La Comunicazione - Note, Recensioni e Notizie n. 68
Anno 2024

Un'analisi sull'implementazione del protocollo HTTPS nei siti web dei Comuni Italiani

Examining the adoption of HTTPS Protocol in websites of Italian Municipalities

Antonio Giovanni Schiavone ♦
♦ Istituto di Analisi dei Sistemi ed Informatica "Antonio Ruberti" - CNR, Roma, Italia

Sommario

L'adozione del protocollo HTTPS è un elemento essenziale per garantire una comunicazione sicura attraverso i siti web, anche per quanto riguarda quelli delle Pubbliche Amministrazioni Locali. Questo protocollo assicura infatti la riservatezza, l'integrità e l'autenticità delle trasmissioni di dati online, proteggendo gli utenti dall'accesso non autorizzato e dalle violazioni dei dati. Implementando HTTPS, le Pubbliche Amministrazioni Locali possono offrire un'esperienza online sicura e affidabile ai propri cittadini e costruire fiducia nei loro servizi digitali. Questo documento presenta il progetto di ricerca Municipality2HTTPS, il cui obiettivo è fornire un'analisi approfondita dello stato attuale dell'implementazione del protocollo HTTPS all'interno dei siti web di circa 8.000 municipi italiani. Lo studio è stato condotto utilizzando una piattaforma software sviluppata appositamente, chiamata MunicipalityEvaluator, e i risultati sono stati aggregati sia geograficamente che demograficamente sulla base di una metrica realizzata ad hoc. Tale metrica è stata ottenuta ampliando i requisiti stabiliti dalle linee guida promosse in tale ambito dall'Agenzia per l'Italia Digitale e applicando una valutazione numerica per la presenza/assenza delle caratteristiche tecniche richieste. I risultati ottenuti hanno identificato diverse aree di miglioramento nell'implementazione del protocollo HTTPS e nella conformità alle citate linee guida, facendo quindi emergere la necessità di maggiore sensibilizzazione sul tema e di maggiore supporto tecnico verso i comuni. I risultati hanno inoltre rivelato sensibili discrepanze tra le regioni e i gruppi demografici in termini di percentuale di implementazione del protocollo HTTPS e conformità tecnica.

Abstract

The usage of HTTPS protocol is essential for secure communication with websites, also when it comes to the websites of local municipalities. This protocol ensures the confidentiality, integrity, and authenticity of online data transmissions, protecting users from unauthorised 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.

Keyword

E-government, Local government, HTTPS adoption, Italian municipalities, Web security

1. Introduzione

Fino a una decade fa, l'uso del protocollo HTTPS per garantire una comunicazione sicura tra un server web e il browser dell'utente (cioè l'uso di un certificato di sicurezza SSL/TLS) era principalmente limitato ai siti di e-commerce, di e-banking o, in generale, a quei siti il cui principale obiettivo era gestire dati nel campo economico/finanziario [1][2].

In Europa, con l'entrata in vigore nel maggio 2018 del Regolamento dell'UE 2016/679 relativo al Regolamento Generale sulla Protezione dei Dati (GDPR) [3], la necessità di utilizzare

comunicazioni web sicure si è estesa anche a tutti quei siti che, per varie ragioni, scambiano dati sensibili con i propri utenti tramite il web.

Un'ulteriore spinta all'adozione del protocollo HTTPS è giunta dai cosiddetti "Giganti del Web", ovvero le principali aziende che operano a livello mondiale in ambito ICT. In particolare, Google nel 2017 ha promosso l'utilizzo di connessioni HTTPS come fattore di ranking sul proprio motore di ricerca, ovvero come uno degli elementi che viene valutato dai suoi algoritmi per definire l'ordinamento dei risultati relativi ad una determinata query di ricerca [4]. Sempre Google ha successivamente introdotto nel suo browser Chrome l'indicazione delle connessioni a siti con vecchio HTTP come "non sicure" [5], venendo nel corso del tempo imitato anche da altri browser (ad es. Firefox).

Purtroppo, nonostante i chiari vantaggi in termini di sicurezza e riservatezza delle comunicazioni, troppo spesso non viene apprezzata l'importanza sempre crescente dell'implementazione del protocollo HTTPS all'interno dei siti web, e, in particolare, all'interno di quelli delle Pubbliche Amministrazioni.

A differenza di altri aspetti dei siti web (ad esempio, l'accessibilità dei siti web delle Pubbliche Amministrazioni, regolata dalla cosiddetta 'Legge Stanca' [6]), in Italia non esiste, infatti, una legislazione che obblighi le Pubbliche Amministrazioni a utilizzare il protocollo HTTPS.

L'unico documento ufficiale riguardante l'uso del protocollo HTTPS (e delle sue tecnologie sottostanti) nei siti web delle Pubbliche Amministrazioni è stato recentemente emesso dall'Agenzia per l'Italia Digitale (AgID) [7]: questo documento fornisce alcune linee guida tecniche sull'argomento, ma non introduce alcun obbligo normativo.

In assenza di obblighi di legge, in molti siti web delle Pubbliche Amministrazioni italiane il protocollo HTTPS non è adottato o non è correttamente implementato. Questo mancato utilizzo di comunicazioni sicure sul web espone potenzialmente i cittadini italiani a varie tipologie di rischi durante la loro interazione digitale con le Pubbliche Amministrazioni.

Questo rischio è particolarmente alto nelle comunicazioni digitali con le Pubbliche Amministrazioni Locali (come i comuni), con cui i cittadini interagiscono frequentemente per svariate necessità.

Questo articolo presenta i risultati del progetto Municipality2HTTPS [8], il cui obiettivo è valutare la diffusione del protocollo HTTPS tra i siti web dei comuni italiani e la qualità dell'implementazione tecnica.

Nei paragrafi successivi verranno presentati MunicipalityEvaluator, la piattaforma di analisi dell'implementazione HTTPS all'interno di un sito web, insieme alla metrica di valutazione formalizzata per il progetto Municipality2HTTPS e che ha permesso il confronto fra i siti web dei vari comuni.

I risultati ottenuti saranno aggregati sia secondo dimensioni geografiche che demografiche, al fine di estrapolare informazioni rilevanti sui siti web considerati.

Infine, saranno tratte alcune conclusioni e fornite alcune indicazioni per un futuro ampliamento del progetto.

2. Organizzazione amministrativa e raggruppamento demografico in Italia

Da un punto di vista amministrativo, l'Italia è composta da 20 Regioni, che costituiscono il suo secondo livello amministrativo della Nomenclatura delle Unità Territoriali Statistiche (NUTS) [9], ognuna delle quali ha il proprio capoluogo regionale. Queste Regioni sono raggruppate in 5 Macro-Regioni, che rappresentano il primo livello amministrativo della NUTS, come mostrato nella Tabella 1.

Ogni Regione è ulteriormente suddivisa in un numero variabile di province, per un totale di 107 province italiane: a loro volta, ogni provincia è composta da un numero variabile di comuni, per un totale, al momento, di 7.904 comuni italiani. Inoltre, vi sono 15 "città metropolitane" italiane (Bari, Bologna, Cagliari, Catania, Firenze, Genova, Messina, Milano, Napoli, Palermo, Reggio Calabria, Roma, Sassari, Torino e Venezia).

Tabella 1. Macro-Regioni in Italia

Macro-Regione	**Regioni (in ordine alfabetico)**
Nord-Ovest	Liguria, Lombardia, Piemonte, Valle d'Aosta
Nord-Est	Emilia-Romagna, Friuli-Venezia Giulia, Trentino-Alto Adige, Veneto
Centro	Lazio, Marche, Toscana, Umbria
Sud	Abruzzo, Basilicata, Calabria, Campania, Molise, Puglia
Isole	Sardegna, Sicilia

Questa organizzazione amministrativa costituirà successivamente il criterio utilizzato per l'aggregazione dei risultati su base geografica.

Inoltre, secondo il "Testo unico delle leggi sull'ordinamento degli enti locali"[10], in base alla dimensione della loro popolazione i comuni possono essere raggruppati in 12 categorie demografiche distinte, come descritto nella Tabella 2.

Tabella 2. Categorie demografiche definite dalla legislazione italiana

Categoria	**Popolazione**
I° categoria	Meno di 500 abitanti
II° categoria	500 – 999 abitanti
III° categoria	1.000 - 1.999 abitanti
VI° categoria	2.000 - 2.999 abitanti
V° categoria	3.000 - 4.999 abitanti
VI° categoria	5.000 - 9.999 abitanti
VII° categoria	10.000 - 19.999 abitanti
VIII° categoria	20.000 - 59.999 abitanti
IX° categoria	60.000 - 99.999 abitanti
X° categoria	100.000 - 249.999 abitanti
XI° categoria	250.000 - 499.999 abitanti
XII° categoria	Oltre 500.000 abitanti

Questa categorizzazione servirà successivamente come criterio per l'aggregazione dei risultati su base demografica.

