AGID Agenzia per l'Italia Digitale

CERT-AGID

Guida alla lettura dell'esito delle verifiche HTTPS e CMS automatizzate dal CERT-AgID

Premesse di contesto generale sulle tematiche

Cos'è HTTPS?

HTTPS è un protocollo per la trasmissione **sicura** di informazioni con da/verso i siti web .

Perché i portali della mia amministrazione hanno bisogno di HTTPS?

La tecnologia alla base del protocollo HTTPS è nata per dare due **forti garanzie** ai suoi utilizzatori:

1. Garantire la **confidenzialità** ed **integrità** dei dati scambiati tra i portali ed i loro utenti. Nessun attore terzo, neanche chi gestisce le infrastrutture fisiche di rete, può **leggere** o **modificare**, durante il transito, i dati scambiati.
2. Garantire agli utenti di poter **autenticare**[1] il portale visitato. Nessun attore terzo può **ingannare l'utente** dichiarando, falsamente, di essere il portale.

Le informazioni contenute nel portale di un'amministrazione rappresentano dati istituzionali ed è quindi importante che si mantengano **non modificati e non falsificati,** per cui è importante adottare HTTPS per garantire agli utenti che il materiale prelevato o letto da un portale **sia sempre autentico**.
Qualora invece si trattassero dati personali o password, l'utilizzo di HTTPS diviene fondamentale per garantire la **riservatezza in transito di questi dati sensibili**.

1 Si può anche leggere *identificare*. Tuttavia è doveroso notare che, nella sua versione più diffusa, l'autenticazione HTTPS garantisce solo che l'utente stia effettivamente visitando il sito digitato ma non dà garanzie su chi sia l'entità e l'intento dietro tale sito. Cioè, HTTPS garantisce che richiedendo l'indirizzo https://www.bancaministeroitalia.it si comunicherà proprio con il sistema che ha quel nome a DNS ma non si può essere certi di chi sia questa persona/amministrazione/società proprietaria del nome o se abbia effettivamente a che fare con Banca Ministero d'Italia (nome di fantasia).

Chi deve attivare HTTPS?

L'abilitazione del protocollo HTTPS è normalmente a carico dell'**amministratore dei server del sito web.**

In alternativa, altre figure professionali similari possono adempiere all'opera.

Nel caso la gestione del sito sia stata delegata a fornitori esterni, l'attivazione di HTTPS spetta a questi.

Quanto è difficile e quanto tempo ci vuole?

L'attivazione di HTTPS è una procedura **semplice e ben documentata**.
La conoscenza base del meccanismo di funzionamento di HTTPS risulterà utile al tecnico incaricato. E' comunque bene sapere che la comunità online ha speso considerevoli sforzi per la promozione del protocollo HTTPS, inclusa la **redazione di guide** che ne facilitano l'attivazione anche ai meno esperti**.**

Come requisito di base, la prima attivazione di HTTPS necessita di una **richiesta ad un'autorità certificatrice (CA - Certification Authority)** del certificato legato al sito da proteggere. L'autorità risponde solitamente **entro poco tempo con l'emissione dello specifico certificato**.
Una volta in possesso di un certificato valido, le modifiche alla propria configurazione HTTPS possono essere espletate nel **giro di pochi minuti**.

Quanto costa?

Il costo finale del certificato varia in base alla tipologia di certificato richiesto. Le differenze risiedono nei diversi livelli di controllo che vengono effettuati per verificare l'identità dei richiedenti.
Esistono comunque diversi servizi online che possono emettere certificati validi **gratuitamente**. Questi servizi si limitano a verificare il solo il reale possesso dell'indirizzo internet[2] del portale da proteggere.

Spetta all'Amministrazione quindi decidere quanto forte debba essere la garanzia di autenticità data ai propri utenti.

2 Viene controllato il reale possesso del nome a dominio DNS in questione.

Ci sono controindicazioni?

No. Alcuni browser per la navigazione web **obsoleti** possono avere problemi con le versioni più recenti di HTTPS ma si tratta di un problema che risiede sul lato del **visitatore**.

Utilizziamo già il protocollo HTTPS, perché non basta?

Il protocollo HTTPS deve essere configurato **correttamente** per garantire che tutte le funzionalità siano sempre adeguate agli **standard correnti**. E' quindi necessario tenere costantemente aggiornata la propria configurazione HTTPS ed assicurarsi che sia sempre corretta ed aggiornata.

