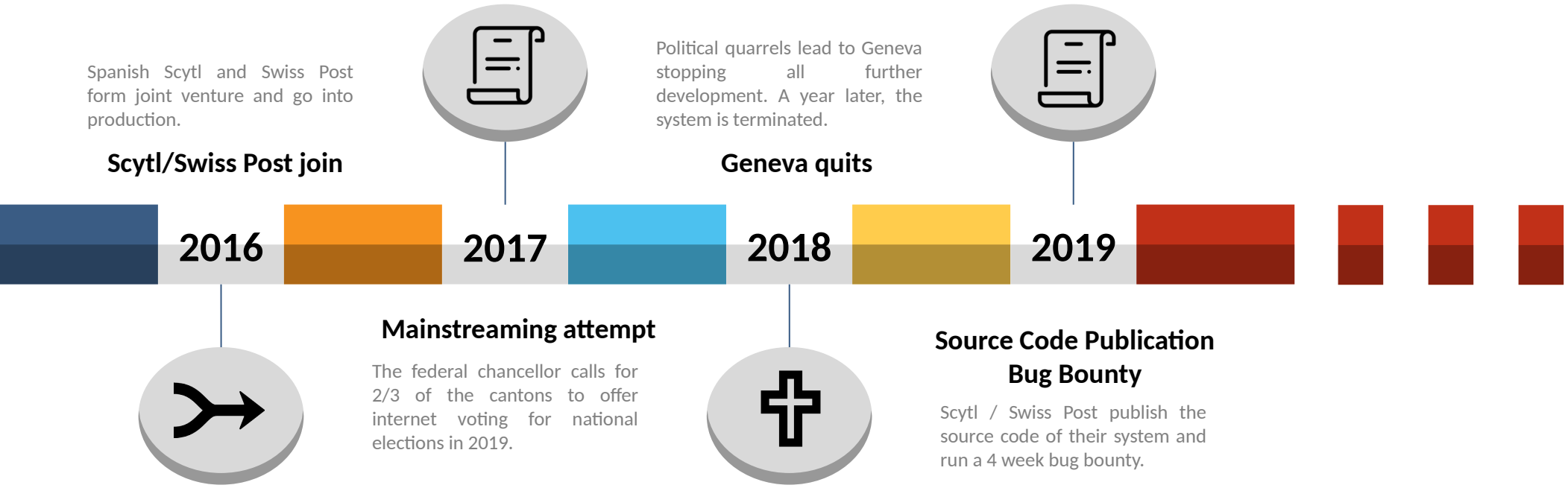


Geneva Quits

2018: Development stopped
2019: System terminated

Source: Twitter: @GE_chancellerie (1141332323025195009)

