

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

Christian Folini / @ChrFolini

Plan for Today

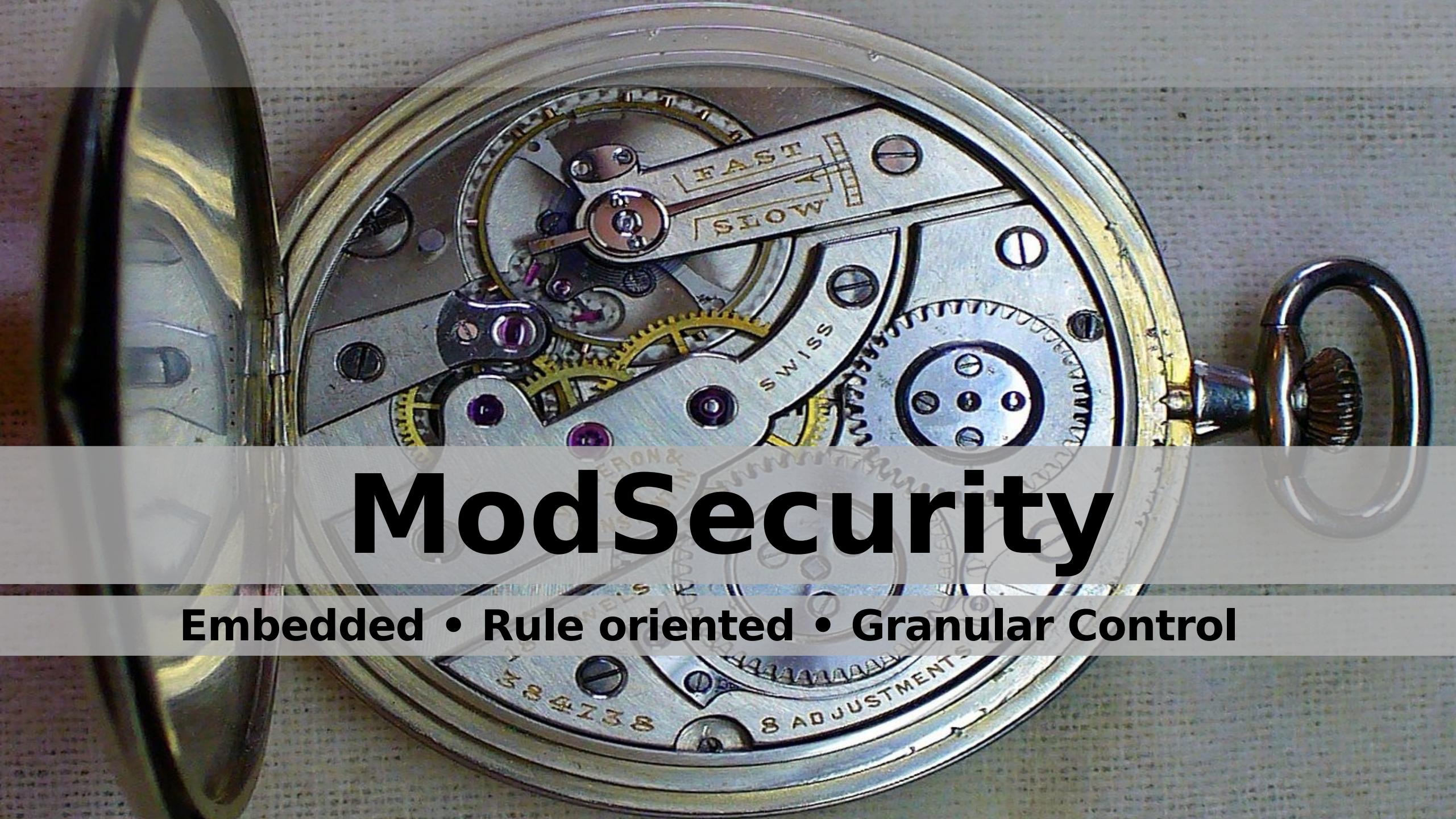
- **Intro to the OWASP ModSecurity Core Rule Set**
- **History of Internet Voting in Switzerland**
- **Applying ModSec & CRS for maximum security**





