IL PATRIMONIO DIGITALE DELL'OSPITALITÀ SARDA

Osservazione passiva dei siti delle strutture ricettive a quattro e cinque stelle

Roberto Pinna · 23 ottobre 2026

robpinna.com/studio/patrimonio-digitale-ospitalita-sarda/

Studio · 23 ottobre 2026

Il patrimonio digitale dell'ospitalità sarda

Osservazione passiva dei siti delle strutture ricettive a quattro e cinque stelle · di Roberto Pinna

Più di un indirizzo su quattro tra quelli che il portale turistico della Regione Sardegna associa agli alberghi a quattro e cinque stelle non conduce al sito ufficiale della struttura, e in quattro casi chi lo apre arriva su pagine di gioco d'azzardo online. In diciotto schede l'email indicata per le richieste degli ospiti si trova su un dominio che non esiste più; per dieci di questi il registro pubblico conferma che chiunque potrebbe registrarlo e ricevere, da quel momento, la posta destinata all'albergo. Tra i siti che funzionano, due su tre dichiarano a chiunque li interroghi con quale software sono costruiti, e una parte consistente usa versioni che non ricevono più correzioni di sicurezza.

Indice

In sintesi
I domini indicati dal portale
La posta degli ospiti
Ciò che i siti dichiarano di sé
I siti non mantenuti
Le protezioni di base
Che cosa rischia una struttura
Che cosa significano i dati
Che cosa fare
Metodo, perimetro e limiti
Glossario
Fonti
Nota per le redazioni

Lo studio riguarda tutte le strutture a quattro e cinque stelle presenti su SardegnaTurismo, il portale turistico della Regione, ed è stato condotto tra il 23 e il 24 ottobre 2026 osservando dall'esterno ciò che ogni sito e ogni dominio mostrano a chi li visita, che si tratti di una persona o di un programma automatico. Si rivolge alle strutture e a chi ne gestisce i siti, a chi si occupa di sicurezza e alle redazioni, e non nomina alcuna struttura.

79 su 288
domini che il portale associa alle strutture e che non portano a un sito ufficiale funzionante (27%)

18
schede con un'email su un dominio che non esiste più; per dieci di questi il registro conferma che il nome è libero

135 su 209
siti funzionanti che rendono leggibile la versione di almeno un componente

108 su 209
siti funzionanti che non attivano nessuna delle sei intestazioni di sicurezza esaminate

In sintesi

Il censimento comprende 439 schede, dalle quali risultano 317 domini distinti, 288 dei quali valutabili. I risultati riguardano quattro aspetti, esaminati nell'ordine in cui interessano chi visita il sito, cioè i domini, la posta, le informazioni che i siti rendono pubbliche su sé stessi e lo stato del loro software.

- **Domini.** 79 indirizzi su 288 non portano a un sito ufficiale funzionante. Dodici conducono a contenuti che la struttura non controlla, quattro dei quali a pagine di gioco d'azzardo online; in un caso la struttura è chiusa dalla fine del 2024 e la scheda non è stata aggiornata.
- **Posta.** Diciotto schede indicano un'email su un dominio che non esiste più, e per dieci di questi il registro conferma che il nome è libero; in almeno altre quattro l'email si trova su un dominio passato a terzi o messo in vendita.
- **Versioni dichiarate.** 135 siti funzionanti su 209 rendono leggibile la versione di almeno un componente, un'informazione che i programmi di scansione raccolgono in modo automatico.
- **Software non mantenuto.** Dei siti WordPress che dichiarano la versione, uno su tre è fermo a rami pubblicati fino al 2023; dei 21 server che dichiarano la versione di PHP, 11 usano rami che non ricevono più correzioni.
- **Protezioni di base.** 108 siti funzionanti su 209 non attivano nessuna delle sei intestazioni di sicurezza esaminate.

