

Lab - Advanced Searches

Objectives

Use Google Advanced Search to perform passive reconnaissance.

- Part 1: Google Advanced Searches (Dorking)
- Part 2: The Google Hacking Database
- Part 3: The Wayback Machine

Background / Scenario

The first step a hacker takes is to learn as much information about a target as possible. The more the attackers know about the target, the better they can hack it with other hacking techniques. Using Advanced Google searches and parsing through archived internet sites are two popular methods of passive reconnaissance. They help inform ethical hackers about a client's vulnerabilities and pave the way for exploitation activities if they are part of the scope of the test.

Through an advanced Google search, the hacker is hoping to find information that has been made public by accident. For example, someone may have accidentally exposed passwords, left a webcam open to the internet, or revealed other useful information. The hacker will search using specific key words and Google search operators to try and find what they are looking for. This is called **Google dorking**. It involves using specific Google search queries to uncover information that was not meant to be publicly available.

The **Wayback Machine web archive** is another useful tool for uncovering potential vulnerabilities. Valuable personal and corporate information can sometimes be gleaned from archived web pages. Using the Wayback machine, a hacker can browse through the history of a website and visit snapshots of the site at various times in the past. This allows the hacker to uncover information no longer available on the live internet that may be useful for further attacks.

Unauthorized access to data, computers, and network systems is a crime in many jurisdictions and often is accompanied by severe consequences, regardless of the perpetrator's motivations. It is the learner's responsibility, as the user of this material, to be cognizant of, and compliant with, computer use and privacy laws.

Required Resources

- Computer or mobile device with internet access

Instructions

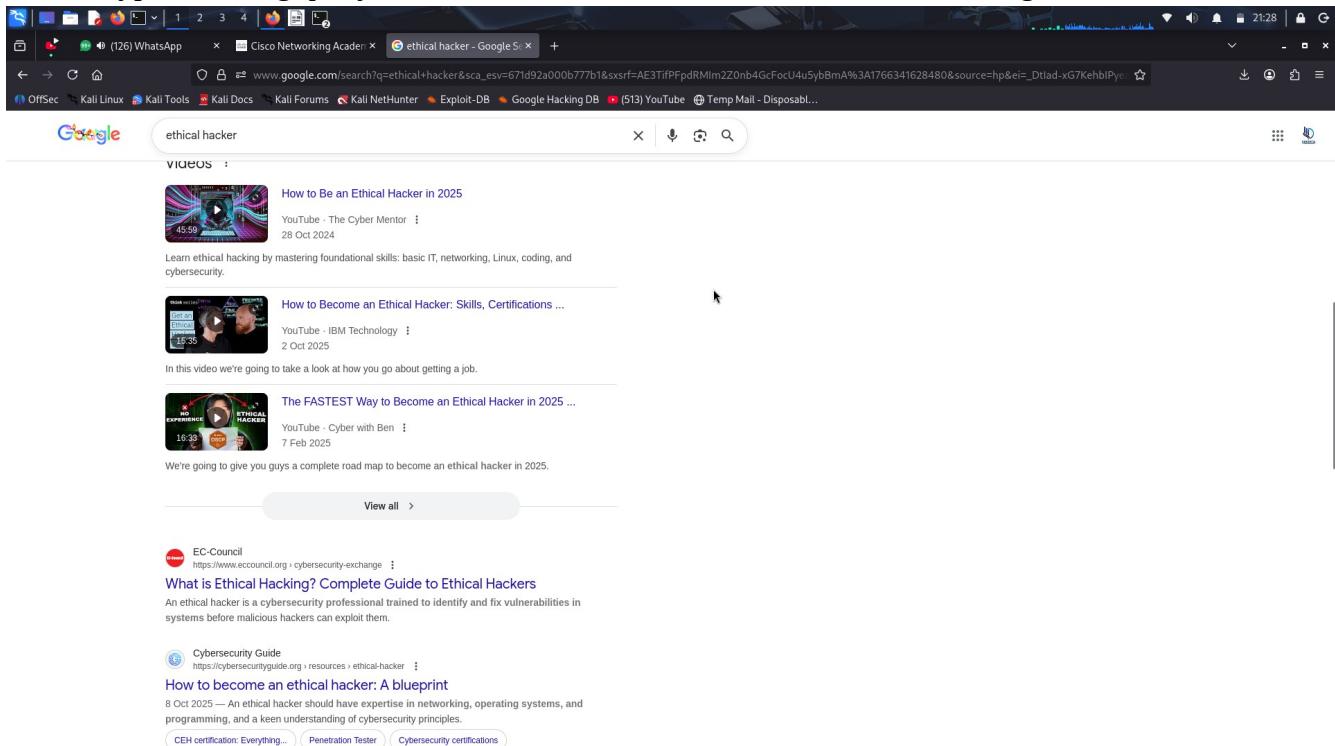
Part 1: Google Advanced Searches (Dorking)

For most people, Google is a tool for searching for text, images, videos, and news on the internet by using simple string queries. However, for some, Google is a powerful and useful hacking tool and can be used for performing passive reconnaissance by using advanced search operators. The practice of using advanced Google search operators to find information and vulnerable servers is called **Google dorking or Google hacking**. Google dorking is used by hackers to try to find information that was never intended to be revealed publicly. It is a useful technique for conducting passive reconnaissance in penetration tests.

Note: When performing advanced queries, you may be prompted by Google to prove you are not a robot. If this occurs, as it probably will after several searches, simply complete the captcha and continue.

Step 1: Explore Google dorking.

- Navigate to www.google.com to open the Google search engine.
- Type the string query **ethical hacker** in the search window. Scroll through the results.



- Note the variety of results returned. This is how we typically use Google to perform searches. String queries like this return a lot of results. However, about 90% of the results are not specific to what we are after. To restrict results to only what is desired, such as pages from a single site, specific keywords, or specific file types, Google Advanced Search operators can be used.

- d. There are many Google advanced search operators. Lists of them are available on the internet on sites such as SpyFu. Search the internet for “advanced search operators” to see other source of information, some of which have useful examples.

The table below shows the advanced search operators that are used in this lab.

Operator	Description
allintext:	Restricts results to pages with all query words in the page text.
filetype:	Restricts results to pages of the specified file type (.pdf, .ppt, .doc, etc.)
intitle:	Restricts results to pages with a certain word (or words) in the title.
inurl:	Restricts results to pages with a certain word (or words) in the URL.
site:	Restricts results to pages from the specified domain.

the SCORE function.

Try each of the operators in a Google search. When using advanced search, don't put spaces between the operator and the domain or keywords.

- c. Type **ethical hacker site:pearson.com** in the search window. The syntax is **search term operator:domain**. Scroll through the results.

ethical hacker site:pearson.com

AI Mode All Images Videos News Short videos Forums More Tools

P [pearson.com](https://www.pearson.com/en-au/media)
Certified Ethical Hacker (CEH) Exam Cram - Pearson
CEH Certified Ethical Hacker Exam Cram. Creating a Virus ... CEH Certified Ethical Hacker Exam Cram. CHAPTER 8: Hacking Web Servers and Web Applications ...
20 pages

P [Pearson South Africa](https://za.pearson.com/dam/pearson-south-africa)
Certified Ethical Hacker (CEH) Course - Pearson South Africa
Throughout the CEH course, you will be immersed in a hacker's mind set, evaluating not just logical, but physical security. Certified Ethical Hacker (CEH).
2 pages

P [Pearson South Africa](https://za.pearson.com/dam/pearson-south-africa)
Ethical Hacking and Countermeasures
Ethical Hacking and Countermeasures. Exam 312-50 Certified Ethical Hacker. Course Outline. Page | 1.
Ethical Hacking and Countermeasures Copyright © by EC- ...
51 pages

P [Pearson | India](https://in.pearson.com/india/ppp/programs)
PGP in Ethical Hacking & Cybersecurity - Pearson
The program also prepares learners for industry recognized professional certificates like Certified Ethical Hacker (CEH) and Certified Information Systems ...
11 pages

Images

Type **ethical hacker site:pearson.com filetype:pdf** in the search window. Scroll through the results.

ethical hacker site:pearson.com filetype:pdf

AI Mode All Images Videos News Short videos Forums More Tools

P [pearson.com](https://www.pearson.com/en-au/media)
Certified Ethical Hacker (CEH) Exam Cram - Pearson
Denial of service (DoS) attacks, as the name suggests, are not about breaking into a system but rather about denying legitimate users the.
20 pages

P [Pearson South Africa](https://za.pearson.com/dam/pearson-south-africa)
Certified Ethical Hacker (CEH) Course - Pearson South Africa
Throughout the CEH course, you will be immersed in a hacker's mind set, evaluating not just logical, but physical security. Certified Ethical Hacker (CEH).
2 pages

P [Pearson South Africa](https://za.pearson.com/dam/pearson-south-africa)
Ethical Hacking and Countermeasures
Module 01: Introduction to Ethical Hacking. » Internet is Integral Part of Business and Personal Life - What Happens Online in 0. Seconds.
51 pages

P [Pearson | India](https://in.pearson.com/india/ppp/programs)
PGP in Ethical Hacking & Cybersecurity - Pearson
It teaches industry relevant concepts and skills to protect data, information and hardware assets from cyberthreats in the form of ransomware, malware, phishing ...
11 pages

P [pearson.com](https://www.pearson.com/one-dot-com/files)
Pearson IT Cybersecurity Curriculum (ITCC)
Penetration testing or Ethical Hacking is the process of applying a variety of tools and hacking

Type **ethical hacker intitle:certification** in the search window. Scroll through the results.