Safety Belts

Baseline / 1st Line of Defense



ModSecurity

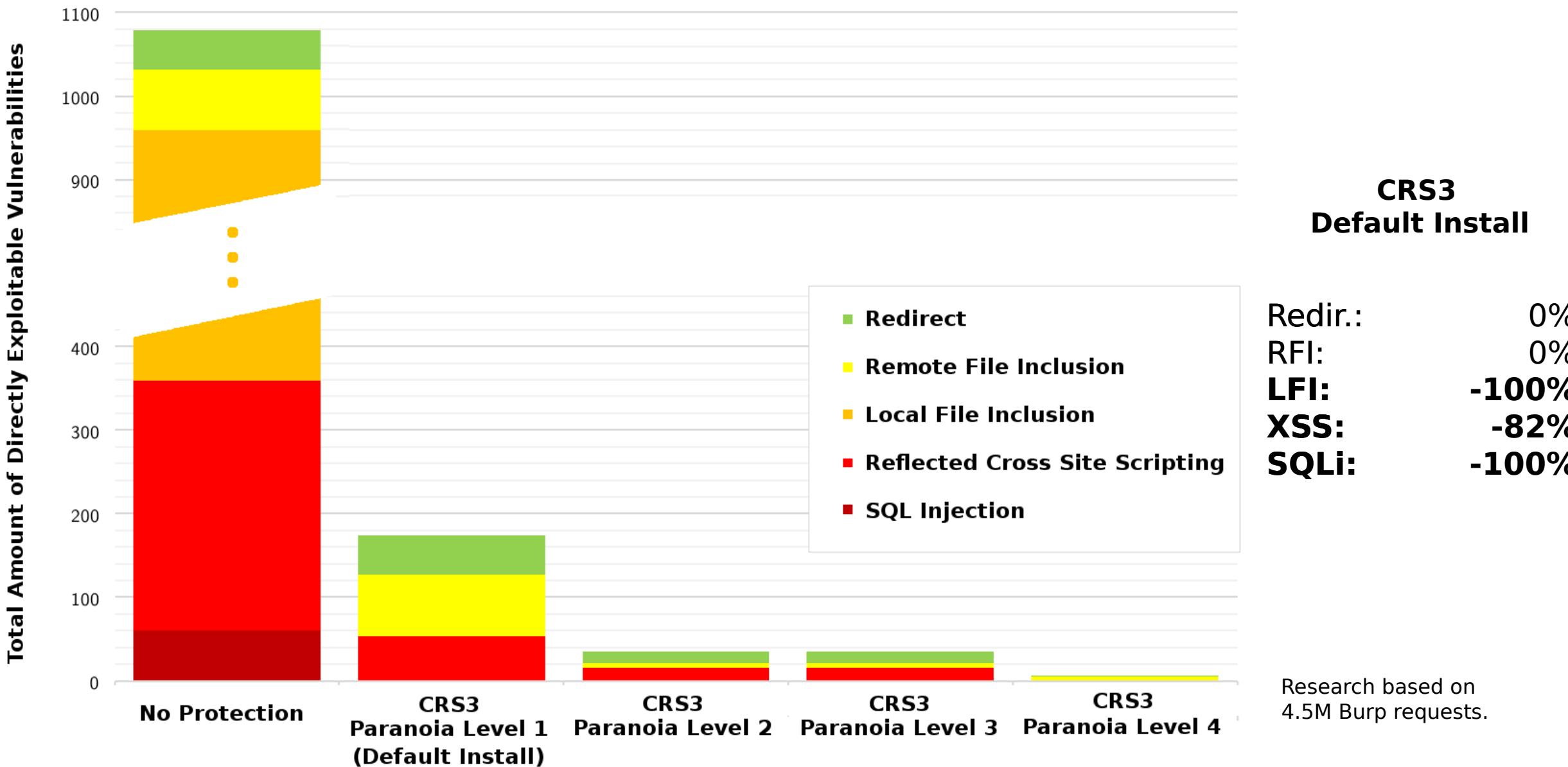
Embedded • Rule oriented • Granular Control



CRS

OWASP
ModSecurity
Core Rule Set
THE 1ST LINE OF DEFENSE

Burp vs. OWASP ModSecurity Core Rule Set 3.0



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

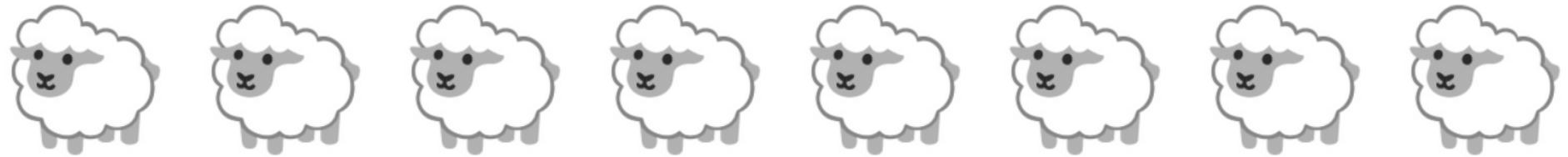
<https://blog.fraktal.fi/cloud-waf-comparison-part-2-e6e2d25f558c>



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!



true positive



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



RULE EXCLUSIONS

ENTIRE RULES
<p>STARTUP TIME</p> <p>WHEN STARTING SERVER WHEN RELOADING SERVER PLACE AFTER CRS INCLUDE</p> <p>SecRuleRemoveById SecRuleRemoveByTag</p> <p>SecRuleRemoveById 942100,... SecRuleRemoveByTag "attack-sqli"</p>
<p>RUN TIME</p> <p>WHEN EXAMINING A REQUEST PLACE BEFORE CRS INCLUDE</p> <p>ctl:ruleRemoveById ctl:ruleRemoveByTag</p> <p>...,ctl:ruleRemoveById:920300 ...,ctl:ruleRemoveByTag:attack-sqli</p>

