

# Esercitazione WEEK 10/D1

## Google Hacking

Ettore Farris - 09/01/2024

### 1) Descrizione sintetica dell'esercitazione

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.

## 2) Svolgimento

Il sito internet preso in considerazione è quello di una PMI che si occupa di riparazioni MacBook: **"https://doslabelectronics.com/"**.

### - Comandi Google Hacking:

site:doslabelectronics.com



site:doslabelectronics.com



Immagini

Video

Libri

Notizie

Maps

Voli

Finanza

Circa 94 risultati (0,18 secondi)

Promozione Google

### [Prova la Google Search Console](#)

[www.google.com/webmasters/](https://www.google.com/webmasters/)

Sei il proprietario di **doslabelectronics.com**? Ottieni dettagli di indicizzazione e ranking da Google.



[doslabelectronics.com](https://doslabelectronics.com)

<https://doslabelectronics.com> · Traduci questa pagina

### [DeeLab Electronics: Home](#)

Welcome to DeeLab Electronics! · DeMux · Hardware Mods · Mail-In Repair · Obsolete Media Recovery Service. Learn more about our obsolete media recovery service ...



[doslabelectronics.com](https://doslabelectronics.com)

<https://doslabelectronics.com> > ... · Traduci questa pagina

### [DeMux: A permanent fix for the MacBook Pro 2011 GPU](#)

DeMux. Firmware to disable the defective dedicated AMD GPU on 2011 MacBook Pro models. A permanent solution for radeongate.



[doslabelectronics.com](https://doslabelectronics.com)

<https://doslabelectronics.com> > ... · Traduci questa pagina

### [DyingLight](#)

Introduction. DyingLight is compatible with any operating system that will run on your MacBook Pro, including Windows, various Linux distros, and of course, Mac ...

inurl:de[REDACTED]electronics.com



inurl:de[REDACTED]electronics.com



Immagini

Video

Notizie

Maps

Libri

Voli

Finanza

Circa 76 risultati (0,21 secondi)



DeLab Electronics

[https://de\[REDACTED\]electronics.com](https://de[REDACTED]electronics.com) · Traduci questa pagina

## DeLab Electronics: Home

Below you will find our current solutions, services and products. DeMux. A firmware designed to disable the defective dedicated AMD ...

[Hardware](#) · [Repair](#) · [Shop](#) · [DeMux](#)



DeLab Electronics

[https://de\[REDACTED\]electronics.com](https://de[REDACTED]electronics.com) > s... · Traduci questa pagina

## Shop

Available in 128GB and 256GB options. Comes with 3D printed case, DeLab labeling, and serial number. 128GB \$60 + shipping. 256GB \$75 + shipping. [Contact Us](#) » ...



DeLab Electronics

[https://de\[REDACTED\]electronics.com](https://de[REDACTED]electronics.com) > ... · Traduci questa pagina

## DeMux: A permanent fix for the MacBook Pro 2011 GPU

DeMux · Firmware to disable the defective dedicated AMD GPU on 2011 MacBook Pro models. A permanent solution for radeongate. · NOW WITH NATIVE BACKLIGHT CONTROL!

*intext:"index of" site:delelabelelectronics.com*

Ricerchiamo nel sito internet tutti i risultati che contengono nel testo la stringa "index of" per ricercare files e directories che possono contenere informazioni rilevanti. Ho trovato dei risultati interessanti che vedremo nel dettaglio nella sezione successiva:



intext:"index of" site:delelabelelectronics.com



Immagini

Video

Java

Ftp

Program files

Caboara

Mp3

Apk

Salvetti

Circa 3 risultati (0,16 secondi)



delelabelelectronics.com

<https://delelabelelectronics.com/files/> · Traduci questa pagina

### Index of /files

Index of /files. [ICO], Name, Size, Description. [PARENTDIR], Parent Directory, -. [], 7f3afa35-1150-477e-a70a-cab232950ee9-wpa.png, 201.2K. [], 527c71b6-2bd8 ...



delelabelelectronics.com

<https://delelabelelectronics.com/control.aspx> · Traduci questa pagina

### Index of /files

Index of /files. [ICO], Name, Size, Description. [PARENTDIR], Parent Directory, -. [], 59059918-5438-436f-bd36-246ef0396059-control.aspx, 1.3K. [], 7f3afa35- ...



