

Esercitazione W10D1

Google Hacking

Fabio Benevento - 09/01/2024

Traccia

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

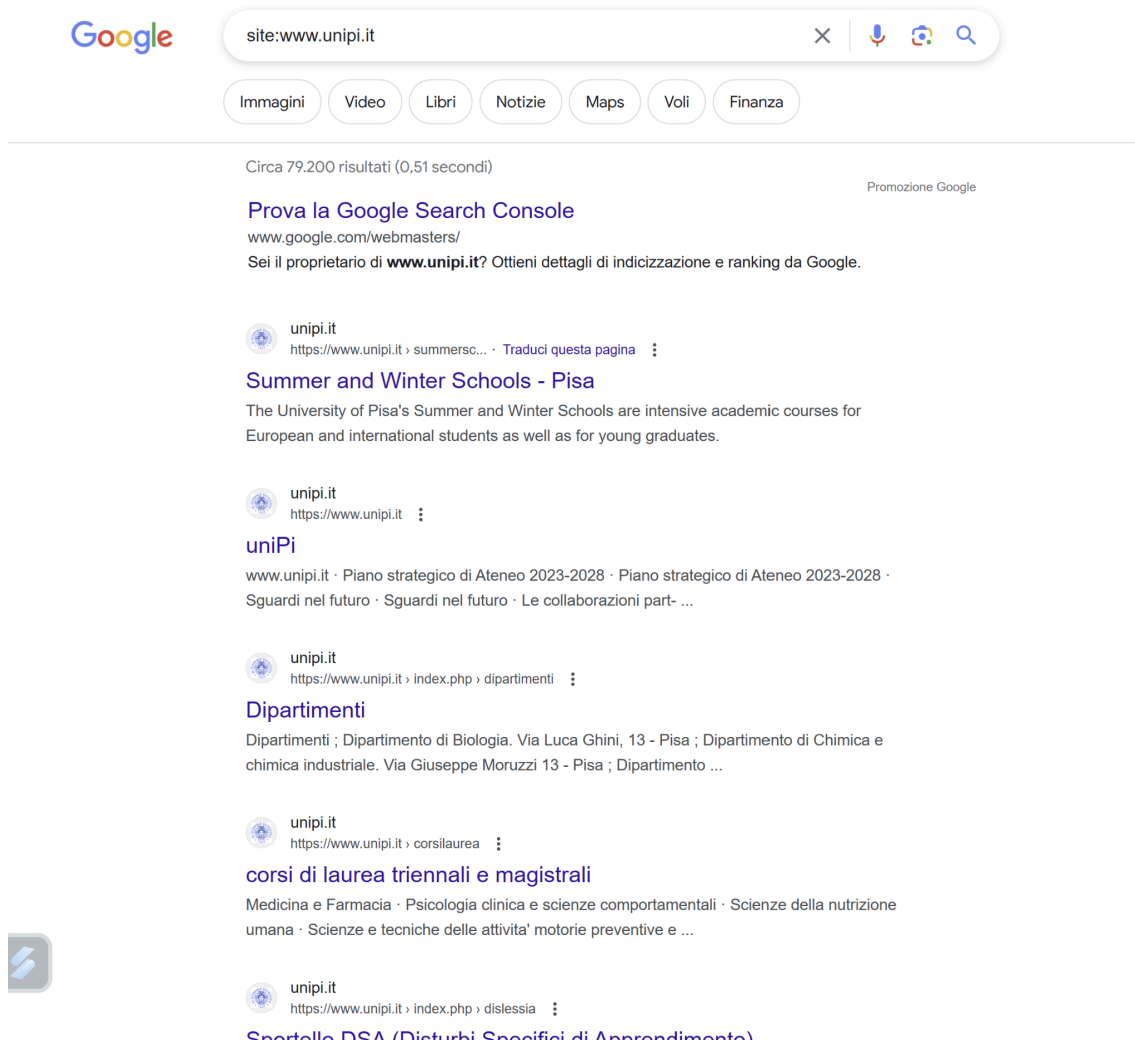
1. Aprire un browser web e accedere a Google.
2. Utilizzare i seguenti comandi di Google Hacking per raccogliere informazioni sul sito web:
 - "site:nome-del-sito.com" per visualizzare tutte le pagine indicizzate di quel sito.
 - "inurl:nome-del-sito.com" per visualizzare tutte le pagine con l'URL contenente 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.

