Municipality2HTTPS: A study on HTTPS protocol's usage in Italian municipalities' websites

Antonio Giovanni Schiavone*

Bank of Italy, Via Nazionale 91, 00184 Rome, Italy

Abstract

The usage of HTTPS protocol is essential for secure communication with websites, especially when it comes to the websites of local municipalities. This protocol ensures the confidentiality, integrity, and authenticity of online data transmissions, protecting users from unauthorized access and data breaches. By implementing HTTPS, municipalities can provide a secure and reliable online experience for their citizens and build trust in their digital services. This paper presents the Municipality2HTTPS research project, which aim is to provide a comprehensive analysis of the current state of HTTPS implementation in approximately 8,000 Italian municipalities' websites. The study was conducted using the purpose-built software platform, named MunicipalityEvaluator, and the results were aggregated both geographically and demographically based on a numerical score derived from a specific scoring system: this system was obtained by expanding the requirements set forth by Italian regulations on the topic. The obtained results identified several areas for improvement in HTTPS implementation and regulatory compliance, including the need for more awareness-raising activities and support for municipalities with limited technical expertise. The results also revealed discrepancies between regions and demographic groups in terms of HTTPS implementation and regulatory compliance.

Keywords: E-government; Local government; HTTPS adoption; Italian municipalities; Web security

1. Introduction

Until a decade ago, the use of the HTTPS protocol to secure communication between the web server and the user's browser (i.e. the use of a SSL/TLS security certificate) was mostly relegated to e-commerce websites, e-banking websites or, in general, to those sites whose main mission was to manage data in the economic/financial field [1][2].

In Europe, with the entry into force in May 2018 of the EU Regulation 2016/67 regarding General Data Protection Regulation (GDPR) [3], the need to use secure web communications has also extended to all those sites that, for various reasons, exchange sensitive data with their users via the web.

* Corresponding author. Tel.: +39-349-4683200.
E-mail address: antoniogiovanni.schiavone@bancaditalia.it

A further push for the adoption of the HTTPS protocol came from the so-called 'Tech Giants', i.e. the most dominant companies in the information technology industry. In particular, starting from 2014 Google promoted the use of HTTPS connections as a ranking factor on its search engine, i.e. as one of the elements that is evaluated by its algorithms to define the ordering of the results for a given search query [4]. Subsequently, Google introduced the indication of connections to sites with old HTTP protocol as 'not secure' in its browser Chrome [5]; over time, a similar indication has been introduced by other browsers (e.g. Mozilla Firefox).

Unfortunately, despite the obvious advantages in terms of security and confidentiality of communications, the Italian legislative bodies have not grasped the growing importance of the implementation of the HTTPS protocol within websites, and in particular within those of Public Administrations.

In fact, in contrast to other aspects of websites (e.g. accessibility of Public Administrations' websites, regulated by the so-called 'Stanca Law' [6]), in Italy there is no legislation that explicitly obliges Public Administrations to use the HTTPS protocol.

The only official document regarding the usage of HTTPS Protocol (and its underlying technologies) on Public Administrations' websites was recently issued by the Agency for Digital Italy (AgID) [7]: unfortunately, this document provides some best practices on the aforementioned topic, but does not introduce any obligations.

As consequence of this regulatory vacuum, in many Italian Public Administrations' websites the HTTPS protocol is not adopted or not correctly implemented. This failure to use secure communications on the web potentially exposes Italian citizens to risks when communicating with Public Administrations.

This risk is especially pertinent in digital communications with local Public Administrations (such as municipalities), which citizens engage with most frequently for diverse needs, including the payment of various types of taxes and fines.

This paper presents the results of the Municipality2Https project, which aim is to assess the diffusion of the HTTPS protocol among the websites of Italian municipalities and the quality of its technical implementation and, consequently, to evaluate the security of their communications with citizens.

After discussing related work, the architecture of MunicipalityEvaluator, a software environment for evaluating HTTPS implementation in municipalities' websites, is presented along with a scoring system that enables the comparison of different website implementations.

The results obtained will be aggregated according to both geographic and demographic dimensions, in order to extrapolate relevant information on the websites under consideration.

Finally, some conclusions are drawn and suggestions for future work are provided.

2. Related Work

Since the development of the HTTPS protocol, various research groups have investigated the implementation of this protocol in large sets of websites: for instance, Felt et al. [8] provided a large-scale evaluation of worldwide HTTPS usage, both on user and developers prospective.

Restricting to the case of country-specific analyses, Vumo et al. [9] performed an analysis of the exposure of web servers and HTTP security headers to attackers in 240 Mozambican websites: nevertheless, the set of websites taken into account was not limited to Public Administrations' websites, nor was a scoring system provided for comparing the implementation of the various websites.

Recently, Patrick Hill et al. [10] examined over 2900 state and local government websites of United States testing their resilience to several types of cyber-attacks, including usage of deprecated HTTPS-related protocols (for instance, SSL 2.0 and 3.0) and related vulnerabilities. Later, Dunbar [11] proposed a similar, but more fine-grained, analysis on the same topic.

Further focusing on the analysis of municipalities' websites, Andersdotter et al. [12], through an ad-hoc evaluation platform, analyzed around 300 Swedish municipalities in order to exploit risks related to personally identifiable information's leakage: however, the analysis of the HTTPS protocol implementation was only a marginal part of the analysis platform and related metrics.

More recently, Gomes et al. [13] [14] exploited the HTTPS usage in Portuguese municipalities' websites, but limiting their analysis to verifying the implementation of the HTTPS protocol, the presence of HTTP to HTTPS redirect and the certificates' correctness. A similar analysis was carried out by Júnior et al. [15], limited to the case of Portuguese city councils.

Considering the case of Italian municipalities, there are few relevant experiences in literature concerning the analysis of websites' communication security: apparently, researchers focused on other topics, such as the accessibility of the websites of some public institutions [16] or the interaction of municipalities with citizens via social media networks [17].

The aim of this paper is therefore to fill this gap, providing a first, but relevant, wide-ranging analysis of secure communications' implementations within the Italian municipalities' websites.

3. Administrative division and demographics categorization in Italy

From an administrative point of view, Italy consists of 20 Regions, constituting its second *Nomenclature of Territorial Units for Statistics* (NUTS) [18] administrative level, each of which has its own regional capital. These Regions are grouped into 5 Macro-Regions, representing the first NUTS administrative level, as shown in Table 1:

Table 1. Macro-Regions in Italy

Macro-Region	Regions (in alphabetical order)
North-West	Aosta Valley, Liguria, Lombardy, Piedmont
North-East	Emilia-Romagna, Friuli-Venezia Giulia, Trentino-South Tyrol, Veneto
Center	Lazio, Marche, Tuscany, Umbria
South	Abruzzo, Apulia, Basilicata, Calabria, Campania, Molise
Islands	Sardinia, Sicily

Each Region is further divided into a variable number of provinces, totaling 107 Italian provinces: in turn, each province is made up of a variable number of municipalities, totaling 7,904 Italian municipalities. Moreover, there are 15 Italian "metropolitan cities" (Bari, Bologna, Cagliari, Catania, Florence, Genoa, Messina, Milan, Naples, Palermo, Reggio Calabria, Rome, Sassari, Turin and Venice), which are a special type of sub-provinces. As defined by law, they include a large core city and the smaller surrounding towns that are closely related to it: some of core cities are also regional capitals, others are not.

These administrative divisions will subsequently serve as the basis for aggregating results geographically.

As per the Italian law titled "*Testo unico delle leggi sull'ordinamento degli enti locali*" [19], municipalities can be classified into 12 distinct demographic categories based on their population size, as outlined in Table 2:

Table 2. Demographics categories according to Italian law

Category	Number of Inhabitants
I° category	Less than 500
II° category	500 – 999
III° category	1.000 - 1.999
VI° category	2.000 - 2.999
V° category	3.000 - 4.999
VI° category	5.000 - 9.999
VII° category	10.000 - 19.999
VIII° category	20.000 - 59.999
IX° category	60.000 - 99.999
X° category	100.000 - 249.999
XI° category	250.000 - 499.999
XII° category	500.000 and more

This categorization will subsequently serve as the basis for aggregating results by demographics.