PARAMETER IN RULES
<p>STARTUP TIME</p> <p>WHEN STARTING SERVER WHEN RELOADING SERVER PLACE AFTER CRS INCLUDE</p> <p>SecRuleUpdateTargetById SecRuleUpdateTargetByTag</p> <p>SecRuleUpdateTargetById 942100 !ARGS:password SecRuleUpdateTargetByTag "attack-sqli" !ARGS:password</p>
<p>RUN TIME</p> <p>WHEN EXAMINING A REQUEST PLACE BEFORE CRS INCLUDE</p> <p>ctl:ruleRemoveTargetById ctl:ruleRemoveTargetByTag</p> <p>...,ctl:ruleRemoveTargetById:942100,ARGS:password ...,ctl:ruleRemoveTargetByTag:attack-sqli,ARGS:password</p>



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

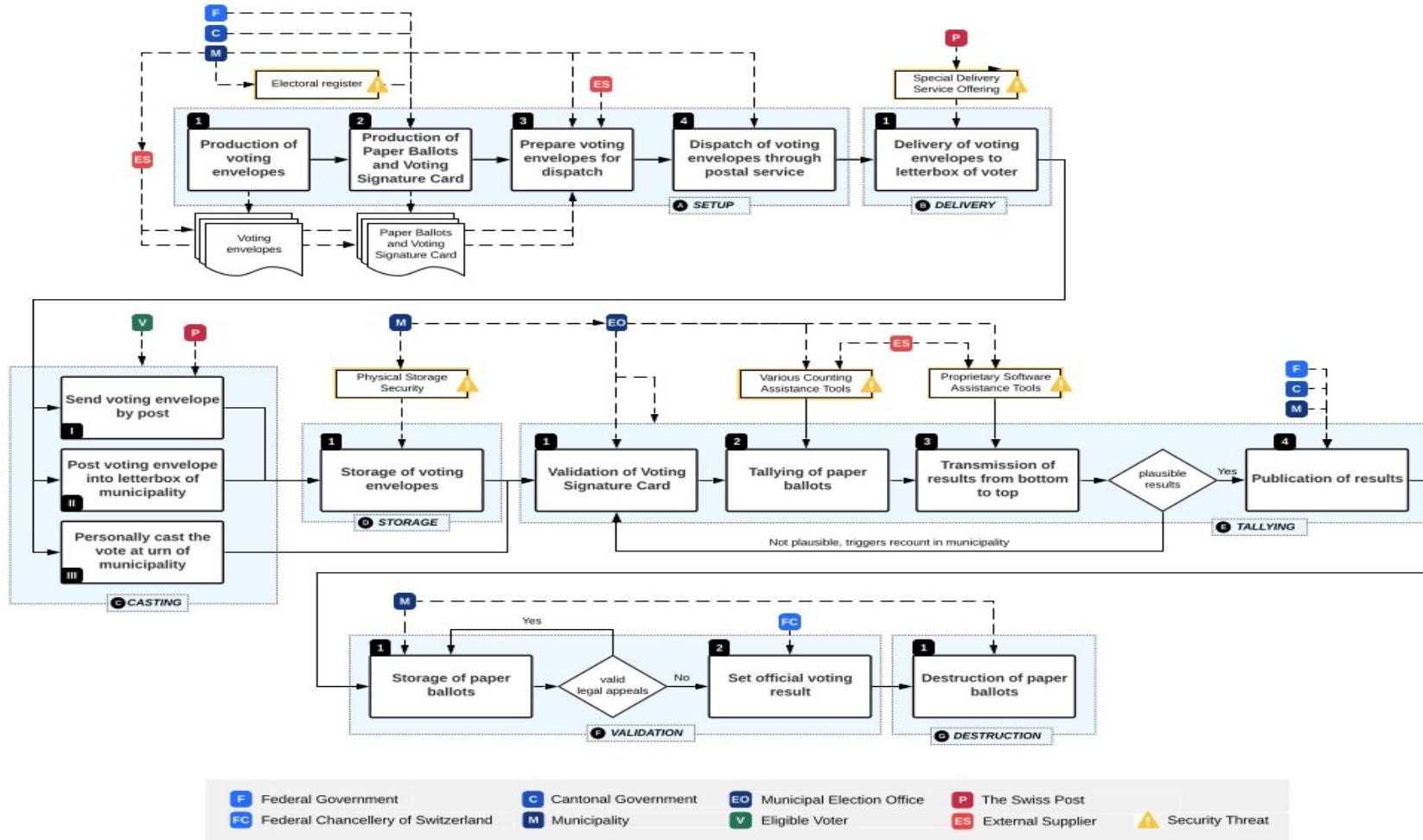


Photo: Gian Ehrensberger



@ChrFolini - Securing Internet Voting - #RomHack2021- 2021-09-25

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	2	
06.03	Peyer Samuel, 1985, BSc in Wirtschaftsinformatik, Unternehmer, Muri	3	
06.04	Masoch Loredana, 1996, BLaw, Masterstudentin Rechtswissenschaften, Wattenschwil	4	
06.05	Stöckli Cornel	5	
06.06	Chande Sabrina, 1989, Projektleiterin Elektroplanung, Mitglied GL, Buttwil	6	
06.07	Weber Ralf, CVP	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 2
06.03	76.01 Budmiger Hans-Peter Peyer Samuel, 1985, BSc in Wirtschaftsinformatik, Unternehmer, Muri 3
06.04	06.05 Masoch Loredana, 1996, BLaw, Masterstudentin Rechtswissenschaften, Wattenschwil Stöckli Cornel 4
06.05	Stöckli Cornel, 1975, Dr. med., Rheumat. & Innere Med., Integrationskom., Muri 5
06.06	06.01 Chande Sabrina, 1989, Projektleiterin Elektroplanung, Mitglied GL, Buttwil Bucher Ralf, CVP 6
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**