Implementazione

Per esercitazione ho raccolto informazioni relativamente al sito target (offuscato volutamente)

- Ricerca site:[target]

Tramite la ricerca site:[target] ho ricercato tutte le pagine indicizzate del sito target



The screenshot shows a Google search interface with the query 'site:www.unipi.it' entered in the search bar. Below the search bar, there are tabs for 'Immagini', 'Video', 'Libri', 'Notizie', 'Maps', 'Voli', and 'Finanza'. The search results are displayed below the tabs, showing approximately 79,200 results in 0.51 seconds. The first result is a link to 'Prova la Google Search Console' with the URL 'www.google.com/webmasters/'. The second result is a link to 'unipi.it' with the URL 'https://www.unipi.it > summersc...'. The third result is a link to 'Summer and Winter Schools - Pisa' with the URL 'https://www.unipi.it'. The fourth result is a link to 'unipi' with the URL 'https://www.unipi.it'. The fifth result is a link to 'Dipartimenti' with the URL 'https://www.unipi.it > index.php > dipartimenti'. The sixth result is a link to 'corsi di laurea triennali e magistrali' with the URL 'https://www.unipi.it > corsilaurea'. The seventh result is a link to 'Sportello DSA (Disturbi Specifici di Apprendimento)' with the URL 'https://www.unipi.it > index.php > dislessia'.

Google

site:www.unipi.it

Immagini Video Libri Notizie Maps Voli Finanza

Circa 79.200 risultati (0,51 secondi)

Promozione Google

[Prova la Google Search Console](#)
www.google.com/webmasters/
Sei il proprietario di **www.unipi.it**? Ottieni dettagli di indicizzazione e ranking da Google.

[unipi.it](#)
https://www.unipi.it > summersc... · Traduci questa pagina

[Summer and Winter Schools - Pisa](#)
The University of Pisa's Summer and Winter Schools are intensive academic courses for European and international students as well as for young graduates.

[unipi.it](#)
https://www.unipi.it

[unipi](#)
www.unipi.it · Piano strategico di Ateneo 2023-2028 · Piano strategico di Ateneo 2023-2028 · Sguardi nel futuro · Sguardi nel futuro · Le collaborazioni part- ...

[unipi.it](#)
https://www.unipi.it > index.php > dipartimenti

[Dipartimenti](#)
Dipartimenti ; Dipartimento di Biologia. Via Luca Ghini, 13 - Pisa ; Dipartimento di Chimica e chimica industriale. Via Giuseppe Moruzzi 13 - Pisa ; Dipartimento ...