Che cos'è un CMS?

Un CMS, acronimo di Content Management System, è un software spesso utilizzato per la **creazione e gestione di portali web**.

Perché è importante?

Si tratta proprio dello strato di software che viene utilizzato dai visitatori del portale e, per la sua natura, spesso esaminato dai malintenzionati alla ricerca di eventuali **falle di sicurezza** in esso presenti.
Tenere **aggiornato** il proprio CMS riduce quindi considerevolmente il rischio di subire violazioni informatiche e loro conseguenze.

Perché è importante l'aggiornamento continuo?

I CMS sono software complessi e, in alcuni casi, con una lunga storia di sviluppo alle spalle che, a volte, risale a prima che la comunità web ponesse seriamente l'accento sulle problematiche legate alla sicurezza informatica.
Non aver considerato da subito questi aspetti rende più probabile la presenza di falle di sicurezza.

Quando una falla di sicurezza viene scoperta, gli sviluppatori lavorano per eliminarla e, una volta eliminata, rilasciano solitamente una nuova versione dello stesso CMS.
E' opportuno quindi che le Amministrazioni mantengano **costantemente aggiornati** i propri CMS, al fine di eliminare le falle di sicurezza che di volta in volta vengono corrette.
I CMS non aggiornati sono proprio uno dei principali veicoli di infezioni e compromissioni sul web.

Chi deve eseguire l'aggiornamento?

Anche in questo caso, l'onere spetta a chi **gestisce il portale**, tipicamente è l'**amministratore di sistema** ma, come per il protocollo HTTPS, altre figure professionali similari possono adempiere all'opera.

Molti CMS possono essere configurati anche per l'**aggiornamento automatico**, semplificando e automatizzando il processo stesso di aggiornamento.

Quanto costa fare l'aggiornamento?

Dipende ovviamente dalla diversa tipologia di CMS.

Per quel che riguarda i CMS a maggior diffusione, gli aggiornamenti vengono rilasciati gratuitamente. Diversamente, il supporto è in genere previsto nei contratti di manutenzione del software del CMS acquisito.
Se una Amministrazione gestisce internamente il proprio portale, la pianificazione degli aggiornamenti deve essere fatta secondo i propri processi e budget.
In caso di fornitori esterni sarà il contratto stipulato con questi ad indicare i costi e la frequenza degli aggiornamenti. Per questo, al fine di garantire la sicurezza dei propri portali, è buona prassi prevedere opportuni contratti di manutenzione.

Dettagli tecnici e legenda dei test effettuati

A cosa serve questo documento?

Questo documento spiega come interpretare l'esito dei risultati delle verifiche HTTPS e CMS, effettuate automaticamente dagli strumenti predisposti dal CERT-AGID, a seguito di una richiesta effettuata dalla vostra Amministrazione.

Il documento PDF allegato a questa comunicazione contiene i suddetti esiti, riportando inoltre l'ora, la data di esecuzione del test ed il nome del sito verificato.

Questo documento **non è una guida alla configurazione del protocollo HTTPS o del proprio CMS:** per quello si consiglia di fare riferimento alla documentazione appropriata reperibile anche online.

Precisiamo fin da subito che gli esiti mostrati nel documento PDF sono stati ottenuti attraverso **strumenti automatici** e quindi, per quanto ci si impegni a renderli i più corretti possibile, questi **non vi possono esimere dalla una verifica puntuale**.

Pertanto, è bene considerare il documento degli esiti come un buon consiglio ricevuto. **La responsabilità finale della verifica** della configurazione HTTPS e dello stato di aggiornamento del CMS **è sempre un onere proprio di ogni Amministrazione**.

Come è stato verificato l'HTTPS del mio portale e come interpreto i risultati?

La verifica di una configurazione HTTPS è più complessa della semplice constatazione della presenza di un server in grado di comunicare su canali SSL o TLS.

L'approccio adottato dal CERT-AGID è stato quello di rilevare le possibili configurazioni ormai deprecate, anche qualora non esista la possibilità che queste siano utilizzate da un browser (es: SSL 2.0).

L'idea è di avere una configurazione HTTPS intrinsecamente sicura, indipendentemente dalle politiche di sicurezza in uso dai potenziali browser dei visitatori.

