

MODULO 3 - Pratica 2. Raccolta informazioni

Esercizio: Utilizzare i comandi di Google Hacking per raccogliere informazioni su un sito web.

Istruzioni:

1. Aprire un browser web e accedere a Google.
2. Utilizzare i seguenti comandi di Google Hacking per raccogliere informazioni sul sito web:
 - **"site:nome-del-sito.com"** per visualizzare tutte le pagine indicizzate di quel sito.
 - **"inurl:nome-del-sito.com"** per visualizzare tutte le pagine con l'URL contenente il nome del sito.
 - **"intext:'parola chiave' site:nome-del-sito.com"** per visualizzare tutte le pagine che contengono la parola chiave specificata nel testo del sito.
 - **"filetype:estensione site:nome-del-sito.com"** per visualizzare tutti i file con l'estensione specificata presenti sul sito.
3. Utilizzare i risultati **per identificare eventuali informazioni sensibili o vulnerabilità** presenti sul sito.
4. Utilizzare queste informazioni per **valutare la sicurezza del sito e prendere le misure necessarie** per proteggere le informazioni sensibili.

SVOLGIMENTO

SITO WEB ANALIZZATO: aslroma2.it

MOTIVAZIONE: La scelta di valutare la sicurezza di questo sito è legata all'importanza che esso detiene; si tratta di un sito che si collega a diverse altre piattaforme ed applicativi, come nel caso di AREAS e UNICA, e che permette inoltre di visionare anche file personali e privati legati al personale medico e all'organizzazione stessa.

ANALISI CON GOOGLE DORKS

1. **PRIMA RICERCA:** Google Dork "site:".
Utilizzando "site:" in un comando di ricerca verranno forniti risultati solo dal sito Web specifico menzionato.

“site:aslroma2.it”:

Possiamo vedere come siano sorti 4930 risultati.

The screenshot shows a Google search interface with the query "site:aslroma2.it" in the search bar. The search results page displays "Circa 4.930 risultati (0,22 secondi)". Below the search bar, there are tabs for "Tutti", "Prodotti", "Immagini", "Video", "Libri", and "Altro", along with a "Strumenti" link. The first result is a "Promozione Google" for "Prova la Google Search Console" with the URL "www.google.com/webmasters/". The second result is for "aslroma2.it" with the URL "https://www.aslroma2.it", titled "ASL Roma 2 - Home", and a description: "Il nuovo sito internet della ASL Roma 2 · In evidenza · COME E DOVE · strutture sanitarie · Servizi · Dedicato a · comunicazioni news · Sezione banner." The third result is also for "aslroma2.it" with the URL "https://screening.aslroma2.it", titled "Screening ASL ROMA 2", and a description: "Consiste nell'offerta attiva e gratuita di un test per la ricerca del sangue occulto nelle feci (SOF) ogni due anni, di eventuali esami di approfondimento e, se ...". The fourth result is for "aslroma2.it" with the URL "https://videoroom.aslroma2.it", titled "ASL ROMA 2 e-learning", and a description: "Benvenuti nella piattaforma di e-Learning dell'ASL ROMA 2. Benvenuti nella piattaforma di e-Learning dell'ASL ROMA 2." The fifth result is for "aslroma2.it" with the URL "https://anticorruzione.aslroma2.it", titled "Asl Roma 2", and a description: "TICKET RICEZIONE E GESTIONE DELLE SEGNALAZIONI DI CASI DI CORRUZIONE · Apri un Nuovo Ticket · Verifica Stato Ticket. Accedi qui per verificare lo stato delle ...".

2- SECONDA RICERCA: Google Dork “inurl:”.


Questo Dork specifico permette di visionare tutti gli URL in cui è presente il nome del sito preso in esame.

“inurl:aslroma2.it”

Otteniamo 7 soli risultati.

Circa 7 risultati (0,26 secondi)

Risultati per **Lazio** · [Scegli l'area](#) ⋮

 ASL Roma 2
<https://www.aslroma2.it> ⋮

ASL Roma 2 - Home

ASL Roma 2, Azienda Sanitaria Locale, Roma, Ex ASL Roma B, Ex ASL Roma C.

Servizi Online

ASL Roma 2, Azienda Sanitaria Locale, Roma, Ex ASL Roma B ...

Concorsi

Inserimento 18/12/2023. Ultima modifica 18/12/2023. AVVISO ...

