Cybersecurity

Activity File

Activity File: Google Hacking

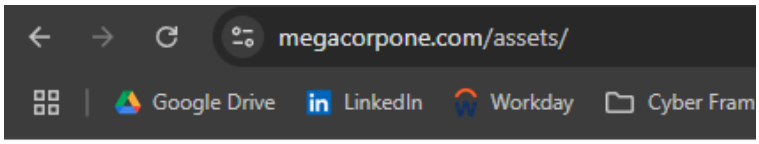
- As a penetration tester for GoodCorp, you must conduct an engagement against the fictional company, MegaCorpOne.com
- Now that you've accepted a contract as a penetration tester and have signed all the legal documentation, you will begin OSINT.
- You will start by using Google hacking to find information about MegaCorpOne.
- Specifically, you will search for usernames, emails, and hidden files.

⚠️ **Reminder:** Don't forget to save your findings, as you will add them to your report on Day 4!

Instructions

1. In a browser, navigate to Google.

2. Using the `site` Google operand, identify the web service name and version. MegaCorpOne's website is megacorpone.com.
   site:megacorpone.com



Index of /assets

Name	Last modified	Size	Description
Parent Directory		-	
css/	2016-08-21 11:21	-	
fonts/	2016-08-21 11:21	-	
img/	2017-10-03 09:08	-	
js/	2016-08-21 11:21	-	

Apache/2.4.62 (Debian) Server at www.megacorpone.com Port 4

3. Using the `intext` and `site` operands, create a list of user names and their email addresses. site:megacorpone.com intext:email

Joe joe@megacorpone.com joe

Mike Carlow mcarlow@megacorpone.com mcarlow

Alan Grofield agrofield@megacorpone.com agrofield

Executive Team

Name: Joe Sheer

Title: CEO
Email: joe@megacorpone.com

Name: Mike Carlow

Title: VP Of Legal
Email: mcarlow@megacorpone.com

Name: Alan Grofield

Title: IT and Security Director
Email: agrofield@megacorpone.com

Contact Our Departments

Department: Human Resources

Email: hr@megacorpone.com

Department: Sales

Email: sales@megacorpone.com

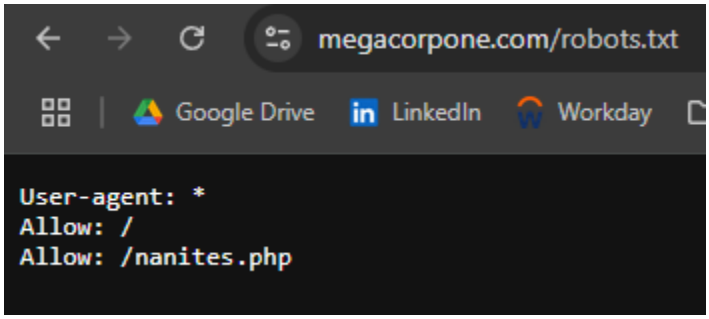
Department: Shipping

Email: shipping@megacorpone.com

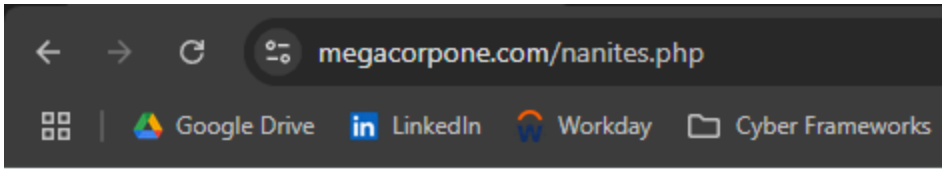
Bonus

By searching for specific file types using the `ext` operand, find a hidden file.

site:megacorpone.com ext:txt



site:megacorpone.com ext:php



Current Nanite Levels (ppm) in Rachel, NV

2.1
2.8
0.9
1
2.1
1.6
1.6
2.5
1.3
0.2
1.7
0.8
1.1
2.5
1
2.6
0.6
2
1.7
0.1

Last sample collected: 2025-04-13