Public Intrusion Test

Final Report

Classification	PUBLIC
Reference	CHLSAD290320191-5

SCRT
Information Security

LE TRÉSI 6
1028 PRÉVERENGES
INFO@SCRT.CH

T +41 21 802 64 01
F +41 21 802 64 02

WWW.SCRT.CH

1 Introduction

The present document is the final report providing information about the Public Intrusion Test (PIT) of Swiss Post's e-voting system, as operated by SCRT on behalf of Swiss Federal Chancellery.

It is based on data obtained from various systems operated by SCRT for a period ranging from Feb 07th 2019 to March 25th 2019.

2 Analysis and conclusions

2.1 Purpose

On request of the Federal Chancellery and the Cantons, SCRT provides here an interpretation of the PIT's statistics and data detailed in the rest of the report.

This analysis is based on SCRT's experience as well as on the observations made and lessons learned by operating the submission platform, classifying the submissions and being the participants' single point of contact during the PIT itself.

2.2 Participation

As demonstrated by the large number of registered users (more than 3 000) as well as by the number of press articles and references including general international press sites (e.g. Euronews[1]), main-stream technology related news sites (e.g. The Verge[2], Slashdot[3]) and security specific channels (e.g Portswigger[4]), the PIT appears to have benefited from a good communication coverage and generated a large interest amongst the IT and IT-security communities.

Based on the distribution of registration dates, this interest was at its peak in the days following the PIT's announcement, with a (much smaller) new peak on the day of PIT's start.

This large number of registered participants (often referenced in the press) does however not necessarily fully reflect the actual number of active researchers during the PIT. Indeed, only roughly a third of them (1 090) logged-in at least once during the PIT itself. Additionally, only 822 requested voting cards and among those, "only" 388 requested more than one voting card.

While these numbers may appear to be low (when compared to the total number of registered participants), in our opinion, these "active" accounts still represent a very significant set of participants.

Moreover, these available metrics may not be fully representative of the testing itself as many tests and attacks (including those leading to some of the accepted vulnerabilities) do not require a voting card at all to be performed. SCRT does however not have any view of the actual activity on the target e-voting platform and only Swiss Post are able to provide additional insights about it.

[1] https://www.euronews.com/2019/02/13/switzerland-offers-cash-to-hackers-who-can-crack-its-e-voting-system

[2] https://www.theverge.com/2019/2/12/18221570/swiss-e-electronic-voting-public-intrusion-test-hacking-white-hack-bug-bounties

[3] https://it.slashdot.org/story/19/02/13/1547211/swiss-e-voting-trial-offers-150000-in-bug-bounties-to-hackers

[4] https://portswigger.net/daily-swig/switzerland-launches-e-voting-bug-bounty

2.3 Relevance of testing

From SCRT's perspective – which is mostly based on findings submitted by participants – it is impossible to have a complete overview on the relevance of testing performed during the PIT.

While submissions were made in all available vulnerability categories, most of them (and all the accepted ones) fall into the "BEST PRACTICES" section. It is however impossible for us to know if other aspects were overlooked or if they were thoroughly tested but no vulnerability was discovered.

The scope of the PIT seems properly defined and relevant in order to assess the security of the system against malicious voters and attackers targeting the e-voting system over the Internet. However, the attack surface on critical concepts like server-side vote secrecy or server-side vote corruption was very limited since the back-end was not directly accessible to the participants.

It thus does not come as a surprise that those vulnerability categories were much less represented in the reported findings. Even if a few meaningful submissions related to these aspects were actually submitted, they were generally based on source-code observation, not directly exploitable in the PIT and thus deemed "out-of-scope" in the PIT's context.

2.4 Quality of submissions

As detailed further in this report, a total of 173 submissions were performed by 80 different participants. Among those submissions, a total of 157 were rejected, most of them because they did not actually constitute a vulnerability[5].

A significant portion of submissions received were considered by SCRT as being of poor quality, either based on formal criteria (poorly detailed, lacking explanations) or on the contents themselves (lack of substantial content, no actual vulnerability), some of them appearing as "quick-win" attempts referencing easily identifiable breaches of best-practices (or elements wrongfully identified as such).

That consideration being made, it can however be noted that almost 10% (16 on 173), of the submissions were actually accepted. In addition to those, some rejected vulnerabilities were considered as being of good quality and derived from interesting ideas thus demonstrating the good research work done by a significant portion of the participants.

[5] See chapter *4.4* Rejected vulnerabilities for details.