Speciale vaccini

è possibile richiedere una ricerca sull'Archivio Storico Vaccinale ...


Azienda

L'azienda sanitaria ASL Roma 2 · Modello assistenziale per ...

Distretti


ASL Roma 2, Azienda Sanitaria Locale, Roma, Ex ASL Roma B ...

[Altri risultati in aslroma2.it](#) »

 asl roma 2 - amministrazione trasparente
<https://ammtrasp.aslroma2.it> ⋮

asl roma 2 - amministrazione trasparente

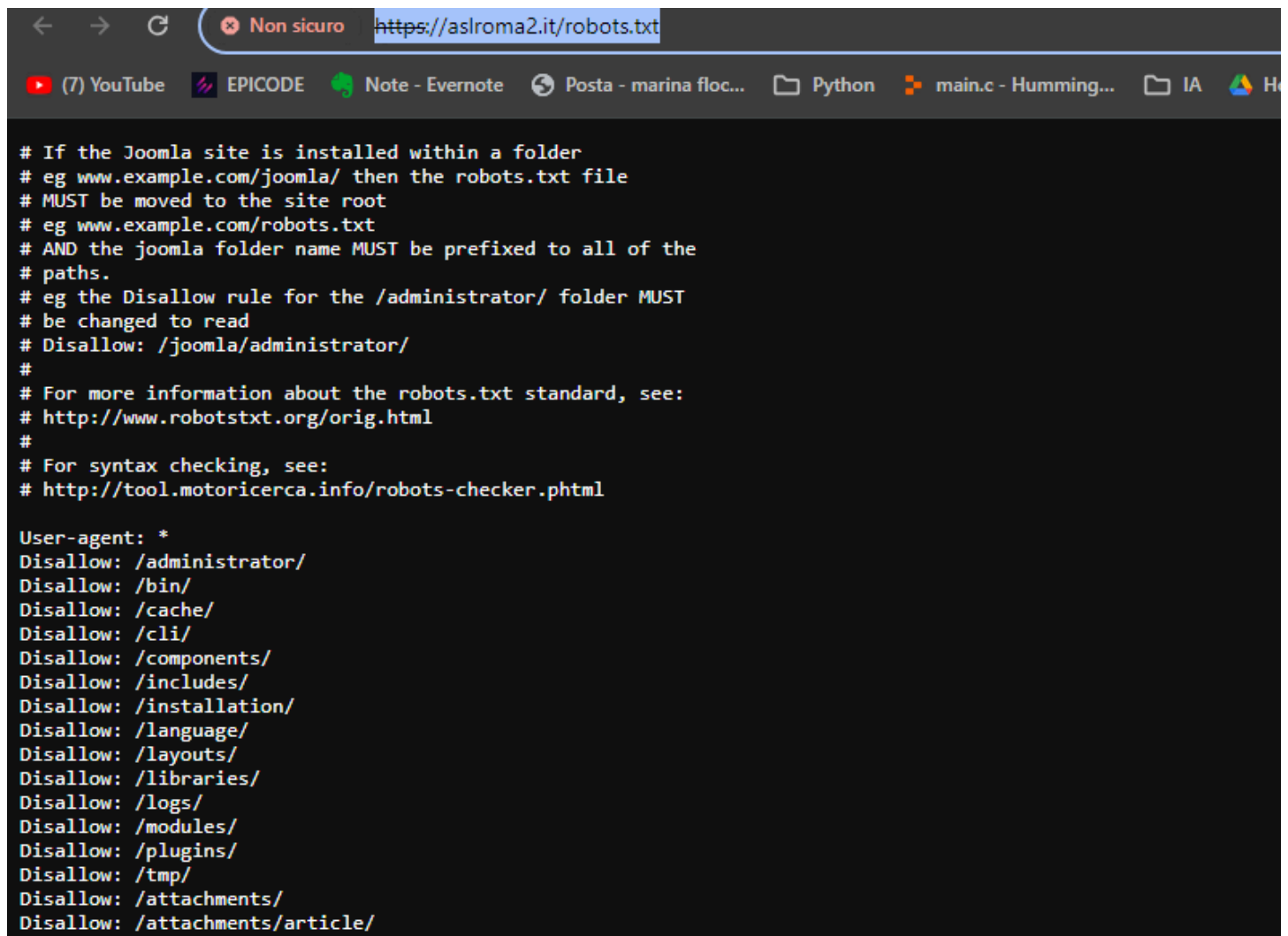
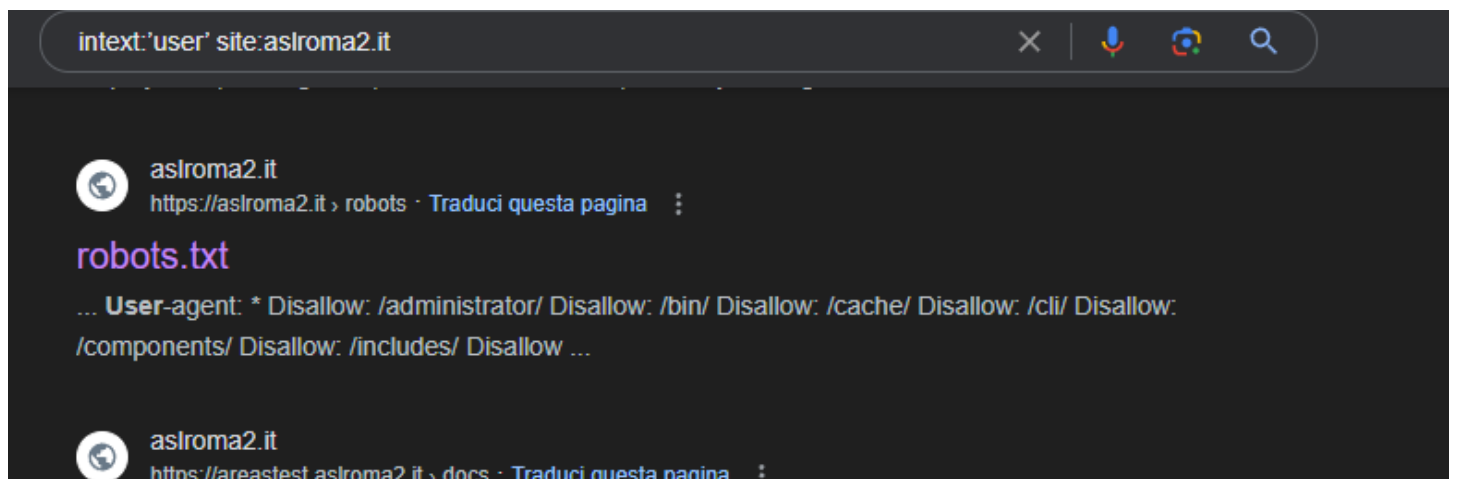
Questa è una sezione del sito ufficiale della ASL Roma 2 relativa all'Amministrazione Trasparente. La trasparenza è accessibilità totale ai dati e ai ...