All the results should be related to ethical hacking and include the keyword **certification** in the page title.

ethical hacker intitle:certification

Certifications require passing an exam and often commanding education credits to maintain. [View details](#)

This video provides a guide on what the CEH certification is and how it can benefit your career.

Show more ▾

EC-Council <https://www.eccouncil.org/Train & Certify>

CEH Certification | Ethical Hacking Training & Course
Earn your ethical hacking certification with EC-Council's Certified Ethical Hacker (CEH v13) course. Learn the latest tools and techniques to advance your ...

Cybersecurity Guide <https://cybersecurityguide.org/cybersecurity-certifications>

CEH Certification: Get Certified as Ethical Hacker
16 Oct 2025 — The CEH certification is a globally recognized credential that validates your knowledge and skills in ethical hacking. The EC-Council ...

People also ask :

- How much does a CEH exam cost?
- Which is better, CCNA or CEH?
- Is CEH certification difficult?
- Is a CEH certificate free?

Certified ethical hacker

Certified Ethical Hacker is a qualification given by EC-Council and obtained by demonstrating knowledge of assessing the security of computer systems by looking for vulnerabilities in target systems, ...

Source: [Wikipedia](#)

Focus: Ethical hacking
Issuing Organization: EC-Council

Global Knowledge <https://www.globalknowledge.com/section/ec-council>

f. Type **ethical hacker inurl:free** in the search window. Scroll through the results.

All the results should be related to ethical hacking and should have the keyword **free** in the URL.

ethical hacker inurl:free

AI Mode All Videos Images Short videos News Forums More Tools

Great Learning <https://www.mygreatlearning.com/Cyber-Security>

Free Ethical Hacking Course with Certificate [2025]
Join our free online ethical hacking course and quickly learn penetration testing, cybersecurity essentials, and ethical hacking methods to safeguard ...
4.5 ★★★★☆ (11,922)

EC-Council <https://www.eccouncil.org/cyber-novice-free-cyber...>

Free Online Cyber Security Courses with Certificates in 2026
Ethical Hacking Essentials (EHE). With this cybersecurity course, students will gain strong foundations in ethical hacking and penetration testing that ...

Cybrary <https://www.cybrary.it/free-content>

Free Cybersecurity Courses & Hacking Training
Free Cyber Security courses & hacking training from Cybrary, with hacking course training helping educate individuals, businesses & organizations.

Cisco Learning Network <https://learningnetwork.cisco.com/question/cisco-eth...>

Cisco Ethical Hacking Free Certification
29 May 2025 — Cisco, a global leader in networking and cybersecurity, offers a fantastic free certification course for ethical hacking enthusiasts.

Udemy <https://www.udemy.com/.../Ethical-Hacking>

Ethical Hacking Free Course 2025
Ethical Hacking Free Course 2025 is designed for absolute beginners who want to understand how hackers think, operate, and exploit vulnerabilities — and more ...

- g. Type **allintext:free ethical hacker practice test questions** in the search window. This performs virtually the same function as a normal Google search, but it only returns results with every keyword in the page text. It won't return results with the keywords in only the title. Try putting quotes around your search text.

The results should include all the keywords in the page text.

A screenshot of a web browser window showing search results for "allintext:free ethical hacker practice test questions". The browser has multiple tabs open, including WhatsApp, Cisco Networking Academy, and the search results tab. The search bar contains the query. Below the search bar are filters: "AI Mode" (selected), "All", "Short videos", "Videos", "Forums", "Images", "News", "More", and "Tools". The search results list several links:

- QuickStart** - Sample Questions - Certified Ethical Hacking Practice Test
We have provided a practice test to better aid in certification. 100% of the questions are real test questions; from a recent version of the Certification Exam ... US\$99.00
- Whizlabs** - 25 Free Questions on Certified Ethical Hacker Certification
Want to ace the Certified Ethical Hacker Certification exam? Here, we're providing you with practice tests wherein you can learn and practice accordingly.
- ITExams.com** - Popular Free ECCouncil Exam Questions and Answers
Check these Popular Free ECCouncil Exam Questions and Answers to prepare for your IT exam. Each question has community assistance.
- SecureValley** - Free CEH Practice Questions with Answers
25 Apr 2025 — We 15 free CEH practice questions with detailed answers and explanations. These questions cover a range of topics from the CEH v12 blueprint.

Below the search results, there are sections for "Images" showing three thumbnail images related to CEH study guides.

Step 2: Conduct searches using the Google Advanced Search form.

The Google Advanced Search form offers the same result filtering functionality as the common text operators.

- Type **advanced search** in the Google search window. This will return a link to the advanced search form.
- Use the advanced search form to perform the same searches that were conducted in the previous step.

The screenshot shows a Google search results page with the query 'ethical hacker site:pearson.com pearson.com "ethical hacker site"'. The results include several links from Pearson's website:

- Certified Ethical Hacker (CEH) Exam Cram - Pearson**: A PDF document titled 'CEH Certified Ethical Hacker Exam Cram. Creating a Virus ... CEH Certified Ethical Hacker Exam Cram. CHAPTER 8: Hacking Web Servers and Web Applications ...'.
- Ethical Hacking and Countermeasures**: A PDF document titled 'Ethical Hacking and Countermeasures. Exam 312-50 Certified Ethical Hacker. Course Outline. Page | 1. Ethical Hacking and Countermeasures Copyright © by EC- ...'.
- CEH Certified Ethical Hacker Cert Guide - Pearson**: A book titled 'CEH Certified Ethical Hacker Cert Guide, 4th edition. Published by Pearson IT Certification (January 20, 2022) © 2022. US\$57.99 · In stock'.
- CEH Certified Ethical Hacker Cert Guide, 4th edition - Pearson**: A book titled 'CEH Certified Ethical Hacker Cert Guide, 4th edition. Published by Pearson IT Certification (December 29, 2022) © 2022. US\$50.94 · In stock'.

Below the search results, there is a section titled 'Images' showing three small thumbnail images related to ethical hacking.

Step 3: Conduct passive reconnaissance with advanced search operators.

Advanced search operators are useful for narrowing down search results as you have seen. This makes them useful for performing passive reconnaissance as well. Hackers will use advanced search operators to find vulnerabilities and information about potential targets. While the results of the searches may seem harmless on their own, when pieced together, they can provide valuable intelligence to a hacker. The hacker hopes to find sites or files that the target company did not intend to make public, or to find information that can be used for future attacks, such as social engineering attacks.

When performing these searches, use a target company of your choice. Passive reconnaissance is legal but stop there because using any information you uncover for active reconnaissance is not. If you do find vulnerabilities, consider informing the company so that they can correct the issue.

- Search the target company site using the **inurl:** operator.

In the search window type the command **site:*examplecompany.com* inurl:*admin*** replacing *examplecompany.com* with a company of your choice.

This will return pages that have the keyword **admin** somewhere inside the URL.

site:Uber.com inurl:admin

AI Mode All Images Videos News Short videos Forums More Tools

[Uber](https://m.uber.com/dropoff[&nickname]=Right+Hand...) https://m.uber.com/dropoff[&nickname]=Right+Hand... ⓘ
[https://m.uber.com/ui/?client_id=Md64GYThBYoDtZvyO... ⓘ](https://m.uber.com/ui/?client_id=Md64GYThBYoDtZvyO...)