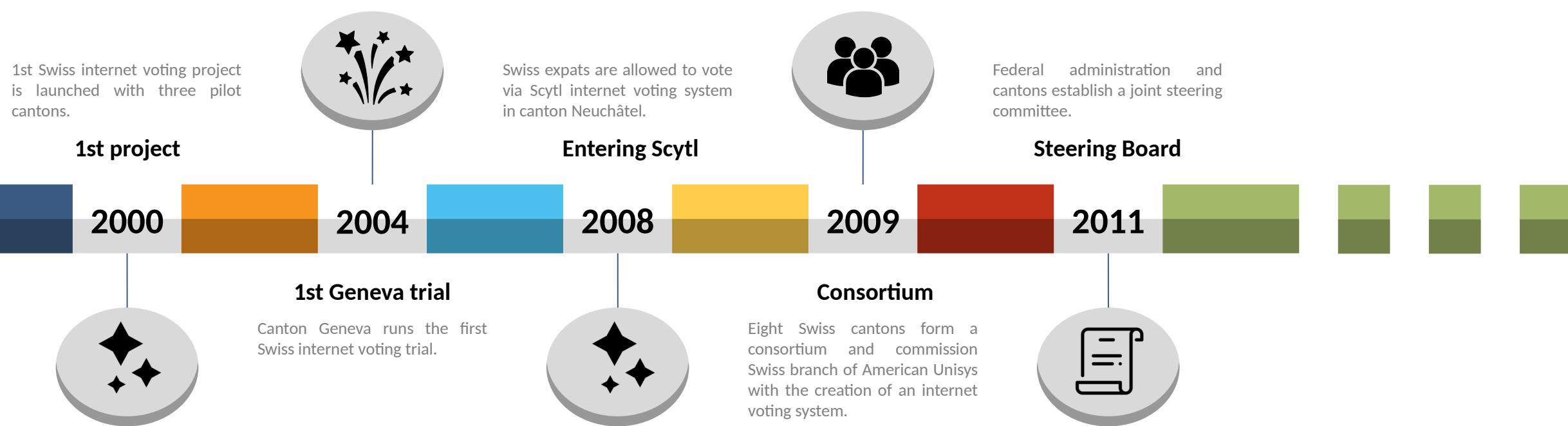
The Cantons of Switzerland



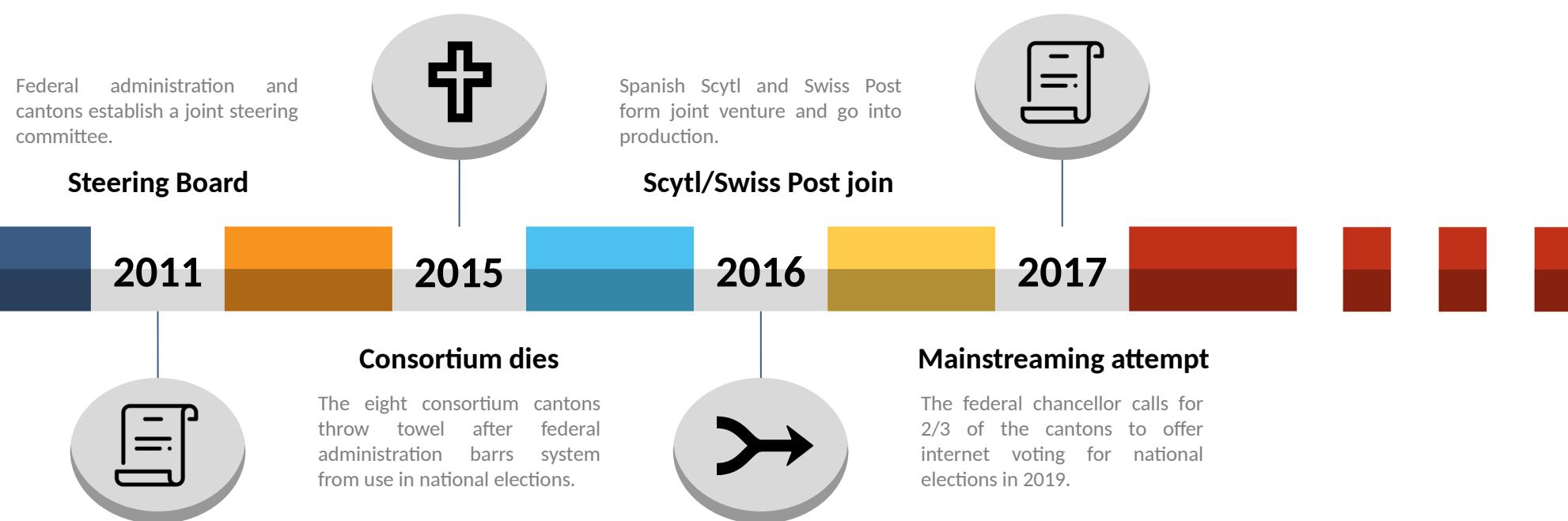
Graphic: Wikipedia



Timeline Internet Voting in Switzerland



Timeline Internet Voting in Switzerland



Geneva Quits

 **Chancellerie Genève** @GE_chancellerie · 19. Juni 2019 ...
Elections fédérales 2019: le canal de vote électronique ne sera pas proposé