[unipi.it](#)
https://www.unipi.it > corsilaurea

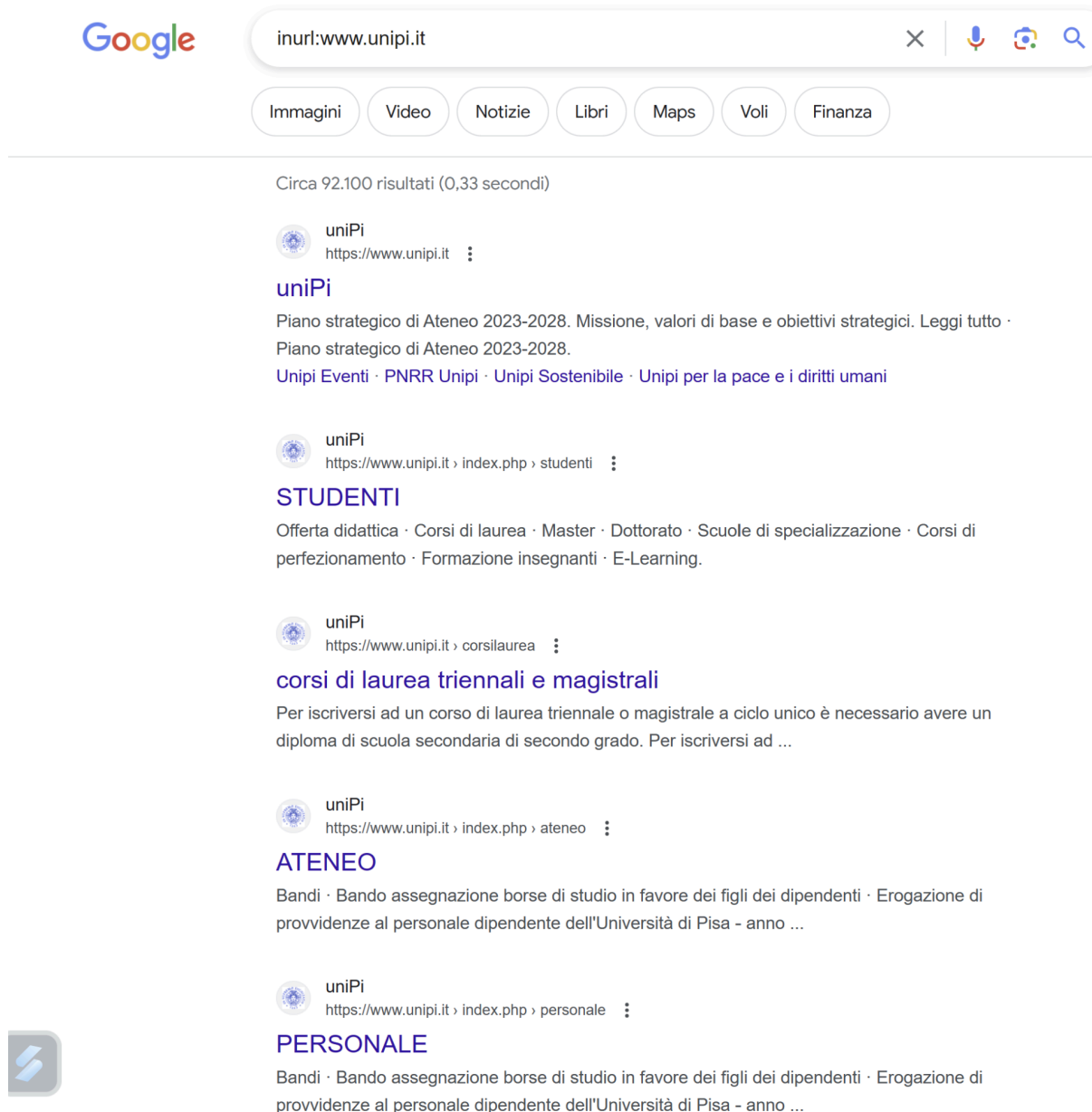
[corsi di laurea triennali e magistrali](#)
Medicina e Farmacia · Psicologia clinica e scienze comportamentali · Scienze della nutrizione umana · Scienze e tecniche delle attività motorie preventive e ...

[unipi.it](#)
https://www.unipi.it > index.php > dislessia

[Sportello DSA \(Disturbi Specifici di Apprendimento\)](#)

- Ricerca inurl:[target]

Tramite la ricerca inurl:[target] ho ricercato tutte le pagine contenenti nell'url l'indirizzo target



The screenshot shows a Google search interface. The search bar contains the query 'inurl:www.unipi.it'. Below the search bar are tabs for 'Immagini', 'Video', 'Notizie', 'Libri', 'Maps', 'Voli', and 'Finanza'. The search results show 'Circa 92.100 risultati (0,33 secondi)'. The first result is for 'uniPi' with the URL 'https://www.unipi.it'. Below this is a link to 'STUDENTI' with a description of the university's strategic plan and links to 'Unipi Eventi', 'PNRR Unipi', 'Unipi Sostenibile', and 'Unipi per la pace e i diritti umani'. The second result is also for 'uniPi' with the URL 'https://www.unipi.it > index.php > studenti', followed by a link to 'corsi di laurea triennali e magistrali' with a description of the admission process. The third result is for 'uniPi' with the URL 'https://www.unipi.it > corsilaurea', followed by a link to 'ATENEEO' with a description of the university's strategic plan and links to 'Bando assegnazione borse di studio' and 'Erogazione di provvidenze al personale dipendente dell'Università di Pisa - anno ...'. The fourth result is for 'uniPi' with the URL 'https://www.unipi.it > index.php > personale', followed by a link to 'PERSONALE' with a description of the university's strategic plan and links to 'Bando assegnazione borse di studio' and 'Erogazione di provvidenze al personale dipendente dell'Università di Pisa - anno ...'.