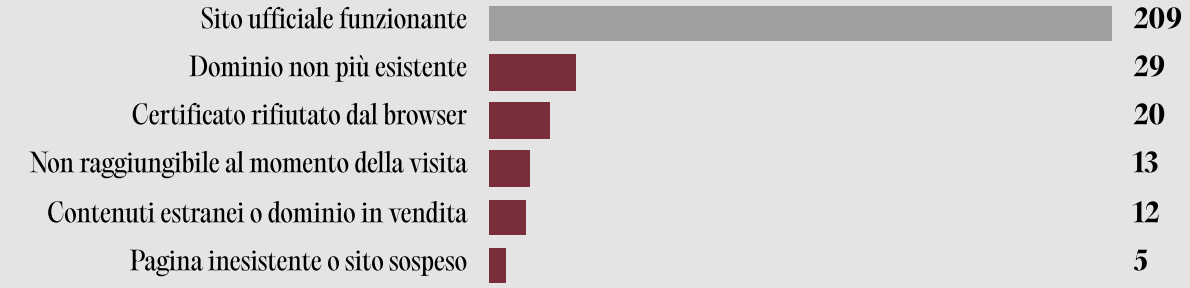
Prima della pubblicazione ho informato in via riservata le strutture coinvolte nei casi più delicati, chi ne gestisce i siti e la redazione del portale SardegnaTurismo, trasmettendo a ciascuno quanto rilevato.

I domini indicati dal portale

Il dominio è il primo elemento che un ospite incontra, e quello da cui dipendono tutti gli altri; il sito, la posta e la reputazione che la struttura ha costruito in rete restano legati a quel nome finché qualcuno lo rinnova.

Più di un dominio su quattro non porta a un sito ufficiale funzionante

79 domini su 288 (27%): esito della visita alla pagina principale, 23–24 ottobre 2026



Osservazione passiva dei 288 domini valutabili delle strutture a 4 e 5 stelle presenti su SardegnaTurismo, 23–24 ottobre 2026

In 79 casi su 288 (27%; intervallo indicativo 23–33%) l'indirizzo che il portale regionale associa alla struttura non conduce a un sito ufficiale funzionante. Il gruppo più numeroso, 29 domini, non esiste più nel DNS, e per molti di questi il registro conferma che il nome è oggi libero; venti siti presentano un certificato che il browser rifiuta in ogni forma dell'indirizzo, sicché l'ospite riceve un avviso di sicurezza a tutta pagina; tredici non rispondevano al momento della visita, e cinque conducono a pagine inesistenti di siti di gruppo o a un sito sospeso dal fornitore.

Altri dodici domini portano a contenuti che la struttura non controlla. Quattro conducono a pagine di gioco d'azzardo online, tra cui casinò privi di concessione in Italia; gli altri a un blog di fotografia, a una rivista di viaggi straniera, alla pagina promozionale di un'altra agenzia, a un sito generico di contenuti turistici o a una pagina che offre il dominio in vendita. In almeno un caso il dominio è stato abbandonato perché la struttura, un cinque stelle, è chiusa dalla fine del 2024 (La Nuova Sardegna); la scheda del portale continua tuttavia a indicarlo, e chi cerca la struttura dalla fonte ufficiale della Regione approda su contenuti estranei.

Due casi aiutano a comprendere come un dominio possa sfuggire alla struttura. Il dominio di un albergo della Gallura, lasciato scadere, è stato registrato di nuovo nell'aprile 2026 da un servizio specializzato nell'intercettare i domini in scadenza, ed è oggi offerto in vendita mentre il portale regionale continua a indicarlo; è il modo più frequente in cui un dominio si perde, e basta un mancato rinnovo perché accada. Il dominio di una struttura del nord-est dell'isola, invece, reindirizza ogni visitatore a un sito di scommesse online indonesiano pur conservando un proprio server di posta presso un fornitore italiano; il quadro è compatibile con una compromissione del sito più che con la perdita del dominio, e la scheda del portale indica come recapito un'email sullo stesso dominio.

La posta degli ospiti

In diciotto schede l'email di contatto appartiene a un dominio che non esiste più. In un caso si tratta di un refuso, una lettera in più nel nome dell'albergo, mentre il dominio corretto esiste ed è attivo; negli altri il dominio dell'email è scaduto senza essere sostituito, e in uno la scheda rimanda al sito di un albergo omonimo in un'altra regione. Per dieci di questi nomi il registro conferma che oggi chiunque potrebbe registrarli, e da quel

momento riceverebbe le richieste di prenotazione, i recapiti e talvolta i documenti che gli ospiti credono di inviare all'albergo, con la possibilità di rispondere in suo nome. In almeno altre quattro schede l'email si trova su un dominio già passato a terzi o messo in vendita.

