

Gathering Information About Websites

Here are some key pieces of information that a security expert usually gathers about a website:

1. Related domains and subdomains

2. Technology and programming languages being used

3. Cached pages

4. Website history

5. Publically indexed files on search engines

6. Default pages and login forms

7. Related IP addresses

8. Other services running on those IP addresses

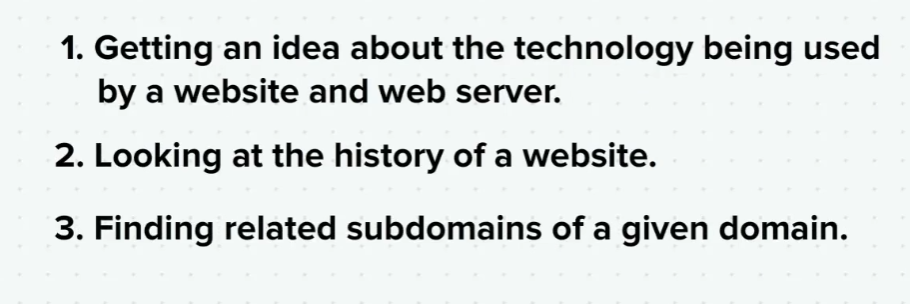
9. Version of the services/softwares being used

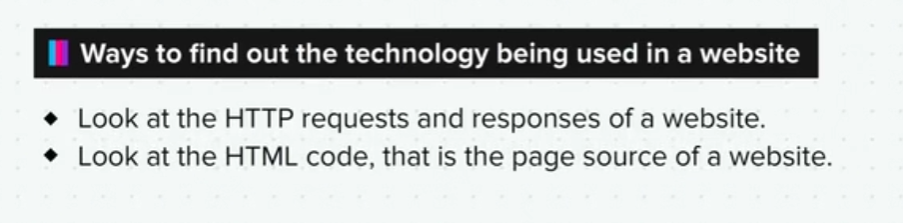
10. Publicly disclosed vulnerabilities in the softwares being used

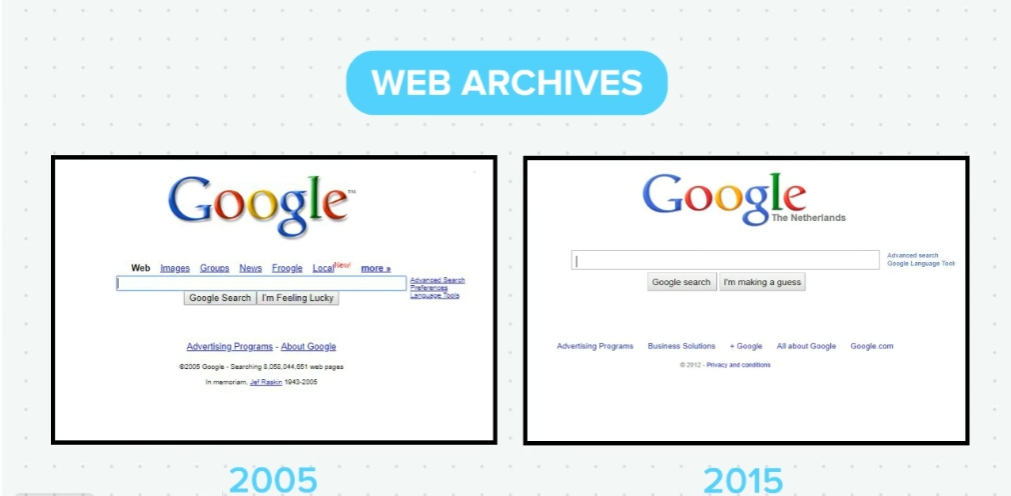
11. Default users

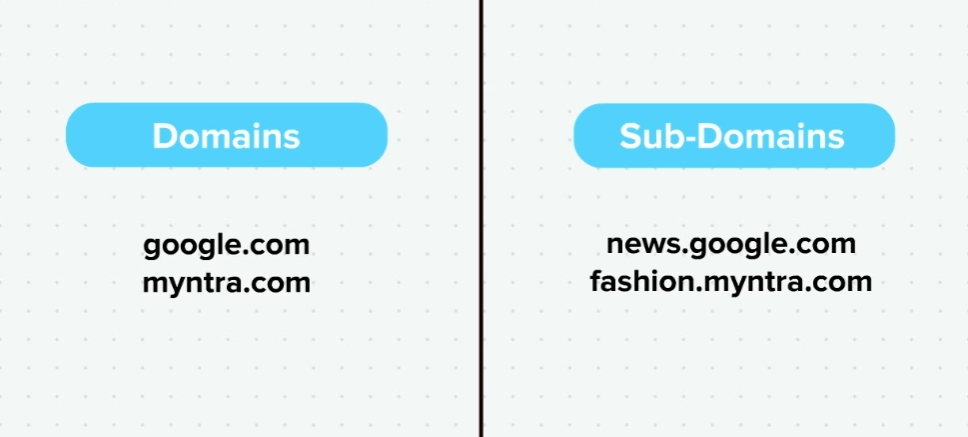
12. Default passwords

13. Valid email address and usernames









Gathering Targeted Information

Gathering targeted information about people

1. Name-How to find out full names and their related information:

Social media platforms

Professional platforms

2. Email- How to find out the name behind an email address:

Forgot password

Services linked to that email

Google search

3. Mobile numbers- How to find out the name behind a phone numbers:

Login and forgot password pages

Google search

Gathering targeted information about organisations

1. How to find information about an organisation:

Social media platforms

Company review services

Organisation financial analysis services

Gathering information about websites and web servers

1. Getting an idea about the technology being used by websites and web servers:

[www.builtwith.com](https://trainings.internshala.com/learn/hacking/screen/www.builtwith.com)

Important sections:

Frameworks: To see the programming languages used

Hosting providers: To see where the website is hosted

Webserver: To see the server software being used

2. Going through the history of a website

To see how the website looked in the past, its features, additions and deletions that have been made over time:

[web.archive.org](https://trainings.internshala.com/learn/hacking/screen/web.archive.org)

Important sections:

Go to the year you want to see

Check out screenshots taken on any day, and also see the website as it was on that day

3. Finding out sub domains related to a domain

[www.dnsdumpster.com](https://trainings.internshala.com/learn/hacking/screen/www.dnsdumpster.com)

Important sections:

Host Records (A): To see a list of all the sub domains of any given domain.

Exercise

Q1. Run a search for your own name, email and mobile number using all the methodologies discussed in this topic and find what information about you is available in the open.

Q2. Gather builtwith information about a known website and try understanding the output.

Q3. Gather the names of the subdomains of a known website and see what kind of applications are running on them.

Q4. Try using various features of web.archive.org.

ummary

Now that we have come to the end of this topic, you should be able to:

1. Gather targeted information about an organisation or a person using the basic information acquired earlier

2. Use social media, yellow pages and other listing services to gather detailed information about the target