Google

inurl:www.unipi.it

Immagini Video Notizie Libri Maps Voli Finanza

Circa 92.100 risultati (0,33 secondi)

uniPi
https://www.unipi.it

uniPi

Piano strategico di Ateneo 2023-2028. Missione, valori di base e obiettivi strategici. Leggi tutto · Piano strategico di Ateneo 2023-2028.

[Unipi Eventi](#) · [PNRR Unipi](#) · [Unipi Sostenibile](#) · [Unipi per la pace e i diritti umani](#)

uniPi
https://www.unipi.it > index.php > studenti

STUDENTI

Offerta didattica · Corsi di laurea · Master · Dottorato · Scuole di specializzazione · Corsi di perfezionamento · Formazione insegnanti · E-Learning.

uniPi
https://www.unipi.it > corsilaurea

corsi di laurea triennali e magistrali

Per iscriversi ad un corso di laurea triennale o magistrale a ciclo unico è necessario avere un diploma di scuola secondaria di secondo grado. Per iscriversi ad ...

uniPi
https://www.unipi.it > index.php > ateneo

ATENEEO

Bandi · Bando assegnazione borse di studio in favore dei figli dei dipendenti · Erogazione di provvidenze al personale dipendente dell'Università di Pisa - anno ...


uniPi
https://www.unipi.it > index.php > personale

PERSONALE

Bandi · Bando assegnazione borse di studio in favore dei figli dei dipendenti · Erogazione di provvidenze al personale dipendente dell'Università di Pisa - anno ...

- Ricerca intext:'matricola' site:[target]

Tramite la ricerca [intext:'matricola' site:\[target\]](#) ho ricercato tutte le pagine indicizzate del sito target contenenti la parola matricola

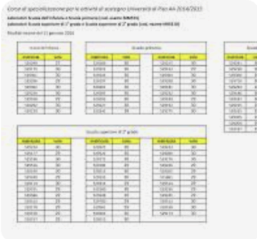


intext:'matricola' site:www.unipi.it


ImmaginiVideoNotizieIn ingleseEnpalsFantozziSignificatoAbbreviazioneNumero

Circa 898 risultati (0,38 secondi)


Immagini :



Corso di specializzazione per...
uniPI




Matricola 000000
uniPI



Matricola 000000
uniPI

Feedback


6 altre immagini



uniPI.it
<https://www.unipi.it/item/download/PDF>

matricola corso Riconoscimento Area Disciplinare ...


matricola corso. Riconoscimento Area Disciplinare. Riconoscimento Tirocini. Riconoscimento Area. Comune. 500093. A051. 528526. A060. Il dottorato non viene ...



uniPI.it
<https://www.unipi.it/servizi-di-segreteria/item/14...>

Tessera "Studente della Toscana": rilascio e duplicato

Per gli immatricolati alla laurea magistrale provenienti da altri atenei, oppure provenienti da Pisa con attivazione di nuova **matricola**: non deve essere fatta ...