Tra gli aspetti esaminati è quello che tocca più da vicino gli ospiti e i loro dati, e anche quello che si corregge con minore sforzo, con una modifica alla scheda o con il rinnovo di un nome.

Ciò che i siti dichiarano di sé

Ogni volta che una pagina viene aperta, il server e il codice della pagina possono indicare quale software li fa funzionare e in quale versione. L'informazione è leggibile da chiunque, e a raccoglierla in modo sistematico sono soprattutto programmi automatici; i motori di scansione che percorrono la rete alla ricerca di server da attaccare, come i sistemi che raccolgono contenuti per gli indici e per i modelli di intelligenza artificiale, la registrano insieme al resto della pagina.

In 135 siti funzionanti su 209 (65%; 58–71%) la pagina dichiara la versione di almeno un componente, che sia WordPress, PHP o il software del server. Una versione dichiarata non prova che il sito sia vulnerabile; permette però di stabilire, senza alcuna interazione, se il sito usa un componente per il quale è nota una vulnerabilità, e di inserirlo in un elenco di bersagli prima ancora che qualcuno lo visiti. Nei giorni successivi a PHP2Shell, il caso descritto più avanti, sono circolati strumenti e richieste di elenchi pensati proprio per individuare in grande numero i server non aggiornati.

I siti non mantenuti

Un sito è composto da parti che invecchiano a ritmi diversi, dal software del server a quello dell'applicazione, dal certificato che scade ogni pochi mesi al dominio che va rinnovato; ciascuna ha un proprio calendario di correzioni, e se nessuno ha il compito di seguirle restano ferme al giorno in cui il sito è stato consegnato. Le versioni dichiarate permettono di misurare questa distanza.

Indicatori sui siti funzionanti: conteggio, quota e intervallo indicativo al 95%

Indicatore, sui siti funzionanti	Conteggio	Quota	Intervallo indicativo (95%)
Costruiti con WordPress	124 su 209	59%	53–66%
WordPress con versione visibile all'esterno	87 su 124	70%	62–78%
di cui sul ramo corrente 7.1	50 su 87	57%	47–67%
di cui su rami pubblicati tra il dicembre 2013 e il novembre 2023	29 su 87	33%	24–44%
Versione di PHP dichiarata dal server	21 su 209	10%	7–15%
di cui su rami che il progetto PHP non corregge più (dalla 5.6 alla 8.1)	11 su 21	52%	32–72%
di cui su versioni supportate ma anteriori alla correzione	2 su 21	10%	3–29%

Indicatore, sui siti funzionanti	Conteggio	Quota	Intervallo indicativo (95%)
di cui già sulla versione corretta per PHP2Shell	8 su 21	38%	21–59%
Nessuna delle sei intestazioni di sicurezza	108 su 209	52%	45–58%
Tutte e sei le intestazioni	3 su 209	1%	0–4%
Servizio di protezione riconoscibile davanti al sito	45 su 209	22%	16–28%
Versione di almeno un componente visibile all'esterno	135 su 209	65%	58–71%

Dei 124 siti costruiti con WordPress, 87 lasciano leggere la versione; 50 sono sul ramo corrente 7.1, mentre 29 sono fermi a rami pubblicati tra il dicembre 2013 e il novembre 2023, per i quali sono note vulnerabilità corrette soltanto nelle versioni successive. Il più datato appartiene al ramo 3.8, del dicembre 2013. Dei 21 server che dichiarano la versione di PHP, 11 usano rami che il progetto non corregge più, 2 versioni supportate ma anteriori all'ultima correzione, e 8 erano già aggiornati a pochi giorni dal rilascio.

