

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

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

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" 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

$$\text{punteggio}(I) = 90 + 10 = 100$$

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

$$\text{punteggio}(\text{Morlupo}) = 40 + 10 - 10 - 5 * 2 = 30$$

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.

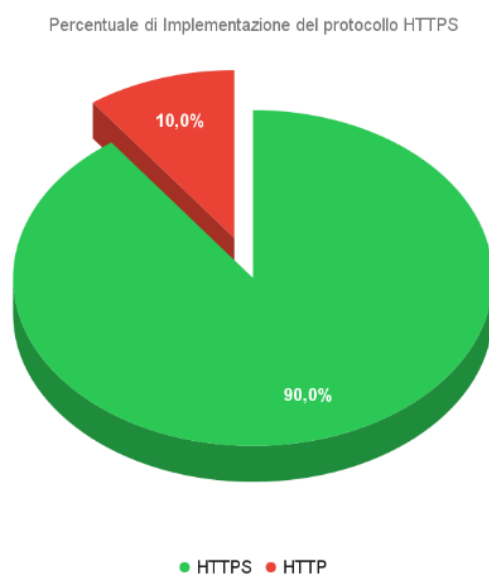


Figura 2 - Percentuale di Implementazione del protocollo HTTPS

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.

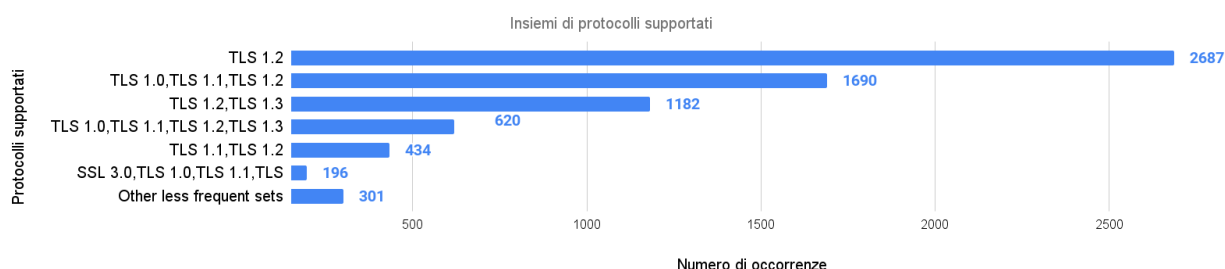


Figura 3 - Insiemi di protocolli supportati

Un'analisi sull'implementazione del protocollo HTTPS nei siti web dei Comuni Italiani.
Examining the adoption of HTTPS Protocol in websites of Italian Municipalities
A.G. Schiavone

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

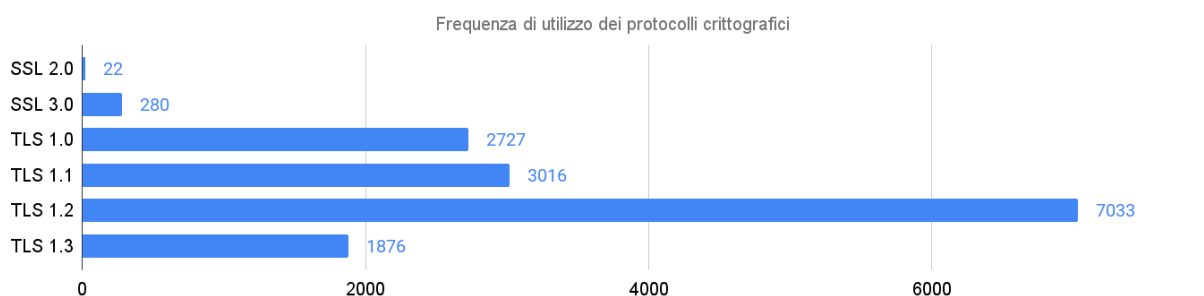


Figura 4 - Frequenza di utilizzo dei protocolli crittografici

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.