4. Regulation on web security in Italy

As previously noted, in November 2020, the Agency for Digital Italy (AgID), in partnership with the Department for Digital Transformation (DTD) of the Italian Ministry for Technological Innovation and Digital Transition (MITD), developed a document titled "AgID Recommendations on Transport Layer Security (TLS) Standard". This document currently serves as the exclusive authoritative Italian reference for HTTPS implementation on Public Administrations' websites.

This document presents a series of security protocol recommendations along with cipher suites that, as of its creation, embody the cutting-edge standards in this domain. Specifically, this document stipulates that websites of Public Administrations should:

- Implement TLS version 1.2 or higher while disallowing usage of lower protocol versions.
- Adopt one of the 'Modern' or 'Intermediate' configurations outlined within this document.

Indeed, the document references a TLS configuration classification previously put forth by the Mozilla Foundation [20], encompassing three distinct configurations:

- Modern configuration, using:
  - TLS version: 1.3 (1.2 is not accepted)
  - TLS curve: X25519, prime256v1 or secp384r1
  - Certificate type: ECDSA (P-256)
  - Certificate duration: 90 days

    - Encryption suites:
        - TLS_AES_128_GCM_SHA256
        - TLS_AES_256_GCM_SHA384
        - TLS_CHACHA20_POLY1305_SHA256

- Intermediate configuration, using:
    - TLS version: 1.3 and/or 1.2
    - TLS curve: X25519, prime256v1 or secp384r1
    - Certificate type: ECDSA (P-256) (recommended) o RSA (2048 bits)
    - Certificate duration: 90 days (recommended) up to 366 days
    - DH parameter size: 2048 (only for Intermediate RFC7919)
    - Encryption suites (TLS 1.3):
        - TLS_AES_128_GCM_SHA256
        - TLS_AES_256_GCM_SHA384
        - TLS_CHACHA20_POLY1305_SHA256
    - Encryption Suites (TLS 1.2):
        - ECDHE-ECDSA-AES128-GCM-SHA256
        - ECDHE-RSA-AES128-GCM-SHA256
        - ECDHE-ECDSA-AES256-GCM-SHA384
        - ECDHE-RSA-AES256-GCM-SHA384
        - ECDHE-ECDSA-CHACHA20-POLY1305
        - ECDHE-RSA-CHACHA20-POLY1305
        - DHE-RSA-AES128-GCM-SHA256
        - DHE-RSA-AES256-GCM-SHA384

- Old configuration:
    - All configurations that, for any reason, do not adhere to the specifications outlined for either the 'Modern' or 'Intermediate' configurations.

Regrettably, the AgID document lacks guidance on various other facets concerning the implementation of secure communications.

The first aspect not addressed by the mentioned document is the implementation of a redirect from HTTP URLs to their corresponding HTTPS URLs: this redirect is indeed essential to ensure that a user always interacts with a website through encrypted communication.

Another aspect not analyzed by the AgID document is the characteristics of the certificate used to encrypt communication: in particular, neither the certificate's validity (i.e., whether it has expired or not) nor the match of the 'Common Name' contained within it with the domain of the website where it is actually used is assessed.

Furthermore, the possible presence of known vulnerabilities is not taken into consideration. In fact, over the years, various types of attacks that can be launched against encrypted communications have been discovered, exploiting defects and design errors present in outdated versions of the SSL or TLS protocols [21].

Lastly, this document fails to offer any guidance for conducting a precise assessment of the current implementations. For instance, as per the categorization presented in this document, both of these implementations are grouped under the same classification (referred to as the 'Old' configuration):

- An implementation reliant on outdated protocols (such as SSL 3.0).
- An implementation of TLS 1.2 featuring a certificate duration exceeding 366 days.

While both implementations receive the same categorization, it's evident that the latter approach is generally less vulnerable than the former. These considerations have been taken into account in the development of the scoring system, as detailed later in the paper.

5. Municipality2Https

5.1. General architecture

As previously mentioned in the preceding paragraphs, the objective of our project is to conduct a comprehensive assessment of the implementation of the HTTPS protocol on websites, with a particular focus on those belonging to Italian municipalities. To accomplish this goal, we have developed a software environment called MunicipalityEvaluator.

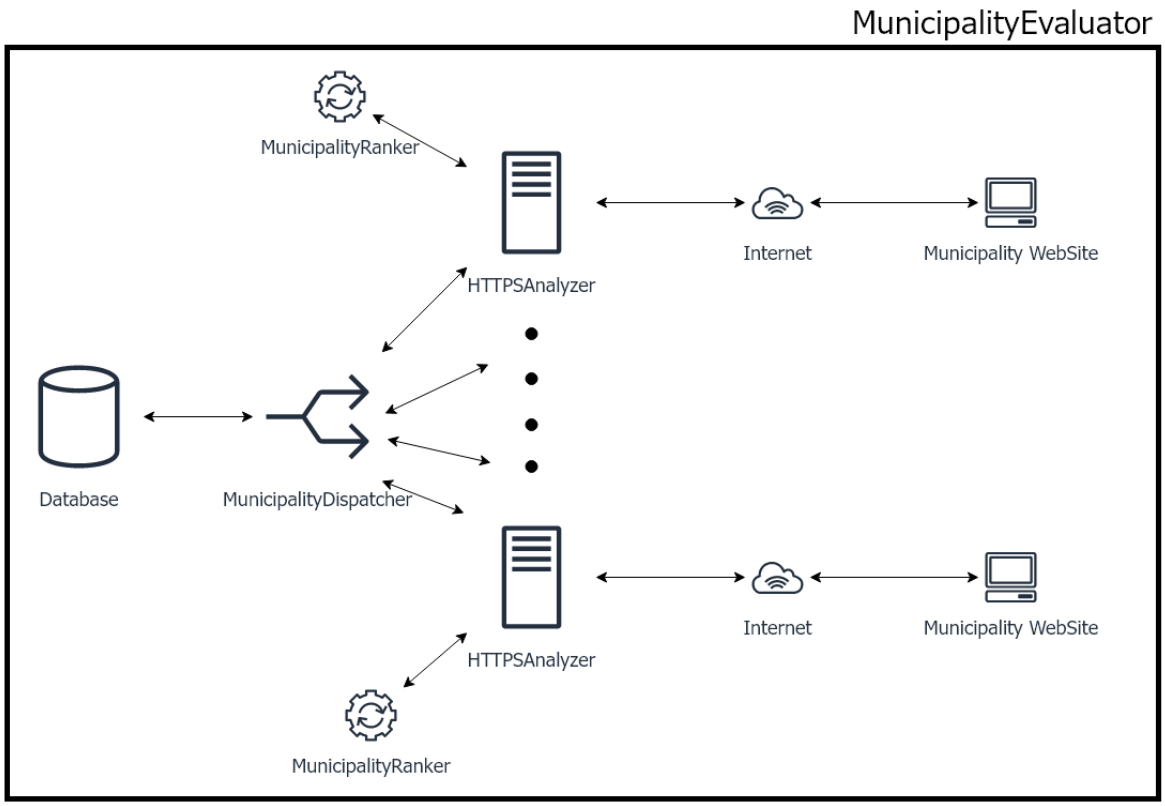

Fig. 1. General architecture of the software environment

This tool is designed to analyze various facets of HTTPS protocol implementation and generate a concise evaluation index. This index serves as a valuable resource for comparing different websites and aggregating the resulting data, both from a geographic and demographic perspective.