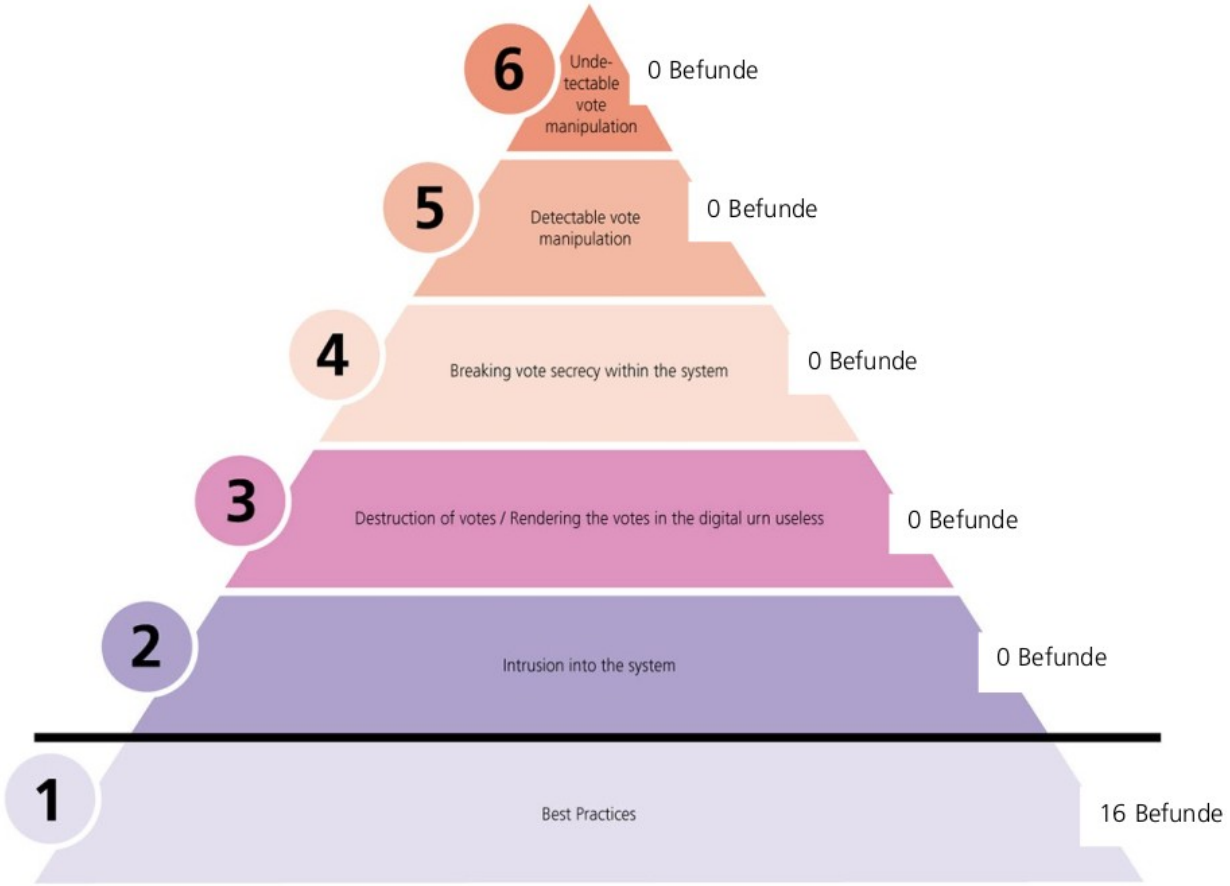
Timeline Internet Voting in Switzerland



Swiss Post Bug Bounty: We got this!

Abschlussbericht Öffentlicher Intrusionstest

DIE POST



[BEST PRACTICES] Incorrect 'HTTP-Strict-Transport-Security' header on 'pit-admin.evoting-test.ch'

REDMINE ID: #188
SUBMISSION: Feb. 25th 2019, 23:19 (GMT+1)
RESEARCHER(S): Jacob.Rees-Earcher
COMPENSATION: CHF 200.-

When connecting to 'pit-admin.evoting-test.ch' on port 443, the server sends an HTTP-Strict-Transport-Security header even for plaintext HTTP connections, which is a violation of RFC 6797. The additional header also does not contain the 'includeSubdomain' directive, which would be a security best-practice.

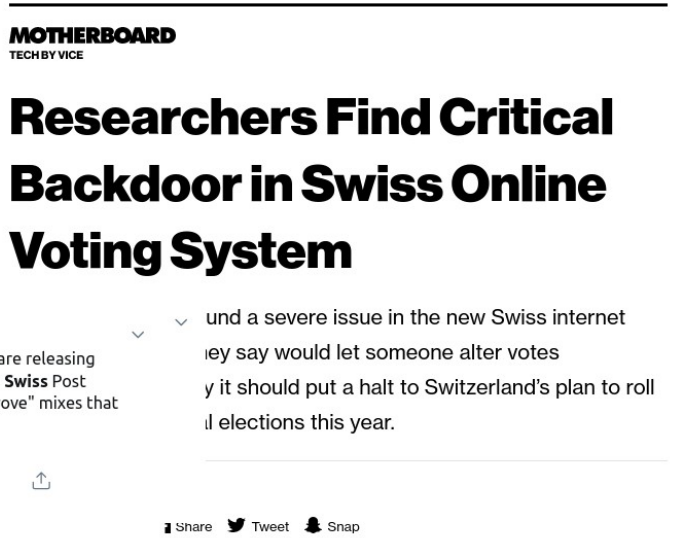
[BEST PRACTICES] Use of 'unsafe-eval' and 'unsafe-inline' in Content Security Policy