Sempre per amor di completezza, la verifica HTTPS è stata effettuata su tutti i server elencati nei record DNS *A* e *AAAA* associati al dominio del portale testato.
Pertanto è possibile che più di un server web sia stato testato; in questo modo una configurazione errata su un server secondario o "dimenticato nel DNS" viene comunque rilevata.
Inoltre, qualora il portale testato si limiti a fare un redirect HTTP[3] verso un altro sito, anche quest'ultimo sarà fatto rientrare nel perimetro di test poiché, per gli utenti finali, la sicurezza del portale dipende anche dalla sicurezza di questo.

Esempio

Viene richiesta la verifica del sito https://www.amministrazione.it, il quale possiede un server con IP 1.2.3.4 e effettua un redirect su portale.amministrazione.it che, a sua volta, possiede due server con IP (1.2.3.5 e .1.2.3.6).

Si avranno quindi tre risultati individuati dalle seguenti triple:

1. Dominio = www.amministrazione.it, Host = www.amministrazione.it, IP = 1.2.3.4
2. Dominio = www.amministrazione.it, Host = portale.amministrazione.it, IP = 1.2.3.5
3. Dominio = www.amministrazione.it, Host = portale.amministrazione.it, IP = 1.2.3.6

Nella nomenclatura usata nel documento degli esiti, la parola *dominio* fa riferimento al nome host del sito di cui è stata richiesta la verifica.

Ogni server è testato verificando la **presenza o l'assenza di un insieme di funzionalità SSL o TLS** (ad esempio: la presenza di compressione).

A tal fine, è necessario ricordare alcuni fattori che possono **confondere l'esito** dei test:

- SSL e TLS **non hanno un meccanismo di enumerazione delle proprie funzionalità**. E' quindi necessario effettuare **diversi handshake** SSL/TLS per verificarne tutte le funzionalità. Alcuni sistemi di sicurezza di rete potrebbero bloccare **solo alcuni** di questi tentativi di enumerazione, alterando l'esito finale dei test effettuati.
- I protocolli SSL e TLS non hanno una firma che permetta di identificarli con certezza, per cui potrebbero verificarsi dei falsi positivi durante l'identificazione delle versioni SSL e TLS supportate.

3 I redirect sono un elemento del protocollo HTTP e per tanto sono sempre detti "redirect HTTP" al di là dell'utilizzo di HTTPS o meno.

- Alcuni firewall considerano le connessioni fatte dallo strumento di test come tentativi di attacco e **bloccano permanentemente o parzialmente** i tentativi di enumerazione. In questo caso i test non possono essere effettuati liberamente e i risultati presentati saranno falsati.
- Molti server non sono completamente conformi alle specifiche SSL/TLS.

In questi casi, l'esito dei test **perde di significatività**, riportando anche risultati **contraddittori**.

Non è possibile compensare gli effetti dei fattori elencati sopra poiché effetti identici sono causati da fattori diversi (perdendo quindi la possibilità di distinguerli).

Le funzionalità testate da questo strumento sono elencate qui sotto (con gli stessi nomi con i quali sono identificati nel documento degli esiti):

Nome funzionalità	Descrizione
SSL/TLS	Indica se il server ha accettato un handshake SSL/TLS durante almeno un test. Nei casi ambigui (non tutti i test accettano handshake SSL/TLS), questo campo tende ad attribuire la presenza di SSL/TLS. Se non è possibile determinare le versioni di SSL/TLS supportate, questo campo contiene un valore probabilmente falsato.
SSL 2.0	Indica se il server supporta SSL 2.0. SSL 2.0 è vulnerabile e non deve essere usato.
SSL 3.0	Indica se il server supporta SSL 3.0. SSL 3.0 è vulnerabile e non deve essere usato.
TLS 1.0	Indica se il server supporta TLS 1.0. TLS 1.0 è stato deprecato e non dovrebbe essere usato.
TLS 1.1	Indica se il server supporta TLS 1.1. TLS 1.1 è stato deprecato e non dovrebbe essere usato.
TLS 1.2	Indica se il server supporta TLS 1.2. TLS 1.2 è la versione maggiormente supportata dai browser ed era, fino a poco tempo fa, la versione di riferimento del TLS. Sebbene sia stata superata dal TLS 1.3, si consiglia di mantenere ancora attiva anche questa versione, per motivi di compatibilità con sistemi legacy.