The general architecture of MunicipalityEvaluator is illustrated in Figure 1, and it is composed by:

- A database designed to store the initial dataset of each municipality along with the results of its analysis.
- A software component called MunicipalityDispatcher, responsible for managing the flow of analysis for municipalities' websites.
- A software component known as HTTPSAnalyzer, tasked with analyzing both the implementation of the HTTPS protocol and elements considered significant by the provided metrics for a given website.
- A software component called MunicipalityRanker, which calculates the score of a given website based on the results of the analysis conducted by the HTTPSAnalyzer component and in accordance with the proposed scoring system.

5.2. Initial Dataset

To conduct the analyses outlined in our project, it was imperative to gather preliminary information on Italian municipalities from various authoritative sources. The primary sources utilized during this data retrieval process were IndicePA and ISTAT.

IndicePA is a digital repository managed by AgID, that serves as a trusted directory housing comprehensive information on Public Administrations and Public Service Providers. It offers two modes of access: interactive consultation via repository's website or bulk data extraction through available APIs [22]. The specifics regarding the quantity and nature of data to be included can be found in the document titled 'Guidelines for the Index of Digital Domiciles of Public Administrations and Public Service Providers' [23].

The wealth of information offered by IndicePA far exceeds our specific needs, such as obtaining the name of the Mayor of a municipality. Consequently, we found it imperative to streamline the data retained for each municipality to include only the following essential details:

- IPA_code: Unique ID of the Municipality inside IndicePA dataset.
- Entity_name: Municipality's name.
- Istat_code: Unique ID of the Municipality inside ISTAT dataset.
- Institutional_site: URL of the Municipality's official website.

The information provided by IndicePA lacks details regarding the provinces and regions to which the municipalities belong, as well as their respective population figures. Therefore, it was essential to complement this data with information sourced from the Italian National Institute of Statistics (ISTAT). ISTAT serves as the primary authority for official statistics in Italy, accessible through its Data Portal [24]. The linkage between the data from IndicePA and ISTAT was established using the ISTAT code.

The obtained dataset was subsequently subjected to a custom script designed to identify errors in website URLs. Despite IndicePA being a reputable source and Public Administrations being required to verify their data every six months, a significant portion of municipalities had inaccuracies in their institutional website URLs.

These errors were mainly due to:

- Typing errors.
- Old and no longer used domains.
- References to subfolders within the supplier's website, which originally designed the institutional site.
- Wrong presence/absence of the 'www' prefix in relation to the server settings.

The URLs identified as erroneous were manually corrected through online searches and/or by consulting references from non-authoritative sources (e.g., Wikipedia).

5.3. MunicipalityDispatcher

The MunicipalityDispatcher serves as the central component responsible for initiating and orchestrating the analysis flow carried out by the HTTPSAnalyzer component. Additionally, it is responsible for gathering and storing the outcomes generated by the other two software components.

To this end, for each municipality:

- The MunicipalityDispatcher interacts with the relational database where municipality-related data has been preloaded.
- The MunicipalityDispatcher initiates a request to the HTTPSAnalyzer component to evaluate HTTPS implementation of the municipality's official website.
- MunicipalityDispatcher stores the evaluation results within the relational database.
- If the website is unreachable, MunicipalityDispatcher will make up to five retry attempts at validation, with a time interval between each attempt.

5.4. HTTPSAnalyzer

HTTPSAnalyzer serves as the cornerstone of the Municipality2Https project. It is the component responsible for analyzing the security of a website's connection when provided with its URL. Specifically, its role includes evaluating the following aspects:

- The presence of an HTTPS protocol implementation, and cascading:
  - The presence of redirection from HTTP to HTTPS.
  - The correct configuration of the SSL Common Name Certificate (i.e. the absence of a Certificate Name Mismatch Error).
  - The validity of the certificate used.
  - The list of cryptographic protocols supported by the HTTPS implementation.
  - The technical details of the Cipher Suites used by each of the supported cryptographic protocols.

- Exposure to known SSL/TLS vulnerabilities.
- The possible exposure of additional information on the type and version of Web servers used, language interpreters installed, CMS installed, software libraries installed, etc.

In performing some of its analyses, the component uses some services promoted by third parties via public APIs and/or open source software.

In particular, to ensure the integrity of the Common Name Certificate, validate certificate authenticity, assess exposure to known SSL/TLS vulnerabilities, and retrieve a list of employed cryptographic protocols and their corresponding Cipher Suites, HTTPSAnalyzer employs SSL Labs [25]. This online service, provided by the American company Qualys, is accessible via an API interface and has previously been utilized in research studies to analyze various aspects of websites (e.g. in [11]). The API allows simultaneous querying across multiple domains, supporting a maximum parallelism degree of 10.

Utilizing the analysis capabilities of the mentioned APIs, our tool is able to verify the presence of the following known vulnerabilities:

- Browser exploit against SSL/TLS (BEAST) [26]
- BLEICHENBACHER [27]
- Decrypting RSA using obsolete and weakened eNcryption (DROWN) [28]
- Factoring RSA Export Keys (FREAK) [29]
- HEARTBLEED [30]
- LuckyMinus20 [31]
- OpenSSL ChangeCipherSpec (OpenSSLCCS) [32]
- Padding Oracle On Downgraded Legacy Encryption (POODLE) [33].

5.5. MunicipalityRanker

MunicipalityRanker is the module tasked with generating a score derived from the analysis results obtained through the HTTPSAnalyzer component. Its main purpose is to offer a straightforward, albeit inherently approximate, evaluation of the effectiveness and precision of secure communication protocol implementations on a given website.

This index is computed by applying the scoring system described in the subsequent section to the findings derived from the analysis performed by the HTTPSAnalyzer component.

5.6. Execution Platform and Optimization

The evaluation platform has been fully developed in Java, including the libraries used for connecting to SSLLabs APIs, while the database was built using PostgreSQL version 13.

To improve the overall project efficiency and reduce processing time, we introduced the capability to concurrently execute the HTTPSAnalyzer component (and consequently the MunicipalityRanker component)

across multiple municipalities. We achieved this functionality by employing Multithreading programming techniques.

After a testing and optimization phase, during which we took into account the DDOS protection mechanisms of the external service (SSL LABS), we determined that the optimal level of parallelism, should be set to 4.

The analysis of the websites of all 7,904 Italian municipalities was conducted in May 2021, with an average processing time of 210 seconds per website. This resulted in an estimated total processing time of approximately 17 days.

By implementing the multithreaded approach with a parallelism degree of 4, we reduced this processing time to approximately 5 days, leading to a significant time savings of around 68%.

6. Definition of Scoring System

During the initial stages of platform development and testing, it became apparent that the landscape of HTTPS protocol implementations within Italian municipal websites was highly diverse, featuring markedly distinct and not readily comparable situations.

It has become evident, therefore, that there is a clear need for the formulation of a scoring system capable of aligning disparate evaluations under a common framework, facilitating both comparisons and aggregations across various dimensions.

The concept of developing a scoring system is not novel within the literature; in fact, referring to previously cited papers:

- In [8] authors introduced an intriguing numerical scoring system based on the assessment of the best-supported protocol by the analyzed website. According to this approach, the ideal implementation, which employs the latest protocol, is assigned a score of 100, while implementations using older or even deprecated protocols receive lower scores. However, this system fails to consider other crucial aspects for the correct implementation of the HTTPS protocol, such as redirects, the presence of vulnerabilities, and certificate validity. It also relies on the assumption that users, when accessing the website, always use the most recent version of the HTTPS protocol.
- In [12] authors introduced an alternative scoring system, which relies on a five-tier assessment framework rather than numerical values. In this approach, the evaluation criteria are limited to the presence or absence of the HTTPS protocol and the existence of third-party cookies, without delving into other aspects of HTTPS protocol implementation.
- Both in [13] and [14] authors employed a scoring system comprising four categories (Good, Reasonable, Minimum, and Bad). This system was based on the presence or absence of the HTTPS protocol, the use of resources in HTTP or exclusively in HTTPS, and the presence of a redirect from HTTP to HTTPS. However, it is worth noting that the analysis of the implementation, in this case as well, is relatively shallow and does not take into account other relevant aspects.