Due resort dello stesso gruppo, sulla costa settentrionale, dichiarano a ogni visitatore un server web del ramo Apache 2.2, che non riceve correzioni dalla fine del 2017, su un sistema operativo il cui supporto è terminato nel 2020, insieme a PHP 5.6 e 7.0, che il progetto ha smesso di correggere tra la fine del 2018 e l'inizio del 2019, e a WordPress 4.6 e 4.7, rami pubblicati nel 2016; è il profilo più datato dell'intero censimento. In un altro gruppo di siti, almeno cinque portano nel piè di pagina la firma dello stesso fornitore locale, e una decina condivide con essi server, configurazione o gestore del DNS. Presentano tutti lo stesso schema, privo delle intestazioni di sicurezza e, dove la versione è leggibile, con WordPress fermo a rami pubblicati tra il 2021 e il 2023; due di essi dichiarano di essere stati realizzati «con finanziamenti dell'Unione Europea e con il supporto della Regione Autonoma della Sardegna», e nulla, nella pagina, indica che alla realizzazione sia seguita una manutenzione.

Un esempio recente, PHP2Shell

Il 21 ottobre 2026 il progetto PHP ha pubblicato le correzioni per due vulnerabilità dell'interprete, note come PHP2Shell (CVE-2026-109618 e CVE-2026-109619), che consentono a chiunque, senza credenziali, di eseguire codice sul server; la gravità attribuita è di 9,2 su 10 secondo lo standard CVSS 4.0. PHP è il linguaggio con cui funziona circa il 70% dei siti di cui si conosce la tecnologia, WordPress compreso. Le correzioni sono uscite per i rami ancora supportati, con le versioni 8.2.35, 8.3.36, 8.4.27 e 8.5.12, mentre per i rami 8.1 e precedenti il progetto non rilascia aggiornamenti. I dettagli erano trapelati prima della data concordata, e tentativi di sfruttamento erano stati osservati già il 17 ottobre; nei giorni del rilascio Germania, Francia, Belgio, Paesi Bassi, Finlandia e Repubblica Ceca hanno oscurato in via precauzionale siti governativi, e il CSIRT Italia ha diramato un'allerta con impatto sistemico alto. In Italia, alla data di questo studio, non risultano documentati spegnimenti di siti istituzionali né compromissioni di imprese.

PHP2Shell mostra in concreto il rischio che corre un sito non mantenuto. L'aggiornamento automatico di WordPress, dei temi e dei plugin non corregge PHP, che appartiene al server; la correzione spetta a chi gestisce il server e, per i rami fuori supporto, dipende interamente dal fornitore. Tra i siti del censimento che dichiarano la versione di PHP, undici usano rami per i quali il progetto non ha pubblicato alcuna correzione, e due versioni immediatamente precedenti a quella corretta, la 8.2.34 e la 8.3.35.

Le protezioni di base

I browser offrono gratuitamente alcune protezioni che il sito può attivare con poche righe di configurazione, contro il furto della sessione, l'inserimento del sito in pagine altrui e la lettura non cifrata delle comunicazioni. Su 209 siti funzionanti, 108 non ne attivano nessuna tra le sei esaminate e tre soltanto le attivano tutte, mentre 45 sono protetti da un servizio riconoscibile come Cloudflare. La loro assenza rende più facile sfruttare gli eventuali difetti del sito, e indica in genere che nessuno ne ha curato la configurazione dopo la pubblicazione.

Che cosa rischia una struttura

Ciascuna delle circostanze osservate corrisponde a un rischio preciso, che non resta confinato al sito; tocca la posta degli ospiti, le prenotazioni, la reputazione della struttura e, quando sono coinvolti dati personali, gli obblighi che la legge le attribuisce. La tabella pone ogni circostanza in relazione con ciò che può accadere, con ciò che ne deriverebbe per la struttura e con l'intervento che lo previene.