No information is available for this page.
Learn why

[Uber](https://help.uber.com/business/article/recover-you...) https://help.uber.com/business/article/recover-you... ⓘ
Recover your business account (admin departure)
If your sole admin has left your organization, please reach out to business-support@uber.com. We will respond with a request for specific documents to verify ...

[Uber Developers](https://developer.uber.com/voucher-api-build-guide) https://developer.uber.com/voucher-api-build-guide ⓘ
Administrative Workflows
Track program spending using the usage_amount field. Use the Search Voucher Program endpoint to enable customized searches in the UI. Review Active Programs.

[Uber](https://businesses.uber.com/amex-admin) https://businesses.uber.com/amex-admin ⓘ
American Express Corporate Benefit | Uber for Business
American Express Corporate Card Members can earn Uber Cash on rides with Uber and orders with Uber Eats when using an eligible Corporate Card on a business ...

[Uber](https://businesses.uber.com/blo-...) https://businesses.uber.com/blo-... - Translate this page ⓘ
Uber para Empresas
Empresas como a sua estão utilizando nosso painel online para gerenciar facilmente os programas de transporte terrestre e refeições para suas equipes. Por que ...

[Uber](https://help.uber.com/article/re...) https://help.uber.com/article/re... - Translate this page ⓘ

Review the returned pages and click a few to see if there is any interesting information.

Ride with Uber | Request | +

Uber | Ride | Earn | Business | Uber Eats | About | EN | Help | Log In | Sign up

Ride

Nairobi, KE Change city

Request a ride for now or later

Add your trip details, hop in, and go.

Pickup location Dropoff location

See prices Schedule for later

Request a ride Reserve a ride See prices Explore ride options Airport rides

Suggestions

Ride Reserve Courier

b. Do another search, this time using the **intitle:** operator.

In the search window type the command **site:examplecompany.com intitle:login**.

This will return pages that have the keyword **login** in the title.

site:Uber.com intitle:login

AI Mode All Images News Videos Short videos Web More Tools

- [Uber Login | Uber Official Site](https://www.uber.com/global/sign-in)
- [Single Sign-On \(SSO\) based login | Uber for Business](https://help.uber.com/business/article/single-sign-on)
- [Login issues | Merchants & Restaurants](https://help.uber.com/section/login-issues)
- [Login Issues | Merchants & Restaurants](https://help.uber.com/section/login-issues)
- [Uber](https://www.uber.com/blog/us-ubers-unified-signin)

Again, review the results and click a few to see if there is any interesting information.

Uber Login | Uber Official

Uber Rider Drive Business Uber Eats About Log in Sign up

Log in to access your account

Rider → Driver

Uber

Visit Help Center

c. Next, try using the **filetype:** operator.

In the search window, type the command **site:examplecompany.com filetype:pdf**.

This will return PDF files.

site:Uber.com filetype:pdf

uber.com https://uber.com > consultationlivreurs2020 PDF

Consultation des livreurs

Au printemps 2019, nous lancions la première édition de la consultation nationale pour donner la parole aux livreurs. A l'issue de 45 tables rondes et grâce ...

uber.com https://uber.com > notice_axa_fr PDF

Santé & Prévoyance

1 Jun 2018 — Important : Faire remplir et signer le certificat médical par votre médecin dans les 5 jours après l'accident.

uber.com https://uber.com > ... PDF

Les Dangers des Batteries Lithium-ion

Si une batterie surchauffe ou si vous remarquez une odeur, un changement de forme/couleur, une fuite ou des bruits étranges provenant d'un.

uber.com https://uber.com > precautions PDF

Guide des précautions sanitaires à respecter dans le cadre ...

AVANT DE PASSER EN LIGNE. Avant de prendre la route, nettoyez votre matériel de livraison (deux-roues et sac), particulièrement les zones en contact avec ...

uber.com https://uber.com > hicolorcontest_pdf PDF

我的五星好爸爸

小童姓名Name of child. 小童年龄Age of child. Uber 登記電郵Email. Uber 登記電話Phone Number. 我的五星好爸爸. Page 2. 小童姓名Name of child.

Uber https://tb-static.uber.com / custom_assets / drivers PDF

Review some of the files to see if there is any interesting information that is not intended for public access or is useful for social engineering attacks.

- d. Try a search with multiple operators. Use the **intext:** and **filetype:** operators. In the search window, type the command **site:examplecompany.com intext:employee filetype:pdf**

This will return PDF pages containing the text **employee**.

site:Uber.com intext:employee filetype:pdf

Uber https://tb-static.uber.com > UnitedStates > licensed PDF

Platform Access Agreement (P2P) ...

This is not an employment agreement and you are not an employee. You confirm the existence and nature of that contractual relationship each time you access ...
27 pages

Uber https://tb-static.uber.com > country > UnitedStates PDF

Platform Access Agreement

This is not an employment agreement and you are not an employee. You confirm the existence and nature of that contractual relationship each time you access ...
22 pages

Uber https://tb-static.uber.com > prod > consents PDF

Car Dealership Delivery Platform Agreement

5 Nov 2023 — This is not an employment agreement and you are not an employee. You confirm the existence and nature of that contractual relationship each ...
24 pages

Uber https://investor.uber.com / files / doc_governance PDF

Related Party Transaction Policy v.10

The purpose of this Policy is to set forth the Uber Technologies, Inc. (the "Company") policy governing the notification, review, approval, ratification and ...

Uber https://investor.uber.com / files / doc_governance PDF

AMENDED AND RESTATED BYLAWS OF UBER ...

competent employee of the corporation or its transfer agent appointed with respect to the class of stock affected, or other agent, specifying the name and ...

Experiment with **site:*examplecompany.com* intext:<keyword> filetype:<file type>** using different key words and different filetypes.

- LinkedIn can offer valuable information about a company and employees. In the search window, type the command **site:linkedin.com intitle:*example company***. Experiment by searching for the company name with and without the .com at the end.

The screenshot shows a Google search results page with the query "site:linkedin.com intitle:4gcapital". The results are filtered under "All Mode". The first result is a LinkedIn post from "4G Capital" with 20+ reactions, posted 1 month ago. The post discusses the FT Live Africa Summit 2025. The second result is a LinkedIn post from "Camila Diaz C." with 90+ reactions, posted 3 months ago. It mentions #4capital #kenya #fintech | Camila Diaz C. The third result is a LinkedIn post from "4G Capital" with 10+ reactions, posted 1 week ago. It celebrates Jamhuri Day. The fourth result is a LinkedIn post from "4G Capital's Post" with 40+ reactions, posted 11 months ago. It wishes Happy New Year from the JGP Team. The fifth result is a LinkedIn post from "4G Capital" with 60+ reactions, posted 2 months ago. The results are presented in a standard Google search format with links to the LinkedIn posts.

Experiment with **site:<social media site> intitle:<example company>** and search other social media sites.

The screenshot shows a Google search results page with the query "site:X.com intitle:4gcapital". The results list several tweets from the account @4gCapital:

- X - 4gCapital 1.3k+ followers 4G Capital (@4gCapital) / Posts / X We empower small businesses to grow and succeed. Posts. 4G Capital profile. 4G Capital. ✓. 4gCapital. Dec 15. On the Ground in Luzira As we continue ...
- X https://x.com / Explore 4G Capital (@4gCapital) / Highlights / X Big dreams need bold moves. Apply for a UPIA loan today and take your business to the next level. Fast, simple, reliable. Just *Dial 612#. Your business. Your ...
- X Twitter https://x.com / kenyawallstreet / status Kenyan Wall Street CEO Julian Mitchell opening remarks. Image. 5:24 AM · May 19, 2025 from Nairobi, Kenya. . 649. Views. 1.
- X https://x.com / BankerMagazine / status African Banker magazine on X: "RT @4gCapital RT @4gCapital: Still celebrating the win! Being named Fintech of the Year at the African Banker Awards 2025 is more than a trophy, it's a..."
- X 2 likes · 3 weeks ago It's in your interest to stop your bad manners. Dear @4gCapital: It's in your interest to stop your bad manners - or face lawful consequences thereof. Kenya is NOT yet a banana republic.
- X - AfricaTechSMT 11 months ago

Part 2: The Google Hacking Database

The **Google Hacking Database (GHDB)** is an index of user-created dorks that are designed to uncover interesting, and potentially sensitive, information that was unintentionally made publicly available on the internet.

Step 1: Explore the Google Hacking Database main page.

- Do a Google search for **GHDB**. The first returned page should be The Google Hacking Database.
- On the GHDB main page, click the **Filters** button in the top right of the window.

This allows you to filter the database results by Category or Author. There is also a **Quick Search**.