 [trustpilot.com](https://www.trustpilot.com)

3- TERZA RICERCA: Google Dork “intext:'parola chiave'.

Questo servirà a ridurre i risultati di ricerca andando a trovare solo le pagine contenenti al loro interno il termine specificato.

intext:'user' site:aslroma2.it



Adesso abbiamo individuato un primo elemento importante, ovvero il file “robots.txt”.

Esso contiene informazioni sulla struttura di un sito web, e può essere utilizzato da un utente malintenzionato per conoscere risorse che non possono essere raggiunte semplicemente scansionando ripetutamente i collegamenti ipertestuali.

Se seguiamo le comuni pratiche di sicurezza durante la costruzione di un server web, dobbiamo sicuramente aver disabilitato l'elenco delle directory e creato alcune regole per l'accesso alle

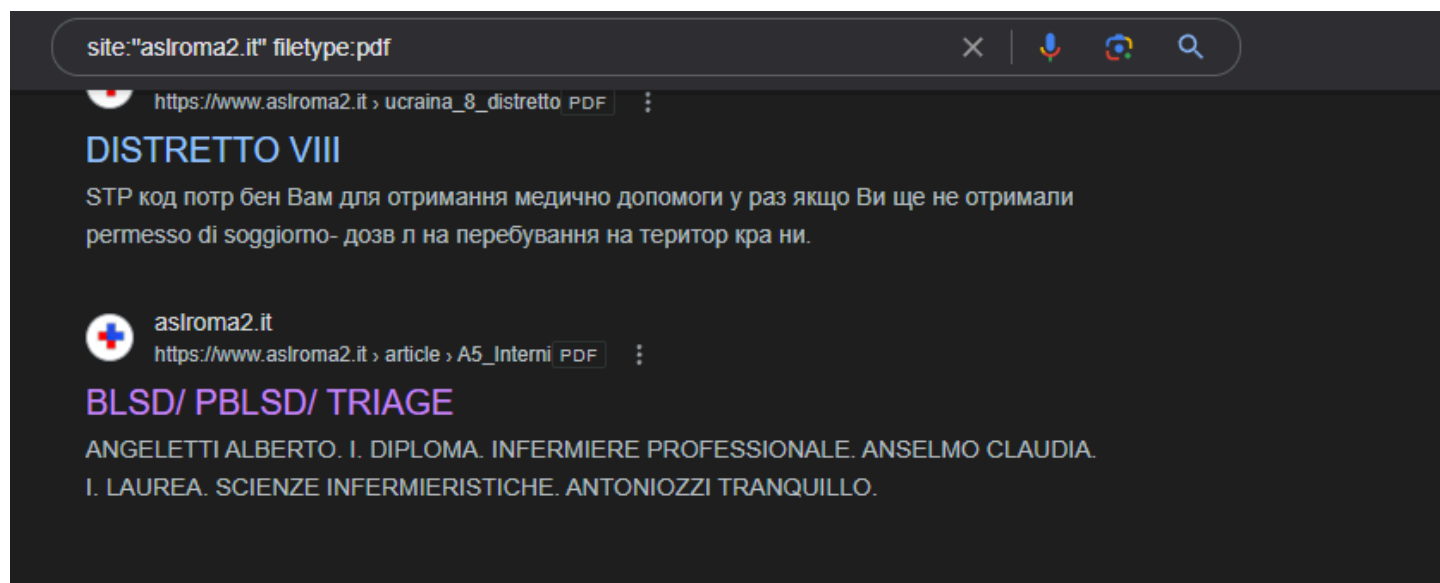
risorse.

Esiste tuttavia il rischio che gli aggressori approfittino del file robots per conoscere la struttura del nostro server web.

4- **QUARTA RICERCA:** Google Dork "filetype:estensione".

Con esso si mira a trovare ed ottenere file di un formato particolare, come ad esempio file Word o PDF presenti in un sito specifico.

site:aslroma2.it filetype:pdf



Troviamo diversi tipi di file pdf disponibili per la visione, tra cui anche un documento contenente nominativi e titoli di studio di alcuni membri dello staff medico del TRIAGE della ASL Roma 2.

aslroma2.it/attachments/article/584/A5_interni.pdf

EPICODE Note - Evernote Posta - marina flo... Python main.c - Humming... IA Home page - Goog... (4) Feed | Linkedln Posta in arrivo (389...