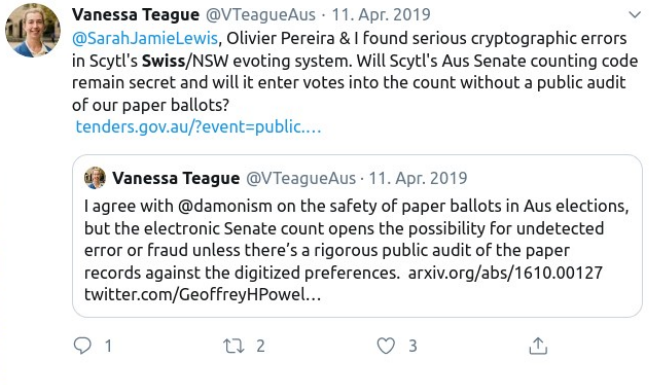
[BEST PRACTICES] Multiple occurrences of 'X-XSS-Protection' HTTP header

REDMINE ID: #234
SUBMISSION: Feb. 28th 2019, 14:57 (GMT+1)
RESEARCHER(S): pitbull
COMPENSATION: CHF 100.-

Some error messages sent as responses by the web server (specifically, the '403 Forbidden' status code) include two identical occurrences of the 'X-XSS-Protection' security header. This behavior is non-standard, and could lead to undefined behavior in some browsers.

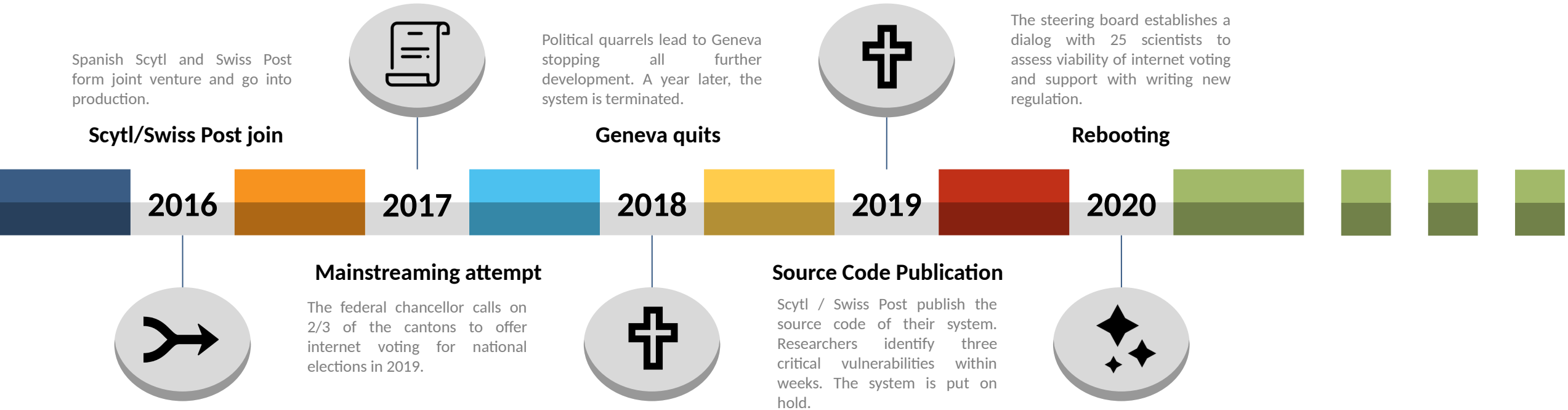
Swiss Post / Scytl Source Code: Not so good





to be continued ...

Timeline Internet Voting in Switzerland



Scientific report

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Bundeskanzlei BK
Sektion Politische Rechte

Summary of the expert dialog

Redesign of Internet Voting Trials in Switzerland 2020

19th November 2020

Contents

https://www.bk.admin.ch/bk/en/home/politische-rechte/e-voting.html

Timeline Internet Voting in Switzerland

2020.2

Survey

The dialogue starts with a survey over 62 questions sent to 25 scientists

2020.3

Covid-19 hits

When the on-site workshops were slowly taking shape, Switzer-land entered a lock-down and the on-site gatherings had to be called off.

2020.4

Online dialogue

The workshops are replaced with a 12 weeks online dialogue on a dedicated gitlab platform.

2020.7

Additional research

Several separate re-search articles are commissioned with individual scientists to bring up more infor-mation on individual questions.

2020.11

Scientific report

The steering board publishes the 70 pages report with the re-commendations of the scientists.