The screenshot shows a web browser window with multiple tabs open. The active tab is titled "Google Hacking Database" and displays the "Exploit Database" website. The page has a dark blue header with the site's logo and navigation links. Below the header, there are search filters for "Category" (set to "Any") and "Author" (empty), along with "Filters" and "Reset All" buttons. A "Quick Search" input field is also present. The main content area is titled "Google Hacking Database" and lists search results. On the left, there is a sidebar with various icons and a dropdown menu set to "Dork". The results table includes columns for "Date Added", "Category", and "Author". The results are ordered by date added, showing 15 entries from July 2024. The first few entries include:

Date Added	Category	Author
2024-08-23	site:github.com "BEGIN OPENSSH PRIVATE KEY"	kstrawn0
2024-08-23	ext:nix "BEGIN OPENSSH PRIVATE KEY"	kstrawn0
2024-07-26	inurl:home.htm intitle:1766	Kishoraram
2024-07-04	inttitle:"SSL Network Extender Login" <checkpoint.com	Everton Hyd43n
2024-07-04	inttext:"siemens" & inurl:"/portal/portal.mwaa"	Kishoraram
2024-07-04	Google Dork Submission For GlobalProtect Portal	Gurudatt Choudhary
2024-07-04	inurl:"cgi-bin/koha"	Hillary Soita
2024-07-04	inttext:"aws_access_key_id" inttext:"aws_secret_access_key" filetype:json filetype:yaml	Joel Indra
2024-07-04	inttext:"proftpd.conf" "index of"	Fernando Mengali
2024-07-04	site:.edu filetype:xls "root" database	defaltredmode
2024-07-04	inttitle:index of /etc/ssh	Shivam Dhingra
2024-05-13	'START test_database' ext:log	Nadir Boulacheb (RubX)
2024-05-13	'Header for logs at time' ext:log	Nadir Boulacheb (RubX)
2024-05-01	inttext:"dhcpcd.conf" "index of"	Prathamesh Waidande
2024-05-01	site:uat.* * inurl:login	Jagdish Rathod

At the bottom, it says "Showing 1 to 15 of 7944 entries" and provides navigation links for FIRST, PREVIOUS, NEXT, LAST, and page numbers 1, 2, 3, 4, 5, ..., 530.

Step 2: Use Quick Search to find specific dorks.

- Select each of the filter categories and observe some of the dorks available in that category.
Select a few interesting looking dorks in the results and note the descriptions of each.

What information is provided about the Dorks?

The GHDB-ID number, the author, the date published, a brief description of the function of the dork, and a clickable link that will launch the dork in a new window.

site:github.com "BEGIN OPENSSH PRIVATE KEY"

GHDB-ID: 8451 **Author:** KSTRUWNO

Published: 2024-08-23

Google Dork Description:
site.github.com "BEGIN OPENSSH PRIVATE KEY"

Google Search: site.github.com "BEGIN OPENSSH PRIVATE KEY"

Databases **Links** **Sites** **Solutions**

Databases	Links	Sites	Solutions
Exploits	Search Exploit-DB	OffSec	Courses and Certifications
Google Hacking	Submit Entry	Kali Linux	Learn Subscriptions
Papers	SearchSploit Manual	VulnHub	OffSec Cyber Range
Shellcodes	Exploit Statistics		Proving Grounds
			Penetration Testing Services

Step 3: Select Categories to find interesting Dorks.

- Conduct a search for **tsweb**.
- Click the **allinurl:tsweb/default.htm** Dork.

Google Hacking Database

Show 15

Quick Search: tsweb

Date Added	Dork	Category	Author
2020-07-29	intitle:"Remote Desktop Web Connection" inurl:tsweb	Pages Containing Login Portals	Aditya Rana
2020-06-30	allinurl:tsweb/default.htm	Pages Containing Login Portals	Alexandros Pappas
2005-05-02	inurl:gntsweb.pl	Pages Containing Login Portals	anonymous
2004-04-28	intitle:Remote.Desktop.Web.Connection inurl:tsweb	Pages Containing Login Portals	anonymous

Showing 1 to 4 of 4 entries (filtered from 7,944 total entries)

Databases **Links** **Sites** **Solutions**

Databases	Links	Sites	Solutions
Exploits	Search Exploit-DB	OffSec	Courses and Certifications
Google Hacking	Submit Entry	Kali Linux	Learn Subscriptions
Papers	SearchSploit Manual	VulnHub	OffSec Cyber Range
Shellcodes	Exploit Statistics		Proving Grounds
			Penetration Testing Services

Results

GHDB-ID: 6343 Author: ALEXANDROS PAPPAS

Published: 2020-06-30

Google Dork Description:
allinurl:tsweb/default.htm
Google Search: allinurl:tsweb/default.htm

Google Dork: allinurl:tsweb/default.htm
Juicy information and sensitive directories regarding Remote Desktop Web Connection
Date: 29/06/2020
Exploit Author: Alexandros Pappas

Databases	Links	Sites	Solutions
Exploits	Search Exploit-DB	OffSec	Courses and Certifications
Google Hacking	Submit Entry	Kali Linux	Learn Subscriptions
Papers	SearchSplot Manual	VulnHub	OffSec Cyber Range
Shellcodes	Exploit Statistics		Proving Grounds

Click a few of the returned pages. Besides fields for log in credentials you may see some interesting information that could be leveraged by a hacker. For example, look at the figure. The terminal services server is running it-labts. Knowing this, a hacker can focus on the window it-labts vulnerabilities.

Microsoft® Windows®
Remote Desktop Web Connection

Type the name of the remote computer you want to use, select the screen size for your connection, and then click **Connect**.

When the connection page opens, you can add it to your Favorites for easy connection to the same computer.

Server: it-labts **Size:** Full-screen Send logon information for this connection

User name: _____
Domain: _____

Connect

Step 4: Combine Category filters with search terms.

You can combine category filters with search terms to further refine and filter results to specific information.

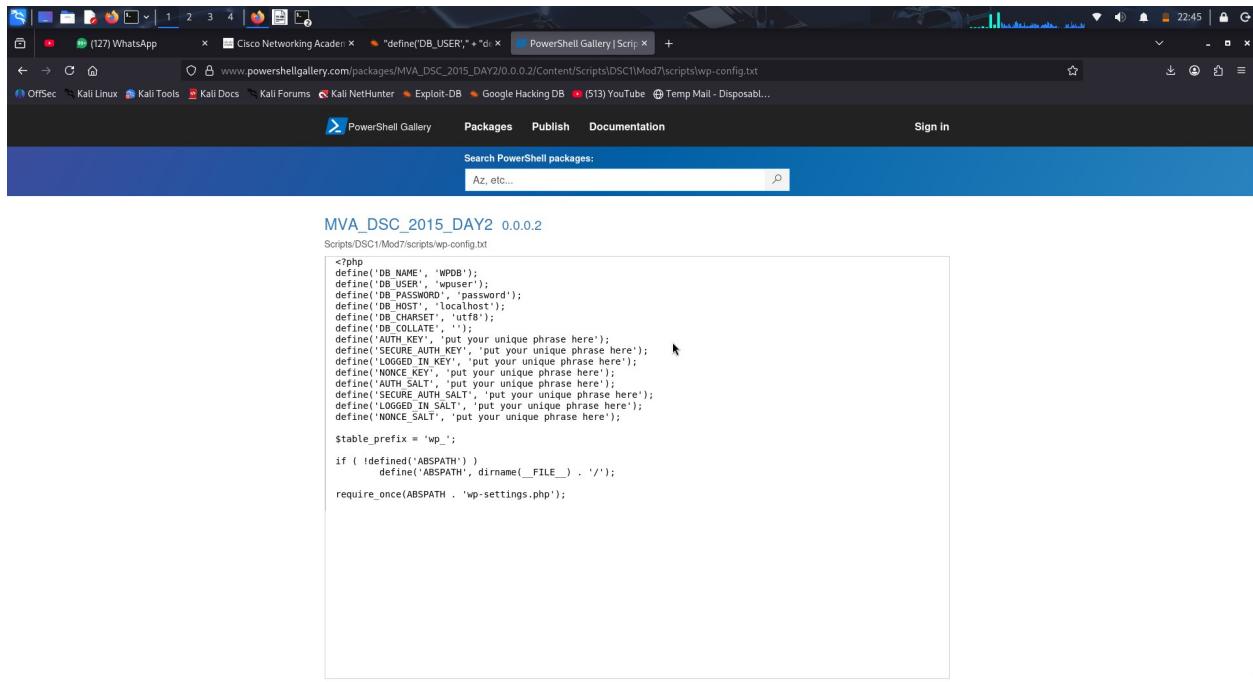
- a. Select **Files Containing Passwords** in the **Categories** drop down.
- b. In the **Quick Search** window, type **db_pass**. This will return dork searches for database passwords.