Point presse du Conseil d'Etat du 19 juin 2019
Elections fédérales 2019: le canal de vote électronique ne sera pas proposé. Adoption du plan d'actions développement durable 2019-2023...
ge.ch

Q t 1 H V ↑

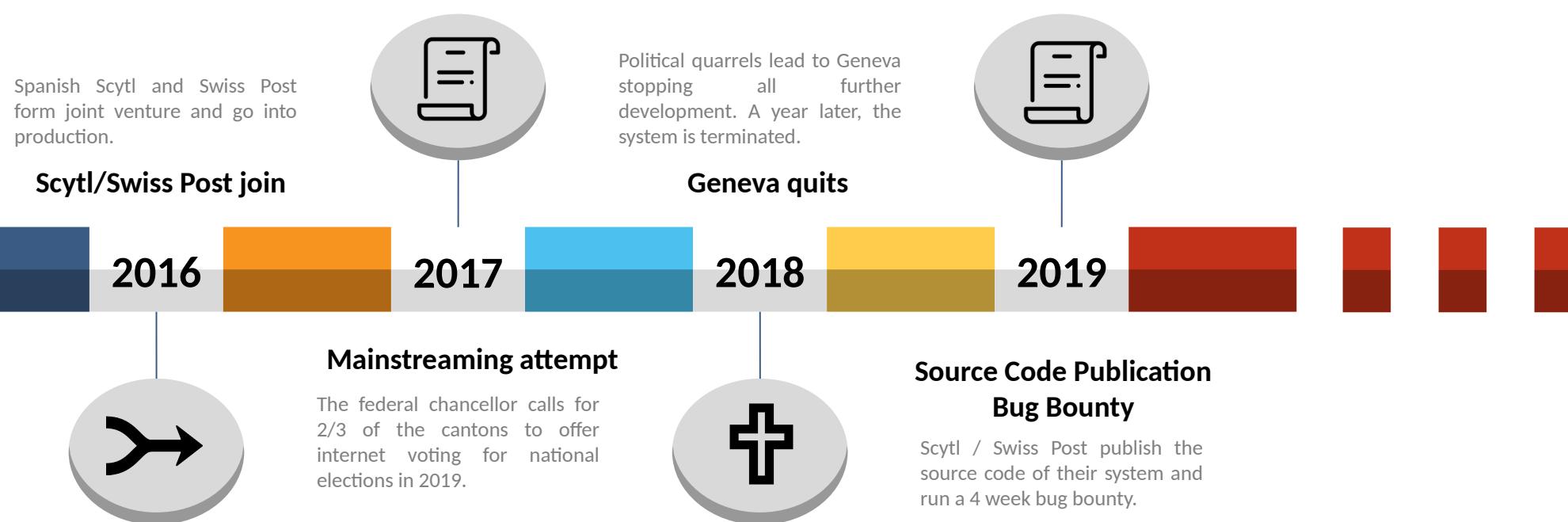
*2018: Development stopped
2019: System terminated*



Source: Twitter: @GE_chancellerie (114133232025195009)