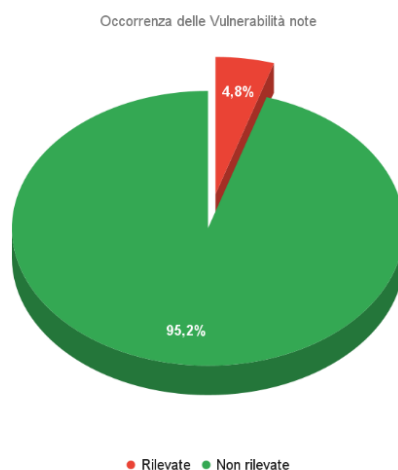


Figura 5 - Occorrenza delle Vulnerabilità note

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%).

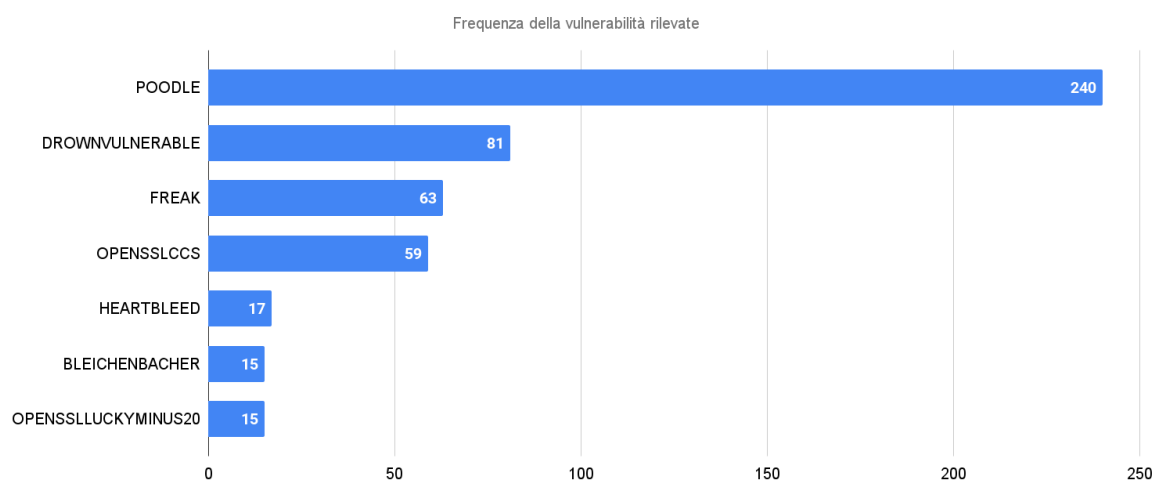


Figura 6 - Frequenza della vulnerabilità rilevate

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.

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

Examining the adoption of HTTPS Protocol in websites of Italian Municipalities

A.G. Schiavone

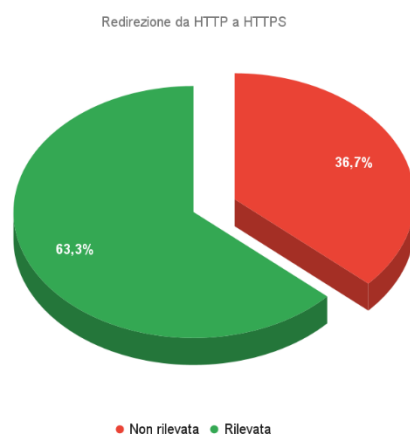


Figura 7 - Redirezione da HTTP a HTTPS

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.