3. Normativa italiana sulla sicurezza delle comunicazioni digitali

Come già osservato, nel novembre 2020, l'Agenzia per l'Italia Digitale (AgID), in collaborazione con il Dipartimento per la Trasformazione Digitale (DTD) del Ministero per l'Innovazione Tecnologica e la Transizione Digitale (MITD) italiano, ha pubblicato un documento intitolato "Raccomandazioni AgID in merito allo standard Transport Layer Security (TLS)". Attualmente, queste linee guida rappresentano in Italia l'unico documento ufficiale relativo all'implementazione del protocollo HTTPS nei siti web delle Pubbliche Amministrazioni.

Questo documento presenta una serie di raccomandazioni sia sui protocolli crittografici che delle correlate suite di cifratura da utilizzare.

In particolare, questo documento stabilisce che, all'interno dell'implementazione del protocollo HTTPS, i siti web delle Pubbliche Amministrazioni dovrebbero:

- Utilizzare il protocollo crittografico TLS, versione 1.2 o superiore, evitando l'uso di versioni precedenti o di protocolli precedenti.
- Adottare una delle configurazioni "Modern" o "Intermediate" definite all'interno del documento.

Il documento fa infatti riferimento a una classificazione delle configurazioni TLS precedentemente proposta dalla Fondazione Mozilla [11], che comprende tre configurazioni distinte:

- Configurazione "Modern", che prevede:
  - Versione TLS: 1.3 (la 1.2 non è consentita)
  - Curva TLS: X25519, prime256v1 or secp384r1
  - Tipo Certificato: ECDSA (P-256)
  - Validità Certificato: 90 giorni
  - Suite di cifratura:
    - TLS_AES_128_GCM_SHA256
    - TLS_AES_256_GCM_SHA384
    - TLS_CHACHA20_POLY1305_SHA256
- Configurazione "Intermediate", che prevede:
  - Versione TLS: 1.3 e/o 1.2
  - Curva TLS: X25519, prime256v1 or secp384r1
  - Tipo Certificato: ECDSA (P-256) (raccomandato) o RSA (2048 bits)
  - Validità Certificato: 90 days (raccomandato) fino a 366 giorni
  - Dimensioni parametro DH: 2048
  - Suite di cifratura (TLS 1.3):
    - TLS_AES_128_GCM_SHA256
    - TLS_AES_256_GCM_SHA384
    - TLS_CHACHA20_POLY1305_SHA256

  - Suite di cifratura (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
- Configurazione “Old”:
  - Tutte le implementazioni che, per qualsiasi motivo, non rispettano i requisiti delineati per le configurazioni “Modern” o “Intermediate”.

Sebbene il documento "Raccomandazioni AgID in merito allo standard Transport Layer Security (TLS)" rappresenti un importante punto di riferimento sul tema dell’uso del protocollo HTTPS all’interno dei siti della Pubblica amministrazione, esso presenta comunque alcune criticità.

Una prima osservazione è che la configurazione “Modern” proposta, sebbene valida dal punto di vista della sicurezza, presenta alcune difficoltà nella sua applicazione in un reale contesto d’uso all’interno della Pubblica Amministrazione.

Infatti, secondo le stime di CanIUse.com, sito specializzato nella verifica della compatibilità delle varie versioni dei browser rispetto a varie tecnologie web-related, circa il 3,5% degli utenti utilizza ancora browser non compatibili con il TLS 1.3.

Tale percentuale, sebbene minoritaria, potrebbe essere non trascurabile per un Comune, ovvero una Pubblica Amministrazione che ha l’obbligo istituzionale di comunicare con tutti i suoi cittadini. Inoltre, il requisito di aggiornare i certificati ogni 90 giorni può essere difficilmente applicabile, soprattutto da quei comuni di dimensioni piccole e piccolissime, che, non avendo un proprio ufficio ICT, si affidano a fornitori esterni per la gestione di tutta la loro comunicazione digitale.

Un'altra osservazione sulle linee guida AgID è che tale documento non fornisce indicazioni su altri aspetti correlati all’implementazione dei TLS, quali ad esempio la presenza della redirezione (redirect) automatica dalle url in HTTP alle corrispondenti url in HTTPS: questo reindirizzamento è infatti essenziale per garantire che un utente interagisca con il sito web sempre attraverso una comunicazione cifrata.

Un altro aspetto non definito dal documento dell'AgID sono le caratteristiche del certificato utilizzato per criptare la comunicazione: in particolare, tale documento non definisce né l'obbligatorietà della validità del certificato (ossia se è esso sia scaduto o meno) né della corrispondenza del 'Common Name' (informazione contenuta all'interno del certificato) con il dominio del sito web dove esso è effettivamente utilizzato.

Inoltre, non viene presa in considerazione la possibile presenza di vulnerabilità note. Infatti, nel corso degli anni, sono state scoperte varie tipologie di attacchi che possono essere lanciati contro le comunicazioni criptate, sfruttando difetti ed errori di progettazione presenti nelle versioni obsolete o deprecate dei protocolli SSL o TLS [12].

Infine, il documento non offre alcuna guida per condurre una valutazione accurata delle implementazioni attuali.

Ad esempio, secondo la classificazione proposta, entrambe queste implementazioni sono raggruppate sotto la stessa configurazione 'Old':

- Un'implementazione basata su protocolli crittografici obsoleti (come SSL 3.0).
- Un'implementazione di TLS 1.2 che presenta una durata del certificato superiore a 366 giorni.

Anche se entrambe le implementazioni ricevono la stessa classificazione, è evidente che la seconda implementazione è in generale meno vulnerabile rispetto alla prima.

Queste osservazioni sono state tenute in considerazione nello sviluppo della metrica di valutazione, come illustrato nei paragrafi successivi.

3.1. Architettura Generale

Come affermato nei paragrafi precedenti, l'obiettivo del nostro progetto è svolgere una valutazione completa dell'implementazione del protocollo HTTPS, con particolare attenzione ai siti dei comuni italiani.

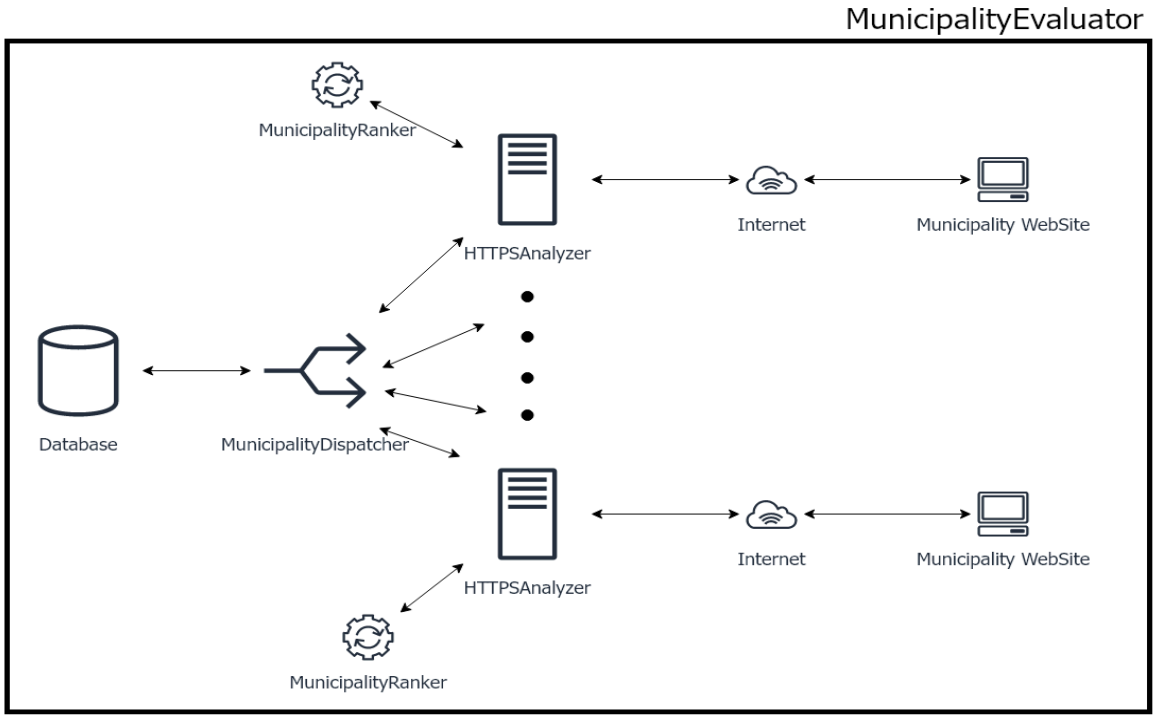

Figura 1 – *Architettura generale della piattaforma software MunicipalityEvaluator*

Per raggiungere questo obiettivo, abbiamo sviluppato una piattaforma software chiamata MunicipalityEvaluator.