All the mentioned experiences highlight the absence of a common reference point. In fact, unlike other aspects of web development (consider the case of accessibility with the WCAG issued by the W3C [6]), there are no officially issued guidelines from an international standards organization regarding the proper implementation of the HTTPs protocol and related aspects.

The only guidelines that can be considered as a de facto standard are those previously mentioned and proposed by Mozilla [20], from which the AgID document originates.

Furthermore, in many of the cited cases, the criterion for assessing the confidentiality of communications relies solely on analyzing the presence of the HTTPS protocol.

In reality, the use of obsolete or deprecated cryptographic protocols, and the resulting exposure to known vulnerabilities, poses interception risks similar to those associated with unencrypted communications.

In such instances, the "false sense of security" resulting from the use of incorrect HTTPS implementations can lead to catastrophic situations, particularly when it involves sensitive or economic/financial data communications.

Considering all the aforementioned factors, both those outlined above and in the preceding sections, we have formulated a scoring system that meets the following criteria:

- It refers to a de-facto standard (the Mozilla's guidelines).
- It is a numerical scoring system that enables aggregations, averages, and other statistical assessments.
- As outlined in [8], the "ideal" configuration have a score of 100.
- As outlined in [8], the presence of elements that compromise the correctness of the implementation lowers the evaluation.
- Contrary to what is proposed in [8], it evaluates all supported versions, not assuming that the user always uses the most recent one.
- The score is not capped downwards: the use of obsolete and/or deprecated cryptographic protocols, exposure to known vulnerabilities, or the presence of other implementation issues can result in a negative score, serving as a warning against a dangerous false sense of security.

The resulting scoring system is defined by the following formula:

$$score(w) = C_w + 10R_w\text{-}10E_w\text{-}10M_w\text{-}5\sum O_w\text{ -}10\sum D_w\text{ -}10\sum V_w$$

Where

C_w is the Compliance Score for a generic website w, namely the score related to how compliant the implementation of website w is with the guidelines used as a reference, calculated according to what is indicated in Table 3.

R_w is a Boolean variable, equal to 1 if the website w has an automatic redirection from HTTP to HTTPS, 0 otherwise.

E_w is a Boolean variable, equal to 1 if the website w uses an expired certificate, 0 otherwise.

M_w is a Boolean variable, equal to 1 if the website w uses a certificate with a common name that differs from the domain of website w (Certificate Name Mismatch), 0 otherwise.

$\sum O_w$ represents the number of cryptographic protocols categorized as 'Old' and supported by the website w. On our platform, TLS 1.0 and TLS 1.1 protocols are categorized as “Old."

$\sum D_w$ represents the number of cryptographic protocols categorized as 'Deprecated' and supported by the website w. On our platform, SSL 2.0 and SSL 3.0 protocols are categorized as “Deprecated."

$\sum V_w$ represents the number of known vulnerabilities detected within the website W.

Table 3. Configuration Score

Outcome	Score
Satisfaction of the "Modern" configuration	90 points
Satisfaction of "Intermediate" configuration	65 points
Satisfaction with "Old" configuration	40 points
Absence of HTTPS protocol implementation	0 points

Ideal implementation I should:

- Meet “Modern” configuration requirements.
- Automatically redirect from HTTP to HTTPS.
- Have no issues related to certificates.
- Not support outdated or deprecated cryptographic protocols.
- Be free from vulnerabilities.

Therefore, the score of I is:

$$score(I) = 90 + 10 = 100$$

To illustrate a real-life case, consider the case of the Municipality of Morlupo, a small town approximately 30 km north of Rome, whose official website exhibits the following features:

- Satisfaction of the "Old" configuration
- Presence of redirect from HTTP to HTTPS
- Presence of a certificate name mismatch
- Support for two "Old" protocols

The total score of the Municipality of Morlupo is therefore given by the formula:

$$score(Morlupo) = 40 + 10 - 10 - 10 = 30$$

7. Results

7.1. General Discussion

The software environment was employed to assess the websites of 7,904 Italian municipalities. Out of these, 7,110 municipalities (approximately 90%) have implemented the HTTPS protocol, while the remaining 794 utilize only the HTTP protocol. Although not encompassing the entirety of websites, the analysis results affirm that the adoption of HTTPS has become a prevalent practice among municipal websites.

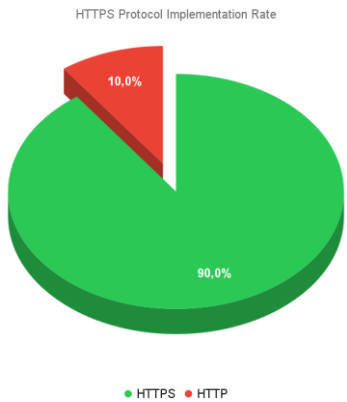

Fig. 2. HTTPS Protocol Implementation rate

7.2. Use of TLS Protocols, compliance with AgID Recommendations and vulnerabilities

Focusing the analysis on municipalities that adopt the HTTPS protocol, it is noteworthy that none of these implementations align with either the 'Modern' or 'Intermediate' configurations. This reiterates our earlier critique of the 'AgID Recommendations,' which we found overly stringent given the existing technological and administrative context.

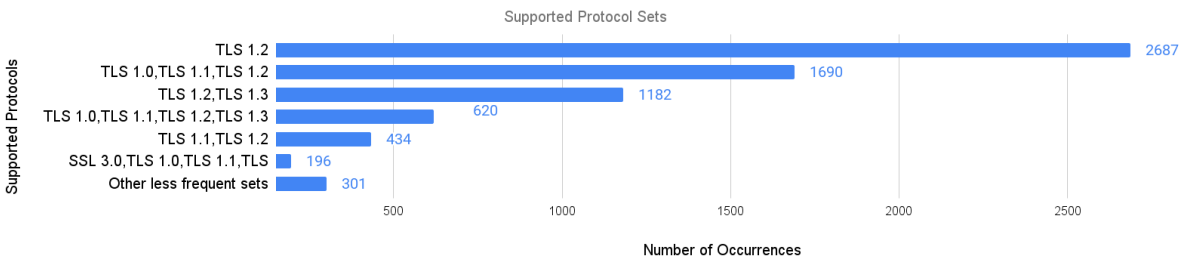

Fig. 3. Supported Protocol Sets

Specifically, there is just one site that solely employs TLS 1.3, potentially meeting the criteria for the Modern configuration.

Nevertheless, owing to a certificate validity period that exceeds the Modern configuration's maximum acceptable duration, the site was categorized as 'Old'.

Similarly, some other websites employ TLS 1.2, either on its own or in conjunction with TLS 1.3, but fail to meet the requirements of the 'Intermediate' configuration for various reasons.

As many as 3,231 municipalities, approximately 45% of them, still maintain support for at least one 'old' protocol, namely TLS 1.0 and/or 1.1. Additionally, 280 municipalities, around 4% of them, continue to support one or more obsolete protocols such as SSL 2.0 and/or SSL 3.0. Despite these protocols having been disabled by leading modern browsers, their continued server support presents a potential vulnerability.

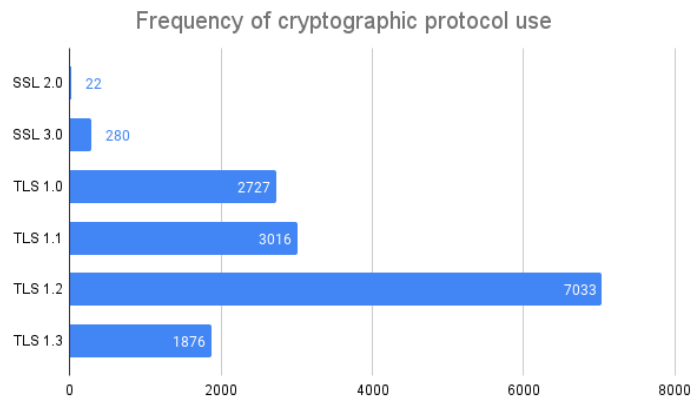

Fig. 4. Frequency of cryptographic protocol usage

Figure 4 illustrates the frequency of usage of cryptographic protocols. Approximately 99% of the examined websites support TLS 1.2 either independently or in combination with other protocols, while TLS 1.3, the most contemporary among the currently available protocols, is supported by only 1876 websites, representing roughly 26% of the total.