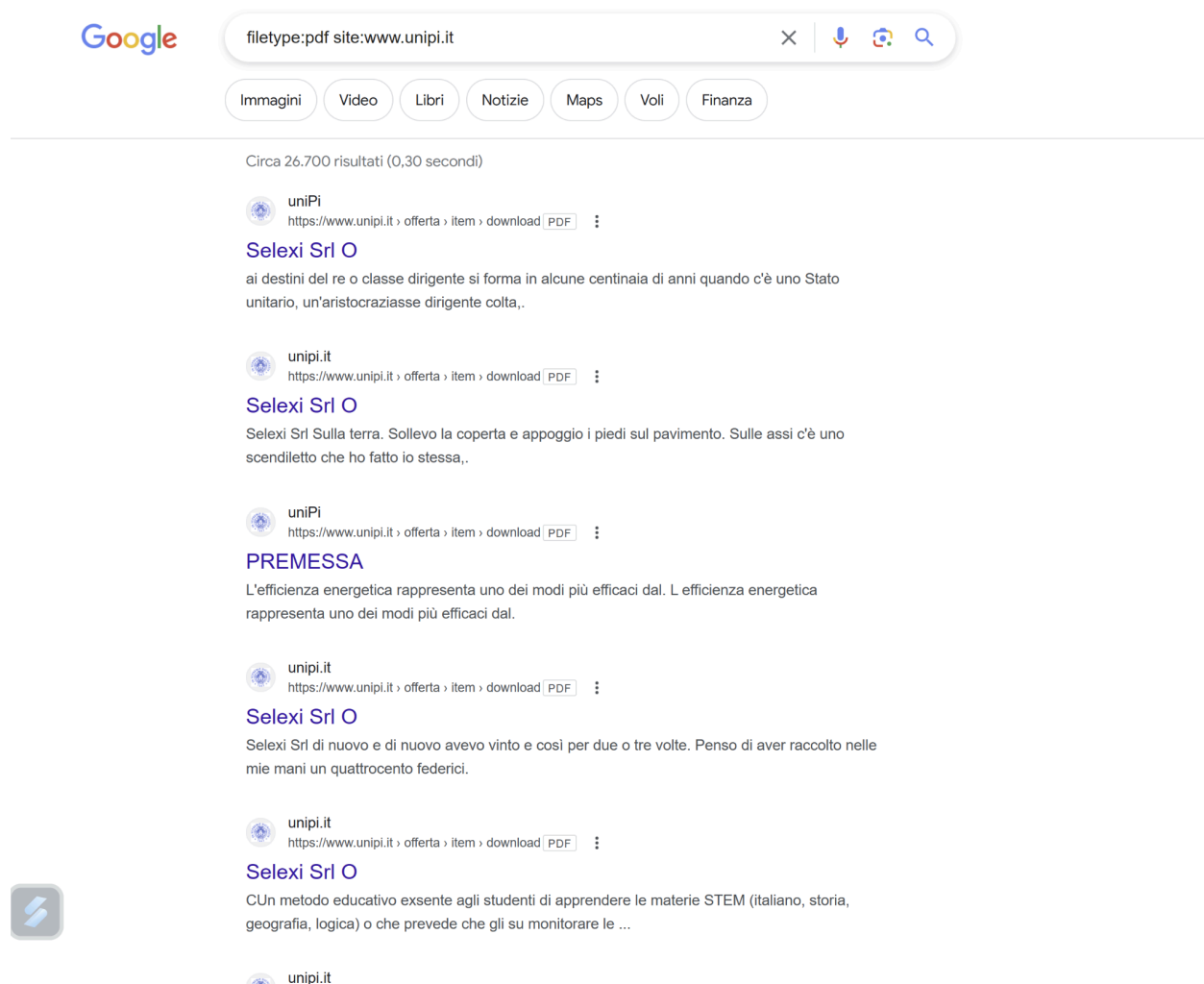


uniPI.it
<https://www.unipi.it/matricola>

Matricolandosi 2007


- Ricerca filetype:pdf site:[target]

Tramite la ricerca `filetype:pdf site:[target]` ho ricercato tutti i documenti di tipo pdf indicizzati del sito target alla ricerca di documenti sensibili



- Analisi e conclusioni

Il sito espone diverse informazioni sensibili. Infatti soprattutto con la ricerca per parola chiave sono usciti risultati con documenti esponenti informazioni come nome cognome, data di nascita, reddito.



Queste informazioni dovrebbero naturalmente essere il più possibile protette e non esposte magari mediante l'utilizzo di hash per la condivisione del link invece che dell'URL completo.

Per maggiori informazioni fare riferimento alla versione non offuscata