Questo strumento è progettato per analizzare le varie caratteristiche dell'implementazione del protocollo HTTPS di un sito web e, a partire dai risultati dell'analisi, applicare una metrica per generare un indice numerico sintetico. Questo indice rappresenta una risorsa preziosa per confrontare diversi siti web e aggregare i dati risultanti, sia da un punto di vista geografico/amministrativo che demografico.

L'architettura generale di MunicipalityEvaluator è illustrata nella Figura 1 ed è composta da:

- Un database progettato per memorizzare il dataset iniziale di ciascun comune, insieme ai risultati della sua analisi.
- Il componente software MunicipalityDispatcher, responsabile della gestione del flusso di analisi per i siti web dei comuni.
- Il componente software HTTPSAnalyzer, incaricato di analizzare sia l'implementazione del protocollo HTTPS che gli elementi considerati significativi dalla metrica.
- Il componente software MunicipalityRanker, che calcola il punteggio di un determinato sito web in base ai risultati dell'analisi condotta dal componente HTTPSAnalyzer e in conformità con la metrica proposta.

3.2. Initial Dataset

Per condurre le analisi delineate nel nostro progetto, è stato necessario raccogliere informazioni preliminari sui comuni italiani da varie fonti autorevoli. Le fonti primarie utilizzate durante questo processo di recupero dati sono state IndicePA e l'ISTAT.

IndicePA è un repository digitale gestito da AgID, che funge da fonte autoritativa contenente informazioni esaustive sulle Pubbliche Amministrazioni e sui Fornitori di Servizi Pubblici. Offre due modalità di accesso: consultazione interattiva tramite il sito web del repository o estrazione bulk dei dati tramite le API disponibili [13]. I dettagli relativi alla quantità e alla natura dei dati da includere possono essere trovati nel documento intitolato “Linee guida per l'Indice delle Domiciliazioni Digitali delle Pubbliche Amministrazioni e dei Fornitori di Servizi Pubblici” [14].

La ricchezza di informazioni offerta da IndicePA supera di gran lunga le nostre esigenze specifiche, come ad esempio ottenere il nome del sindaco di un comune. Di conseguenza, abbiamo ritenuto opportuno ottimizzare il volume dei dati conservati per ciascun comune, includendo solo i seguenti dettagli essenziali:

- IPA_code: Identificatore univoco del Comune all'interno del dataset di IndicePA.
- Entity_name: Nome del Comune.
- Istat_code: Identificatore univoco del Comune all'interno del dataset dell'ISTAT.
- Institutional_site: URL del sito web ufficiale del Comune.

L'informazione fornita da IndicePA manca di dettagli riguardanti le province e le regioni a cui appartengono i comuni, così come i rispettivi dati sulla popolazione residente. Pertanto, è stato essenziale integrare questi dati con informazioni provenienti dall'Istituto Nazionale di Statistica (ISTAT). ISTAT funge da fonte autoritativa per dati statistici italiani, accessibile attraverso il suo Portale Dati [15]. Il collegamento tra i dati di IndicePA e quelli di ISTAT è stato stabilito utilizzando il codice ISTAT.

Il dataset ottenuto è stato successivamente sottoposto a uno script progettato per identificare gli errori negli URL dei siti web. Nonostante IndicePA sia una fonte affidabile e le Amministrazioni Pubbliche siano tenute a verificare i propri dati ogni sei mesi, una parte significativa dei comuni presentava imprecisioni negli URL dei loro siti web istituzionali.

Questi errori erano principalmente dovuti a:

- Errori di battitura.
- Domini vecchi e non più utilizzati.
- Riferimenti a sottocartelle all'interno del sito web del fornitore, che originariamente ha progettato il sito istituzionale.
- Errata presenza/assenza del prefisso 'www' in relazione alle impostazioni del server.

Gli URL identificati come errati sono stati corretti manualmente attraverso ricerche online e/o consultando riferimenti provenienti da fonti non autoritative (ad es. Wikipedia).

3.3. MunicipalityDispatcher

Il MunicipalityDispatcher funge da componente centrale, responsabile dell’avviamento e orchestrazione del flusso di analisi eseguito dal componente HTTPSAnalyzer. Inoltre, è responsabile della raccolta e memorizzazione dei risultati generati dalle altre due componenti software.

A questo scopo, per ciascun comune:

- Il MunicipalityDispatcher interagisce con il database relazionale, dove sono stati precaricati i dati relativi ai singoli comuni.
- Il MunicipalityDispatcher avvia una richiesta al componente HTTPSAnalyzer per valutare l'implementazione di HTTPS del sito web ufficiale del comune.
- Il MunicipalityDispatcher memorizza i risultati della valutazione all'interno del database relazionale.
- Se il sito web non è raggiungibile, il MunicipalityDispatcher effettuerà fino a cinque tentativi di verifica, distanziati da un predefinito intervallo di tempo tra ciascun tentativo.

3.4. HTTPSAnalyzer

HTTPSAnalyzer rappresenta il cuore del progetto Municipality2HTTPS in quanto è il componente che, data la URL di un sito web, ha il compito di analizzare correttezza e qualità dell'implementazione del protocollo HTTPS. In particolare, esso valuterà:

- La presenza di una implementazione de protocollo HTTPS, e a cascata:
  - La presenza di un redirezione da HTTP ad HTTPS.
  - La corretta configurazione del Common Name Certificate (ovvero l'assenza di un Certificate Name Mismatch Error).
  - La validità del certificato utilizzato.
  - La lista dei protocolli crittografici supportati dall'implementazione HTTPS in esame.
  - L'aderenza alle configurazioni "Modern", "Intermediate" oppure "Old" secondo quanto definito dalle linee guida AgID.
  - L'esposizione a vulnerabilità SSL/TLS note, quali ad esempio Heartbleed, POODLE o FREAK.
  - L'eventuale esposizione di informazioni aggiuntive su tipologia e versione del Web server utilizzato, dei linguaggi di programmazione installati, dei CMS installati, delle librerie software installate, etc.

Per eseguire alcune delle sue analisi, il componente utilizza alcuni servizi promossi da terze parti tramite API pubbliche e/o software open source.

In particolare, per verificare la correttezza del Common Name Certificate, verificare la validità del certificato, valutare l'esposizione a vulnerabilità SSL/TLS note e recuperare l'elenco dei protocolli crittografici impiegati e le relative Suite di cifratura, HTTPSAnalyzer utilizza SSL Labs [16].

Questo servizio online, fornito dall'azienda americana Qualys, è accessibile tramite un'interfaccia API ed è stato utilizzato in precedenti progetti di ricerca per analizzare vari aspetti dei siti web (ad esempio, in [17]). L'API consente interrogazioni simultanee su più domini, supportando un grado massimo di parallelismo pari a 10.

Utilizzando le capacità di analisi delle API menzionate, il nostro strumento è in grado di verificare la presenza delle seguenti vulnerabilità note:

- Browser exploit against SSL/TLS (BEAST) [18]
- BLEICHENBACHER [19]
- Decrypting RSA using Obsolete and Weakened eNcryption (DROWN) [20]
- Factoring RSA Export Keys (FREAK) [21]
- HEARTBLEED [22]
- LuckyMinus20 [23]
- OpenSSL ChangeCipherSpec (OpenSSLCCS) [24]
- Padding Oracle On Downgraded Legacy Encryption (POODLE) [25].

3.5. MunicipalityRanker

Il MunicipalityRanker è il modulo incaricato di calcolare un indice numerico sintetico (ossia un punteggio) a partire dei risultati dell'analisi ottenuti attraverso il componente HTTPSAnalyzer. Il suo scopo principale è quello di offrire una rappresentazione numerica, seppur intrinsecamente approssimativa, dell'efficacia e della precisione delle implementazioni dei protocolli di comunicazione sicura su un determinato sito web.
Questo indice è calcolato applicando la metrica descritta nella sezione successiva ai risultati derivati dall'analisi eseguita dal componente HTTPSAnalyzer.

3.6. Dettagli tecnici e Ottimizzazione

La piattaforma di valutazione è stata interamente sviluppata in Java, includendo le librerie utilizzate per la connessione alle API di SSLLabs, mentre il database è stato costruito utilizzando PostgreSQL versione 13.
Per migliorare l'efficienza complessiva del progetto e ridurre il tempo di elaborazione, abbiamo introdotto la capacità di eseguire contemporaneamente il componente HTTPSAnalyzer (e di conseguenza il componente MunicipalityRanker) su più comuni.

Abbiamo raggiunto questa funzionalità impiegando tecniche di programmazione Multithreading: ciò ha implicato replicare più istanze dei componenti HTTPSAnalyzer e MunicipalityRanker su vari Thread Java, opportunamente orchestrati dal componente MunicipalityDispatcher.

Dopo una fase di testing e ottimizzazione, durante la quale abbiamo tenuto conto dei meccanismi di protezione DDOS del servizio esterno (SSL LABS), abbiamo determinato che il livello ottimale di parallelismo dovesse essere impostato su 4.