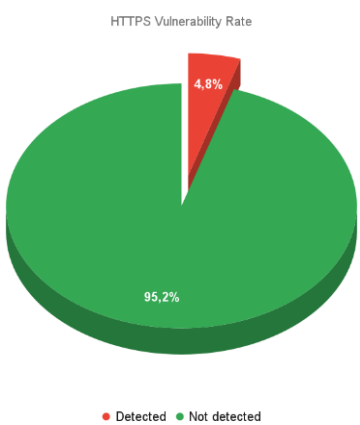

Fig. 5. HTTPS Vulnerability Rate

As a direct outcome of the aforementioned statistics, it is evident that 343 municipalities, or approximately 4.8% of them, are vulnerable to at least one known security vulnerability.

The most prevalent vulnerability is POODLE, impacting 240 municipalities (i.e., over 3%). This is followed by DROWN, which affects 81 municipalities (approximately 1%), and FREAK, affecting 63 municipalities (less than 1%).

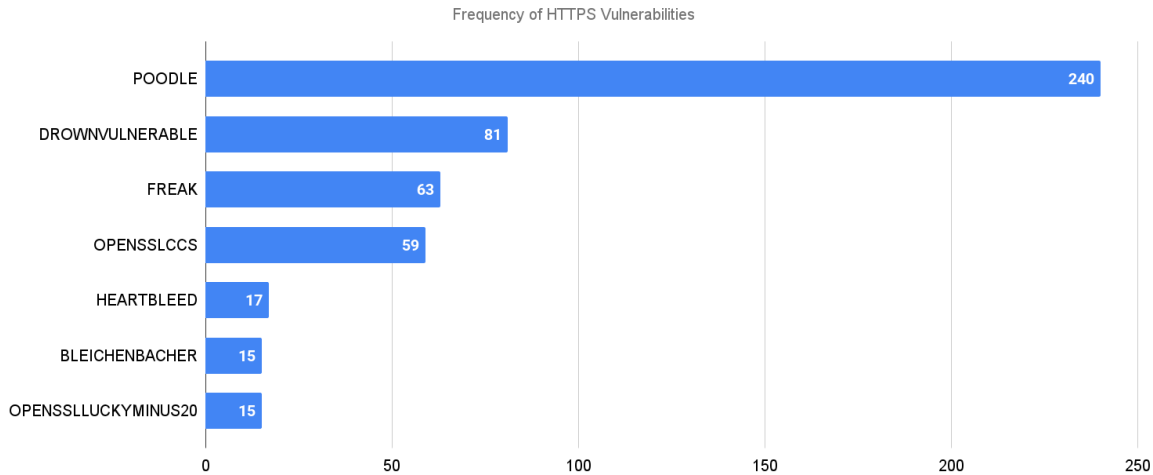

Fig. 6. Detected vulnerabilities' rate

7.3. Redirection, certificate name mismatch and certificate expiry

Regarding redirection from HTTP to HTTPS, this feature is only implemented in 4,502 municipalities (approximately 63%).

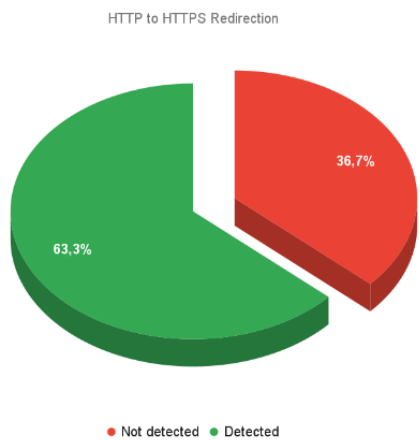

Fig. 7. HTTP to HTTPS Redirection

Consequently, more than one-third of the analyzed websites do not compel users to use the encrypted version of their website.

This suggests that a potentially significant portion of the website's users, specifically those who arrive at the website by entering the website's URL into the browser without specifying the protocol or through a hyperlink, may be accessing an unencrypted version of the website. This situation is exacerbated by the fact that the encrypted version of the website, accessible through the HTTPS protocol, is available. As a result, users are unnecessarily exposed to security risks.

The results also reveal that 1,914 municipalities, roughly accounting for 27%, experience a Certificate Name Mismatch issue. In many instances, this problem arises from the practice of outsourcing website development and management to external providers, who employ a single certificate for all their clients' websites.

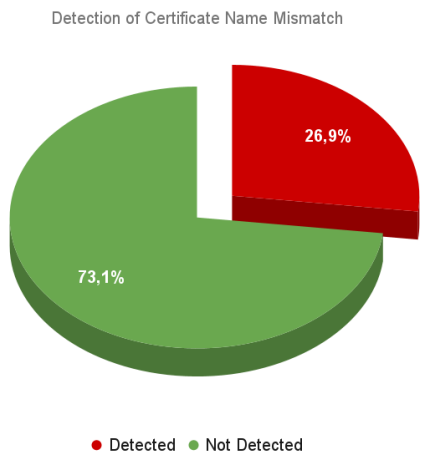

Fig. 8. Detection of Certificate Name Mismatch

Furthermore, aside from the critical security concerns, it is important to mention that major web browsers have been displaying a warning page (which may not always be very informative) when detecting a certificate name mismatch during navigation, as depicted in Figure 9.

A page like this could instill fear or confusion in users, leading them to abandon their municipality's website and consequently miss out on the digital services it provides, thereby undermining ICT investments.

Similar considerations can be applied to situations where an expired certificate is employed, although this occurred in only 306 municipalities (approximately 4%).

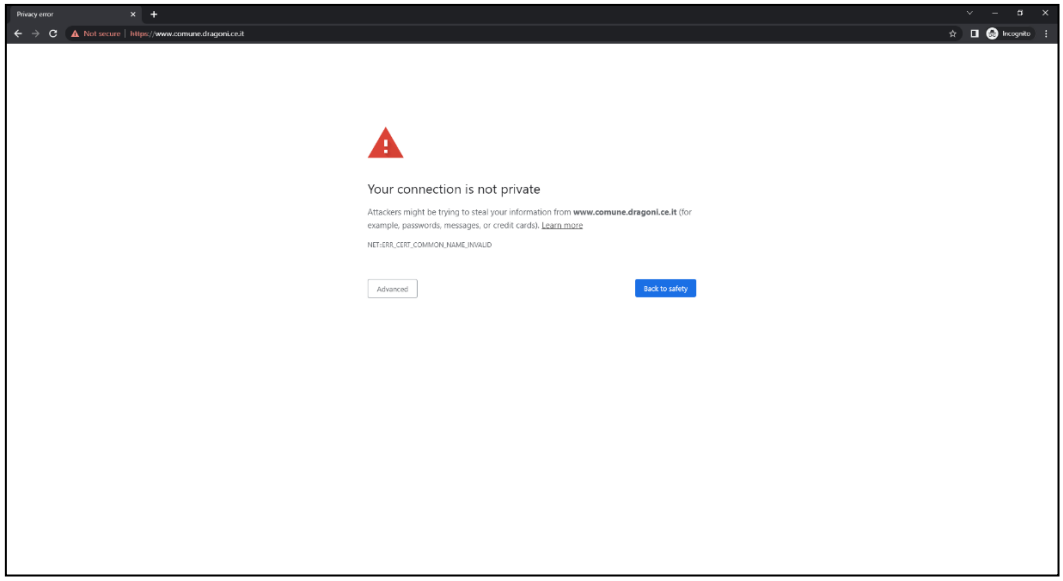

Fig. 9. Browser warning page due to certificate-related issue

7.4. Disclosure of other types of information

Diving further into various aspects of the analyzed websites' configurations, the results reveal that 3,183 municipalities (approximately 45%) disclose both the name and version of the web server they are utilizing, as illustrated in Figure 10.