The screenshot shows the Exploit Database interface with the following details:

- Category:** Files Containing Passwords
- Author:** Begin typing...
- Quick Search:** db_pass
- Date Added:** Dork
- Show:** 15
- Results:** A table listing 14 entries from 2003 to 2020, each containing a dork query related to database passwords.
- Table Headers:** Date Added, Dork, Category, Author
- Table Data:** (Partial list)

Date Added	Dork	Category	Author
2020-11-24	'define('DB_USER'); + *define('DB_PASSWORD'; ext:txt	Files Containing Passwords	Alexandros Pappas
2020-10-13	"db.username" + "db.password" ext:properties	Files Containing Passwords	Alexandros Pappas
2020-09-22	intitle:"database.php" inurl:"database.php" intext:"db_password" -git -github	Files Containing Passwords	Alexandros Pappas
2020-07-23	inttext:"db_database" ext:env intext:"db_password"	Files Containing Passwords	Alexandros Pappas
2020-06-17	filetype:env 'DB_PASSWORD'	Files Containing Passwords	Shivanshu Sharma
2020-03-05	inttext:"WPENGINE_SESSION_DB_USERNAME" "WPENGINE_SESSION_DB_PASSWORD"	Files Containing Passwords	Hilary Soita
2019-05-06	inurl:wp-config.php intext:DB_PASSWORD -stackoverflow -wpbeginner	Files Containing Passwords	vouzli
2018-08-14	"whoops! there was an error: "db_password"	Files Containing Passwords	Rootkit_Pentester
2018-04-04	CakePHP inurl:database.php intext:db_password	Files Containing Passwords	Kiran S
2017-06-22	inttext:DB_PASSWORD intext:"MySQL hostname" ext:txt	Files Containing Passwords	anonymous
2016-01-11	inurl:wp-config -intext:wp-config "DB_PASSWORD"	Files Containing Passwords	anonymous
2015-05-29	inttext:DB_PASSWORD ext:env	Files Containing Passwords	anonymous
2011-10-11	filetype:php~ (pass1passwd password dbpass db_pass pwd)	Files Containing Passwords	anonymous
2003-06-24	inttitle:"Index of" spwd.db passwd -pam.conf	Files Containing Passwords	anonymous
- Pagination:** FIRST, PREVIOUS, 1, NEXT, LAST

Explore some of the search results and see what interesting information they reveal.



The screenshot shows a browser window with multiple tabs open. The active tab is for the PowerShell Gallery, specifically the package `MVA_DSC_2015_DAY2`. The page displays the package details and its contents. The contents section shows the `wp-config.txt` file, which contains the following PHP code:

```
<?php
define('DB_NAME', 'WPDB');
define('DB_USER', 'wpuser');
define('DB_PASSWORD', 'password');
define('DB_HOST', 'localhost');
define('DB_CHARSET', 'utf8');
define('DB_COLLATE', '');
define('SECURE_AUTH_KEY', 'put your unique phrase here');
define('LOGGED_IN_KEY', 'put your unique phrase here');
define('NONCE_KEY', 'put your unique phrase here');
define('AUTH_SALT', 'put your unique phrase here');
define('SECURE_AUTH_SALT', 'put your unique phrase here');
define('LOGGED_IN_SALT', 'put your unique phrase here');
define('NONCE_SALT', 'put your unique phrase here');

$table_prefix = 'wp_';

if ( !defined('ABSPATH') )
    define('ABSPATH', dirname(__FILE__) . '/');

require_once(ABSPATH . 'wp-settings.php');
```

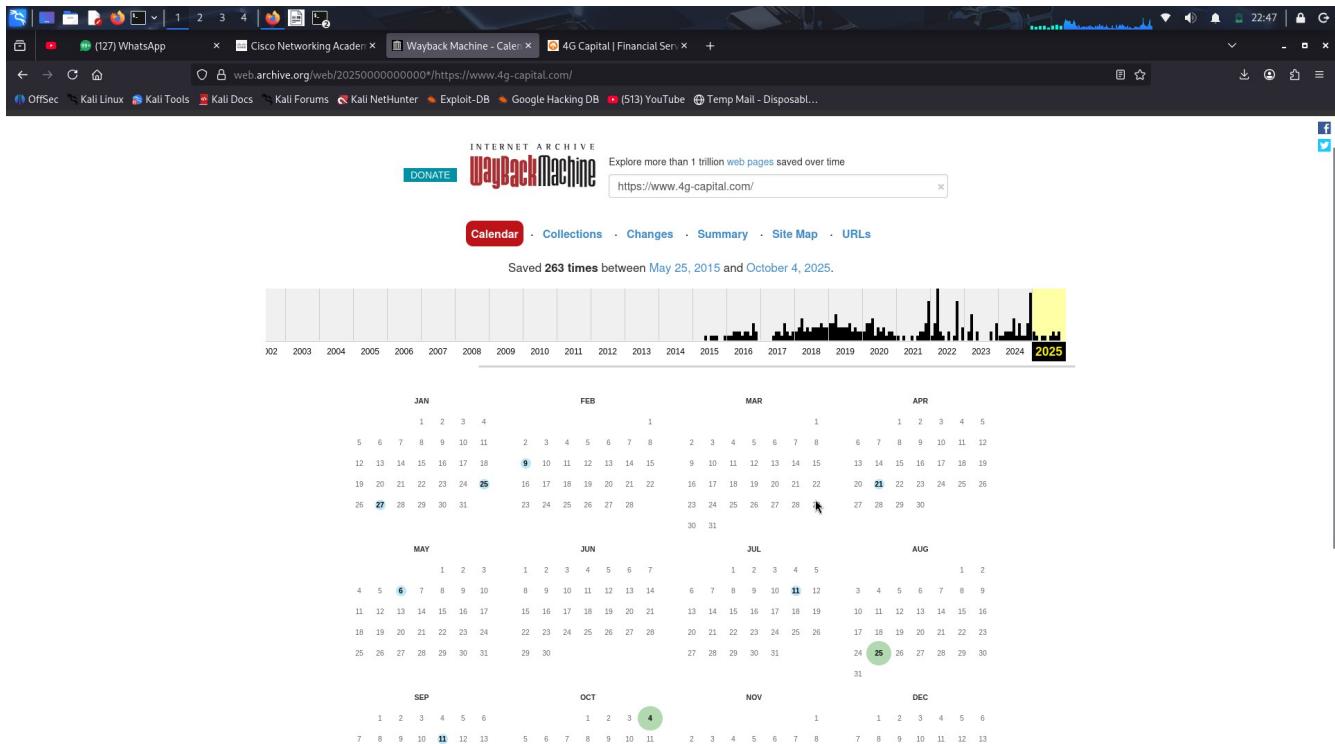
Review the course materials and try some of the searches that are shown there.

Part 3: The Wayback Machine

Website security has evolved over the decades. Websites used to publish information that is no longer considered safe. Webpage archives can reveal interesting information that is no longer available. The Wayback Machine is a useful tool for passively collecting information about a target that could be used in social engineering or other attacks. The Wayback Machine is an archive of the entire internet. It accesses every website and crawls it while taking screenshots and logging the data to a database. These endpoints can then be queried to pull down every path the site has ever crawled.

Step 1: Explore the Wayback Machine database.

- Navigate to <https://web.archive.org> to bring up the Wayback Machine home page.
- Enter the URL of a target company in the Search box.