TLS 1.3	Indica se il server supporta TLS 1.3. TLS 1.3 è la versione ultima di TLS ma non è ancora completamente supportata. TLS 1.3 è sicuro *by design* e dovrebbe essere adottato quanto prima. Se si imposta l'utilizzo esclusivo di TLS1.3 non vi è al momento modo di usare una configurazione non sicura.
Certificato	Indica se il certificato presentato dal server è valido o, in caso contrario, per quale motivo esso non lo sia. Un certificato valido è essenziale per garantire la confidenzialità ed l'integrità del canale di comunicazione HTTPS.
Aut. nulla	Indica se il server supporta il metodo di autenticazione nullo, ovvero nessuna autenticazione dei parametri crittografici. Questa funzionalità compromette il canale di comunicazione HTTPS e dovrebbe essere disabilitata.
Cifr. nullo	Indica se il server supporta il metodo di cifratura nullo, ovvero nessuna cifratura. Questa funzionalità compromette il canale di comunicazione HTTPS e dovrebbe essere disabilitata.
Cifr. deboli	Indica se il server supporta cifrari obsoleti o con lunghezza delle chiavi ritenuta non più sufficiente. I seguenti cifrari sono considerati deboli: *LOW:RC2:RC4:DES:MD4:MD5:EXP:EXP1024:SEED:IDEA* La stringa è in formato **OpenSSL**, alla cui documentazione si rimanda per maggiori dettagli.

Cifr. CBC	Indica se il server supporta cifrari in modalità CBC. Questi sono potenzialmente soggetti ad attacchi noti. La presenza dei seguenti cifrari è verificata in questo test: *DES-CBC3-MD5:DES-CBC3-SHA:DES-CBC-MD5:DES-CBC-SHA:DH-DSS-DES-CBC3-SHA:DH-DSS-DES-CBC-SHA:DH-RSA-DES-CBC3-SHA:DH-RSA-DES-CBC-SHA:ECDH-ECDSA-DES-CBC3-SHA:ECDHE-ECDSA-DES-CBC3-SHA:ECDHE-RSA-DES-CBC3-SHA:ECDH-RSA-DES-CBC3-SHA:EDH-DSS-DES-CBC3-SHA:EDH-DSS-DES-CBC-SHA:EDH-RSA-DES-CBC3-SHA:EDH-RSA-DES-CBC-SHA:EXP-RC2-CBC-MD5:IDEA-CBC-MD5:IDEA-CBC-SHA:PSK-3DES-EDE-CBC-SHA:PSK-AES128-CBC-SHA:PSK-AES256-CBC-SHA:RC2-CBC-MD5:SRP-3DES-EDE-CBC-SHA:SRP-AES-128-CBC-SHA:SRP-AES-256-CBC-SHA:SRP-DSS-3DES-EDE-CBC-SHA:SRP-DSS-AES-128-CBC-SHA:SRP-DSS-AES-256-CBC-SHA:SRP-RSA-3DES-EDE-CBC-SHA:SRP-RSA-AES-128-CBC-SHA:SRP-RSA-AES-256-CBC-SHA*
Compressione	Verifica se il server comprime i dati prima di cifrarli. La compressione compromette la sicurezza del canale di comunicazione HTTPS e non dovrebbe essere usata.
HTTPS	Verifica se la porta 443 è effettivamente usata per servire richieste HTTP. Non influisce sull'esito del test.

HTTP → HTTPS	Verifica se il server effettua un redirect HTTP dalla porta 80 (HTTP) alla porta 443 (HTTPS). Il sito dovrebbe forzare l'uso di HTTPS attraverso questo *redirect* e questo dovrebbe avvenire verso lo stesso host o un suo sotto dominio. Queste ultime due condizioni sono imposte perché il redirect non è protetto da SSL/TLS ed è quindi potenzialmente vulnerabile a modifiche durante il transito. Se il *redirect* avviene verso siti terzi non è possibile stabilire, durante i test, se sia intenzionale o se sia il risultato di una compromissione[4].
HTTPS → HTTP	Verifica se il server effettua un redirect HTTP dalla porta 443 (HTTPS) alla porta 80 (HTTP), potenzialmente anche di altri host. Gli utenti non dovrebbero mai essere reindirizzati verso siti non HTTPS in quanto questo rompe la catena di fiducia garantita da SSL/TLS.

Nel caso non sia possibile verificare una di queste determinate funzionalità, nel rapporto finale sarà presente un trattino che indica un valore assente.