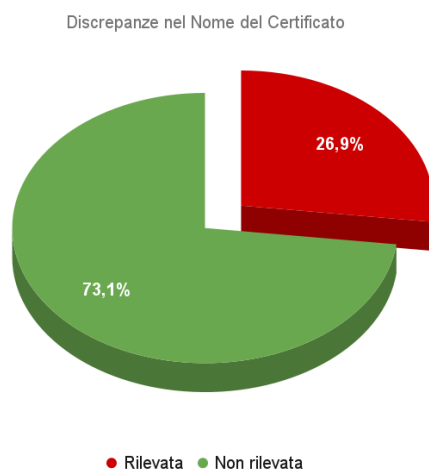


Figura 8 - Rilevamento di discrepanze del nome nel certificato

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%).

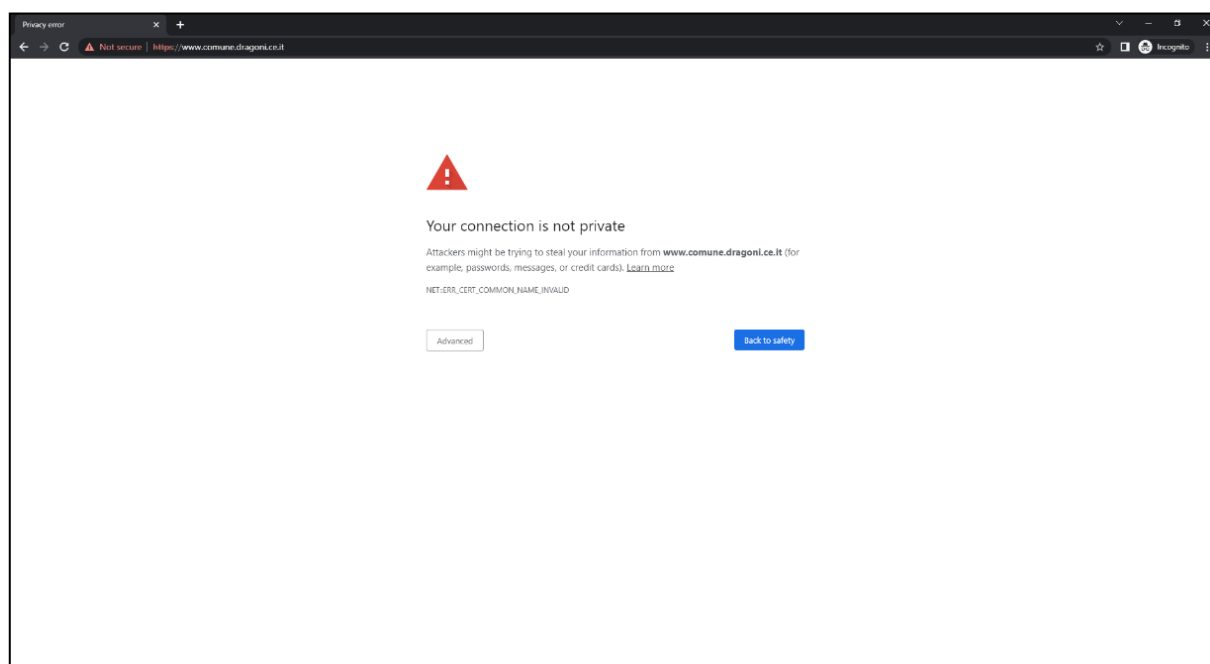


Figura. 9 - Schermata di notifica del browser, dovuta ad un problema legato al certificato

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. OPENSLL (816 comuni, superando l'11%).