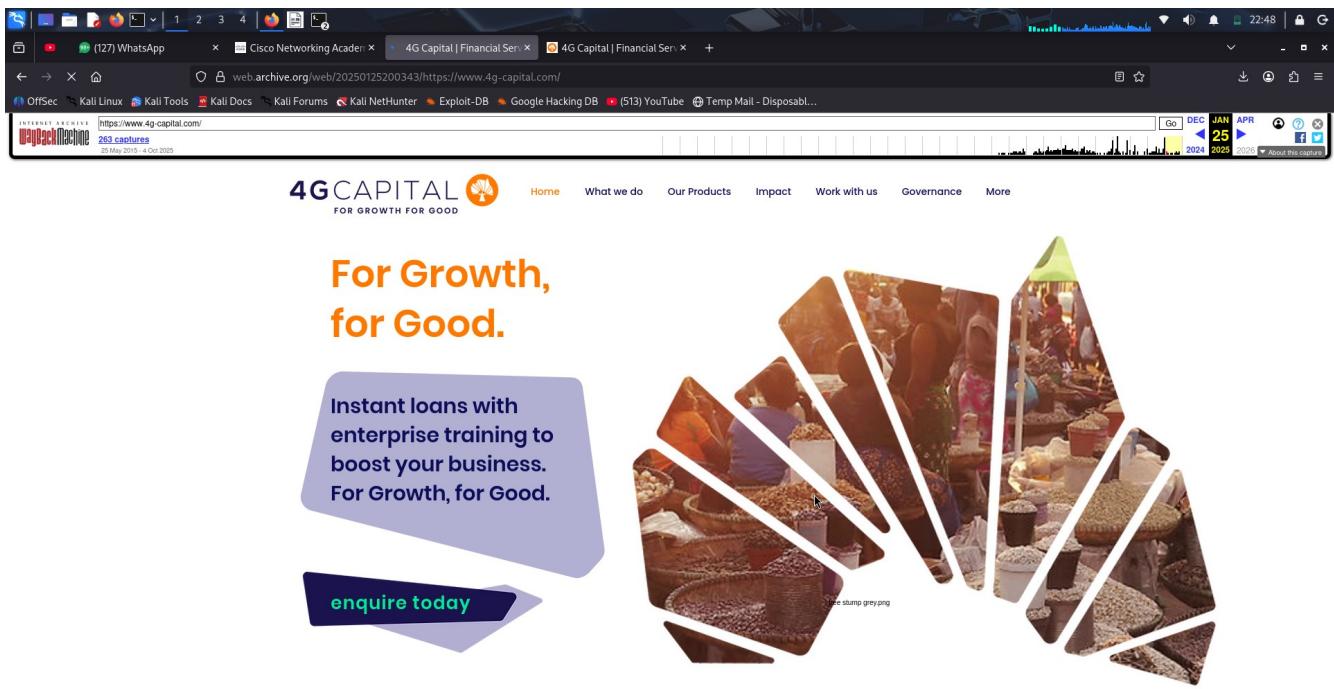


Step 2: Explore the Calendar tab.

- Click the **Calendar** tab if not already selected.

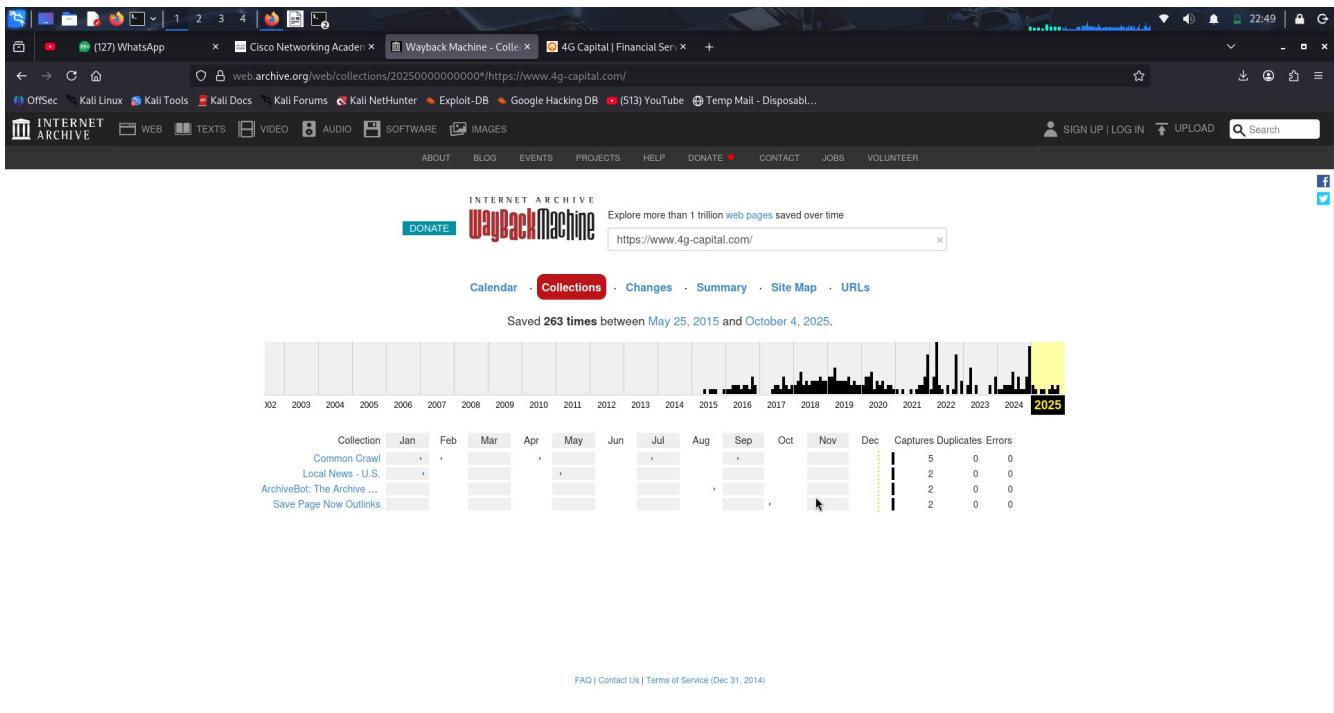
At the top of the page is a graph that shows how many times the website has been crawled by the Wayback Machine and a calendar at the bottom showing at what day the archive entry was created. You can click these to open snapshots from the past.

- Select a year and a date for a snapshot in the calendar. Some dates may have more than one snapshot. Click a snapshot to open the achieved web page. Depending on the site, you may be able to navigate the page as if it was live, seeing all the dated information.



Step 3: Explore the Collections tab.

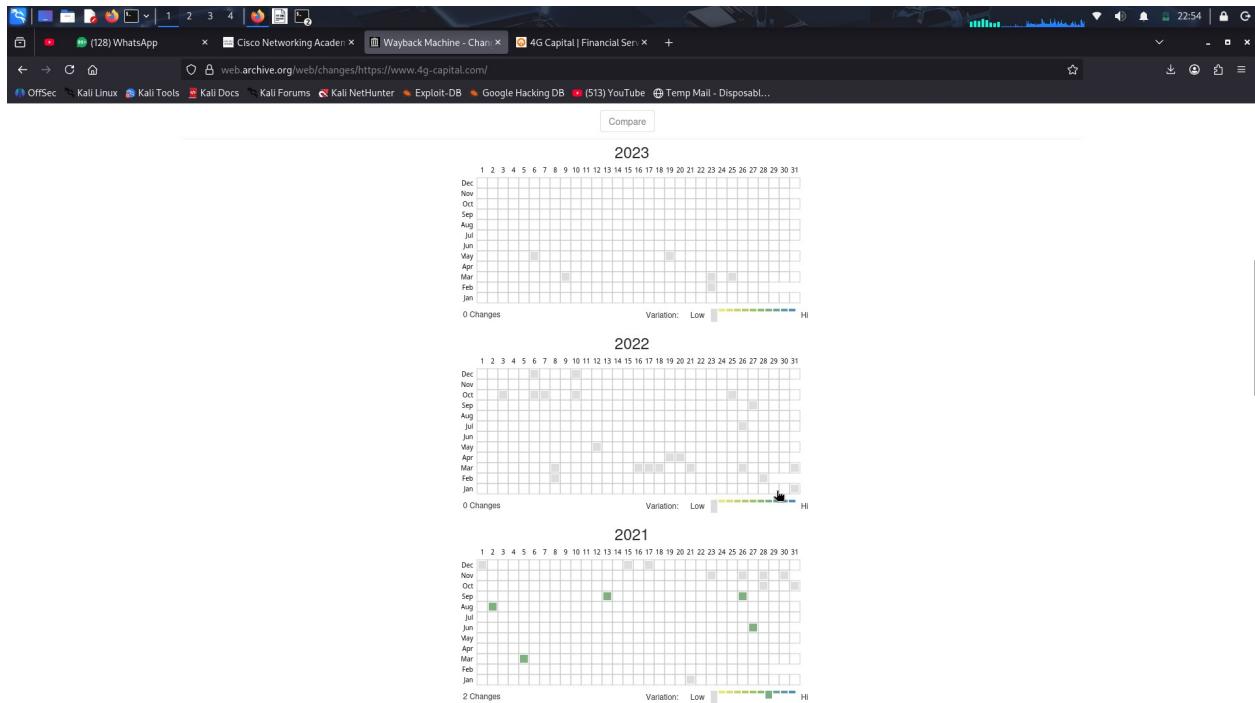
- Click the **Collections** tab.
- This provides archives organized by source. The collections that crawled the page are in the column on the left. The months Jan – Dec show when it was crawled over time.