2021.12

New regulation

Following the public hearing on a draft new law, the federal chancellery is meant to put the new regulation on internet voting into practice. Swiss Ppost has announced to return into production in 2022.

Summary Internet Voting in Switzerland

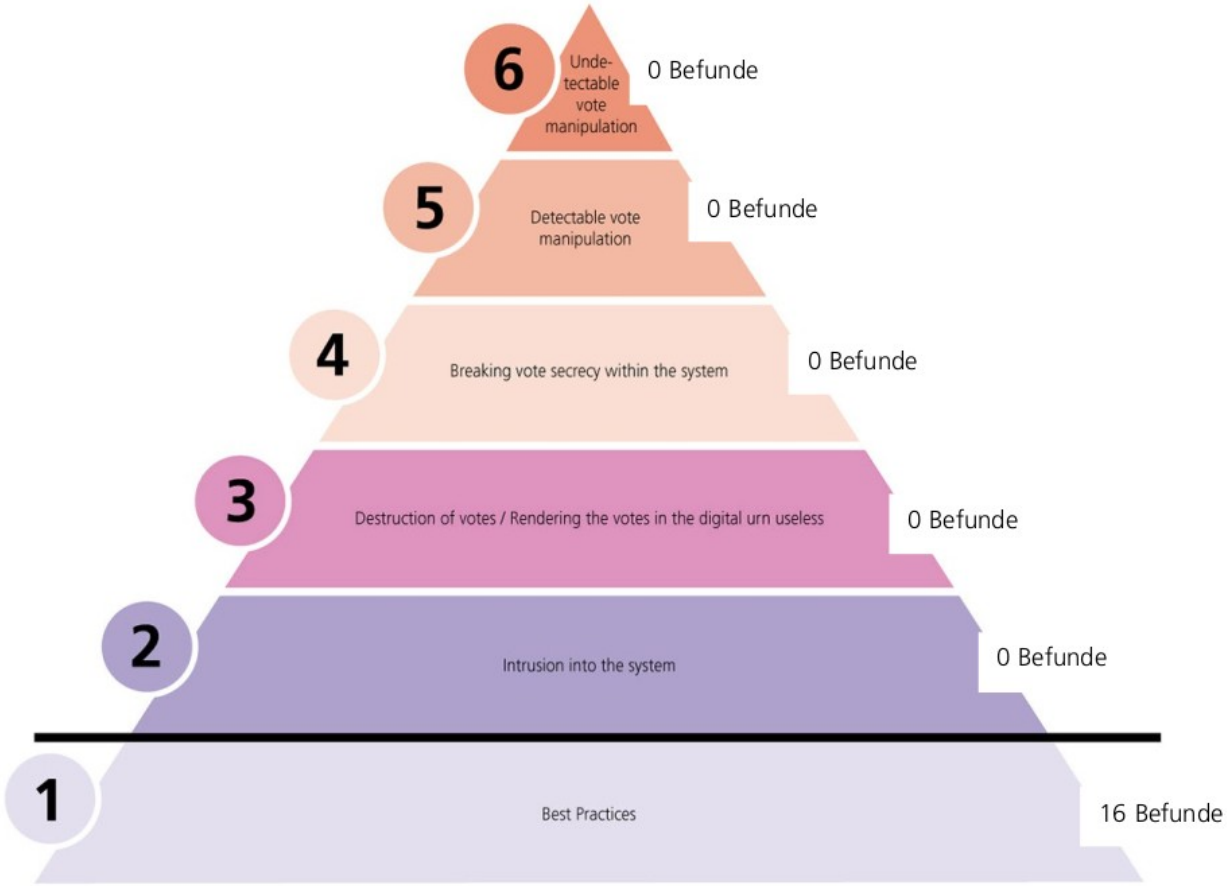
- **Switzerland is a useful test bed for online voting**
- **Iterative process with strict supervision on federal level**
- **Expert dialogue with recommendations in 2020**
- **New regulation 2021**
- **New online voting trials scheduled for 2022**

Download English version of scientifc report / expert dialogue from https://www.bk.admin.ch/bk/en/home/politische-rechte/e-voting.html

How do you pull this off?