L'analisi dei siti web di tutti i 7.904 comuni italiani è stata condotta nel maggio 2021, con un tempo di elaborazione medio di circa 210 secondi per sito web. Ciò ha comportato un tempo di elaborazione totale stimato in circa 17 giorni.

Implementando l'approccio multithreaded con un grado di parallelismo di 4, abbiamo ridotto questo tempo di elaborazione a circa 5 giorni, ottenendo un significativo risparmio di tempo del 68%.

4. Metrica di valutazione

Durante le fasi iniziali dello sviluppo e del test della piattaforma MunicipalityEvaluator, è emerso chiaramente che il panorama delle implementazioni del protocollo HTTPS all'interno dei siti web dei comuni italiani è altamente variegato, presentando situazioni marcatamente distinte e non facilmente confrontabili.

È divenuto quindi subito evidente che vi fosse una impellente necessità di formulare un sistema di valutazione in grado di allineare valutazioni disparate sotto un comune quadro di riferimento, facilitando sia i confronti che le aggregazioni attraverso varie dimensioni di analisi.

Il concetto di sviluppare un sistema di valutazione non è nuovo nella letteratura scientifica. Infatti, a titolo di esempio:

- Felt et al. [26] hanno introdotto un interessante sistema di valutazione numerica basato sulla valutazione del miglior protocollo supportato dal sito web analizzato. Secondo questo approccio, l'implementazione ideale, che utilizza il più recente protocollo, riceve un punteggio di 100, mentre le implementazioni che utilizzano protocolli più vecchi o addirittura deprecati ricevono punteggi più bassi. Tuttavia, questo sistema non tiene conto di altri aspetti cruciali per la corretta implementazione del protocollo HTTPS, come i reindirizzamenti, la presenza di vulnerabilità e la validità del certificato. Si basa anche sull'assunzione che gli utenti, quando accedono al sito web, utilizzino sempre la versione più recente del protocollo HTTPS.
- Andresdotter et al. [27] hanno introdotto un sistema di valutazione alternativo, che si basa su un quadro di valutazione a cinque livelli anziché su valori numerici. In questo approccio, i criteri di valutazione sono limitati alla presenza o all'assenza del protocollo HTTPS e all'esistenza di cookie di terze parti, senza approfondire altri aspetti dell'implementazione del protocollo HTTPS.
- Gomes et al. [28] [29] hanno utilizzato un sistema di valutazione composto da quattro categorie (Buono, Ragionevole, Minimo e Cattivo). Questo sistema si basava sulla presenza o sull'assenza del protocollo HTTPS, sull'uso di risorse in HTTP o esclusivamente in HTTPS e sulla presenza di un reindirizzamento da HTTP a HTTPS. Tuttavia, è importante notare che l'analisi dell'implementazione, anche in questo caso, è piuttosto superficiale e non tiene conto di altri aspetti rilevanti.

Tutte le esperienze menzionate evidenziano l'assenza di un punto di riferimento comune. Infatti, a differenza di altri aspetti dello sviluppo web (pensiamo al caso dell'accessibilità con le WCAG emesse dal W3C [6]), non esistono linee guida ufficialmente emesse da un'organizzazione internazionale riguardanti la corretta implementazione del protocollo HTTPS e degli aspetti correlati.

Le uniche linee guida che possono essere considerate come uno standard de facto sono quelle precedentemente menzionate e proposte da Mozilla [20], da cui deriva il documento AgID.

Inoltre, in molti dei casi citati, il criterio per valutare la riservatezza delle comunicazioni si basa esclusivamente sull'analisi della presenza/assenza del protocollo HTTPS.

In realtà, l'uso di protocolli crittografici obsoleti o deprecati, e la conseguente esposizione a vulnerabilità note, comporta rischi di intercettazione potenzialmente simili a quelli associati alle comunicazioni non crittografate.

In tali casi, il "falso senso di sicurezza" derivante dall'uso di implementazioni HTTPS scorrette può portare a situazioni catastrofiche, soprattutto quando coinvolge comunicazioni di dati sensibili o economico/finanziari.

Considerando tutti i fattori sopra menzionati, sia quelli delineati sopra che nelle sezioni precedenti, abbiamo formulato una metrica che soddisfa i seguenti criteri:

- Si riferisce a uno standard de facto (le linee guida di Mozilla).
- È un sistema di valutazione numerico che consente aggregazioni, medie e altre valutazioni statistiche.
- Come illustrato in [26], la configurazione "ideale" ha un punteggio di 100.
- Come illustrato in [26], la presenza di elementi che compromettono la correttezza dell'implementazione abbassa la valutazione.
- Contrariamente a quanto proposto in [26], valuta tutte le versioni supportate, non assumendo che l'utente utilizzi sempre la più recente.
- Il punteggio non è limitato verso il basso: l'uso di protocolli crittografici obsoleti e/o deprecati, l'esposizione a vulnerabilità note o la presenza di altri problemi di implementazione possono risultare in un punteggio negativo, fungendo da avviso contro un pericoloso “falso senso di sicurezza”.

Il sistema di valutazione risultante è definito dalla seguente equazione:

Equazione 1. Formula che esprime la metrica di valutazione

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

dove

C_w è il Punteggio di Conformità per un sito web generico w, ovvero il punteggio relativo a quanto conforme sia l'implementazione del sito web w rispetto alle linee guida utilizzate come riferimento, e viene calcolato secondo quanto indicato nella Tabella 3.

R_w è una variabile booleana, uguale a 1 se il sito web w ha un reindirizzamento automatico da HTTP a HTTPS, altrimenti 0.

E_w è una variabile booleana, uguale a 1 se il sito web w utilizza un certificato scaduto, altrimenti è 0.

M_w è una variabile booleana, uguale a 1 se il sito web w utilizza un certificato con un Common Name che differisce dal dominio del sito web w, altrimenti è 0.

$\sum O_w$ rappresenta il numero di protocolli crittografici categorizzati come 'Obsoleti' e supportati dal sito web w. Sulla nostra piattaforma, i protocolli TLS 1.0 e TLS 1.1 sono categorizzati come 'Obsoleti'.

$\sum D_w$ rappresenta il numero di protocolli crittografici categorizzati come ‘Deprecati' e supportati dal sito web w. Sulla nostra piattaforma, i protocolli SSL 2.0 and SSL 3.0 sono categorizzati come “Deprecati."

$\sum V_w$ rappresenta il numero di vulnerabilità note rilevate all'interno del sito web w.

Tabella 3. Punteggio di Conformità

Casistica	Punteggio
Soddisfacimento di tutti i requisiti della configurazione "Modern"	90 points
Soddisfacimento di tutti i requisiti della configurazione "Intermediate"	65 points
Presenza del protocollo HTTPS, ma mancato soddisfacimento dei requisiti delle precedenti configurazioni (ovvero configurazione "Old")	40 points
Assenza dell'implementazione del protocollo HTTPS	0 points

Quindi, una implementazione "ideale" $\boldsymbol{I}$ dovrebbe:

- Soddisfare i requisiti di configurazione "Modern".
- Reindirizzare automaticamente da HTTP a HTTPS.
- Non avere problemi legati ai certificati.
- Non supportare protocolli crittografici Obsoleti o Deprecati.
- Essere privo di vulnerabilità.

In tal caso, il punteggio di I sarebbe:

Equazione 2. Punteggio del caso ideale

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

Per illustrare un caso concreto, riportiamo l'esito dell'analisi del sito web istituzionale del Comune di Morlupo, una piccola città situata circa 30 km a nord di Roma, il cui sito web ufficiale presenta le seguenti caratteristiche:

- Mancato soddisfacimento delle configurazioni "Modern" e "Intermediate"
- Presenza di reindirizzamento da HTTP a HTTPS
- Presenza di una discrepanza nel nome del certificato
- Supporto per due protocolli "Obsoleti"

Applicando la metrica precedentemente definita, il punteggio del Comune di Morlupo è quindi dato dalla formula:

Equazione 3. Punteggio calcolato sull'esito della valutazione del comune di Morlupo

$$punteggio(Morlupo) = 40 + 10 - 10 - 5 * 2 = 30$$

5. Risultati

5.1. Discussione Generale

La piattaforma software MunicipalityEvaluator è stata impiegata per valutare i siti web di 7.904 comuni italiani. Di questi, 7.110 comuni (circa il 90%) hanno implementato il protocollo HTTPS, mentre i restanti 794 utilizzano solo il protocollo HTTP. Quindi, sebbene l'adozione del protocollo HTTPS non coinvolga tutto l'insieme dei siti web considerati, i risultati dell'analisi confermano che essa è diventata una pratica prevalente tra i siti web dei comuni.