Circostanze osservate, rischi connessi e interventi correttivi

Ciò che si osserva	Che cosa può accadere	Che cosa comporta per la struttura	Come si rimedia
Dominio scaduto o non più esistente, ancora indicato sul portale	Chiunque può registrarlo e pubblicarvi ciò che vuole, compresa una falsa pagina di prenotazione che raccoglie pagamenti e dati delle carte	Ospiti sottratti o truffati in nome della struttura; reclami e danno d'immagine che ricadono comunque su di essa	Rinnovare il dominio, oppure chiedere alla Regione di aggiornare la scheda
Email su un dominio libero, in vendita o scritto con un refuso	Chi acquista il dominio riceve le richieste degli ospiti, con nomi, date, recapiti e talvolta documenti, e può rispondere al posto della struttura	Prenotazioni perdute; dati personali consegnati a terzi, con i conseguenti obblighi verso il Garante quando ne derivi un rischio per gli ospiti	Correggere l'email nella scheda; mantenere attivo il vecchio dominio anche dopo un cambio di indirizzo
Sito che rimanda al gioco d'azzardo o a contenuti estranei	Il sito è nelle mani di altri, che possono servirsene anche per diffondere codice malevolo tra i visitatori	Gli ospiti approdano su pagine illecite; motori di ricerca e browser segnalano il dominio come pericoloso	Riprendere il controllo del sito, ripulirlo e accertare se siano stati esposti dati
Versioni dei componenti dichiarate a chiunque	Gli strumenti automatici selezionano i bersagli proprio a partire da queste informazioni	Il sito entra negli elenchi dei bersagli prima di altri	Nascondere le versioni nelle intestazioni e nel codice delle pagine
PHP su rami fuori supporto o anteriori alla correzione	Vulnerabilità come PHP2Shell consentono a chiunque di eseguire comandi sul server senza credenziali	Sito alterato o oscurato, dati di moduli e prenotazioni sottratti, server impiegato per attaccare altri	Portare PHP alla versione corretta del proprio ramo, o a un ramo supportato
WordPress su rami datati	Le vulnerabilità corrette negli anni restano aperte e sono sfruttate in grande numero da strumenti automatici	Pagine contraffatte, reindirizzamenti, link di spam che penalizzano il posizionamento nei motori di ricerca	Aggiornare nucleo, temi ed estensioni con una cadenza stabilita

Ciò che si osserva	Che cosa può accadere	Che cosa comporta per la struttura	Come si rimedia
Certificato rifiutato dal browser	L'ospite riceve un avviso a tutta pagina, e la connessione non garantisce che il sito sia quello autentico	Visitatori che abbandonano prima di prenotare; moduli inviati senza garanzia di riservatezza	Rinnovare il certificato e predisporne il rinnovo automatico
Nessuna intestazione di sicurezza	Il sito può essere incorporato in pagine altrui, e i difetti presenti diventano più facili da sfruttare, compreso il furto delle sessioni	Un difetto minore si trasforma più facilmente in un incidente	Configurare le intestazioni, un intervento di poche ore

Nessuno di questi interventi richiede di rifare il sito; per la maggior parte si tratta di rinnovi, aggiornamenti e configurazioni che chi lo gestisce può completare in pochi giorni, e che costano assai meno di quanto costerebbe rimediare a una sola delle conseguenze descritte. La struttura, inoltre, in quanto titolare del trattamento dei dati degli ospiti, è tenuta dal Regolamento europeo sulla protezione dei dati a proteggerli con misure adeguate allo stato dell'arte (articolo 32), e un componente che non riceve correzioni da anni difficilmente può essere considerato tale.

Il settore alberghiero, del resto, è da tempo un bersaglio costante, perché un albergo di fascia alta conserva dati dei propri ospiti di natura assai personale, dai documenti d'identità alle abitudini di viaggio. Nell'agosto 2025 il CERT-AgID ha segnalato la vendita, su forum criminali, di scansioni di documenti d'identità acquisite al check-in da strutture italiane, oltre centomila secondo le stime riportate, e il Garante è intervenuto sul caso (Cybersecurity360); nell'estate 2026 Bitdefender ha documentato campagne rivolte al personale di ricevimento e prenotazione, con false richieste di ospiti e falsi messaggi di Booking.com, in cui l'Italia figura tra i Paesi più colpiti.