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

Examining the adoption of HTTPS Protocol in websites of Italian Municipalities

A.G. Schiavone

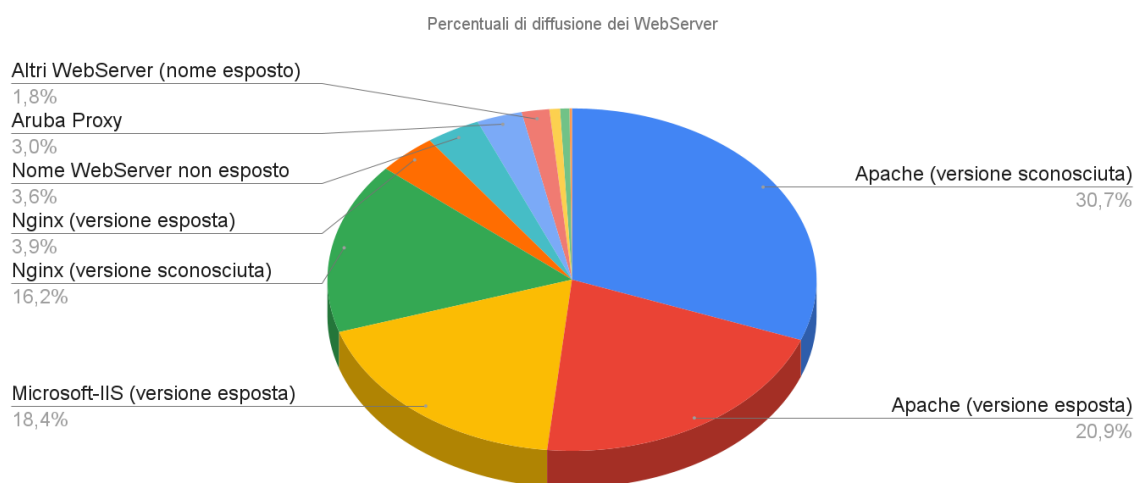


Figura 10 - Percentuali di diffusione dei Web Server

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.

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

Examining the adoption of HTTPS Protocol in websites of Italian Municipalities

A.G. Schiavone

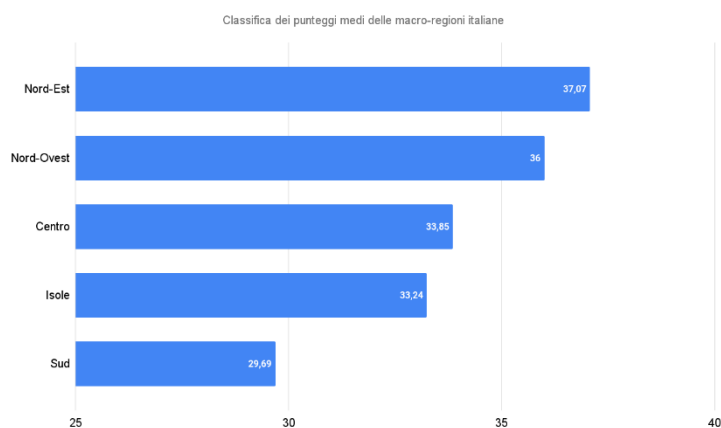


Figura 11 - Classifica dei punteggi medi delle macro-regioni italiane

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 16^a e la 18^a posizione. D'altra parte, la Puglia, situata nella macro-regione Sud, si posiziona al 7^o posto.