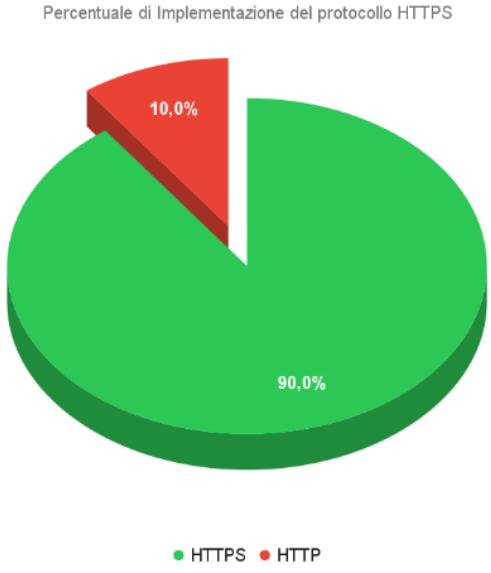

Figura 2 *- Percentuale di Implementazione del protocollo HTTPS*

5.2. Uso dei protocolli TLS, conformità alle Raccomandazioni AgID e vulnerabilità note

Restringendo la discussione sull'analisi dei comuni che adottano il protocollo HTTPS, è importante notare che nessuna delle implementazioni analizzate soddisfa i requisiti della

configurazione 'Modern' o di quella 'Intermediate'. Ciò sembra dare credito alle osservazioni precedentemente esposte, e relative ad una certa severità delle 'Raccomandazioni dell'AgID' rispetto l'attuale contesto tecnologico e amministrativo.

In particolare, c'è solo un sito che utilizza esclusivamente il protocollo crittografico TLS 1.3, potenzialmente soddisfacendo i criteri per la configurazione 'Modern'. Tuttavia, a causa di un periodo di validità del certificato che supera la durata massima accettabile da tale configurazione, il sito è stato valutato come appartenente alla configurazione 'Old'.

Allo stesso modo, alcuni altri siti utilizzano il protocollo crittografico TLS 1.2 (vedi Figura 3), sia da solo che in combinazione con TLS 1.3, ma non riescono a soddisfare i requisiti della configurazione 'Intermediate' per vari motivi (ad es. uso di suite di cifratura non previste da tale configurazione).

Inoltre, 3.231 comuni, approssimativamente il 45% di essi, mantengono ancora il supporto per almeno un protocollo 'Obsoleto', vale a dire il TLS 1.0 e/o TLS 1.1. Osserviamo ancora che 280 comuni, circa il 4% di essi, continuano a supportare uno o più protocolli 'Deprecati' come il SSL 2.0 e/o il SSL 3.0.

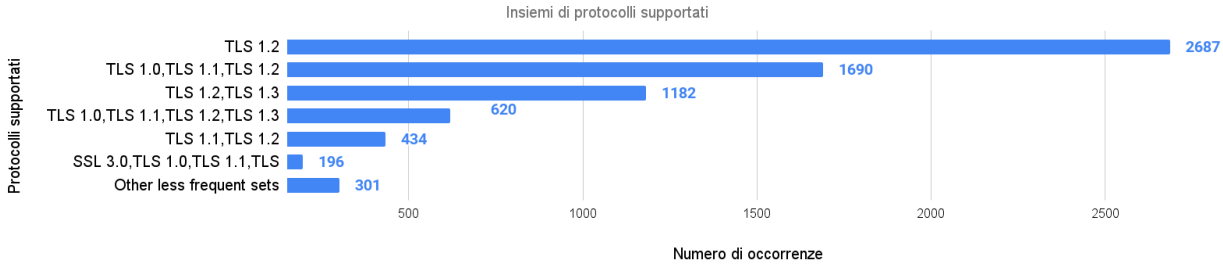

Figura 3 *- Insiemi di protocolli supportati*

Nonostante l'uso di questi protocolli deprecati sia stato disabilitato dai principali browser moderni, il loro continuo supporto lato server rappresenta una potenziale vulnerabilità.

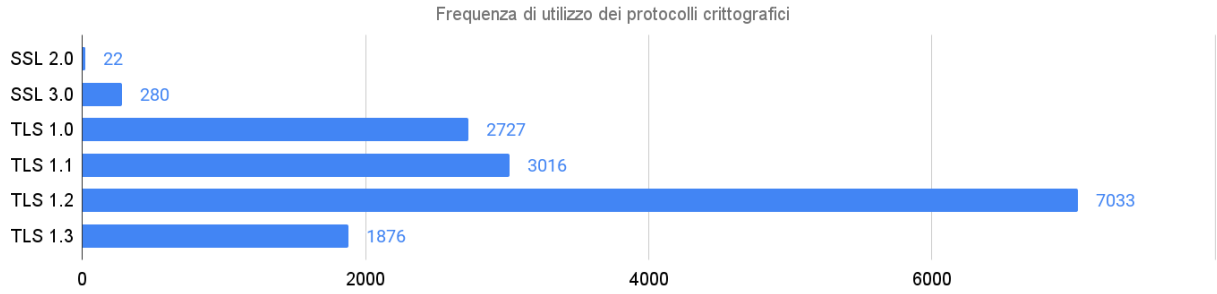

Figura 4 - *Frequenza di utilizzo dei protocolli crittografici*

La Figura 4 illustra la frequenza di utilizzo dei protocolli crittografici. Circa il 99% dei siti web esaminati supporta TLS 1.2 sia da solo che in combinazione con altri protocolli, mentre il TLS 1.3, il più recente tra i protocolli attualmente disponibili, è supportato solo da 1876 siti web, rappresentando approssimativamente il 26% del totale.

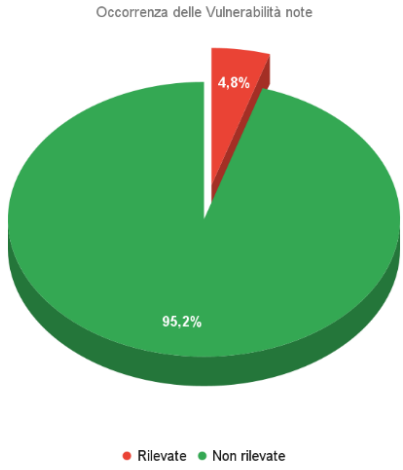

Figura 5 - *Occorrenza delle Vulnerabilità note*

Come diretta conseguenza delle statistiche precedentemente citate, 343 siti web dei comuni (ovvero circa il 4.8% dei siti che implementano il protocollo HTTPS) sono vulnerabili ad almeno una vulnerabilità nota (vedi Figura 5).

Come illustrato da Figura 6, la vulnerabilità più diffusa è POODLE, che colpisce 240 comuni (oltre il 3%).

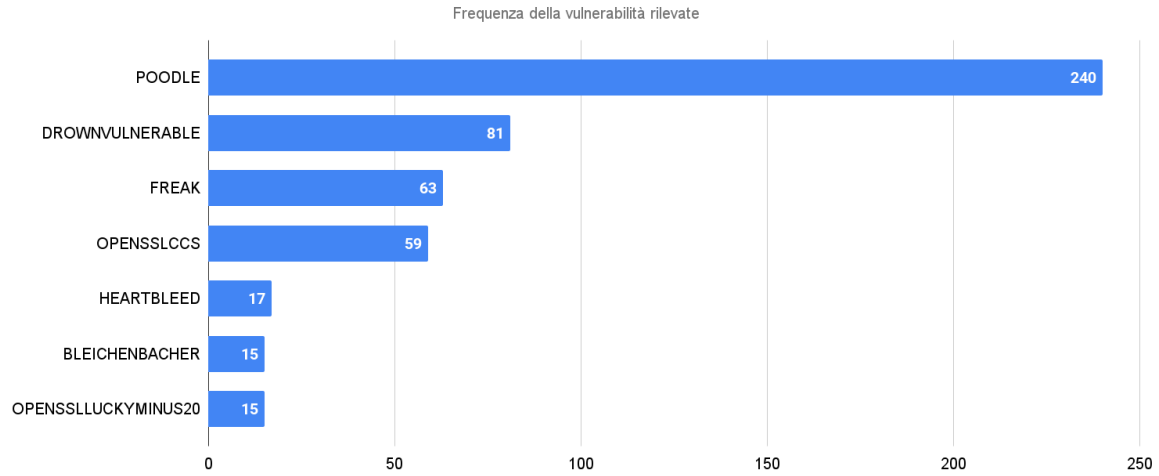

Figura 6 *- Frequenza della vulnerabilità rilevate*

Segue DROWN, che interessa 81 comuni (circa l'1%), e FREAK, che colpisce 63 comuni (meno dell'1%).

5.3. Redirezione, discrepanza del nome del certificato e scadenza del certificato

Riguardo alla redirezione da HTTP a HTTPS, questa funzionalità è implementata solo in 4.502 comuni (circa il 63%). Di conseguenza, più di un terzo dei siti web analizzati non obbliga gli utenti ad utilizzare il proprio sito web tramite comunicazioni crittografate e quindi sicure.

Ciò suggerisce che una parte potenzialmente significativa degli utenti del sito web, in particolare coloro che arrivano al sito web inserendo l'URL del sito nel browser senza specificare il protocollo o tramite un collegamento ipertestuale “non ottimale”, potrebbero accedere a una versione non crittografata del sito web. Questa situazione è aggravata dal fatto che la versione “sicura” del sito web, ossia accessibile tramite il protocollo HTTPS, è in realtà disponibile: dunque gli utenti sono esposti a rischi di sicurezza inutili.