pdf 1 / 2 175%

A5 - Interni

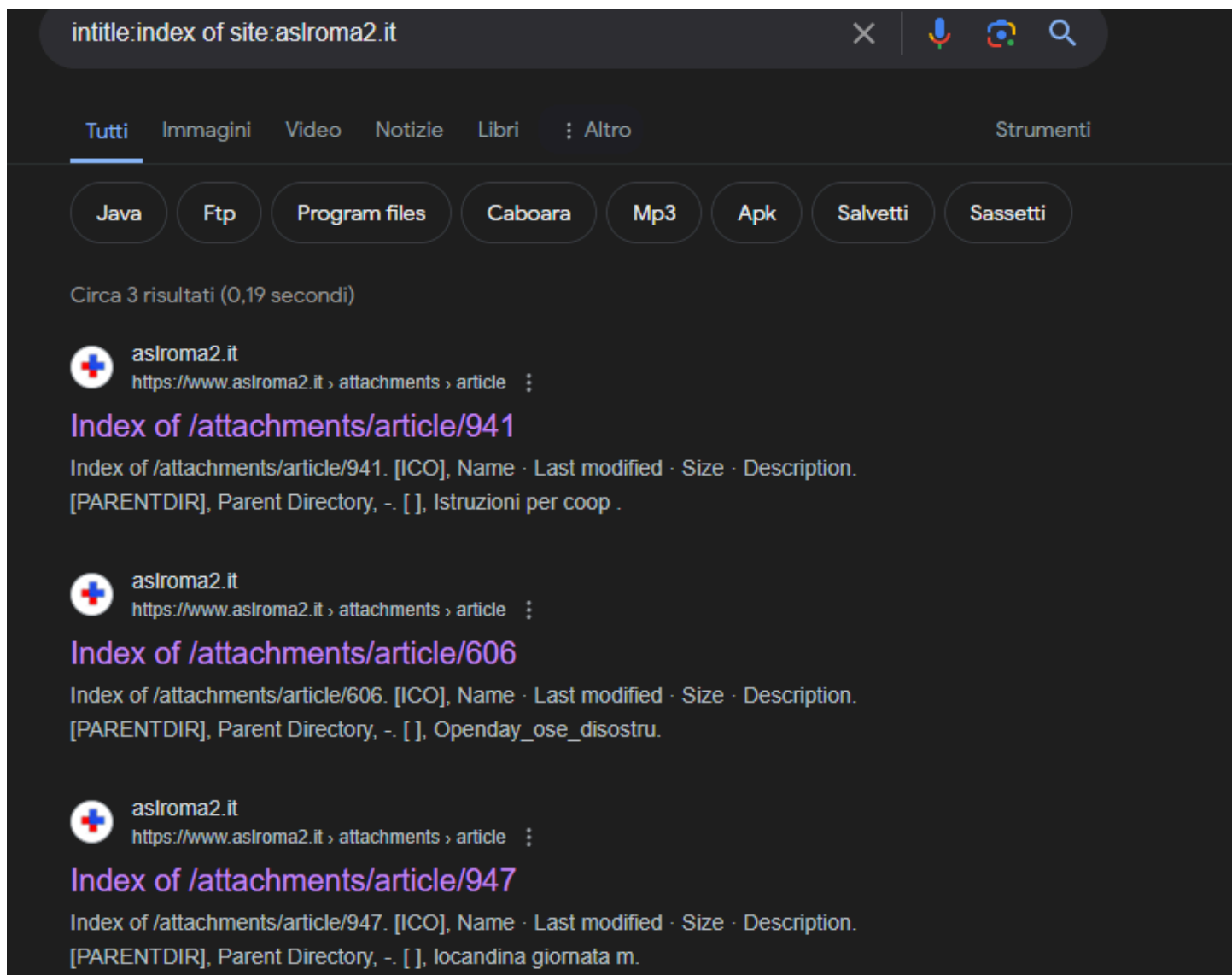
BLSD/ PBLSD/ TRIAGE

NOMINATIVO	INTERNI ESTERNI	REQUISITI SPECIFICI	
		titolo di studio (specializzazione medica, laurea o diploma di scuola superiore inerente all'area di docenza);	
ANGELETTI ALBERTO	I	DIPLOMA	INFERMIERE PROFESSIONALE
ANSELMO CLAUDIA	I	LAUREA	SCIENZE INFERMIERISTICHE
ANTONIOZZI TRANQUILLO	I	SPECIALISTA	IGIENE E MEDICINA PREVENTIVA
ANTONUCCI FABIO	I	LAUREA	INFERMIERE PROFESSIONALE
BALDINI VALENTINA	I	SPECIALISTA	MEDICINA INTERNA
BARLETTA CINZIA	I	SPECIALISTA	MEDICINA INTERNA
BONIFAZI SILVIA	I	DIPLOMA	INFERMIERE PROFESSIONALE
BRUGNOLI ANTONIO	I	SPECIALISTA	ANESTESIA E RIANIMAZIONE
CAPPA MILA	I	SPECIALISTA	ANESTESIA E RIANIMAZIONE
CAPPAROZZA VALENTINA	I	DIPLOMA	INFERMIERE PROFESSIONALE
CASALENA PAOLO ELIO	I	SPECIALISTA	ANESTESIA E RIANIMAZIONE
CASIRAGHI MONICA	I	SPECIALISTA	ANESTESIA, RIANIMAZIONE E TERAPIA DEL DOLORE