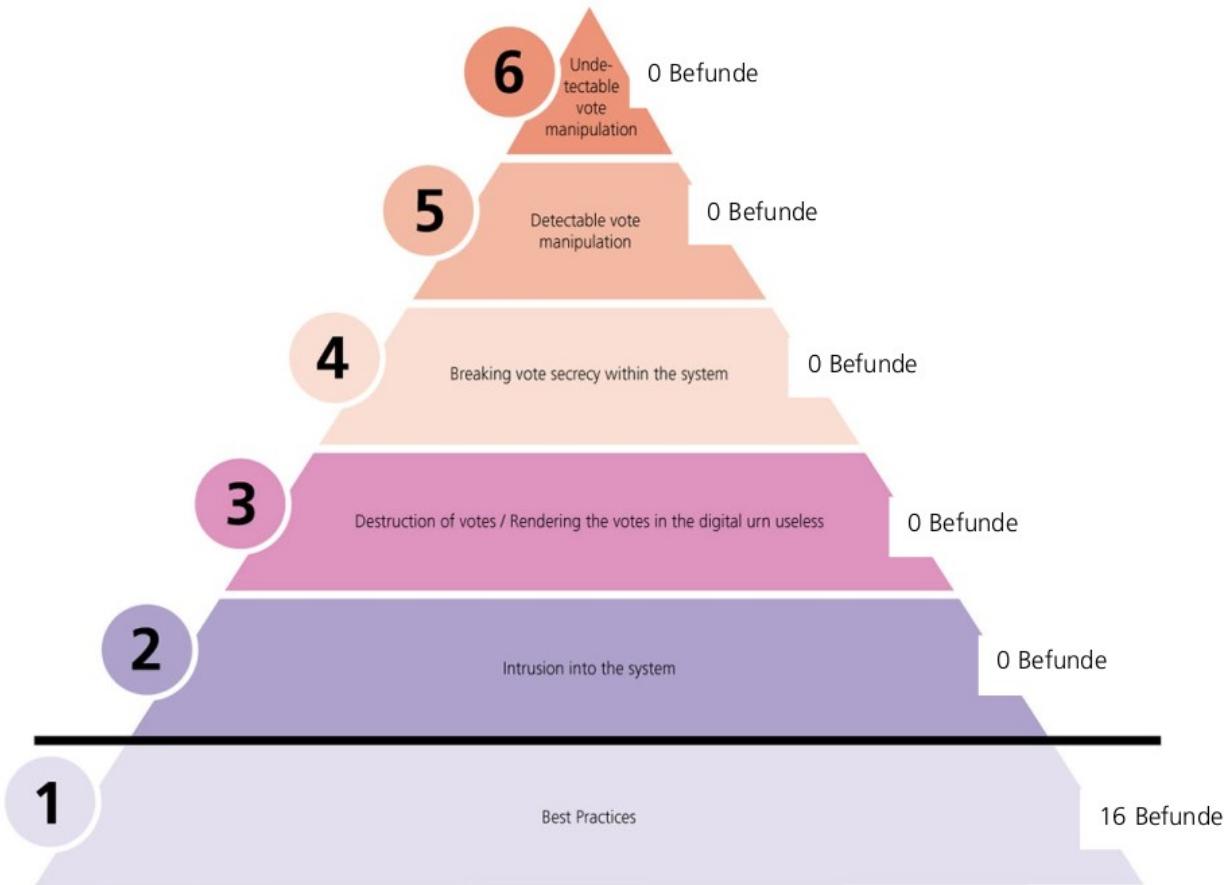
@ChrFolini - Securing Internet Voting - #RomHack2021- 2021-09-25

Timeline Internet Voting in Switzerland



Swiss Post Bug Bounty: We got this!

Abschlussbericht Öffentlicher Intrusionstest



[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

 **Vanessa Teague** @VTeagueAus · 12. März 2019

The trapdoor-commitment issue in the Swiss e-voting system was also independently discovered by Thomas Haines of NTNU and by Rolf Haenni of Bern University of Applied Sciences. [@SarahJamieLewis](#)

The Register®
Biting the hand that feeds IT

Security

Swiss electronic voting system like... wait for it, wait for it... Swiss cheese: Hole found amid public source code audit

Hey, at least it was dis – which is the whole p

By Thomas Claburn in San Francis

16 862 1.194

Diesen Thread anzeigen



Swiss Post puts e-voting on hold after researchers uncover critical security errors

James Walker 05 April 2019 at 08:35 UTC

Election Security Government Encryption

MOTHERBOARD
TECH BY VICE

Researchers Find Critical Backdoor in Swiss Online Voting System

und a severe issue in the new Swiss internet
ey say would let someone alter votes
y it should put a halt to Switzerland's plan to roll
il elections this year.

Share Tweet Snap



Vanessa Teague @VTeagueAus · 11. Apr. 2019

@SarahJamieLewis, Olivier Pereira & I found serious cryptographic errors in Scytl's Swiss/NSW evoting system. Will Scytl's Aus Senate counting code remain secret and will it enter votes into the count without a public audit of our paper ballots? [tenders.gov.au/?event=public....](#)



Vanessa Teague @VTeagueAus · 11. Apr. 2019

I agree with @damonism on the safety of paper ballots in Aus elections, but the electronic Senate count opens the possibility for undetected error or fraud unless there's a rigorous public audit of the paper records against the digitized preferences. [arxiv.org/abs/1610.00127](#) [twitter.com/GeoffreyHPowell...](#)

1 2 3



@ChrFolini - Securing Internet Voting - #RomHack2021- 2021-09-25 *to be continued*

Timeline Internet Voting in Switzerland

Spanish Scytl and Swiss Post form joint venture and go into production.