delelabelelectronics.com

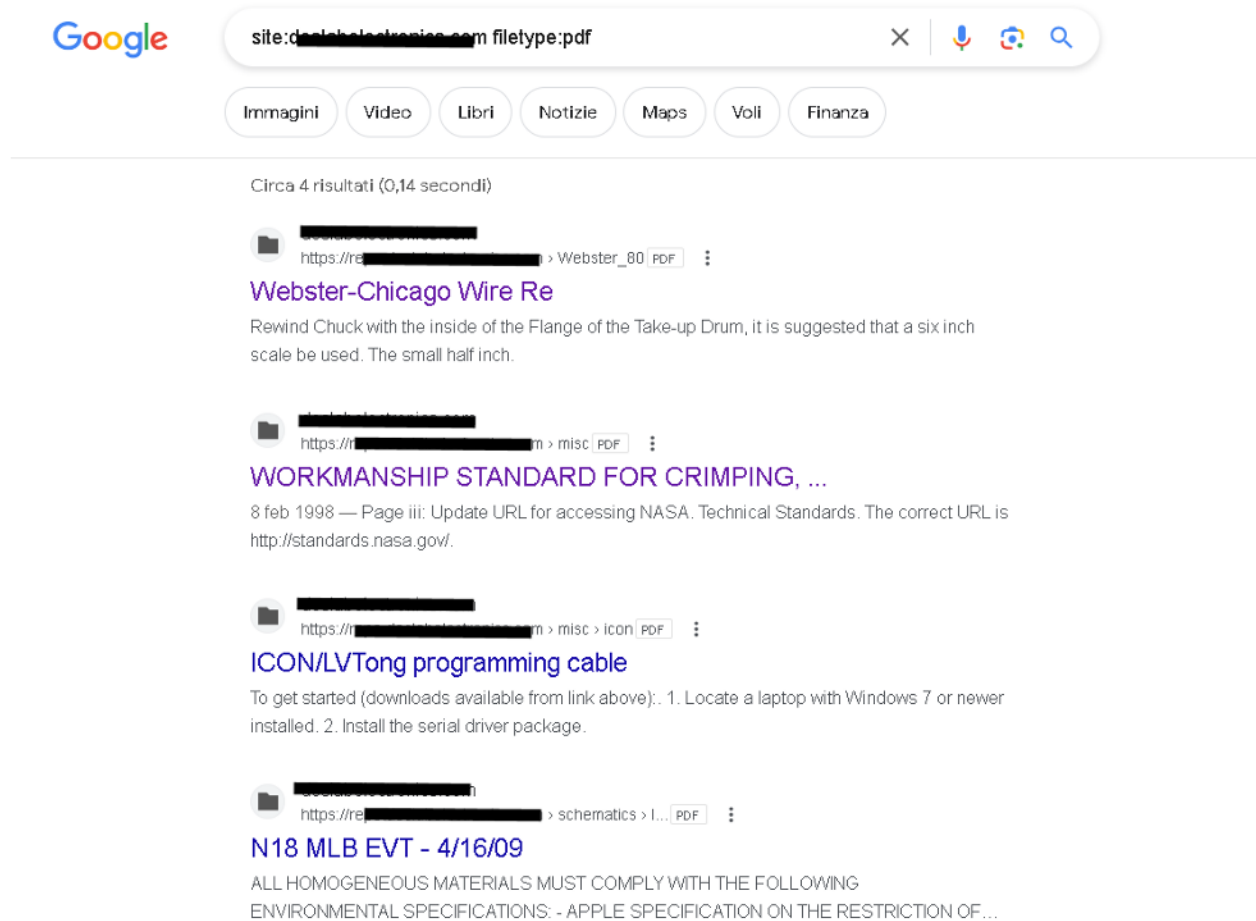
<https://delelabelelectronics.com/uploads/> · Traduci questa pagina

### Index of /uploads

Index of /uploads. [ICO], Name, Size, Description. [PARENTDIR], Parent Directory, -. [], backup, -. [], config.env, 294. [], files, -. [], phpinfo.php, 18.

site:deslabelectronica.com filetype:pdf

Ricerca per files .pdf. La ricerca mostra alcuni risultati, ma di scarso interesse.




Google

site:deslabelectronica.com filetype:pdf


Immagini Video Libri Notizie Maps Voli Finanza

Circa 4 risultati (0,14 secondi)

 [https://re\[redacted\]>Webster\\_80](https://re[redacted]>Webster_80) PDF


**Webster-Chicago Wire Re**

Rewind Chuck with the inside of the Flange of the Take-up Drum, it is suggested that a six inch scale be used. The small half inch.

 [https://re\[redacted\]>misc](https://re[redacted]>misc) PDF


**WORKMANSHIP STANDARD FOR CRIMPING, ...**

8 feb 1998 — Page iii: Update URL for accessing NASA. Technical Standards. The correct URL is <http://standards.nasa.gov/>.

 [https://re\[redacted\]>misc>icon](https://re[redacted]>misc>icon) PDF

**ICON/LVTong programming cable**

To get started (downloads available from link above):. 1. Locate a laptop with Windows 7 or newer installed. 2. Install the serial driver package.