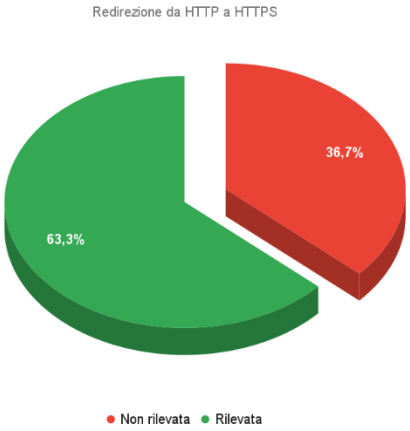

Figura 7 - *Redirezione da HTTP a HTTPS*

I risultati rivelano inoltre che 1.914 comuni, corrispondenti a circa il 27%, presentano un problema di discrepanza (mismatch) del nome del certificato (Common Name). In molte situazioni, questo problema deriva dalla pratica di esternalizzare lo sviluppo e la gestione del sito web a fornitori esterni, che impiegano un unico certificato per tutti i siti web dei loro clienti.

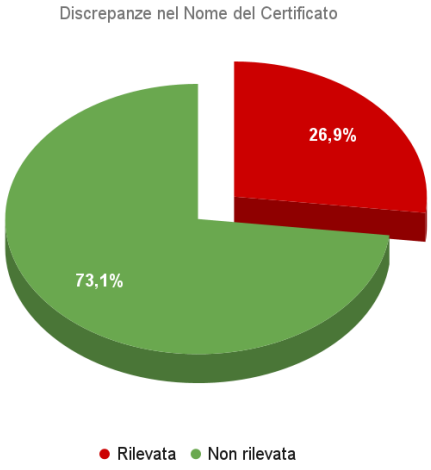

Figura 8 - *Rilevamento di discrepanze del nome nel certificato*

Oltre ai rilevanti problemi di sicurezza, è importante notare che i principali browser web mostrano una schermata di avviso (che potrebbe non sempre essere molto informativa) quando rilevano una discrepanza nel nome del certificato durante la navigazione, come

mostrato nella Figura 9. Una pagina del genere potrebbe suscitare timori o confusione negli utenti, spingendoli ad abbandonare il sito web del proprio comune e, di conseguenza, a non usufruire dei servizi digitali disponibili, compromettendo gli investimenti in ICT sostenuti dal comune. Considerazioni simili possono essere applicate alle situazioni in cui viene utilizzato un certificato scaduto, sebbene questa casistica sia stata rilevata solo in 306 comuni (circa il 4%).

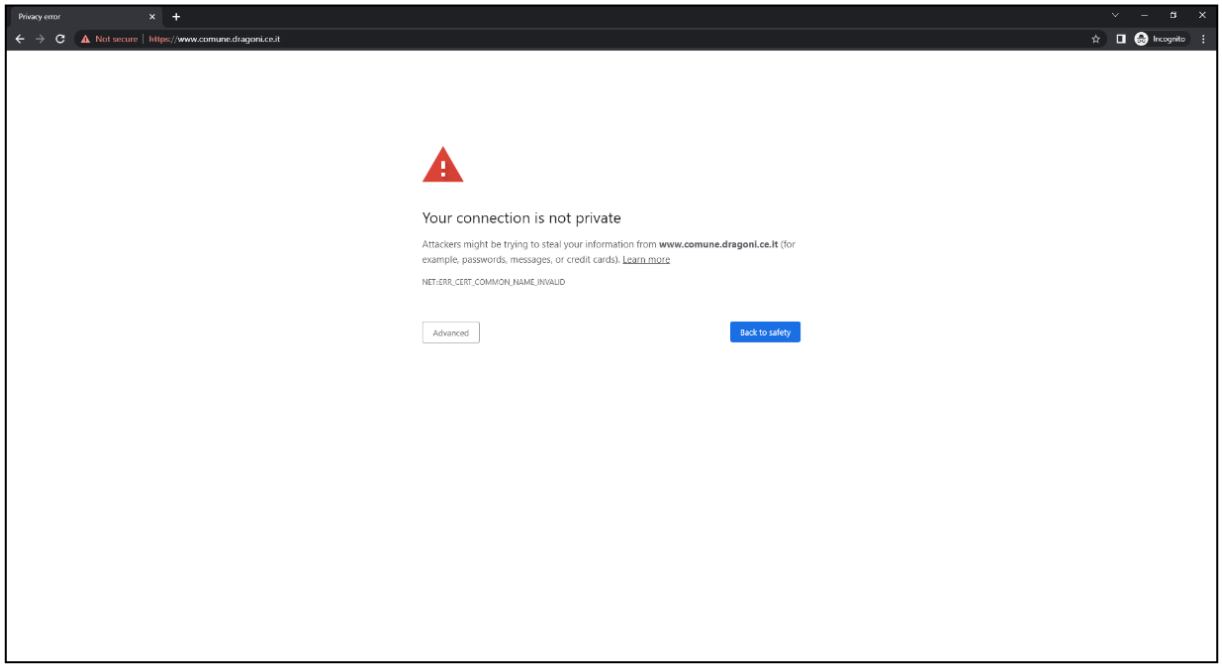

Figura. 9 *- Schermata di notifica del browser, dovuta ad un problema legato al certificato*

5.4. Esposizione di altre tipologie di informazioni

Approfondendo ulteriormente altri aspetti delle configurazioni dei siti web analizzati, i risultati mostrano che 3.183 comuni (circa il 45%) rivelano sia il nome che la versione del Web server che stanno utilizzando, come illustrato nella Figura 10. In certi casi, viene resa nota anche la versione dei linguaggi di programmazione installati sul web server, come ad es. PHP (729 comuni, rappresentanti oltre il 10%) o Python (57 comuni, circa l'1%), oppure di librerie come ad es. OPENSSL (816 comuni, superando l'11%).

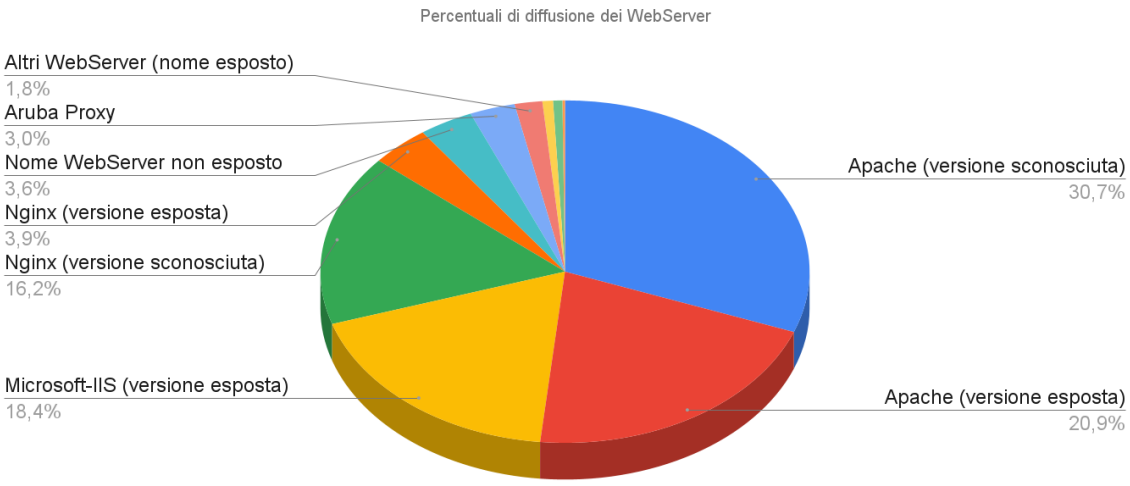

Figura 10 *- Percentuali di diffusione dei Web Server*

Questa esposizione di informazioni costituisce un ulteriore rischio per la sicurezza, poiché potrebbe fornire ad un attaccante dettagli sufficienti per avviare un attacco contro il sito web sfruttando vulnerabilità conosciute in particolari versioni di server web, linguaggi o librerie.

5.5. Classifica aggregata su base nazionale e macro-regionale.

Andando ad analizzare i punteggi dei comuni, i dati sono stati aggregati utilizzando sia criteri geografici che demografici per stabilire una valutazione completa a vari livelli di granularità. Il punteggio medio nazionale si attesta a 34,23 punti, con una deviazione standard nazionale di 17,54.

La Figura 11 mostra i punteggi aggregati a livello macro-regionale: le due macro-regioni settentrionali hanno ottenuto punteggi medi significativamente più alti rispetto al resto dell'Italia, mentre le macro-regioni Centro e Isole hanno registrato punteggi largamente simili tra loro.