Che cosa significano i dati

I siti osservati appartengono a strutture che curano con attenzione l'accoglienza, e molti sono stati realizzati con evidente cura dell'immagine; i dati indicano che, una volta pubblicato, il sito non sempre continua a ricevere la stessa attenzione. Gli otto server aggiornati per PHP2Shell a pochi giorni dal rilascio e i cinquanta siti sul ramo corrente di WordPress sono con buona probabilità quelli che qualcuno segue con regolarità, mentre i domini scaduti, le email inesistenti e le versioni ferme da anni descrivono siti che nessuno ha più in carico.

Per una struttura che vive della propria reputazione, la questione riguarda dunque anzitutto chi abbia oggi la responsabilità del sito, del dominio e della posta, con quale frequenza la eserciti e in che modo lo si possa verificare.

Che cosa fare

Per le strutture: cinque domande a chi gestisce il sito

Le domande che seguono non richiedono competenze tecniche e, poste per iscritto, ottengono di solito una risposta chiara e verificabile.

- **A chi è intestato il dominio, e quando scade?** Il dominio dovrebbe essere intestato alla struttura, con rinnovo automatico e una scadenza nota a più di una persona.
- **Chi aggiorna PHP e il server, e quando lo ha fatto l'ultima volta?** Dopo il 21 ottobre la risposta attesa è una data e una versione corretta del proprio ramo, ossia 8.2.35, 8.3.36, 8.4.27, 8.5.12 o successive.
- **Su quale versione di WordPress, o di altro sistema, gira oggi il sito?** E chi ne aggiorna temi ed estensioni, con quale cadenza.
- **Che cosa accade se il sito viene compromesso di notte o di domenica?** Chi se ne accorge, entro quanto, e chi interviene.
- **Quali dati degli ospiti passano dal sito, e dove finiscono?** Moduli di contatto, prenotazioni, documenti, newsletter: ciascuno ha un luogo e un responsabile.

Per la Regione

Il portale SardegnaTurismo è, per molti visitatori, il primo luogo in cui cercare una struttura, e gli indirizzi che riporta godono della fiducia che si accorda a una fonte istituzionale. Una verifica periodica e automatica dei domini e delle email indicati nelle schede, con la richiesta di aggiornamento alle strutture quando l'esito è negativo, eliminerebbe la maggior parte dei casi descritti in questo studio; lo strumento impiegato per il censimento può essere messo a disposizione a questo fine. Per i siti realizzati con finanziamenti pubblici, inoltre, sarebbe opportuno che tra i requisiti figurasse un periodo di manutenzione successivo alla consegna.

Per chi realizza e gestisce i siti

La consegna di un sito dovrebbe accompagnarsi a un'indicazione scritta di chi, da quel momento, ne curi gli aggiornamenti, il rinnovo del dominio e quello del certificato; quando il contratto non lo prevede, è bene che la struttura ne sia informata in modo esplicito.

Metodo, perimetro e limiti

Lo studio si fonda su un'osservazione passiva, condotta il 23–24 ottobre 2026 con un normale browser: di ogni sito ho aperto la pagina principale, come farebbe un ospite, ne ho letto il codice e, con una seconda richiesta alla stessa pagina, le intestazioni inviate dal server. Non ho richiesto percorsi riservati, inviato parametri, tentato accessi o verificato la presenza di vulnerabilità; nessun dato personale è stato raccolto, e nessuna struttura è nominata.

Come si è formato il campione

- Dal portale SardegnaTurismo della Regione ho tratto tutte le schede delle strutture classificate cinque stelle superior, cinque stelle, quattro stelle superior e quattro stelle: 439 secondo i conteggi del portale al 24 ottobre 2026.
- Per ciascuna ho preso l'indirizzo del sito indicato dal portale oppure, in sua assenza, il dominio dell'email di contatto, escludendo caselle generiche e di posta certificata; ne sono risultati 317 domini distinti.
- Ho escluso 17 domini di catene nazionali e internazionali, di operatori turistici e di società proprietarie, il cui sito è gestito fuori dall'isola o non riguarda una singola struttura; 6 domini che conducono allo stesso sito di un altro già contato; 6 domini non valutabili, perché protetti da verifiche anti-automazione, privi di contenuto al caricamento o non visitabili per le impostazioni del browser. Ne restano 288.
- Le visite si sono svolte tra la sera del 23 e il 24 ottobre 2026; i domini che non rispondevano sono stati visitati una seconda volta, in tutte le forme dell'indirizzo, prima di essere classificati.