2.5 Collaboration with Swiss Post

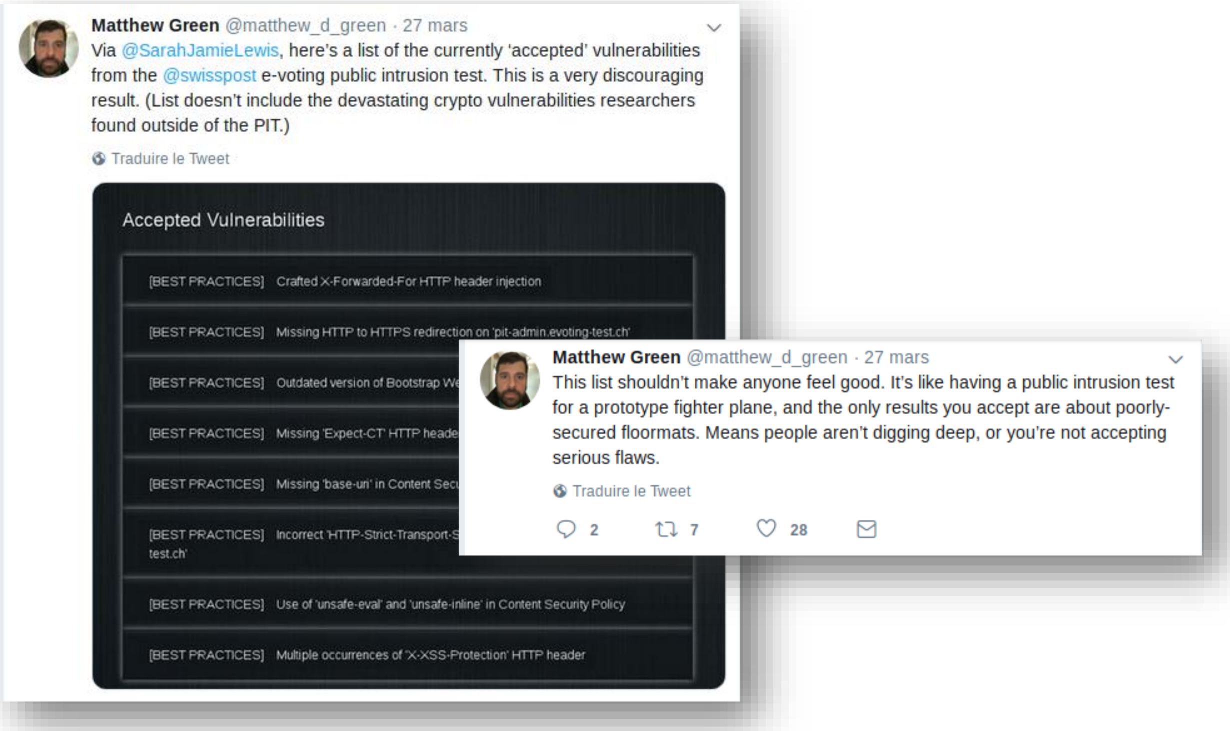
From SCRT's perspective the collaboration with Swiss Post during the PIT was very good. Both parties kept their respective roles and were able to collaborate efficiently.

2.6 Potential shortcomings

While both programs were, at least theoretically, clearly distinct and decorrelated, the overlap of the PIT with the source code program appears to have caused some confusion for participants and the general public.

As a result of that, SCRT received several submissions related to the source code (including some of high relevance). While the researchers themselves did not protest being redirected to the source code program, the distinction between the two programs may not have been clear for everyone.

Furthermore, the general public may not have properly understood why the PIT only referenced 16 minor accepted vulnerabilities while the press was discussing potentially critical findings discovered in the source code. This confusion – pin-pointed by renowned people in the field of security and cryptography (e.g. below[6]) has certainly helped fuelling controversy around the value of the PIT.



Matthew Green @matthew_d_green · 27 mars

Via @SarahJamieLewis, here's a list of the currently 'accepted' vulnerabilities from the @swisspost e-voting public intrusion test. This is a very discouraging result. (List doesn't include the devastating crypto vulnerabilities researchers found outside of the PIT.)

Accepted Vulnerabilities

[BEST PRACTICES] Crafted X-Forwarded-For HTTP header injection

[BEST PRACTICES] Missing HTTP to HTTPS redirection on 'pit-admin.evoting-test.ch'

[BEST PRACTICES] Outdated version of Bootstrap We

[BEST PRACTICES] Missing 'Expect-CT' HTTP heade

[BEST PRACTICES] Missing 'base-uri' in Content Secu

[BEST PRACTICES] Incorrect 'HTTP-Strict-Transport-S
test.ch'

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

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

Matthew Green @matthew_d_green · 27 mars

This list shouldn't make anyone feel good. It's like having a public intrusion test for a prototype fighter plane, and the only results you accept are about poorly-secured floormats. Means people aren't digging deep, or you're not accepting serious flaws.

[6] Source: https://twitter.com/matthew_d_green

2.7 Conclusions

Overall, the PIT was a properly orchestrated “bug bounty”. It was well advertised both in security community and the general public and did benefit from good media coverage.

The definition of the scope was consistent with the objectives, i.e. to assess the security of the system against malicious voters and attackers targeting the e-voting system over the Internet.

The overall participation was good, and the variety of submissions suggested that the system was looked at by a large number of researchers of different levels of competence.

The PIT’s credibility did however probably suffer from the confusion caused by the overlap with source code program.