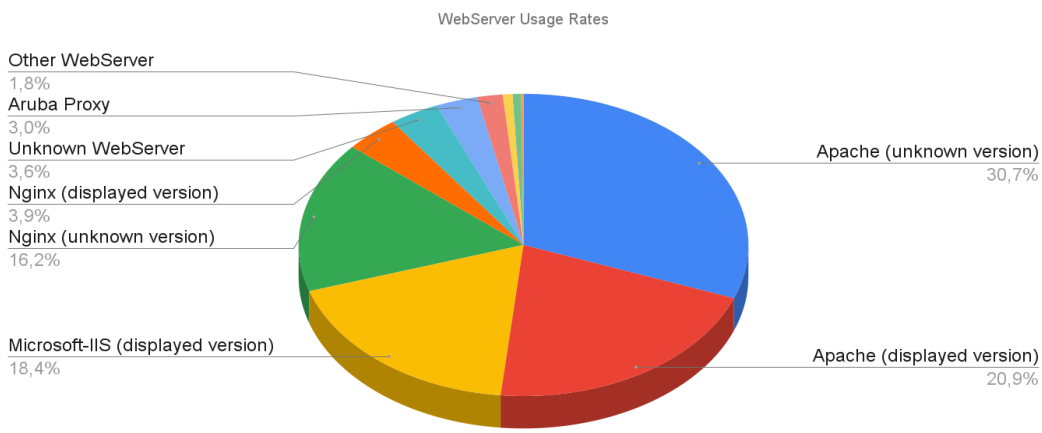

Fig. 10. WebServer usage rates

In certain instances, the used version of programming languages like PHP (729 municipalities, accounting for over 10%) or Python (57 municipalities, roughly 1%), as well as libraries like OPENSSL (816 municipalities, exceeding 11%), is also disclosed.

This exposure of such information constitutes an additional security concern, as it could potentially furnish an attacker with sufficient details to initiate an assault against the website by leveraging known vulnerabilities in particular versions of web servers, languages, or libraries.

7.5. Aggregated ranking on a national and macro-regional basis

Commencing with the municipalities' scores, the data was aggregated using both geographical and demographic criteria to establish a comprehensive assessment at various levels of granularity.

The national average score stands at 34.23 points, with a national standard deviation of 17.54.

Figure 11 displays aggregated scores on a macro-regional level: the two Northern macro-regions attained significantly higher average scores compared to the rest of Italy, whereas the Center and Islands macro-regions recorded scores that were largely similar to each other.

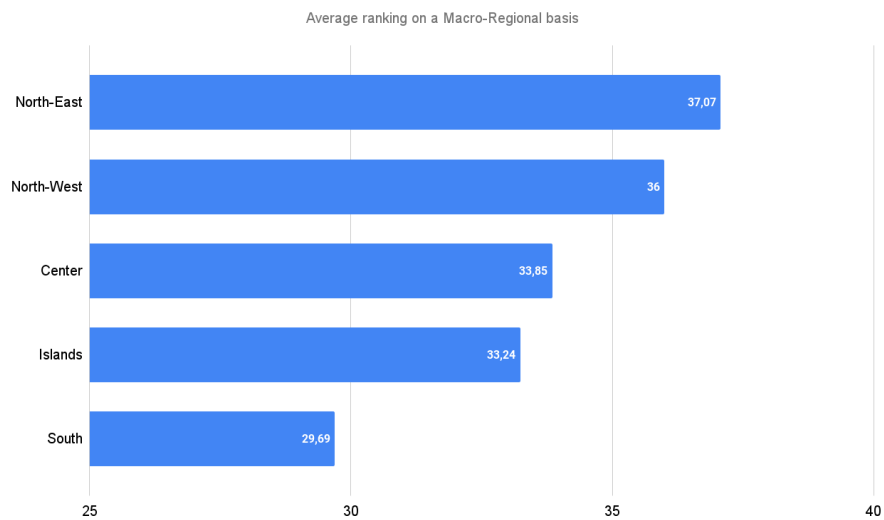

Fig. 11. Average ranking on a Macro-regional basis

7.6. Aggregated ranking on a regional basis

Delving into finer detail and considering the scores of individual regions (as depicted in Figure 12), the results reveal that these regions exhibit diverse rankings, which do not consistently align with the order derived from the analysis conducted at the macro-regional level.

Indeed, regions like Liguria (located in the North-West macro-region) and Friuli-Venezia Giulia (situated in the North-East MacroRegion) find themselves near the lower end of the ranking, occupying the 16th and 18th positions, respectively. On the other hand, Apulia, located in the South macro-region, holds a commendable 7th place.

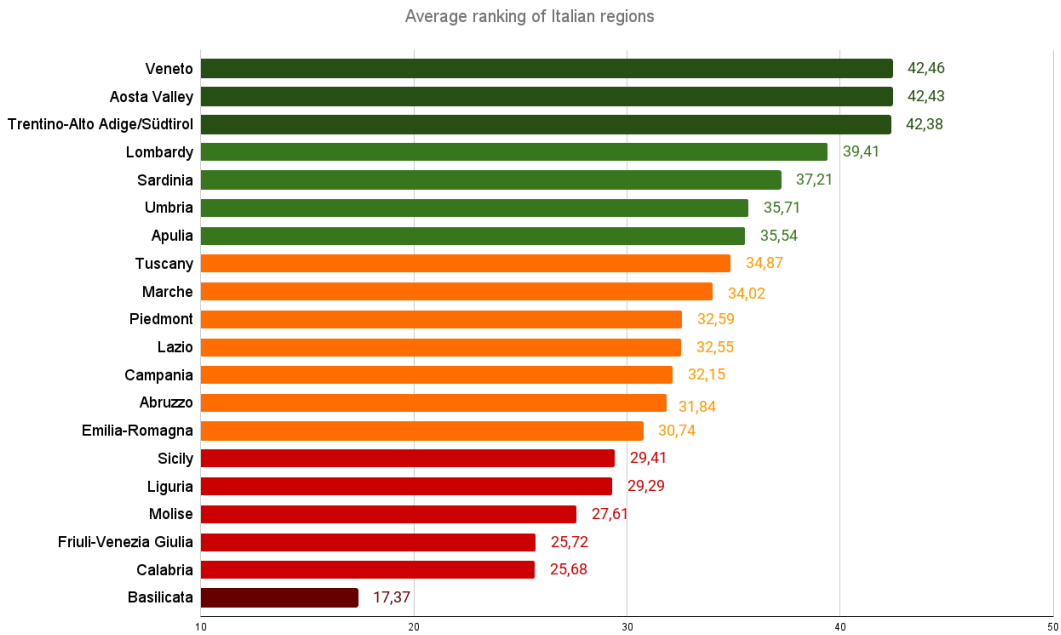

Fig. 12. Average ranking of Italian Regions

7.7. Aggregated ranking on a provincial basis

Proceeding to the ultimate level of detail, while considering the province scores (illustrated in Figure 13).