Che cosa ho osservato

- l'esito della visita: sito funzionante, dominio non più esistente, errore di certificato, sito non raggiungibile, pagina inesistente, contenuti estranei o dominio in vendita;
- per i domini che non rispondevano, la loro presenza nel DNS pubblico e, per i domini .com, lo stato di registrazione nel registro pubblico RDAP di Verisign; per quelli che mostravano contenuti estranei, la data dell'ultima registrazione;
- la piattaforma e, quando dichiarata, la versione di WordPress, ricavata dall'etichetta di generazione della pagina o dai file del nucleo che vi sono richiamati;
- la versione di PHP e del software del server, quando il server la dichiara spontaneamente;
- la presenza di sei intestazioni di sicurezza: HSTS, Content-Security-Policy, X-Frame-Options, X-Content-Type-Options, Referrer-Policy e Permissions-Policy;
- la presenza di un servizio di protezione riconoscibile davanti al sito (Cloudflare, BitNinja, WP Engine).

Quando una forma dell'indirizzo, con o senza «www», in http o in https, restituiva un errore, ho provato anche le altre; l'esito negativo è registrato soltanto se tutte fallivano.

Limiti del metodo

- Si tratta di un censimento delle strutture del perimetro, non di un campione: le percentuali descrivono queste strutture e non vanno estese ad altre categorie. Gli intervalli di confidenza al 95% (metodo di Wilson) sono riportati a titolo indicativo, per dare la misura della variabilità di quote calcolate su numeri talvolta contenuti.
- Una versione dichiarata non equivale a una versione vulnerabile: le distribuzioni Linux e i pannelli come Plesk applicano talvolta correzioni senza cambiare il numero di versione. Per questo il rapporto parla di versioni «dichiarate» e di rami «fuori supporto», mai di siti «vulnerabili».
- La maggior parte dei server nasconde la versione di PHP; il dato su PHP riguarda quindi soltanto 21 siti.

- Per i domini .it ed .eu l'assenza dal DNS non prova che il nome sia libero, perché il registro italiano non offre un'interrogazione automatica; per questi il rapporto parla di domini «non più esistenti nel DNS», e riserva l'affermazione che un dominio sia registrabile ai soli casi verificati nel registro.
- Un certificato è stato considerato rifiutato quando il browser mostrava l'avviso di sicurezza in tutte le forme dell'indirizzo; la causa precisa, che sia la scadenza, un nome non corrispondente o una catena incompleta, non è stata indagata.
- La Content-Security-Policy dichiarata nel codice della pagina, anziché nelle intestazioni, non è stata conteggiata; il dato sulle intestazioni può dunque sottostimare di poco le protezioni presenti.
- Gli esiti «non raggiungibile» fotografano un momento e possono dipendere da un disservizio passeggero; sono tenuti separati dagli altri. Nessuno dei dati raccolti, infine, prova che un sito sia stato compromesso o che lo sarà; ciascuno descrive lo stato in cui il sito si trovava al momento dell'osservazione.

Lo strumento di rilevazione, in Python e senza dipendenze esterne, è disponibile su richiesta e consente di ripetere lo studio con lo stesso metodo.

Glossario

CVE
Codice univoco con cui viene catalogata pubblicamente una vulnerabilità informatica.

CVSS
Scala da 0 a 10 che misura la gravità tecnica di una vulnerabilità; 9,2 rientra nella fascia critica.

Esecuzione di codice da remoto
Possibilità, per chi attacca, di far eseguire al server istruzioni proprie, come se ne avesse il controllo.

PHP
Linguaggio con cui il server costruisce le pagine di gran parte dei siti, WordPress compreso; è distinto dal sito e si aggiorna separatamente.

Ramo fuori supporto
Serie di versioni per cui il progetto ha smesso di pubblicare correzioni; le eventuali correzioni dipendono dal singolo fornitore.

Certificato TLS
Documento digitale che consente la connessione cifrata e attesta l'identità del sito; se è scaduto o non corrisponde, il browser mostra un avviso.