Abschlussbericht Öffentlicher Intrusionstest

DIE POST



[BEST PRACTICES] Incorrect 'HTTP-Strict-Transport-Security' header on 'pit-admin.evoting-test.ch'

REDMINE ID: #188
SUBMISSION: Feb. 25th 2019, 23:19 (GMT+1)
RESEARCHER(S): Jacob.Rees-Earcher
COMPENSATION: CHF 200.-

When connecting to 'pit-admin.evoting-test.ch' on port 443, the server sends an HTTP-Strict-Transport-Security header even for plaintext HTTP connections, which is a violation of RFC 6797. The additional header also does not contain the 'includeSubdomain' directive, which would be a security best-practice.

[BEST PRACTICES] Use of 'unsafe-eval' and 'unsafe-inline' in Content Security Policy

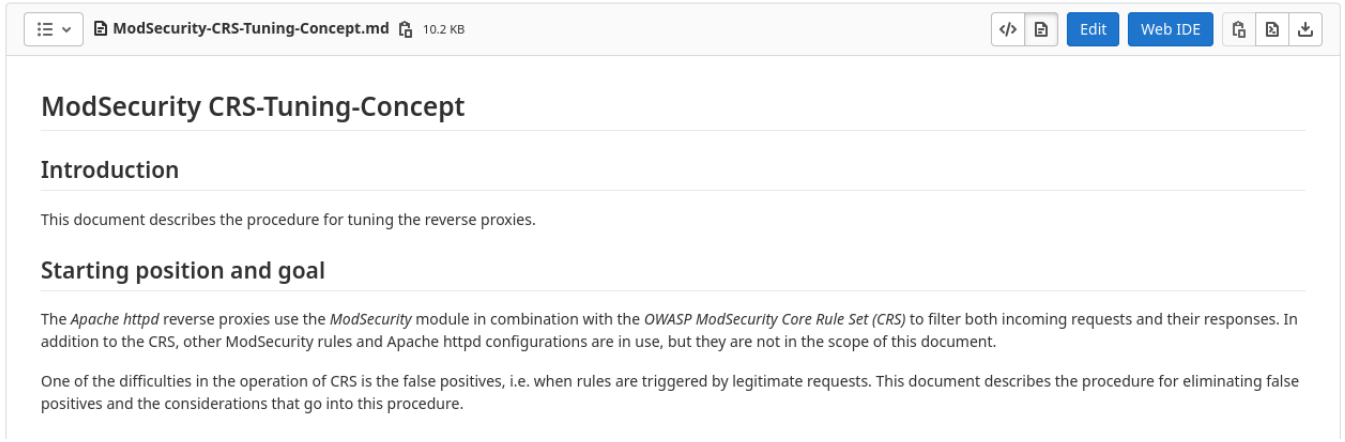
[BEST PRACTICES] Multiple occurrences of 'X-XSS-Protection' HTTP header

REDMINE ID: #234
SUBMISSION: Feb. 28th 2019, 14:57 (GMT+1)
RESEARCHER(S): pitbull
COMPENSATION: CHF 100.-

Some error messages sent as responses by the web server (specifically, the '403 Forbidden' status code) include two identical occurrences of the 'X-XSS-Protection' security header. This behavior is non-standard, and could lead to undefined behavior in some browsers.

Swiss Post Documentation

- **Transparency Initiative (clear advice by scientific report)**
- **Guidelines how to deploy and tune OWASP Core Rule Set**
- **https://gitlab.com/swisspost-evoting/e-voting/e-voting-documentation/-/blob/master/Operations/ModSecurity-CRS-Tuning-Concept.md**



Tune Down to Zero

Absence of False Positives • Trust in Alerts • A Liberating Moment

Positive Security Rule Set

Default Deny • List of Allowed Resources • Reduce Attack Surface

Divide and Rule

Zero tolerance • Ban attackers • fail2ban

Additional Rule Sets Worth Considering

- Monitoring the flow of the application
- Timing and rhythm
- Client Fingerprinting

Defenses Beyond ModSecurity

- Application Layer DDoS
- Quality of Service (QoS)
- IP Reputation / DNS Blacklisting
- GeoIP

Key Elements of a High Security WAF

- OWASP ModSecurity CRS at Paranoia Level 4
- Complementary Positive Security Rule Set
- Application Level DDoS Defense
- QoS
- IP Reputation / DNS Blacklisting
- GeoIP

Questions and Answers, Contact

Contact: @ChrFolini

christian.folini@netnea.com

CRS

THE 1ST LINE OF DEFENSE