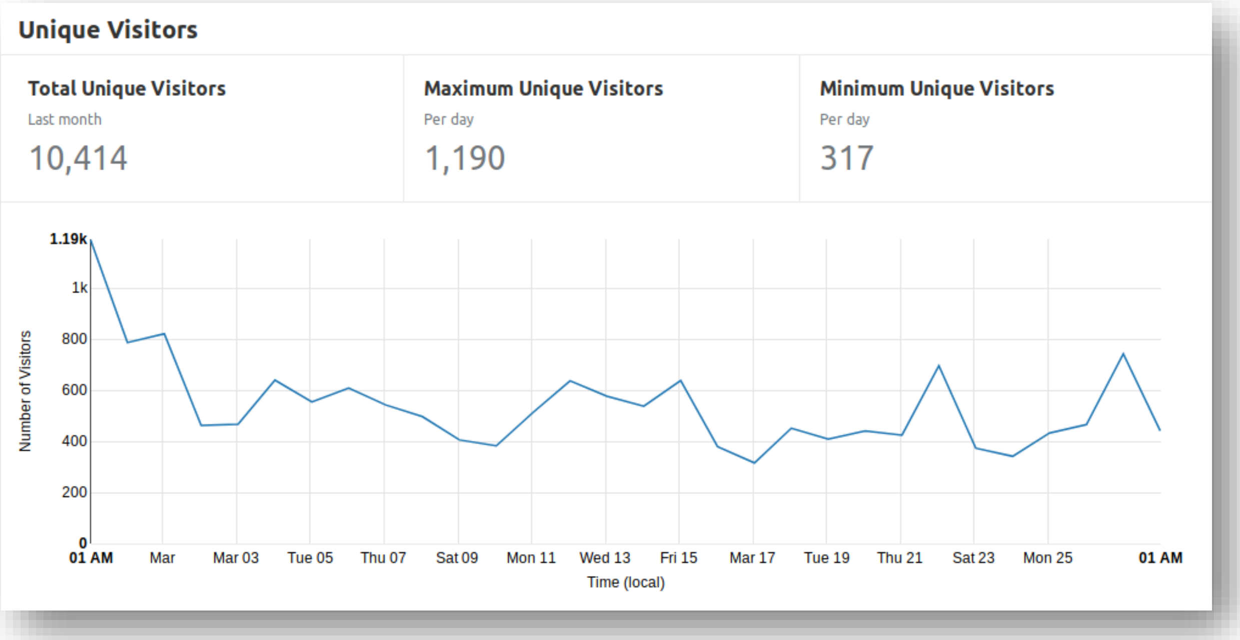
3 Statistics

3.1 Overall platform activity

SCRT's platform for the PIT was composed of two interconnected systems, both reachable under the domain name onlinevote-pit.ch:

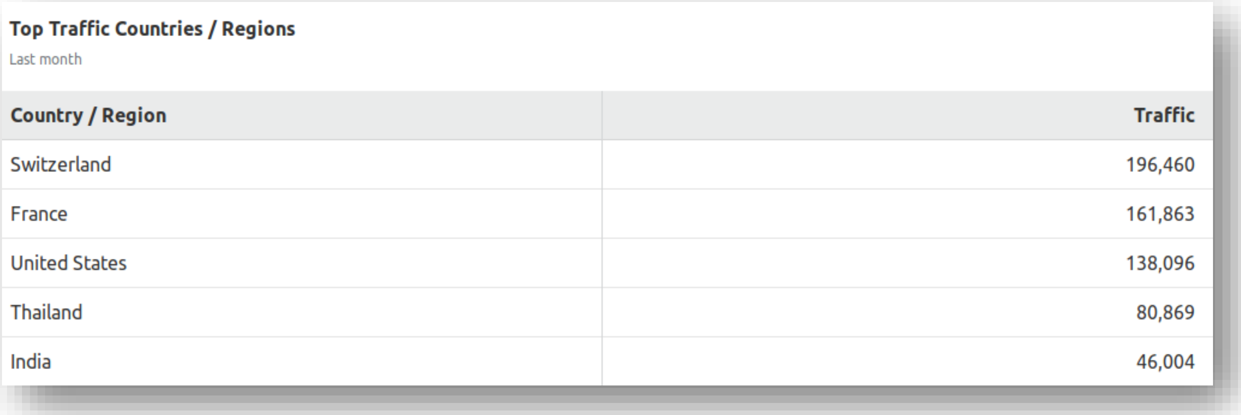
- www.onlinevote-pit.ch
  The main website, used for participant registration, publication of information, support and contact requests as well as for voting card distribution;
- report.onlinevote-pit.ch/redmine
  The vulnerability submission platform.

Graphs below (source: Cloudflare) provide the overall activity on these platforms during the PIT opening period. Note that these graphs are just meant as a rough overview and not as a precise measurement tool. Moreover, the displayed period starts on Feb. 27th and hence do not capture the PIT opening day.