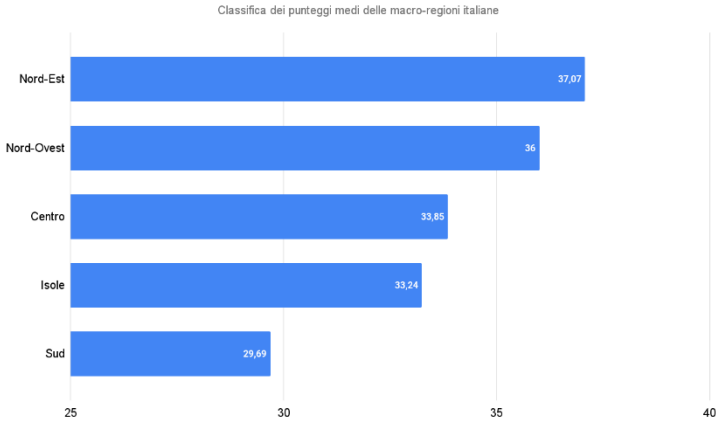

Figura 11 *- Classifica dei punteggi medi delle macro-regioni italiane*

5.6. Classifica aggregata su base regionale

Passando ad una grana più fine di analisi e considerando i punteggi delle singole regioni (come mostrato nella Figura 12), i risultati rivelano che i punteggi regionali non sempre sono allineati a quelli derivati dall'analisi condotta a livello macro-regionale. Infatti, regioni come la Liguria (ubicata nella macro-regione Nord-Ovest) e il Friuli-Venezia Giulia (situate nella macro-regione Nord-Est) si trovano verso la parte inferiore della classifica, occupando rispettivamente la 16ª e la 18ª posizione. D'altra parte, la Puglia, situata nella macro-regione Sud, si posiziona al 7º posto.

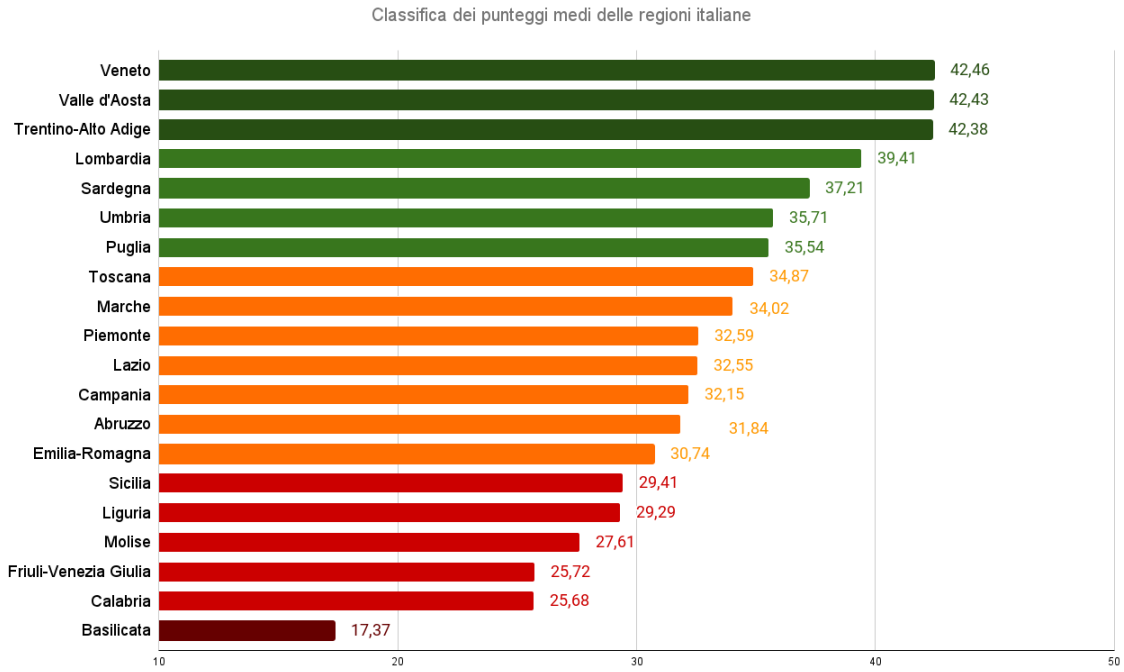

Figura 12 *- Classifica dei punteggi medi delle regioni italiane*

5.7.

5.8. Classifica aggregata su base provinciale.

Procedendo all'ultimo livello di dettaglio e considerando i punteggi delle province (come illustrato nella Figura 13), osserviamo che le province con i punteggi più alti sono state Macerata (49,27 punti), Treviso (47,98 punti) e Venezia (46,25 punti), rispettivamente. Al contrario, Potenza (16,3 punti), Prato (11,43 punti) e Ravenna (7,78 punti) si trovano in fondo alla classifica.

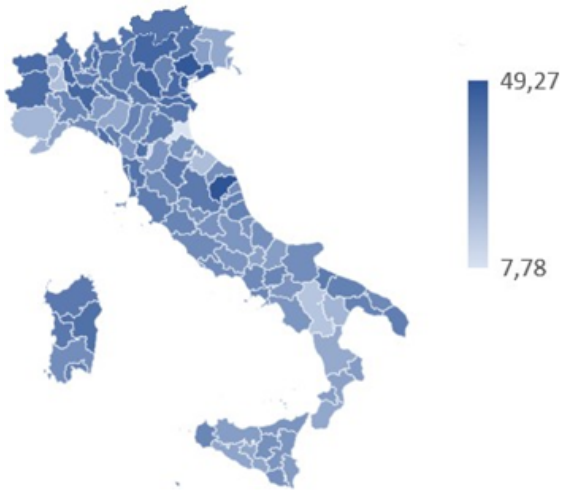

Figura 13 *- Heat map dei punteggi medi province italiane.*

5.9. Classifica aggregata delle città metropolitane e dei capoluoghi regionali.

Concentrandoci infine sui capoluoghi delle 20 regioni italiane, il punteggio medio ammonta a 36,25 punti, con una deviazione standard di 14,41.

All'interno di questo gruppo:

- Solo il comune di Potenza non supporta il protocollo HTTPS.
- Solo 15 comuni implementano la redirezione da HTTP a HTTPS.
- Nessun comune presenta discrepanze del nome del certificato o certificati scaduti.
- 3 comuni supportano ancora protocolli obsoleti e sono di conseguenza vulnerabili all'attacco POODLE.

Passando all'analisi dei capoluoghi delle 15 città metropolitane, il punteggio medio è di 35 punti, con una deviazione standard di 15,57. All'interno di questo sottoinsieme:

- Solo il comune di Reggio Calabria non fornisce supporto al protocollo HTTPS.
- Solo 10 comuni utilizzano la redirezione da HTTP a HTTPS.
- Nessun comune presenta discrepanze del nome del certificato o certificati scaduti.
- 2 comuni mantengono il supporto per protocolli obsoleti e sono quindi suscettibili alla vulnerabilità POODLE.

In entrambi i gruppi sopra menzionati (capoluoghi di regione e capoluoghi delle città metropolitane), il punteggio medio supera la media nazionale, mentre la deviazione standard è minore rispetto al valore nazionale.

5.10. Classifica aggregata su base demografica.

I punteggi dei singoli comuni sono stati ulteriormente categorizzati in base a criteri demografici, seguendo le categorie demografiche delineate dalle leggi italiane precedentemente citate. La distribuzione dei valori medi è illustrata nella Figura 14.

È importante notare una tendenza generale che evidenzia come i comuni con popolazioni più grandi tendono a ottenere punteggi più alti. Tuttavia, vi è un'eccezione significativa nel caso dei comuni che rientrano nella IX° categoria (cioè, da 60.000 a 99.999 residenti), dove si osserva un significativo declino nel punteggio medio. Inoltre, è evidente anche un lieve declino nel caso della XI° categoria (cioè, da 250.000 a 499.999 residenti).