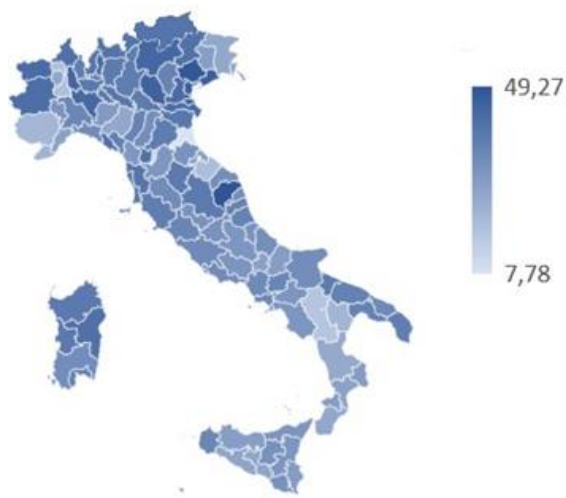

Fig. 13. Heat map of average ranking of Italian Provinces

We observe that the top-ranking provinces were Macerata (49.27 points), Treviso (47.98 points), and Venice (46.25 points), respectively. In contrast, Potenza (16.3 points), Prato (11.43 points), and Ravenna (7.78 points) find themselves at the bottom of the rankings.

7.8. Aggregated ranking of metropolitan city and regional capitals

Focusing on the capitals of the 20 Italian regions, the average score amounts to 36.25 points, with a standard deviation of 14.41. Within this group:

- Only the municipality of Potenza lacks support for the HTTPS protocol.
- Only 15 municipalities implement HTTP to HTTPS redirection.
- No municipality exhibits Certificate Name Mismatch or expired certificates.
- 3 municipalities still support outdated protocols and are consequently vulnerable to the POODLE attack.

Turning our attention to the core cities of the 15 metropolitan areas, the average score is 35 points, with a standard deviation of 15.57. Within this subset:

- Only the municipality of Reggio Calabria does not provide support for the HTTPS protocol.
- Only 10 municipalities employ HTTP to HTTPS redirection.
- No instances of Certificate Name Mismatch or expired certificates are identified.
- 2 municipalities maintain support for outdated protocols and are thus susceptible to the POODLE vulnerability.

In both the aforementioned groups (regional capitals and core cities of metropolitan areas), the average score surpasses the national average, while the standard deviation is narrower than the national value.

7.9. Aggregated ranking on demographic basis

The scores of individual municipalities were further categorized based on demographic criteria, following the demographic categories outlined by the aforementioned Italian laws. The distribution of average values is illustrated in Figure 14.

Notably, a general trend indicates that municipalities with larger populations tend to achieve higher scores. However, there is a noteworthy exception in the case of municipalities falling within the IX° category (i.e., 60,000-99,999 residents), where a significant decline in the average score is observed. Additionally, a slight decline is also evident in the case of the XI° category (i.e., 250,000 – 499,999 residents).

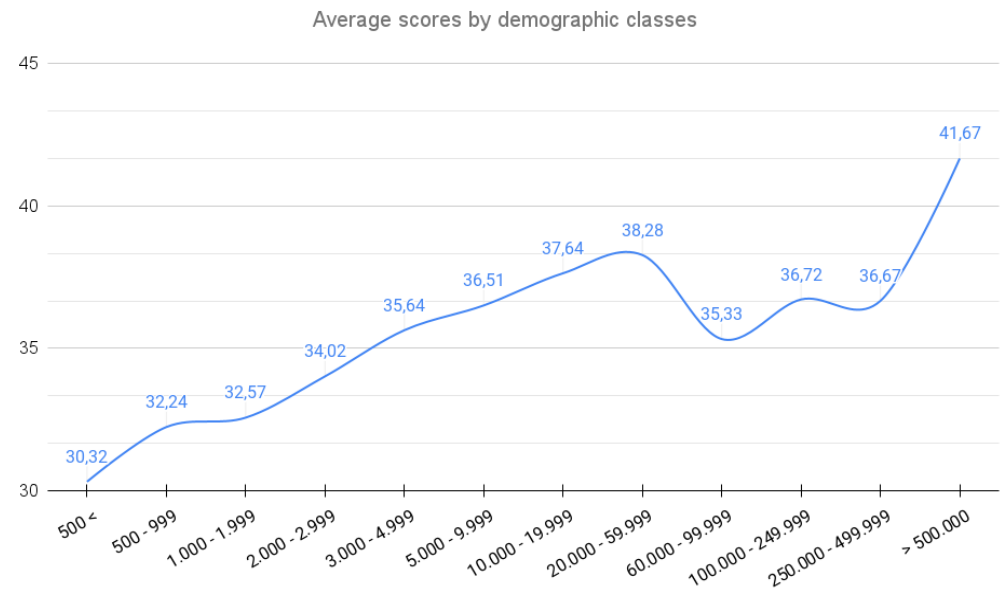

Fig. 14. Average scores by demographic classes

This decline can be partially attributed to a reduced percentage of HTTPS implementation among municipalities in the IX° category (i.e., 60,000-99,999), as illustrated in Figure 15.

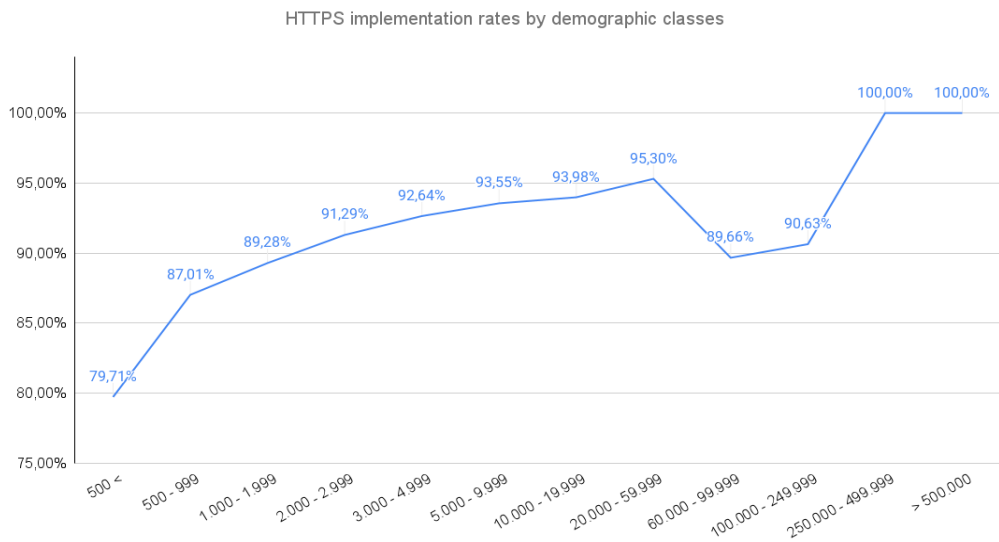

Fig. 15. HTTPS implementation rates by demographic classes

7.10. Further statistics

Since there are no websites adhering to the 'Modern' and 'Intermediate' configurations, the highest score is collectively achieved by 2,652 municipalities (approximately 37%). They scored 50 points, which results from the 'Old' configuration coupled with the presence of HTTP to HTTPS redirection, and without any maluses.

On the other hand, the lowest score was attained by a small municipality in Liguria, totaling -60 points. This low score stems from a multitude of maluses, including:

- Absence of redirection from HTTP to HTTPS
- Certificate name mismatch
- Use of an expired certificate
- Support for 2 obsolete protocols
- Support for 2 outdated protocols
- Vulnerable to 5 known vulnerabilities

The number of municipalities scoring less than 0 amounted to 154, roughly 2%.

8. Conclusions and future work

8.1. Conclusions

HTTPS is a widely used secure communication protocol for web traffic: it offers mutual authentication and establishes a secure channel for providing end-to-end encrypted communication over the Internet, providing authentication, confidentiality, and data integrity channel between the end users and domains.

Despite its widespread use on millions of websites, many sites still do not employ secure communications or use incorrect implementations, failing to harness or minimize the benefits offered by such a protocol. In particular, the use of incorrect implementations can provide website administrators with a false sense of security, which can lead to underestimating the risks present in their servers.

This paper offers a comprehensive analysis of HTTPS implementation across about 8000 Italian municipalities' websites. The study not only sheds light on the current state of HTTPS security but also introduces innovative elements through the utilization of the 'MunicipalityEvaluator' tool, a specialized instrument designed by author for the examination of these websites.