Unique Visitors

Total Unique Visitors	Maximum Unique Visitors	Minimum Unique Visitors
Last month	Per day	Per day
10,414	1,190	317



Top Traffic Countries / Regions

Last month

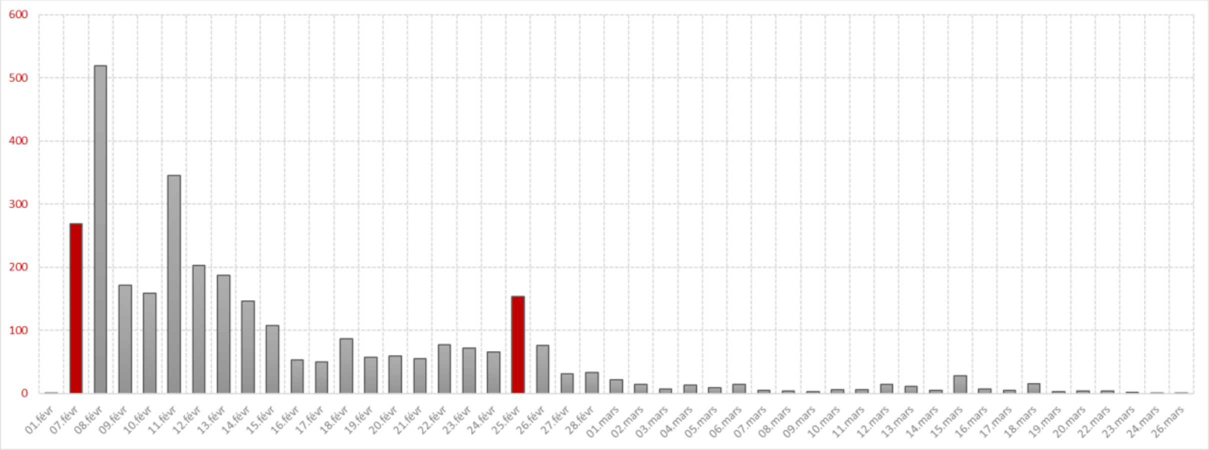
Country / Region	Traffic
Switzerland	196,460
France	161,863
United States	138,096
Thailand	80,869
India	46,004

3.2 Registered participants

A total of **3186** users registered for the PIT (this only includes activated accounts, i.e. users who went through the whole registration process; in addition to those, 257 account were created but never fully activated).

Registered participants	**Total**	**3186**
	Countries	137[7]
	Have logged-in during the PIT	1090
	Have requested voting cards	822
	Have submitted vulnerabilities	80

The chart below provides the distribution of participants registration over time. The two red bars mark the dates of registration opening (Feb. 07th) and PIT's start (Feb. 25th).



[7] Countries are based on information provided by the participants and are not verified in any way.

3.3 Voting cards

3.3.1 Card distribution

A grand total of **99 000** voting cards were delivered to SCRT by Swiss Post in order to be distributed to participants.

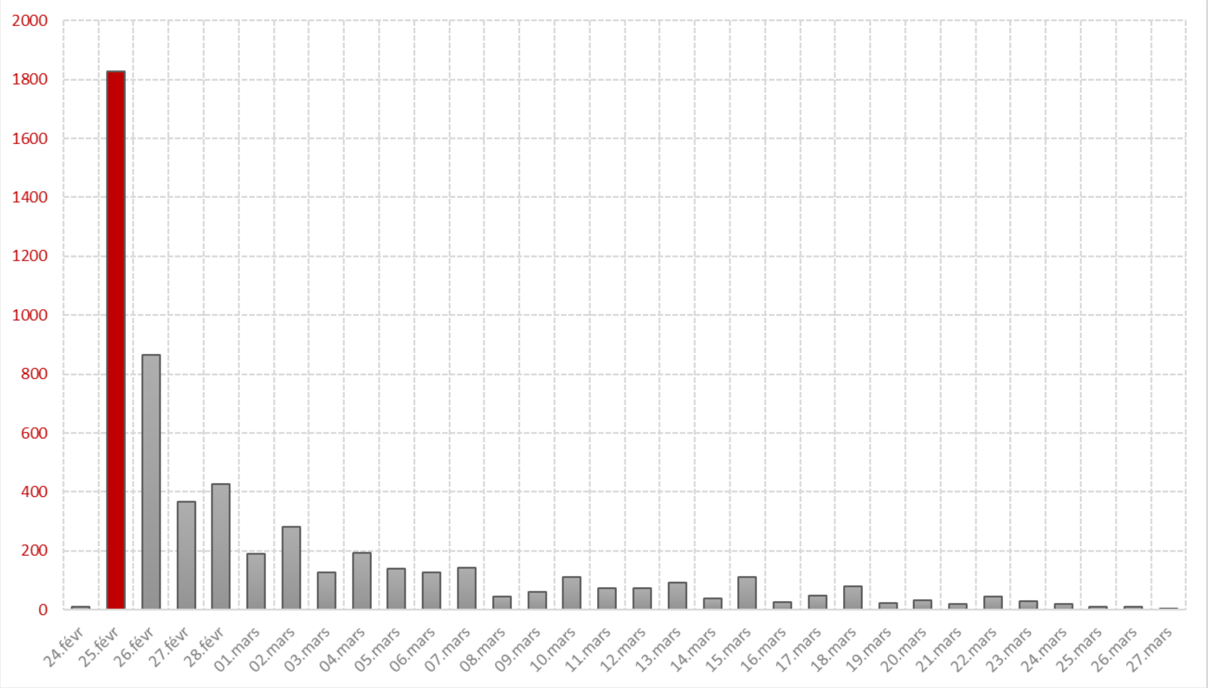
Starting on the PIT's opening date (Feb 25th), registered participants had the possibility of automatically requesting voting cards from SCRT's platform. Those voting cards were distributed in the following manner:

- On initial request, a single voting card was delivered to the participant;
- Subsequent requests, delivered packs of 10 voting cards, up to a total of 51;
- Participants having reached the 51 voting cards limit, were requested to contact SCRT in order to be granted more cards (in such cases, SCRT usually allowed the participant to automatically request up to 5 more packs of 10 cards).

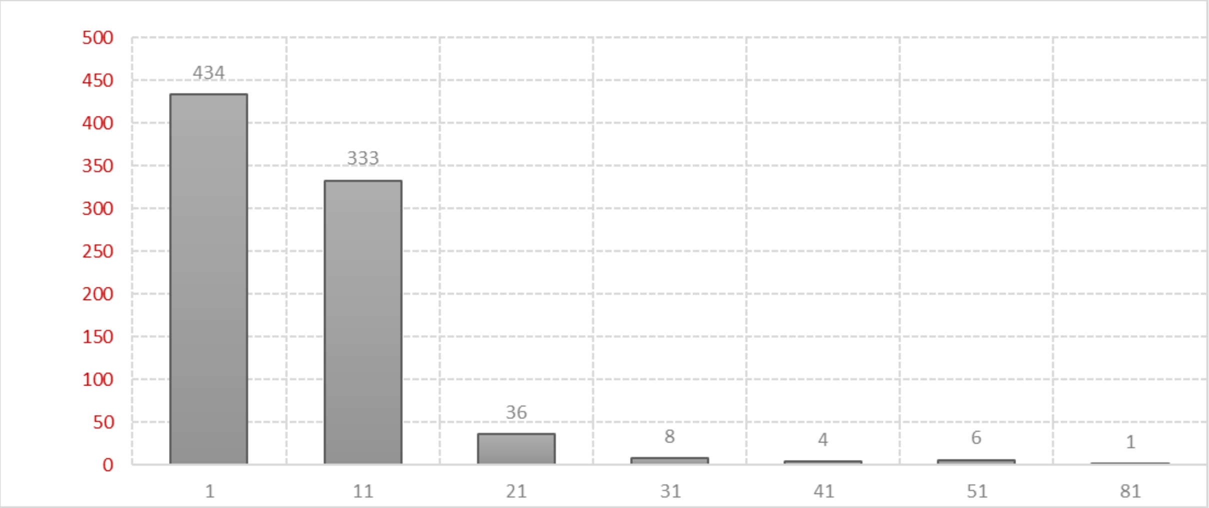
3.3.2 Distribution statistics

A total of **5 652** voting cads were distributed during the PIT. These cards were distributed among a total of **822** participants.

The chart below illustrates the distribution of voting cards over time, during the PIT. As visible, a large portion of the requested cards were distributed during the opening day.



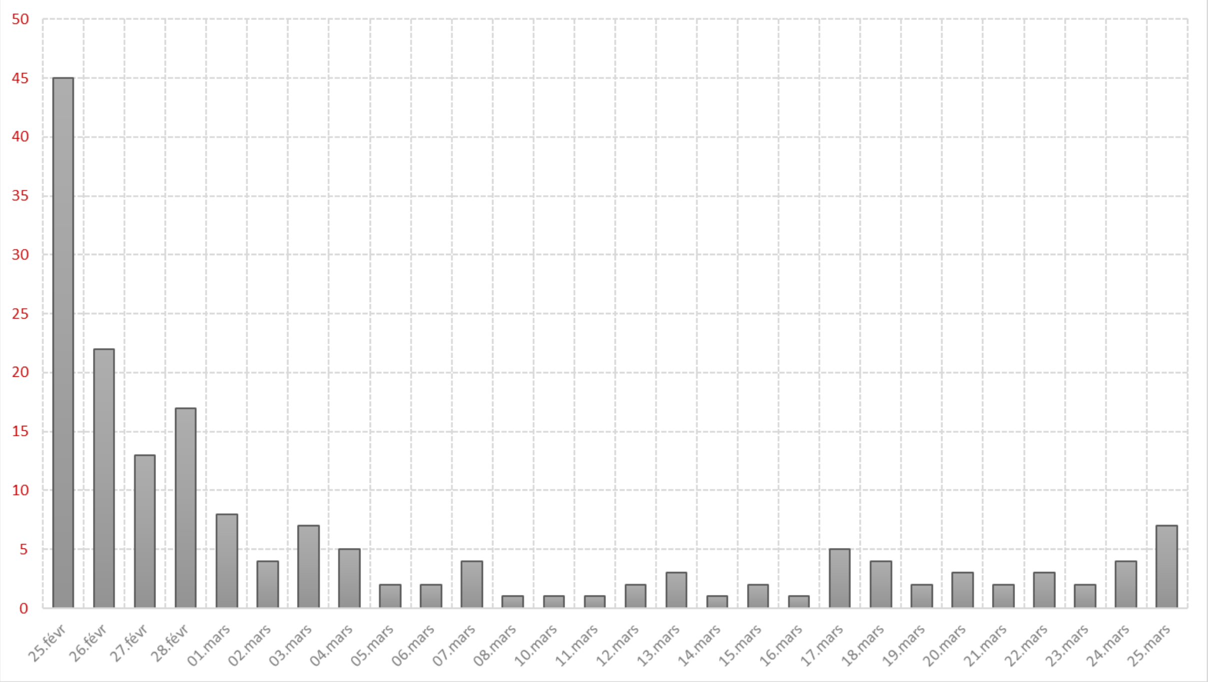
The chart below illustrates the number of distributed voting cards (x axis) per account (y axis). As visible, most of the participants (434) requested a single voting card. Only one participant contacted SCRT in order to unlock the 51 voting cards limit and requested a total of 81 cards.