 [https://re\[redacted\]>schematics>I...](https://re[redacted]>schematics>I...) PDF







**N18 MLB EVT - 4/16/09**

ALL HOMOGENEOUS MATERIALS MUST COMPLY WITH THE FOLLOWING ENVIRONMENTAL SPECIFICATIONS: - APPLE SPECIFICATION ON THE RESTRICTION OF...

## - Informazioni sensibili trovate

Con il comando *intext:"index of" site:doxlabalelectronica.com* ho trovato un risultato interessante che mostra un listing di files e directories.

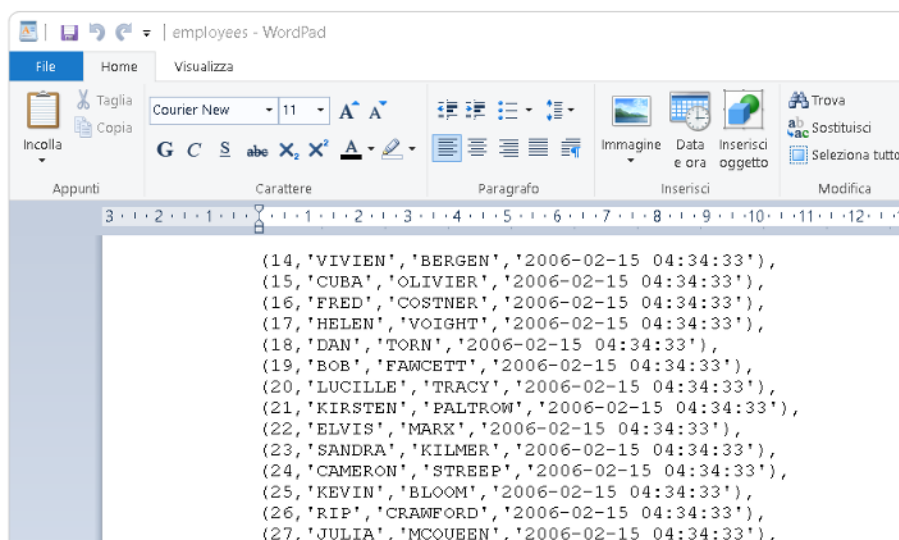
# Index of /uploads

Name	Size	Description
 <a href="#">Parent Directory</a>	-	
 <a href="#">backup</a>	-	
 <a href="#">config.env</a>	294	
 <a href="#">files</a>	-	
 <a href="#">phpinfo.php</a>	18	
 <a href="#">upload.php</a>	1K	

La cartella di backup contiene dei files SQL con dei files privati su

## Index of /backup

Name	Size	Description
 <a href="#">Parent Directory</a>	-	
 <a href="#">employees.sql</a>	3.2M	
 <a href="#">public_html.zip</a>	43.8M	



employees - WordPad

Visualizza

Courier New 11

Taglia Copia Incolla

Appunti

Carattere Paragrafo

Immagine Data e ora Inserisci oggetto

Trova Sostituisci Seleziona tutto

```
{14,'VIVIEN','BERGEN','2006-02-15 04:34:33'},
{15,'CUBA','OLIVIER','2006-02-15 04:34:33'},
{16,'FRED','COSTNER','2006-02-15 04:34:33'},
{17,'HELEN','VOIGHT','2006-02-15 04:34:33'},
{18,'DAN','TORN','2006-02-15 04:34:33'},
{19,'BOB','FAMCETT','2006-02-15 04:34:33'},
{20,'LUCILLE','TRACY','2006-02-15 04:34:33'},
{21,'KIRSTEN','PALTROW','2006-02-15 04:34:33'},
{22,'ELVIS','MARK','2006-02-15 04:34:33'},
{23,'SANDRA','KILMER','2006-02-15 04:34:33'},
{24,'CAMERON','STREEP','2006-02-15 04:34:33'},
{25,'KEVIN','BLOOM','2006-02-15 04:34:33'},
{26,'RIP','CRAWFORD','2006-02-15 04:34:33'},
{27,'JULIA','MCQUEEN','2006-02-15 04:34:33'},
```

Il file config.env contiene delle credenziali per accedere alla mail noreply dell'azienda.

```
[app]
id = >Q71...1-7LW4...Mh...HP...7A==

[aws]
aws_access_key_id = AKIAKYZDQCEHUS3CIBXR
aws_secret_access_key = Wli5tuh-85QHYA500T:-045Xic-00K6L-4BYU71
region = us-east-2

[email]
smtp = smtp.daslebalactronics.com
address = noreply@daslebalactronics.com
password = m20P...Y4P657K-M960U...5505...
```