CASTALDO ERSILIA	I	SPECIALISTA	MEDICINA INTERNA
CENSI ALESSANDRA	I	LAUREA	SCIENZE INFERMIERISTICHE
COLTELLARO ANTONIO	I	LAUREA	SCIENZE INFERMIERISTICHE
COZZANI VALERIA	I	SPECIALISTA	ANESTESIA, RIANIMAZIONE E TERAPIA DEL DOLORE
CRESCENTE ANTONIO	I	DIPLOMA	INFERMIERE PROFESSIONALE
CRESCIMBENI PATRIZIA	I	LAUREA	SCIENZE INFERMIERISTICHE/OSTETRICHE
CRUCIANI GIANLUCA	I	LAUREA	SCIENZE INFERMIERISTICHE/OSTETRICHE
D'ANGELO GIUSEPPE SALVATORE	I	SPECIALISTA	ANESTESIA E RIANIMAZIONE
DANIELE PAOLO	I	SPECIALISTA	MEDICINA INTERNA
D'ANIELLO GENOVEFFA	I	DIPLOMA	INFERMIERE PROFESSIONALE
DE TOMMASI SEBASTIAN	I	LAUREA	SCIENZE INFERMIERISTICHE/OSTETRICHE
DEL SIGNORE STEFANO	I	SPECIALISTA	ORTOPEDIA E TRAUMATOLOGIA
D'ELIA FRANCESCA	I	LAUREA	SCIENZE INFERMIERISTICHE ED OSTETRICHE
DELLA CAMERA TIZIANA	I	DIPLOMA	INFERMIERE PROFESSIONALE
D'ERRICO ROSA RITA	I	SPECIALISTA	ANESTESIA E RIANIMAZIONE
DI FAZIO FABIO	I	SPECIALISTA	MEDICINA INTERNA