4 Submitted findings

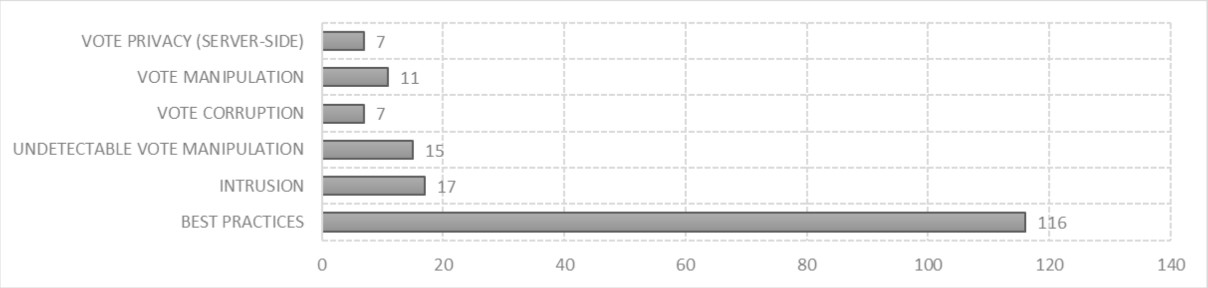
4.1 Overall total

A total of **173** issues were submitted during the PIT, by a total of **80** participants. The chart below provides the distribution of these submissions over time.



4.2 Submissions by categories

These vulnerabilities were submitted in all the available categories, however the category chosen by the participants when submitting was not always appropriate or relevant.



4.3 Accepted submissions

Overall, **16** submissions were accepted as actual vulnerabilities during the PIT. All these issues fall into the **BEST PRACTICES** category.

4.3.1 Crafted X-Forwarded-For HTTP header injection

REDMINE ID: #153
SUBMISSION: Feb. 25th 2019, 12:51 (GMT+1)
RESEARCHER(S): muffinx & xorkwi
COMPENSATION: CHF 400.-

By inserting a crafted X-Forwarded-For HTTP header in the requests performed to some of the web services, an attacker was capable of inserting a chosen IP address into technical logs of the back-end system. No impact on the voting process has been demonstrated. It would however be a security best-practice to prevent this issue. According to Swiss Post this will be fixed in the future.

4.3.2 Missing HTTP to HTTPS redirection on 'pit-admin.evoting-test.ch'

REDMINE ID: #166
SUBMISSION: Feb. 25th 2019, 14:06 (GMT+1)
RESEARCHER(S): Dodoche
COMPENSATION: CHF 100.-

Both HTTP (TCP/80) and HTTPS (TCP/443) ports are available on address 'pit-admin.evoting-test.ch'. Security best practices impose that, upon connecting to the cleartext HTTP port, clients should be automatically redirected to the encrypted (HTTPS) service instead. By blocking the client immediately instead of redirecting it, this system does not act in accordance to security best-practices.

4.3.3 Outdated version of Bootstrap Web Framework

REDMINE ID: #168
SUBMISSION: Feb. 25th 2019, 14:56 (GMT+1)
RESEARCHER(S): punitcingh
COMPENSATION: CHF 100.-

The landing page of the e-voting system uses a well-known front-end Web framework called Bootstrap. The used version of this framework - 4.2.1 - is affected by a known vulnerability potentially leading to Cross-Site Scripting (XSS) occurrences in some specific scenarios that don’t seem to apply here. However it is a security best-practice to use the latest version of a framework. The patch for this vulnerability (CVE-2019-8331) was released on Feb. 15th 2019.

4.3.4 Vulnerable TLS cipher-suites (LUCKY13)

REDMINE ID: #175
SUBMISSION: Feb. 25th 2019, 16:25 (GMT+1)
RESEARCHER(S): PentestPeople_SN
COMPENSATION: CHF 100.-

The front-end systems accessible at https://pit.evoting-test.ch and https://pit-admin.evoting-test.ch support and accept HTTPS connections using a variety of ciphers including cipher suites provided by outdated and vulnerable versions of TLS (TLS 1.0/1.1).