Scytl/Swiss Post join

2016

2017

Geneva quits

2018

2019

2020



Mainstreaming attempt

The federal chancellor calls on 2/3 of the cantons to offer internet voting for national elections in 2019.



Political quarrels lead to Geneva stopping all further development. A year later, the system is terminated.



The steering board establishes a dialog with 25 scientists to assess viability of internet voting and support with writing new regulation.

Rebooting

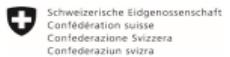


Source Code Publication

Scytl / Swiss Post publish the source code of their system. Researchers identify three critical vulnerabilities within weeks. The system is put on hold.



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

1. Purpose	4
2. Background	4
3. Introductory Remarks.....	4
4. Block 1 - Effectiveness of Cryptography	4
4.1 Overview	4
4.2 Summaries of the answers to the related questions of the questionnaire	5
4.3 Introduction to Block 1 on the platform	6
4.4 Questions and summaries of the discussions on the platform	6
5. Block 2 - Diversity to support security and trust-building	9
5.1 Overview	9
5.2 Summaries of the answers to the related questions of the questionnaire	9
5.3 Introduction to Block 2 on the platform	11
5.4 Questions and summaries of the discussions on the platform	17
6. Block 3 - Printing-Office (Diversity to support security and trust-building - Part 2).....	20
6.1 Overview	20
6.2 Summaries of the answers to the related questions of the questionnaire	20
6.3 Introduction to Block 3 on the platform	21
6.4 Questions and summaries of the discussions on the platform	24
7. Block 4 – Public Bulletin Board	25
7.1 Overview	25
7.2 Summaries of the answers to the related questions of the questionnaire	25
7.3 Introduction to Block 4 on the platform	25
7.4 Questions and summaries of the discussions on the platform	28
8. Block 5 – Examinations Mandated by Government	31
8.1 Overview	31
8.2 Summaries of the answers to the related questions of the questionnaire	31
8.3 Introduction to Block 5 on the platform	33
8.4 Questions and summaries of the discussions on the platform	35
9. Block 6 – Development and Publication	37
9.1 Overview	37
9.2 Summaries of the answers to the related questions of the questionnaire	37
9.3 Introduction to Block 6 on the platform	40
9.4 Questions and summaries of the discussions on the platform	41
10. Block 7 – Public Intrusion Test and Bug Bounty	43