Proviamo ad effettuare qualche altra ricerca.

A questo punto ci interessa provare anche il Google Dork “index of”.

-intitle:index of site:aslroma2.it



Con questa ricerca otteniamo la visibilità di diversi file inseriti sul sito, ma che non dovrebbero essere accessibili pubblicamente. Un esempio si trova nell'immagine sottostante, che mostra una comunicazione interna della ASL alle società e cooperative territoriali.



UOC DIREZIONE AMMINISTRATIVA TERRITORIALE

Ufficio Protezione dei Dati Personali (Privacy)

Dott.ssa Roberta Taurino

Via Monza, 2 - 00182 - Tel.06/51007354

PEC: direzione.amministrativa.territorio@pec.aslroma2.it

E-mail: amministrativa.territoriale@aslroma2.it

Segreteria Tel. 06/51004769-5584

Prot. n. **ASL ROMA 2**
U.O.C. DIREZIONE AMMINISTRATIVA TERRITORIALE
Prot. n. INTELCON (documento lettera formale)
0030383/2023
15/02/2023 07:58:21

Alle Associazioni/Cooperative/
Organizzazioni/Società di trasporto utenti residenti
nel territorio dell'Asl Roma 2 sottoposti a
trattamento dialitico

Oggetto: DCA U00441 del 22.12.2014 avente ad oggetto "Disposizioni normative in materia di nefropatie e dialisi, di contributi per spese di trasporto e prestazioni dialitiche".

Ai sensi del Decreto del Commissario ad Acta meglio evidenziato in epigrafe, "le aziende usl sono tenute ad istituire un elenco delle organizzazioni che operano sul territorio e a vigilare che i servizi di trasporto siano effettuati mediante automezzi adeguati, collaudati e condotti da autisti idonei".

Tutte le Associazioni/Cooperative/Organizzazioni/Società interessate ad effettuare attività di trasporto di pazienti nefropatici nel territorio dell'Asl Roma 2, sono invitate entro e non oltre il **31.03.2023** a produrre la documentazione richiesta dal DCA U00441/2014.

I Legali Rappresentanti delle Associazioni/Cooperative/Organizzazioni/Società dovranno, altresì, sottoscrivere, a pena di esclusione, la "Dichiarazione di presa visione e accettazione del Regolamento recante modalità organizzative per l'espletamento del servizio di trasporto, a cura delle Associazioni/Cooperative/Organizzazioni/Società autorizzate ai sensi del DCA U00441/2014, degli utenti residenti nel territorio della Asl Roma 2 sottoposti a trattamento dialitico". Il Regolamento con l'allegata dichiarazione è consultabile e reperibile sul sito internet aziendale www.aslroma2.it nella sezione "Contributi e Rimborsi" (muovendo dalla Home page cliccare su "Servizi" e successivamente accedere all'Area "Contributi e Rimborsi").

La documentazione può essere trasmessa:































- in formato digitale tramite PEC all'indirizzo protocollo.generale@pec.aslroma2.it;
- in formato cartaceo, tramite posta ordinaria o consegna a mano presso gli Uffici della UOC Direzione Amministrativa Territoriale Via Monza n. 2 00182 Roma nei seguenti orari: da lunedì a venerdì dalle ore 08,00 alle ore 13,00.