While this may appear at first glance as a breach to security best practices, it is actually done on purpose and in a way that does not make the e-voting system vulnerable to flaws deriving from these weak cryptographic protocols. Indeed, connections using weak cipher suites are only accepted by the front-end (and not by the e-voting system itself) and are only used to display a message to the voters, instructing them to use a recent and up-to-date web browser. The e-voting system itself, on the other hand, only accepts connections using TLS 1.2 cipher suites.

However, some specific cipher suites that are part of TLS 1.2 (and accepted by the voting system), specifically those using block ciphers with CBC mode of operation, may be vulnerable to a padding oracle attack known as « Lucky13 ».

While this vulnerability is known to be mostly theoretic, and almost impossible to actually exploit outside of lab environments, it would be a security best practice to disable the use of these cipher suites altogether.

4.3.5 Missing 'Expect-CT' HTTP header

REDMINE ID: #179
SUBMISSION: Feb. 25th 2019, 18:16 (GMT+1)
RESEARCHER(S): paggio
COMPENSATION: CHF 100.-

The 'Expect-CT' header - which is currently an Internet Draft - has been proposed to allow sites opting in to reporting and enforcing Certificate Transparency requirements. The goal of this mechanism is to prevent the use of "rogue" certificates for a given domain from going unnoticed.
E-voting system does not implement this header and does thus not benefit from this mechanism.
Note that this header has not yet been formally adopted as a standard and may not be supported by all browsers yet.

4.3.6 Missing 'base-uri' in Content Security Policy

REDMINE ID: #183
SUBMISSION: Feb. 25th 2019, 20:37 (GMT+1)
RESEARCHER(S): DROOPER
COMPENSATION: CHF 100.-

The Content-Security-Policy HTTP header declared by the e-voting system does not declare the 'base-uri' directive. By doing so, it lowers the protection (at the browser level) against the exploitation of hypothetical Cross-Site Scripting (XSS) vulnerabilities.

4.3.7 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.

4.3.8 Use of 'unsafe-eval' and 'unsafe-inline' in Content Security Policy

REDMINE ID: #232
SUBMISSION: Feb. 28th 2019, 14:48 (GMT+1)
RESEARCHER(S): pitbull
COMPENSATION: CHF 100.-

The e-voting system declares a Content-Security-Policy HTTP header containing the 'unsafe-eval' and 'unsafe-inline' expressions. By doing so, it lowers the protection (at the browser level) against the exploitation of hypothetical Cross-Site Scripting (XSS) vulnerabilities.

4.3.9 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.

4.3.10Use of outdated version of AngularJS

REDMINE ID: #257
SUBMISSION: Mar. 03rd 2019, 19:39 (GMT+1)
RESEARCHER(S): CodeTherapist
COMPENSATION: CHF 100.-

Both voter and admin portals use a well-known Javascript web framework named AngularJS. The version of this framework used by the e-voting system is 1.6.9. While no vulnerability is currently known to affect this version, it is however not supported anymore and should thus be upgraded to a currently supported version.

4.3.11Strict Transport Security Mis-configuration

REDMINE ID: #272
SUBMISSION: Mar. 07th 2019, 11:47 (GMT+1)
RESEARCHER(S): punitcingh
COMPENSATION: CHF 100.-

Upon reception of requests whose content has been tampered with, the server usually responds with an error message. In some specific cases (e.g. 422 status codes) this response may include two occurrences of the 'Strict-Transport-Security' HTTP header with inconsistent contents (the declarations on both headers are not identical).

This behavior is non-standard, and could lead to undefined interpretation of the 'Strict-Transport-Security' directives in some browsers. As HSTS preloading is used, this should however not cause insecure situations.

4.3.12Use of cipher suites without forward secrecy support

REDMINE ID: #285
SUBMISSION: Mar. 15th, 11:00 (GMT+1)
RESEARCHER(S): cryptopathe
COMPENSATION: CHF 100.-

The e-voting system accepts connections from clients (browsers) using TLS 1.2.
However, two specific cipher suites that are part of TLS 1.2 and accepted by the voting system do not provide forward secrecy:

TLS_RSA_WITH_AES_256_GCM_SHA384

TLS_RSA_WITH_AES_128_GCM_SHA256

These cipher suites are not weak or broken. However the lack of forward secrecy implies that decryption would be facilitated in the future if at some point an attacker has access to the encryption keys used by e-voting server. This does not apply to the encryption of the votes, which would remain secure.
Note that these cipher suites will generally only be used by the server and the clients if no stronger and better cipher suite is supported by both of them.

4.3.13Missing charset declaration in some response’s Content-Type header

REDMINE ID: #294
SUBMISSION: Mar. 19th 2019, 00:48 (GMT+1)
RESEARCHER(S): 0x34044[REDACTED FOR PRIVACY]
COMPENSATION: CHF 100.-

Some HTTP responses sent by the e-voting system are missing the charset parameter in the Content-Type header.

While this does not currently have any known impact, it is however a breach of secure development best practices.