- Click some of the collections to find out more about the collections and who runs them.

Click the **Changes** tab.

This shows how much the page has changed over time. Grey = has not changed much since the last crawl. Blue = significant changes. You can also compare changes from two captures to see what has changed.



- b. Select two captures. They can be on the same day or on different days. Click the **Compare** button. Things that have changed will be highlighted.

Yellow indicates content deletion. **Blue** indicates content addition.

The screenshot shows a browser window with multiple tabs open, including WhatsApp, Cisco Networking Academy, and Wayback Machine. The Wayback Machine tab displays a comparison between two versions of the URL <https://www.4g-capital.com/>. The interface includes a header with the Wayback Machine logo and navigation links like Calendar, Collections, Changes, Summary, Site Map, and URLs. Below the header, there are dropdown menus for selecting capture dates (2022 [35], September [3], etc.) and a 'Show differences' button. The main content area is split into two columns, each showing a different version of the website's homepage. The left column (2022) has yellow highlights under 'OUR PURPOSE' (To Unlock Human Potential for Good) and 'OUR VISION' (The First Choice For Micro Enterprise Growth In Africa). The right column (2023) has blue highlights under 'OUR MISSION' (To Grow Business With Capital And Knowledge), which is expanded to show sub-points about economic, social, and product missions. A 'Show differences' button is visible between the two columns.

Step 5: Explore the Summary tab.

- a. Click the **Summary** tab.

The summary applies to the entire domain, whereas calendar, collections, and changes are specific to the URL (single page) searched. This page shows the MIME type of the content that was hosted by the domain in the given date range. This can be text, images, javascript, etc.

Screenshot of a Wayback Machine summary page for www.4g-capital.com. The page shows a summary of 263 captures between May 25, 2015, and October 4, 2025. It includes a pie chart of capture types and a table of MIME-type counts.

MIME-types

Captures	Unique URLs
697	111
425	54
339	39
309	19
106	24
97	16
36	3

Captures

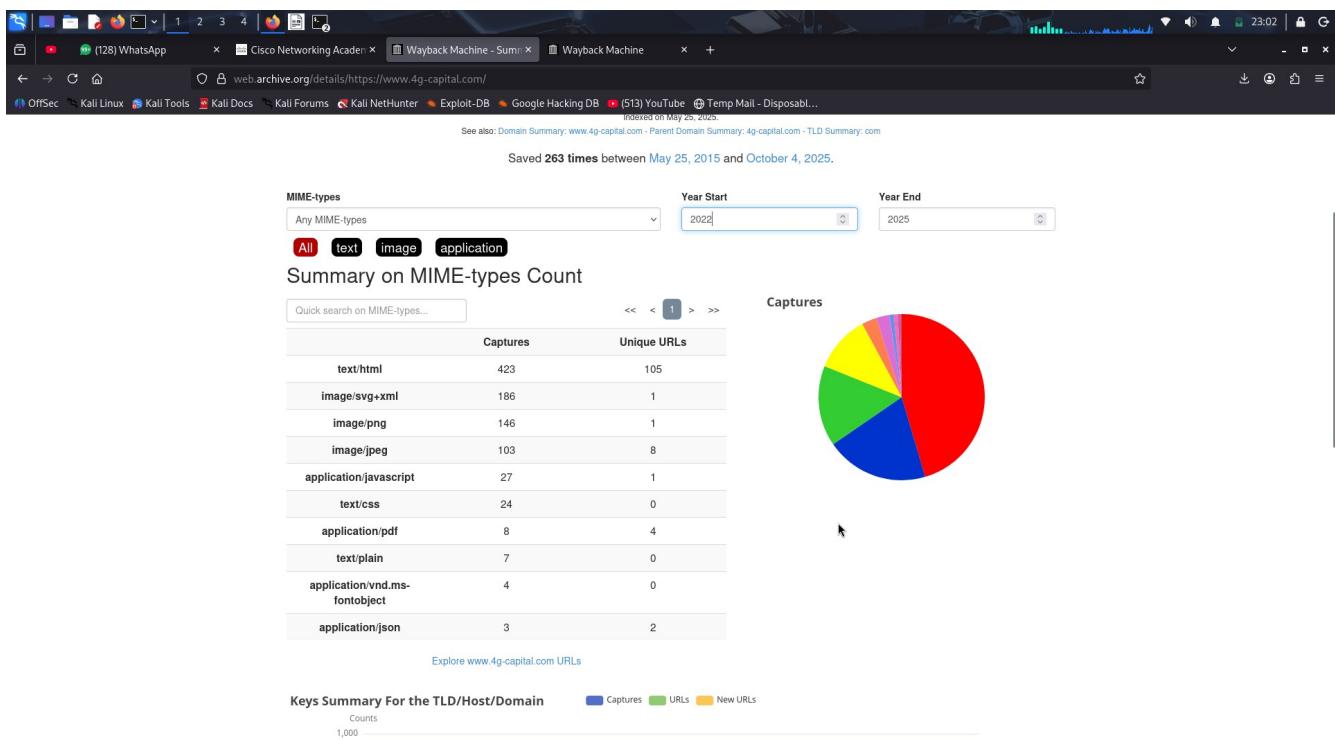
Screenshot of a Wayback Machine summary page for www.4g-capital.com. The page shows a summary of 263 captures between May 25, 2015, and October 4, 2025. It includes a pie chart of capture types and a table of MIME-type counts.

MIME-types

Captures	Unique URLs
697	111
425	54
339	39
309	19
106	24
97	16
36	3
27	13
11	1
8	1

Captures

- Click the dropdown arrow in the MIME-types drop box and review the file types available.
- Change the Year Start and Year End to see how things have changed over a time of period.

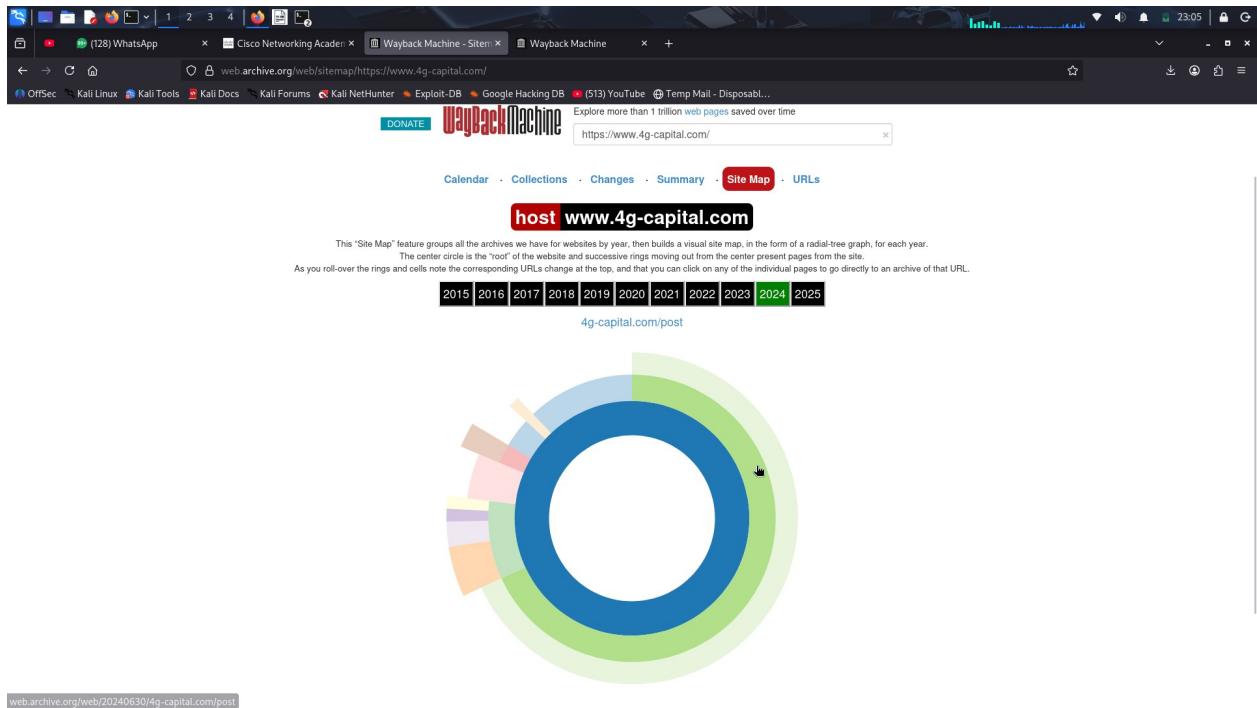


- d. Click each of the data type buttons: All, text, application, image, message, audio, video, and explore the information revealed.