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

Examining the adoption of HTTPS Protocol in websites of Italian Municipalities

A.G. Schiavone

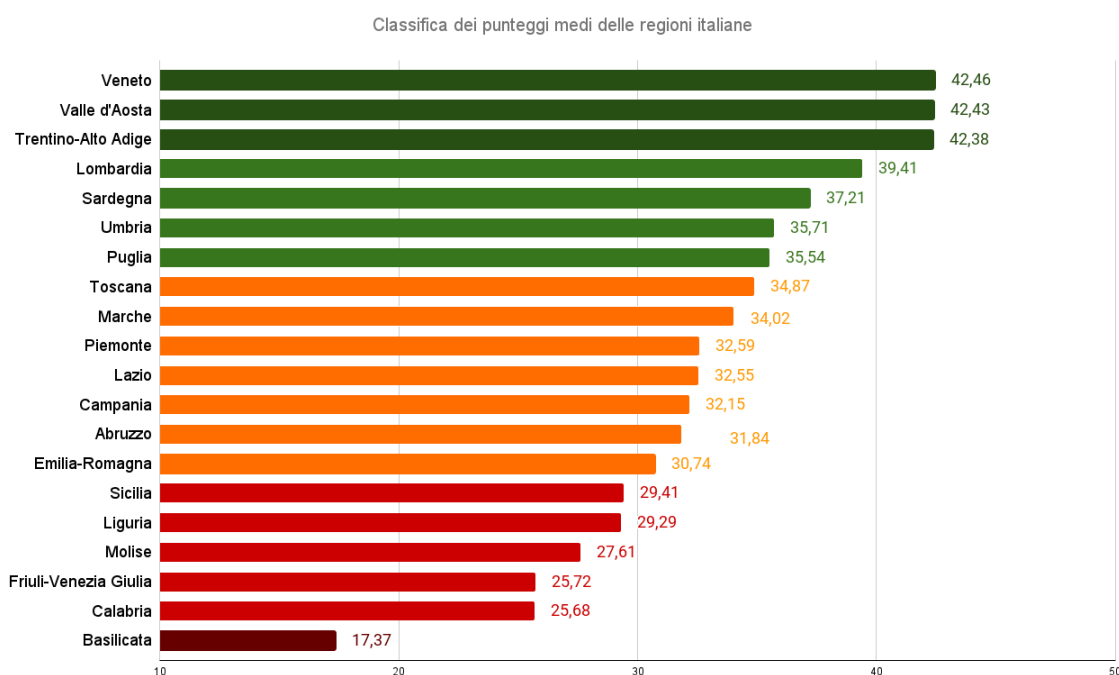


Figura 12 - Classifica dei punteggi medi delle regioni italiane

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.

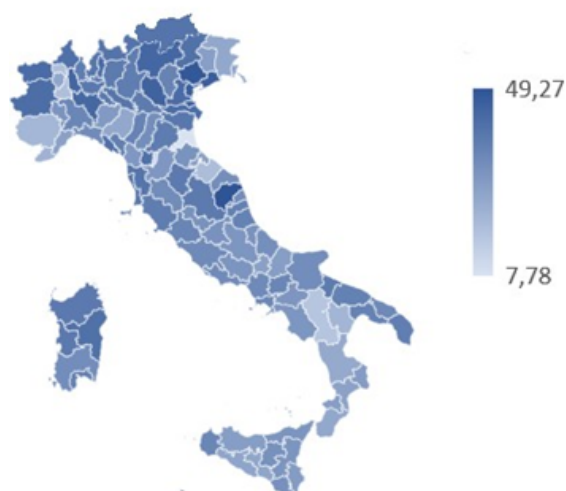


Figura 13 - Heat map dei punteggi medi province italiane.

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 redirectione 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 redirectione 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).