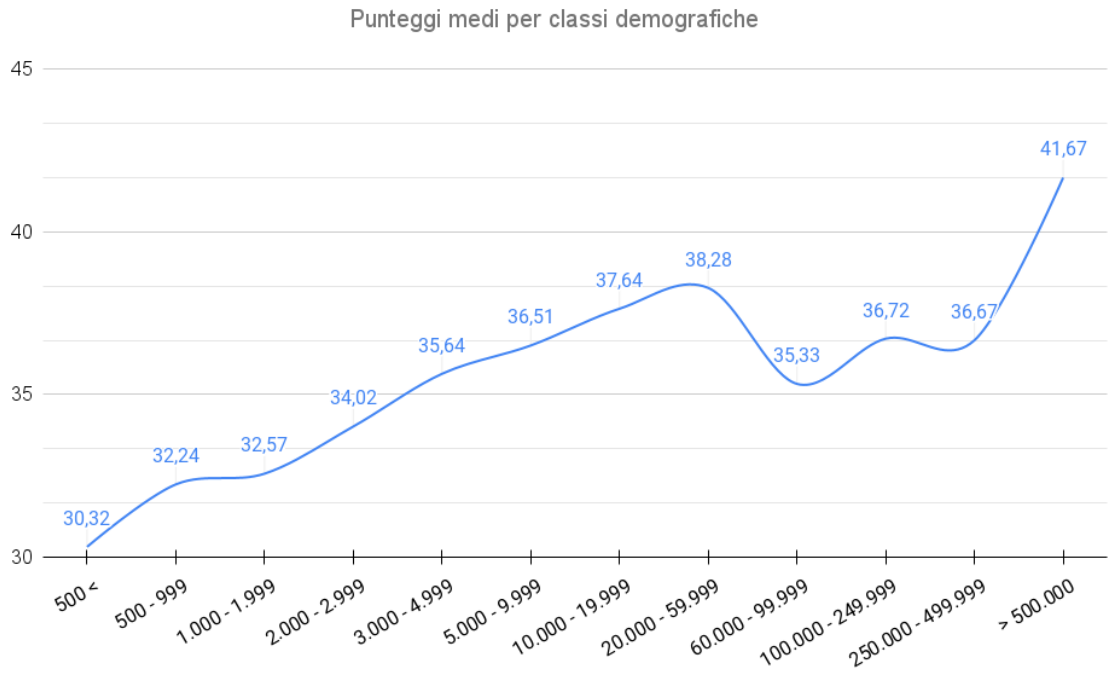

Figura 14 *- Punteggi medi per classi demografiche*

Questo declino può essere attribuito in parte a una minore percentuale di implementazione di HTTPS tra i comuni nella IX° categoria (cioè, da 60.000 a 99.999 residenti), come illustrato nella Figura 15.

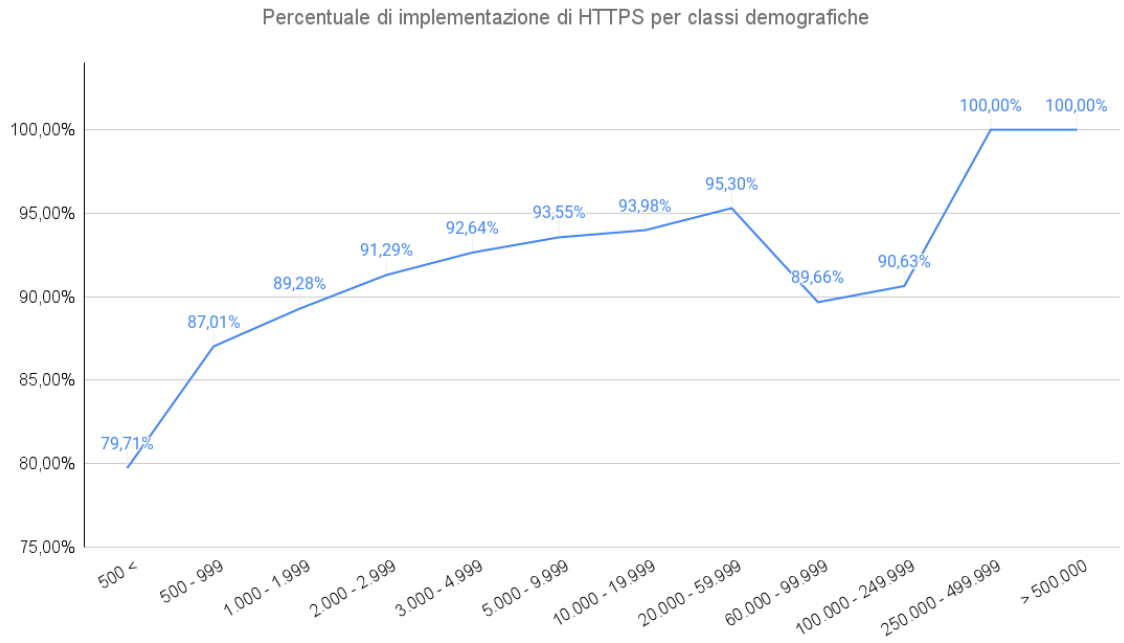

Figura 15 - *Percentuale di implementazione di HTTPS per classi demografiche*

5.11. Ulteriori statistiche

Dato che non vi sono siti web che aderiscono alle configurazioni 'Modern' e 'Intermediate', il punteggio più alto è stato ottenuto collettivamente da 2.652 comuni (circa il 37%). Essi hanno ottenuto 50 punti, risultato della configurazione 'Old' unita alla presenza della redirezione da HTTP a HTTPS, e senza alcun malus. D'altro canto, il punteggio più basso è stato ottenuto da un piccolo comune ligure, totalizzando -60 punti.

Questo punteggio deriva dalla presenza di diversi malus, tra cui:

- Assenza di redirezione da HTTP a HTTPS
- Discrepanza nel nome del certificato
- Utilizzo di un certificato scaduto
- Supporto a 2 protocolli obsoleti
- Supporto a 2 protocolli deprecati
- Vulnerabile a 5 vulnerabilità note

Il numero di comuni con un punteggio inferiore a 0 è stato di 154, ovvero circa il 2%.

6. Conclusioni e future evoluzioni

6.1. Conclusioni

Il protocollo HTTPS è ampiamente utilizzato garantire comunicazioni digitali sicure: tale protocollo offre infatti autenticazione reciproca fra le parti e stabilisce un canale sicuro per fornire comunicazioni crittografate end-to-end su Internet, garantendo riservatezza e integrità dei dati scambiati tra gli utenti finali e i siti web. Nonostante il suo diffuso utilizzo su milioni di siti web, molti di essi non adottano ancora comunicazioni sicure o utilizzano implementazioni errate, non sfruttando completamente o minimizzando i benefici offerti da tale protocollo. In particolare, l'uso di implementazioni errate può fornire agli amministratori del sito web un falso senso di sicurezza, che può portare a sottovalutare i rischi presenti nei loro siti/web server.

Questo studio offre un'analisi approfondita dell'implementazione di HTTPS su circa 8000 siti web di comuni italiani. Lo studio non solo mette in luce lo stato attuale della sicurezza dei siti web correlata al protocollo HTTPS, ma introduce anche elementi innovativi attraverso l'utilizzo dello strumento 'MunicipalityEvaluator', uno strumento specializzato progettato dall'autore per l'esame di questi siti web.

I risultati dello studio indicano che vi è ampio spazio di miglioramento nella qualità e correttezza delle implementazioni HTTPS, al fine di garantire che tutti i siti web dei comuni italiani offrano le misure di sicurezza necessarie affinché i cittadini possano interagire con essi.

Infatti, mentre l'alto tasso di adozione del protocollo HTTPS (intorno al 90%) è un elemento positivo, diversi problemi rilevati ne diminuiscono l'impatto sulla sicurezza dei siti web: questi problemi includono il supporto per protocolli crittografici obsoleti o deprecati, una limitata presenza di redirezioni da HTTP a HTTPS e una notevole presenza di discrepanze nel nome dei certificati utilizzati

Sebbene la percentuale di problemi associati a certificati scaduti e vulnerabilità note sia relativamente minore, tali problemi richiedono immediata attenzione a causa delle loro potenziali conseguenze. Inoltre, la divulgazione di informazioni riguardanti il tipo e la versione del server web utilizzato solleva molta preoccupazione, poiché gli attaccanti potrebbero sfruttare le vulnerabilità note per lanciare attacchi su larga scala.

Lo studio rivela anche che il Sud Italia è in ritardo rispetto al Nord Italia in termini di qualità delle implementazioni HTTPS, e i comuni più piccoli tendono ad avere implementazioni di HTTPS più scadenti.

6.2. Future evoluzioni del progetto

Il progetto Municipality2HTTPS si è principalmente concentrato sull'analisi delle implementazioni del protocollo HTTPS. Tuttavia, nello svolgimento della nostra ricerca, abbiamo rilevato che vi sono ulteriori aspetti che potenzialmente possono compromettere la sicurezza dei siti web, come ad es. l'esposizione di informazioni sensibili riguardanti il web server o delle librerie in uso. Per ampliare il campo di applicazione del progetto, è possibile quindi valutare di estendere la metrica di valutazione per includere punti bonus/malus per tali informazioni.

Un'altra possibile estensione potrebbe coinvolgere l'analisi delle piattaforme tecnologiche impiegate nello sviluppo dei siti web per identificare potenziali vulnerabilità.

Inoltre, si potrebbero esplorare aspetti oltre la sicurezza, come l'accessibilità web, integrando un validatore di accessibilità (ad esempio, MAUVE [30]) nelle metriche di valutazione.

7. Bibliografia

[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] Schiavone, A. G., "Municipality2HTTPS: A study on HTTPS protocol's usage in Italian municipalities' websites." Computers & Security 137 (2024): 103592.

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

[10] "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

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

[12] 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.

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

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

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

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

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

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

[19] 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.

[20] 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).

[21] 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.

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

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

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

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

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

[27] 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.

[28] 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.

[29] 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 28 (pp. 339-348). Springer International Publishing.

[30] 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.