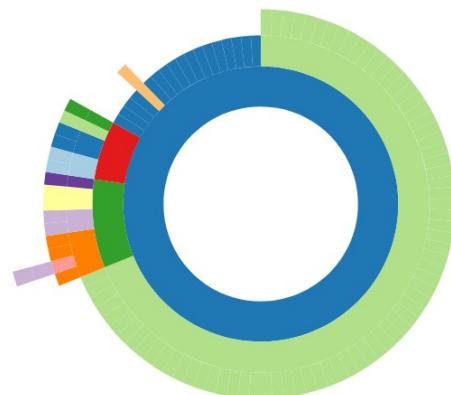
Step 6: Explore the Site Map tab.

- a. Click the **Site Map** tab.

The Site Map also applies to the entire domain. The center circle is the "root" and all the rings that surround the center circle are the various pages or trees of the web site. The further out from the root, the more complex the page is.



- b. Click through the years to see in the graph how the complexity of the site has changed over time.



- c. Click the rings and cells in the graph to open archived pages. The data in the archived pages can be used to find vulnerabilities.

Step 7: Explore the URLs tab.

- Click the URLs tab.

This shows all the URLs containing the domain prefix.

The screenshot shows a browser window with multiple tabs open, including WhatsApp, Cisco Networking Academy, Wayback Machine - URLs, and Wayback Machine. The Wayback Machine URLs tab is active, displaying a list of 373 URLs for the domain https://www.4g-capital.com/. The results are presented in a table with columns for URL, MIME Type, From, To, Captures, Duplicates, and Uniques. A filter box at the top right allows searching by URL or MIME Type. The table includes links to various files like contact.html, CSS fonts, and images, along with their capture dates and counts.

URL	MIME Type	From	To	Captures	Duplicates	Uniques
http://4g-capital.com/	text/html	Dec 5, 2022	Dec 5, 2022	2	0	2
http://4g-capital.com/contact.html	text/html	Mar 5, 2021	Jun 2, 2023	4	3	1
http://4g-capital.com/css/fonts/DINPro-black.eot	warc/revisit	Nov 1, 2018	May 26, 2020	6	4	2
http://4g-capital.com/css/fonts/DINPro-black.ttf	warc/revisit	Nov 1, 2018	May 26, 2020	7	5	2
http://4g-capital.com/css/fonts/DINPro-black.woff	warc/revisit	Nov 1, 2018	May 26, 2020	7	5	2
http://4g-capital.com/css/fonts/DINPro-light.eot	warc/revisit	Nov 1, 2018	May 25, 2020	7	5	2
http://4g-capital.com/css/fonts/DINPro-light.ttf	warc/revisit	Nov 1, 2018	May 25, 2020	7	5	2
http://4g-capital.com/css/fonts/DINPro-light.woff	warc/revisit	Nov 1, 2018	May 25, 2020	7	5	2
http://4g-capital.com/downloads/	text/html	Oct 26, 2022	Oct 26, 2022	2	0	2
http://4g-capital.com/favicon.ico	warc/revisit	Aug 18, 2018	Dec 28, 2024	25	18	7
http://4g-capital.com/images/assets/preloader-gif.gif	warc/revisit	Nov 1, 2018	May 25, 2020	7	5	2
http://4g-capital.com/images/careers/1.jpg	image/jpeg	Aug 25, 2018	May 12, 2020	13	12	1
http://4g-capital.com/images/careers/2.jpg	image/jpeg	Aug 25, 2018	May 12, 2020	13	12	1
http://4g-capital.com/images/careers/3.jpg	image/jpeg	Aug 25, 2018	May 12, 2020	13	12	1
http://4g-capital.com/images/careers/careers-bg.jpg	image/jpeg	Nov 1, 2018	Mar 24, 2023	24	23	1
http://4g-capital.com/images/contact-fs-section-1.jpg	warc/revisit	Nov 1, 2018	May 26, 2020	7	5	2
http://4g-capital.com/images/contact/hero-half-1-2.jpg	warc/revisit	Nov 1, 2018	May 26, 2020	7	5	2
http://4g-capital.com/images/contact/hero-half-1.jpg	warc/revisit	Nov 1, 2018	May 26, 2020	7	5	2

- Use the filter box on the right of the page to search for specific files such as anything that ends in “.bak” to see if they contain any interesting backup information.

Note: Depending on the site searched, this may or may not return any content.

- Experiment with other filters. Some may return content, some may not. Also, experiment with these filters on different domains. Some filters to try:

- .zip
- .backup
- .config
- .csv
- .pdf
- /api/
- /admin/

Not only can you find interesting files by searching the Wayback Machine archives, but careful inspection of the data can lead to finding potential vulnerabilities.

Screenshot of a web browser showing the Wayback Machine interface for the URL prefix <https://www.4g-capital.com/>.

The browser tabs include WhatsApp, Cisco Networking Academy, Wayback Machine - URLs, and Wayback Machine.

The Wayback Machine header includes links for OffSec, Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, YouTube, Temp Mail - Disposab..., INTERNET ARCHIVE, SIGN UP / LOG IN, UPLOAD, and a Search bar.

The main content area shows the Wayback Machine logo and a search bar with the URL <https://www.4g-capital.com/>.

Below the search bar are navigation links: Calendar, Collections, Changes, Summary, Site Map, and URLs.

A message indicates "373 URLs have been captured for this URL prefix." A search input field contains ".jpg".

A table displays the captured URLs, their MIME type, capture dates, and statistics (Captures, Duplicates, Uniques). The table has columns: URL, MIME Type, From, To, Captures, Duplicates, and Uniques.

URL	MIME Type	From	To	Captures	Duplicates	Uniques
http://4g-capital.com/images/careers/1.jpg	image/jpeg	Aug 25, 2018	May 12, 2020	13	12	1
http://4g-capital.com/images/careers/2.jpg	image/jpeg	Aug 25, 2018	May 12, 2020	13	12	1
http://4g-capital.com/images/careers/3.jpg	image/jpeg	Aug 25, 2018	May 12, 2020	13	12	1
http://4g-capital.com/images/careers/careers-bg.jpg	image/jpeg	Nov 1, 2018	Mar 24, 2023	24	23	1
http://4g-capital.com/images/contact/f-section-1.jpg	warc/revisit	Nov 1, 2018	May 26, 2020	7	5	2
http://4g-capital.com/images/contact/hero-half-1-2.jpg	warc/revisit	Nov 1, 2018	May 26, 2020	7	5	2
http://4g-capital.com/images/contact/hero-half-1.jpg	warc/revisit	Nov 1, 2018	May 26, 2020	7	5	2
http://4g-capital.com/images/fullscreen/coming-soon-1.jpg	warc/revisit	Oct 31, 2018	May 26, 2020	7	5	2
http://4g-capital.com/images/fullscreen/coming-soon-1@2x.jpg	warc/revisit	Nov 1, 2018	May 26, 2020	7	5	2
http://4g-capital.com/images/generic/pricing-table.jpg	warc/revisit	Nov 1, 2018	May 26, 2020	7	5	2
http://4g-capital.com/images/news/1.jpg	image/jpeg	Mar 29, 2020	Oct 12, 2022	3	2	1
http://4g-capital.com/images/news/10.jpg	image/jpeg	Mar 29, 2020	Oct 12, 2022	3	2	1
http://4g-capital.com/images/news/11.jpg	image/jpeg	Mar 29, 2020	Oct 12, 2022	3	2	1
http://4g-capital.com/images/news/12.jpg	image/jpeg	Mar 29, 2020	Oct 11, 2022	3	2	1
http://4g-capital.com/images/news/13.jpg	image/jpeg	Mar 29, 2020	Oct 13, 2022	3	2	1
http://4g-capital.com/images/news/14.jpg	image/jpeg	Mar 29, 2020	Oct 13, 2022	3	2	1
http://4g-capital.com/images/news/15.jpg	image/jpeg	Mar 29, 2020	Oct 15, 2022	3	2	1
http://4g-capital.com/images/news/16.jpg	image/jpeg	Mar 29, 2020	Oct 11, 2022	3	2	1