Distinti saluti.

Il Direttore
U.O.C. Direzione Amministrativa Territoriale
Dott.ssa Roberta Taurino

Inoltre è possibile risalire fino alla parent directory di questa sezione del sito, la quale mostra altri diversi articoli.

Index of /attachments/article

Name	Last modified	Size	Description
<hr/>			
 Parent Directory		-	
 238/	2016-09-01 15:30	-	
 239/	2016-09-01 15:34	-	
 228/	2016-09-01 16:38	-	
 241/	2016-09-09 13:24	-	
 229/	2016-09-09 13:53	-	
 230/	2016-09-09 13:59	-	
 242/	2016-09-13 11:29	-	
 243/	2016-09-19 17:03	-	
 221/	2016-09-29 12:57	-	
 248/	2016-09-30 10:42	-	
 249/	2016-10-03 17:36	-	
 236/	2016-10-06 16:03	-	
 252/	2016-10-06 18:04	-	
 105/	2016-10-12 15:47	-	
 128/	2016-10-21 14:45	-	
 108/	2016-11-10 11:08	-	
 122/	2016-11-15 14:00	-	
 246/	2016-11-23 10:22	-	
 183/	2016-12-01 14:04	-	
 267/	2016-12-14 10:19	-	
 177/	2016-12-14 10:39	-	
 205/	2017-01-03 18:52	-	
 206/	2017-01-03 18:53	-	
 270/	2017-01-16 13:34	-	
 191/	2017-01-20 14:18	-	
 166/	2017-01-31 17:49	-	
 285/	2017-02-03 08:57	-	
 287/	2017-02-13 13:13	-	
 289/	2017-02-23 14:49	-	

VULNERABILITA' INDIVIDUATE O POTENZIALI TALI

1. La prima vulnerabilità che abbiamo potuto notare in questa piccola ricerca è stato il file di testo robots.txt. Esso infatti fornisce informazioni utili per comprendere le directory più sensibili, lasciando così indicazioni rilevanti ad un potenziale attaccante a caccia di dati sensibili.
2. La seconda vulnerabilità che abbiamo rilevato è quella riguardante gli articoli pubblicati nel sito della ASL Roma 2. Vi sono comunicazioni interne e pubblicazioni che potrebbero fornire materiale per attacchi su diversi fronti, non solo verso la ASL, ma anche verso i partner, impiegati e aziende collaboratrici.

RIMEDIO

1. Se una determinata risorsa o directory non è accessibile da remoto, non deve essere posizionata su una macchina esposta a Internet oppure l'accesso deve essere limitato tramite le regole di configurazione del server web . Rimuovere tutti i collegamenti che puntano ad esso da qualsiasi altra pagina Web non è sufficiente.

Possiamo anche evitare di suggerire all'aggressore quali sarebbero gli obiettivi più preziosi **non enumerando le risorse a cui i crawler non dovrebbero accedere** . Supponiamo di non consentire generalmente la scansione (indicando *Disallow: /* nel file robots) ma di consentire l'accesso a singole risorse o directory (utilizzando il tasto *Consenti*). In tal caso non menzioneremo esplicitamente i percorsi più sensibili. Possiamo anche limitare del tutto l'utilizzo del file robots includendo le indicazioni rilevanti per i crawler all'interno dell'intestazione HTML di una pagina, con:

```
<meta name="robots" content="noindex" />
```

- 2- Per evitare che il file robots.txt possa risultare utile a degli utenti malintenzionati, si potrebbe modificare il file per disabilitare l'indicizzazione delle directory che desideri mantenere private. Per fare ciò si possono aggiungere istruzioni nel file robots.txt per impedire ai motori di ricerca di indicizzare determinate directory o tutto il sito, se necessario.

Se il sito utilizza Apache come server web, con il file .htaccess si può impedire la visualizzazione dell'elenco di file all'interno delle directory senza un file index.html o index.php.

Aggiungendo ad ogni directory del sito un file index.html o index.php si impedirà al server web di elencare i file contenuti nella directory quando non è presente un file index predefinito.

Le directory sensibili si possono inoltre proteggere con delle password, o impostando nel modo giusto le autorizzazioni dei file.