The study findings indicate that there is ample room for improvement in ensuring that all Italian municipalities' websites offer the necessary security measures for citizens to engage with them. In fact, while the high adoption rate of the HTTPS protocol (around 90%) is a positive development, several issues diminish its impact on website security: these issues encompass support for outdated or obsolete cryptographic protocols, limited HTTP-to-HTTPS redirection, and a substantial occurrence of Certificate Name Mismatch.

Although problems associated with expired certificates and known vulnerabilities are relatively minor, they require immediate attention due to their potential significant consequences. Furthermore, the disclosure of information regarding the type and version of the web server used raises major concerns, as attackers can exploit known vulnerabilities to launch large-scale attacks.

The study also reveals that the South of Italy lags behind the North in terms of technology and HTTPS implementation, and smaller municipalities tend to have subpar HTTPS implementations, resulting in a noticeable decline in the average score for medium-to-large municipalities.

8.2. Possible Project Extensions

The project primarily centered around the analysis of HTTPS protocol implementations. However, it was observed that there are additional aspects pertaining to website security, such as the exposure of sensitive information regarding the web server in use: to enhance the scope of the project, it is conceivable to reconsider the evaluation metrics to encompass bonus/malus points for such information.

Another potential extension could involve scrutinizing the technological platforms employed in website development to identify potential vulnerabilities. Furthermore, one could explore facets beyond security, such as web accessibility, by integrating an accessibility validator (e.g., MAUVE [34]) into the evaluation metrics.

References

[1] Naylor D., Finamore, A., Leontiadis, I., Grunenberger, Y., Mellia, M., Munafò, M., Papagiannaki, K., and Steenkiste, P. "The cost of the S in HTTPS", in Proceedings of the 10th ACM International on Conference on emerging Networking Experiments and Technologies. ACM, 2014, pp. 133–140.

[2] Chomsiri T. (2007). "HTTPS hacking protection", in 21st International Conference on Advanced Information Networking and Applications Workshops (AINAW'07) (Vol. 1, pp. 590-594).

[3] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). https://eur-lex.europa.eu/eli/reg/2016/679/oj

[4] Google Search Central Blog. HTTPS as a ranking signal, 2014. https://developers.google.com/search/blog/2014/08/https-as-ranking-signal

[5] Google Chrome Official Blog. A milestone for Chrome security: marking HTTP as "not secure", 2018. https://blog.google/products/chrome/milestone-chrome-security-marking-http-not-secure/

[6] Paternò, F., Schiavone, A.G. The role of tool support in public policies and accessibility. Interactions, 2015, 22.3: 60-63.

[7] Agenzia per l'Italia Digitale (AgID). Raccomandazioni Agid in merito allo standard Transport Layer Security (TLS), 2020. https://cert-agid.gov.it/wp-content/uploads/2020/11/AgID-RACCSECTLS-01.pdf (italian).

[8] Felt, A. P., Barnes, R., King, A., Palmer, C., Bentzel, C., & Tabriz, P. (2017). Measuring https adoption on the web.

[9] Vumo, A. P., Spillner, J., & Köpsell, S. (2017, August). Analysis of Mozambican websites: How do they protect their users? In 2017 Information Security for South Africa (ISSA) (pp. 90-97). IEEE.

[10] Hill, P., & Lin, Y. J. (2022). Evaluation of Trust Worthiness of State and County Government Websites.

[11] Dunbar, D. J. Survey of United States Related Domains: Secure Network Protocol Analysis. Available at SSRN 4240917.

[12] Andersdotter, A., & Jensen-Urstad, A. (2016). Evaluating Websites and Their Adherence to Data Protection Principles: Tools and Experiences: Contributions to IFIP Summer School Proceedings. Privacy and Identity Management. Facing up to Next Steps: 11th IFIP WG 9.2, 9.5, 9.6/11.7, 11.4, 11.6/SIG 9.2. 2 International Summer School, Karlstad, Sweden, August 21-26, 2016, Revised Selected Papers 11, 39-51.

[13] Gomes, H., Zúquete, A., Dias, G. P., & Marques, F. (2019). Usage of HTTPS by municipal websites in Portugal. In New Knowledge in Information Systems and Technologies: Volume 2 (pp. 155-164). Springer International Publishing.

[14] Gomes, H., Zúquete, A., Dias, G. P., Marques, F., & Silva, C. (2020). Evolution of HTTPS Usage by Portuguese Municipalities. In Trends and Innovations in Information Systems and Technologies: Volume 2 8 (pp. 339-348). Springer International Publishing.

[15] Júnior, J. B. C., Carneiro, P., Paiva, S., & Pinto, P. (2023). An analysis on the Implementation of Secure Web-related Protocols in Portuguese City Councils. International Journal of Marketing, Communication and New Media, (12).

[16] Barricelli, B. R., Sciarelli, P., Valtolina, S., & Rizzi, A. (2018). Web accessibility legislation in Italy: a survey 10 years after the Stanca Act. Universal Access in the Information Society, 17, 211-222.

[17] Capineri, C., Calvino, C., & Romano, A. (2015). Citizens and institutions as information prosumers. The case study of italian municipalities on Twitter. International Journal of Spatial Data Infrastructures Research, 10.

[18] Eurostat - Nomenclature of territorial units for statistics (NUTS): https://ec.europa.eu/eurostat/web/nuts/background

[19] "Testo unico delle leggi sull'ordinamento degli enti locali" (D.Lgs. 18 agosto 2000 n.267): https://dait.interno.gov.it/documenti/tuoel-giugno-2022.pdf

[20] Mozilla Foundation Wiki: https://wiki.mozilla.org/Security/Server_Side_TLS

[21] Paterson, K. G., & van der Merwe, T. (2016). Reactive and proactive standardisation of TLS. In Security Standardisation Research: Third International Conference, SSR 2016, Gaithersburg, MD, USA, December 5–6, 2016, Proceedings 3 (pp. 160-186). Springer International Publishing.

[22] IndicePA: https://indicepa.gov.it

[23] IndicePA API: https://indicepa.gov.it/ipa-dati/organization/agid-ipa

[24] ISTAT DATa Portal: http://dati.istat.it/Index.aspx

[25] Qualys's SSL LABS: https://www.ssllabs.com/ssltest/

[26] Duong, T., & Rizzo, J. (2011). Here come the⊕ ninjas.

[27] Bleichenbacher, D. (1998). Chosen ciphertext attacks against protocols based on the RSA encryption standard PKCS# 1. In Advances in Cryptology—CRYPTO'98: 18th Annual International Cryptology Conference Santa Barbara, California, USA. Springer Berlin Heidelberg.

[28] Aviram, N., Schinzel, S., Somorovsky, J., Heninger, N., Dankel, M., Steube, J., ... & Shavitt, Y. (2016). {DROWN}: Breaking {TLS} Using {SSLv2}. In 25th USENIX Security Symposium (USENIX Security 16) (pp. 689-706).

[29] Beurdouche, B., Bhargavan, K., Delignat-Lavaud, A., Fournet, C., Kohlweiss, M., Pironti, A., & Zinzindohoue, J. K. (2017). A messy state of the union: Taming the composite state machines of TLS. Communications of the ACM, 60(2), 99-107.

[30] Synopsys, The Heartbleed Bug, Synopsys, 2014. http://heartbleed.com.

[31] Somorovsky, J., https://www.openssl.org/news/secadv/20160503.txt

[32] Kikuchi, M. (2014). How I discovered CCS Injection Vulnerability (CVE-2014-0224). Lepidum, June.

[33] Möller, B., Duong, T., & Kotowicz, K. (2014). This POODLE bites: exploiting the SSL 3.0 fallback. Security Advisory, 21, 34-58.

[34] Schiavone, A. G., & Paternò, F. (2015). An extensible environment for guideline-based accessibility evaluation of dynamic Web applications. Universal access in the information society, 14(1), 111-132.