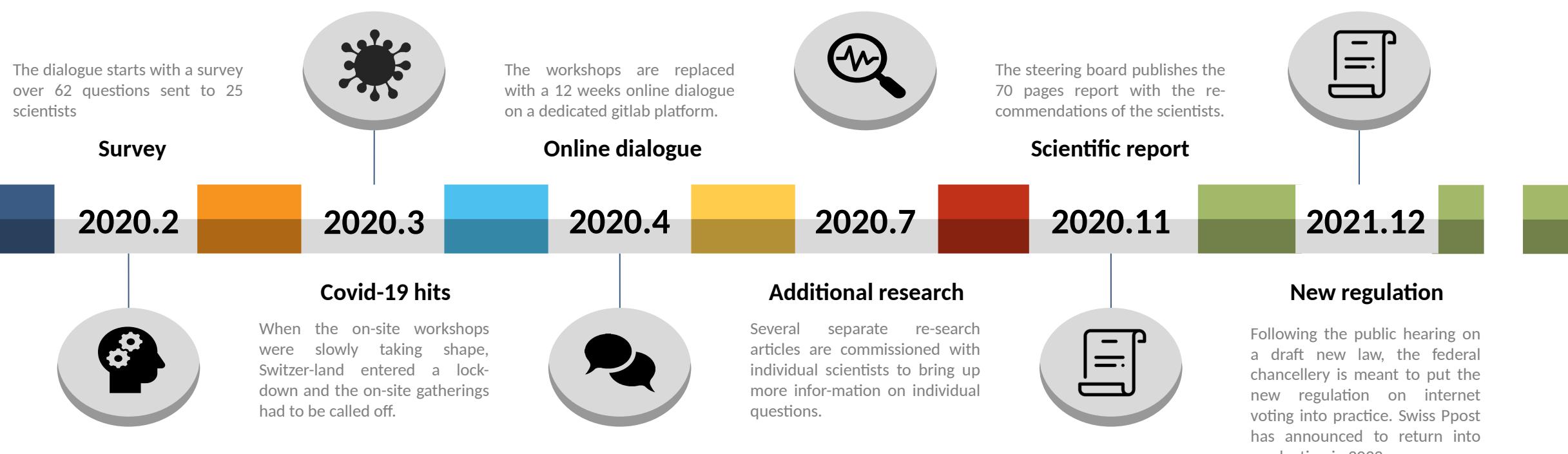
2

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



@ChrFolini - Securing Internet Voting - #RomHack2021- 2021-09-25

Timeline Internet Voting in Switzerland



Summary Internet Voting in Switzerland

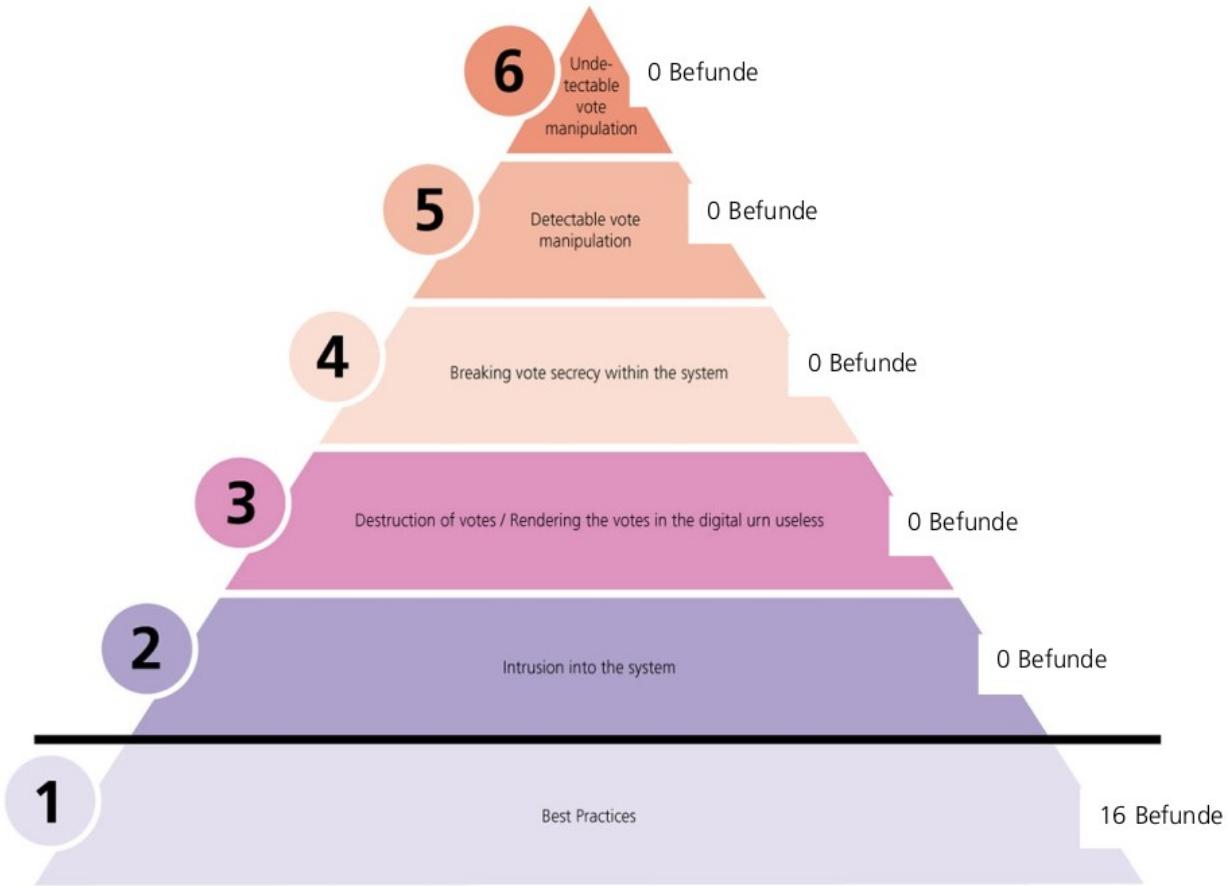
- Switzerland is a useful test bed for online voting
- Iterative process with strict supervision on federal level
- Expert dialogue with recommendations in 2020
- New regulation 2021
- New online voting trials scheduled for 2022

*Download English version of scientific 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



[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>

ModSecurity-CRS-Tuning-Concept.md 10.2 KB

ModSecurity CRS-Tuning-Concept

Introduction

This document describes the procedure for tuning the reverse proxies.

Starting position and goal

The Apache `httpd` reverse proxies use the `ModSecurity` module in combination with the `OWASP ModSecurity Core Rule Set (CRS)` to filter both incoming requests and their responses. In addition to the CRS, other `ModSecurity` rules and Apache `httpd` configurations are in use, but they are not in the scope of this document.

One of the difficulties in the operation of CRS is the false positives, i.e. when rules are triggered by legitimate requests. This document describes the procedure for eliminating false positives and the considerations that go into this procedure.





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
- GeolP



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**
- **GeolP**



Questions and Answers, Contact

Contact:

 @ChrFolini

christian.folini@netnea.com



CRS

THE 1ST LINE OF DEFENSE



@ChrFolini - Securing Internet Voting - #RomHack2021- 2021-09-25