Intestazioni di sicurezza
Istruzioni che il sito invia al browser per attivarne le protezioni, per esempio imporre la connessione cifrata (HSTS) o impedire che il sito venga incorporato in pagine altrui.

Dominio ripreso da terzi
Dominio lasciato scadere e registrato da altri, che ne sfruttano la reputazione e i collegamenti esistenti per contenuti propri.

Osservazione passiva
Lettura di ciò che un sito mostra spontaneamente a qualunque visitatore, senza interagire oltre la normale visita.

Intervallo di confidenza
Fascia entro cui ragionevolmente cadrebbe la quota misurata ripetendo l'osservazione su un campione simile.

Fonti

- Canadian Centre for Cyber Security, AL26-026: versioni coinvolte e corrette.
  https://cyber.gc.ca/en/alerts-advisories/al26-026-critical-vulnerabilities-impacting-php-cve-2026-109618-cve-2026-109619
- watchTowr, PHP2Shell FAQ: punteggio CVSS 4.0, sfruttamento osservato, stato KEV.
  https://watchtowr.com/intelligence/php-cve-2026-109618-faq/
- BleepingComputer, 20 ottobre 2026: fuga di notizie e rilascio anticipato.
  https://bleepingcomputer.com/news/security/php-warns-admins-of-two-critical-flaws-emergency-patches-coming-tomorrow
- ICT Security Magazine: cronologia e allerta del CSIRT Italia.
  https://www.ictsecuritymagazine.com/cyber-security/php2shell-embargo-rotto-finestra-prima-della-patch/
- KELA: primo tentativo del 17 ottobre e reazione negli ambienti criminali.
  https://www.kelacyber.com/blog/php2shell-underground-response/
- Reuters, via MarketScreener: siti oscurati in Europa.
  https://it.marketscreener.com/notizie/siti-web-messi-offline-per-vulnerabilita-di-php-ce785ed9db80f126
- W3Techs, uso di PHP: diffusione di PHP sul web.
  https://www.w3techs.com/technologies/details/pl-php
- WordPress 7.1.3: rilascio di manutenzione e sicurezza del 6 ottobre 2026.
  https://wordpress.org/news/?p=21753
- Cybersecurity360: documenti sottratti a hotel italiani, segnalazione CERT-AgID.
  https://www.cybersecurity360.it/nuove-minacce/furto-di-documenti-didentita-da-hotel-italiani-un-nuovo-caso-di-data-breach-nel-settore-turistico/
- Bitdefender: campagne contro il personale alberghiero, 2026.
  https://www.bitdefender.com/en-us/blog/hotforsecurity/hotel-phishing-booking-com-clickfix-malware
- SardegnaTurismo, Dove dormire: quadro di campionamento.
  https://www.sardegnaturismo.it/it/organizza/alloggi
- La Nuova Sardegna, 3 agosto 2026: chiusura di un resort a cinque stelle incluso nel campione.
  https://www.lanuovasardegna.it/oristano/cronaca/2026/08/03/news/seconda-estate-con-i-cancelli-chiusi-per-il-resort-fantasma-a-cinque-stelle-cosa-sappiamo-1.100902706

Nota per le redazioni

Lo studio è stato curato da Roberto Pinna, consulente per il rischio digitale con base a Cagliari, che si occupa dell'analisi, della realizzazione e del monitoraggio continuo di siti ed e-commerce; è Certified Threat Intelligence Analyst (EC-Council) e certificato CompTIA Security+.

Lo studio non nomina le strutture, e il registro per singolo sito resta riservato. Le tabelle con i dati aggregati e il grafico sono disponibili su richiesta, e l'autore è disponibile per interviste e approfondimenti.

Contatti: Roberto Pinna · direct@robpinna.com · robpinna.com

Come citare

> Pinna, R. (2026). Il patrimonio digitale dell'ospitalità sarda. Osservazione passiva dei siti delle strutture ricettive a quattro e cinque stelle. 23 ottobre 2026. robpinna.com. https://robpinna.com/studio/patrimonio-digitale-ospitalita-sarda/

Versione online: https://robpinna.com/studio/patrimonio-digitale-ospitalita-sarda/