Una volta effettuate le verifiche su tutte le funzionalità, lo strumento di test restituisce un **esito** (relativo al sito testato) in base al peso assegnato alla **presenza o assenza** di alcune di queste funzionalità.
Nel file PDF allegato, oltre all'esito sono elencate le motivazioni del "voto" assegnato al sito. Queste possono essere usate per individuare quale parte della configurazione HTTPS è da migliorare.
Facciamo notare che è facile reperire online configurazioni del protocollo HTTPS aggiornate e corrette e che questo è probabilmente il modo più veloce per mettere in sicurezza i propri siti istituzionali.

Riportiamo in tabella i possibili esiti:

il server non supporta SSL/TLS	E' necessario procedere tempestivamente all'implementazione del protocollo HTTPS.
l'implementazione HTTPS è aggirabile	E' necessario correggere la configurazione tempestivamente.

4 In questo caso il test fallisce poiché il target del redirect non sarebbe comunque un sito controllato dall'Amministrazione.

l'implementazione HTTPS è vulnerabile ad attacchi noti	Sono già noti attacchi che possono compromettere la sicurezza del canale HTTPS per come è stato configurato. E' necessario correggere la configurazione in tempi ragionevolmente brevi.
l'implementazione HTTPS non è più considerata sicura	Non sono noti attacchi per la configurazione HTTPS riscontrata ma sono abilitate funzionalità che sono state deprecate o non più considerate adeguate agli standard attuali.
l'implementazione HTTPS è considerata sicura	La configurazione riscontrata è considerata sicura dagli standard attuali.

Come è stato verificato il CMS del mio sito istituzionale e come ne interpreto i risultati?

L'esito della verifica dello stato di aggiornamento del CMS è di interpretazione più immediata di quello della verifica HTTPS tuttavia l'operazione di verifica presenta **altrettanti punti da tenere in considerazione**.

Il primo è quello della rilevazione del CMS e della sua versione. I CMS non sono progettati per essere comodamente rilevati: **non esiste un metodo standard e sicuro per rilevarli**. Gli algoritmi usati si basano sulla presenza e sull'interpretazione di artefatti tipici delle specifiche versioni del CMS.
Si tratta quindi di un approccio che richiede di **censire gli artefatti dei vari CMS e di tenerli sempre aggiornati**.
Considerando la frequenza con cui i CMS vengono aggiornati e la loro numerosità, risulta evidente la difficoltà di tale procedura.
Quando il tipo di CMS è rilevato, **non è sempre possibile rilevarne la versione esatta** e, talvolta, neanche la versione approssimativa.

E' quindi possibile che il tipo di CMS del vostro sito istituzionale non venga rilevato o che la sua versione non venga individuata correttamente.

Oltre alla difficoltà nel rilevare il tipo di CMS e la sua relativa versione, si deve aggiunge anche la **difficoltà nel conoscere l'ultima versione al momento disponibile** di un CMS.

Non esiste un elenco ufficiale con le ultime versioni rilasciate di tutti i CMS per cui lo strumento di test sfrutta l'aggregazione di varie fonti, alcune delle quali manuali, ma non è sempre possibile garantire che i dati siano aggiornati all'ultima release rilasciata di ogni CMS.

Infine, qualche tipologia di CMS (come ad esempio Drupal o Joomla!) supporta anche **versioni multiple e parallele** (es: Joomla! 1.x, 2.x e 3.x).
Le fonti che forniscono le ultime release disponibili fanno riferimento generalmente solo ad una versione per ogni CMS, tipicamente alla *major release,* tralasciando le altre.
In questo caso si ottiene un'**alta probabilità di falsi positivi**.

In sintesi, la verifica del CMS è un processo che purtroppo poco si presta all'automatismo. Consigliamo quindi di **verificare frequentemente lo stato di aggiornamento del vostro CMS, indipendentemente dall'esito ottenuto dal test**.

Quando il tipo di CMS e la sua versione vengono rilevati ed è chiaramente nota l'ultima release disponibile, queste sono mostrate in una tabella seguita da una breve nota che indica se il CMS è aggiornato o meno.

Per ulteriori approfondimenti sugli argomenti qui trattati, è possibile fare riferimento anche alle seguenti guide tecniche e linee guida:

- La sicurezza nel procurement Ict
- Raccomandazioni AGID - TLS e Cipher Suite
- Linee guida per lo sviluppo del software sicuro