4.3.14Missing CSP header in redirect responses

REDMINE ID: #295 (b)
SUBMISSION: Mar. 19th 2019, 00:59 (GMT+1)
RESEARCHER(S): 0x34044[REDACTED FOR PRIVACY]
COMPENSATION: CHF 100.-

Some responses from the e-voting server - specifically "302 Redirect" re-directions - are missing Content Security Policy HTTP headers. They are thus inconsistent with the rest of the application and in breach of security best practices.

4.3.15Cross Origin Request possible on specific endpoint

REDMINE ID: #296
SUBMISSION: Mar. 19th 2019, 12:27 (GMT+1)
RESEARCHER(S): 0x34044[REDACTED FOR PRIVACY]
COMPENSATION: CHF 100.-

One specific endpoint of the e-voting system - /extended_authenticate - accepts 'text/plain' content-type instead of the 'application/json' observed for other endpoints.

Because of this and due to the fact that for 'text/plain' content-type, the browser does not perform a "pre-flight" CORS check, it is possible to perform requests to this endpoint from any arbitrary origin domain.

While the usefulness of this attack appears to be very limited, it may nevertheless constitute a breach to security best practices.

4.3.16Missing CSP header on http://pit-admin.evoting-test.ch

REDMINE ID: #318
SUBMISSION: Mar. 25th 2019, 14:37 (GMT+1)
RESEARCHER(S): kili
COMPENSATION: CHF 100.-

Upon connection attempts to http://pit-admin.evoting-test.ch/ (using plain HTTP) the server responds with a '403 Forbidden' response effectively rejecting the connection attempt. This response does however not define a Content Security Policy (CSP) header, thus breaching security best practices.

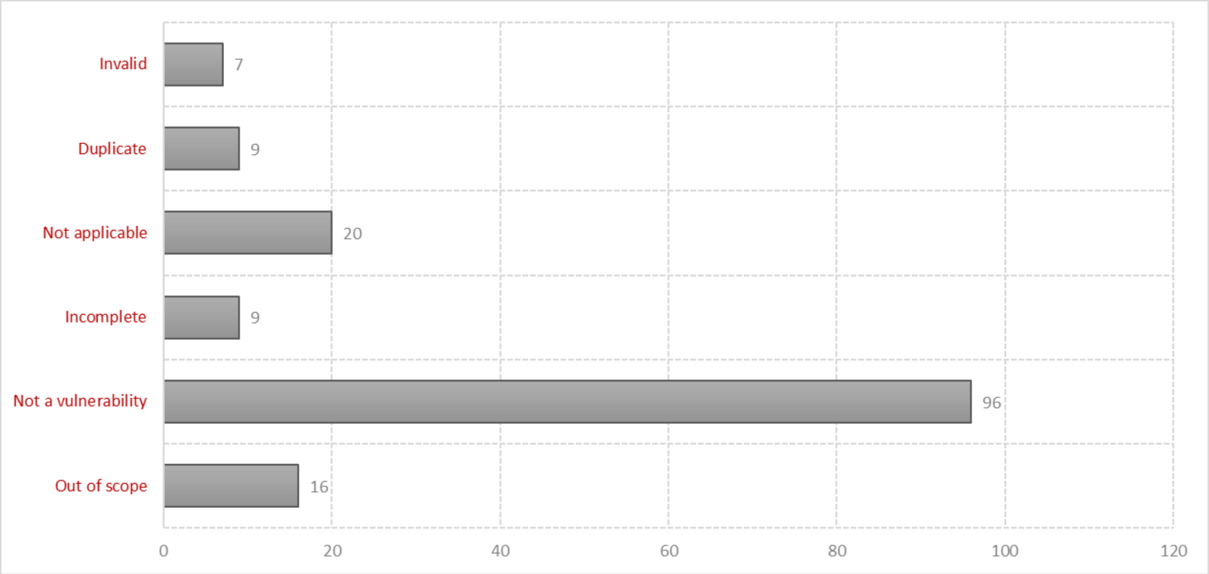
4.4 Rejected vulnerabilities

Overall, **157** vulnerabilities were rejected.

These rejections were either directly performed by SCRT during triage and initial analysis or after deeper investigation by SCRT and Swiss Post jointly, whenever necessary.

The reasons behind these rejections vary and may be specific to the context of each submission, however, these reasons have been distributed amongst the categories below.

Rejection reasons	
Out of scope	The submission refers to a system that is explicitly out of scope (e.g. surrounding infrastructure, SCRT's platform, …)
Not a vulnerability	The submitted element is a desired functionality and/or the researcher failed to demonstrate how it could constitute a vulnerability.
Incomplete	The submission is incomplete or not understandable. It does not provide enough elements for SCRT's team to understand the raised issue or to assess it.
Not applicable	The submission is not applicable for the PIT and cannot be assessed in its context. E.g. a source code submission or a general remark based on documentation.
Invalid	The submission was bogus or invalid (e.g. misplaced support request, test submissions, …)


Invalid
Duplicate
Not applicable
Incomplete
Not a vulnerability
Out of scope