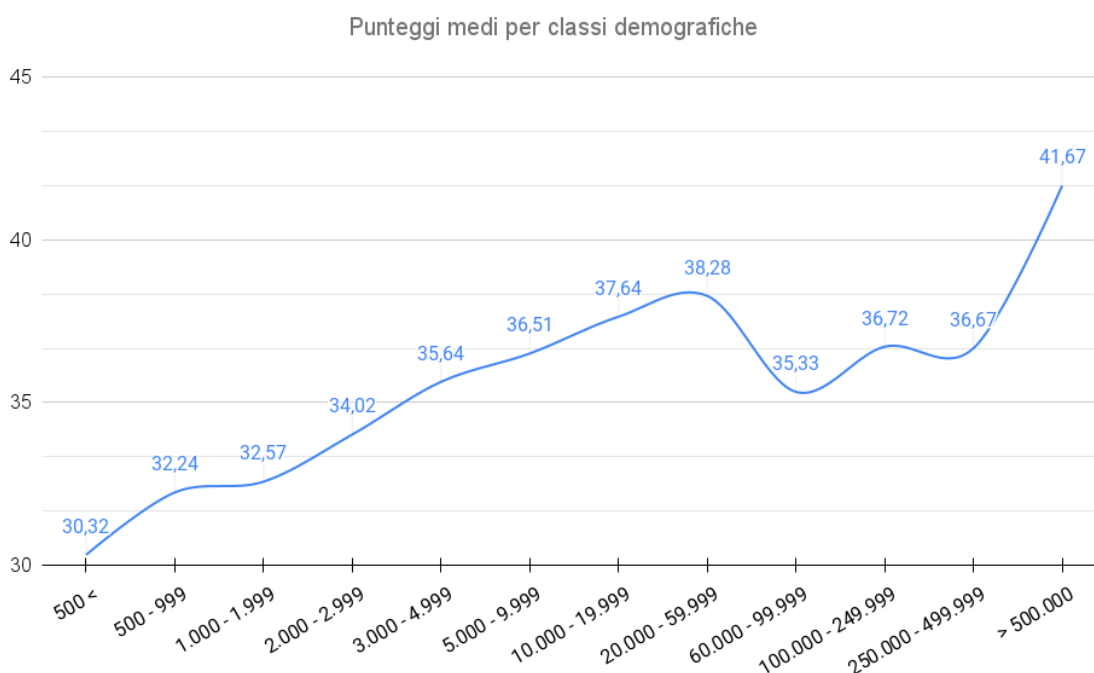


Figura 14 - Punteggi medi per classi demografiche

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.

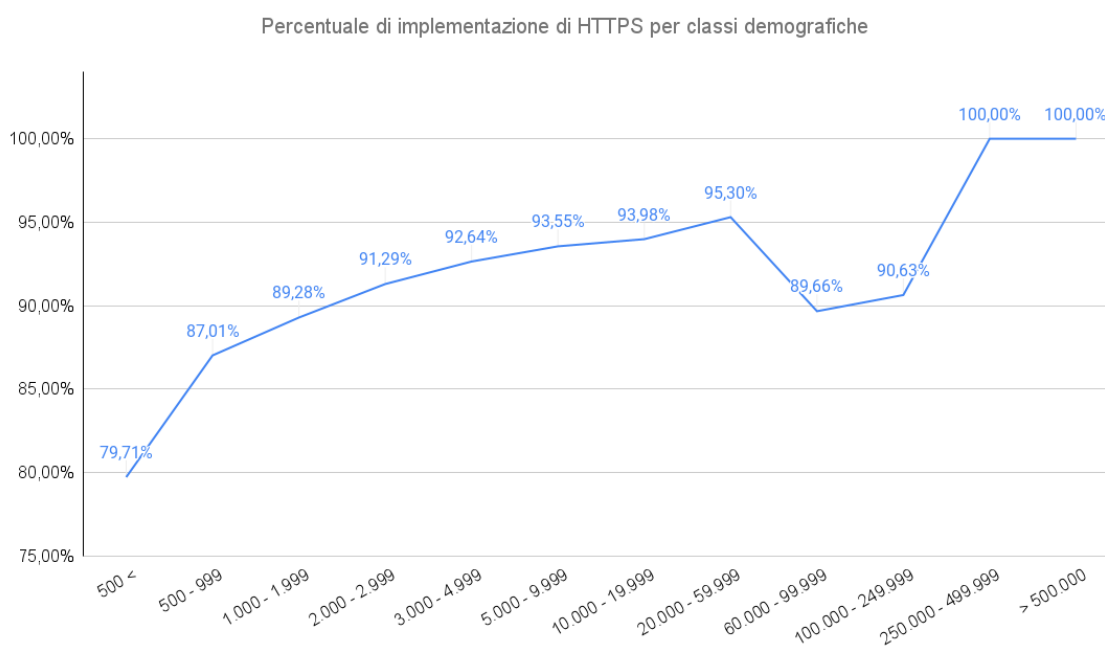


Figura 15 - Percentuale di implementazione di HTTPS per classi demografiche

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 redirectione 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 redirectione 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 \oplus 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.