Indian Institute of Information Technology Surat

Lab Report on

Information Security (CS 602)

Practical Submitted by

Aditya Kumar(UI22CS03)

Course Faculty

Dr. Reema Patel

Department of Computer Science and Engineering
Indian Institute of Information Technology Surat
Gujarat-394190, India

January-2025

Table of Contents

ASSIGNMENT 1

Select any browser and try to secure your browser by following settings:

(i) trusted sites/blocked sites etc.

(ii) by enabling or disabling the cookies.

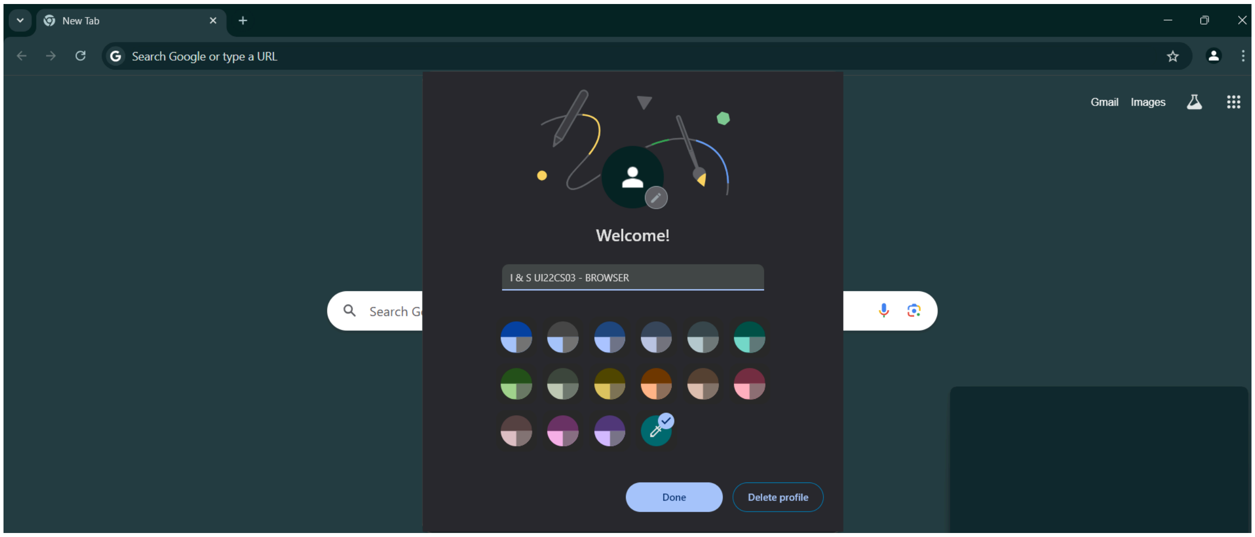
(iii) use of pop up blocker

(iv) by enabling or disabling scripts

(v) browsing history

(vi) saving passwords/master password

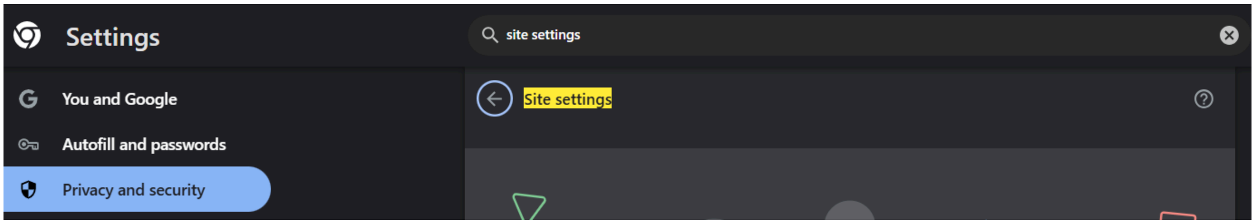
For this assignment I have used Chrome browser and in that i have created a new profile :



(i) Trusted Sites/Blocked Sites

It makes trusted sites help to ensure secure connections and prevents accidental exposure to malicious content. Blocking sites restricts access to potentially harmful or unwanted content, enhancing overall security.

To do so, I have followed below steps:
Steps : **Settings** > **Privacy and security** > **Site Settings**.



Settings

site settings

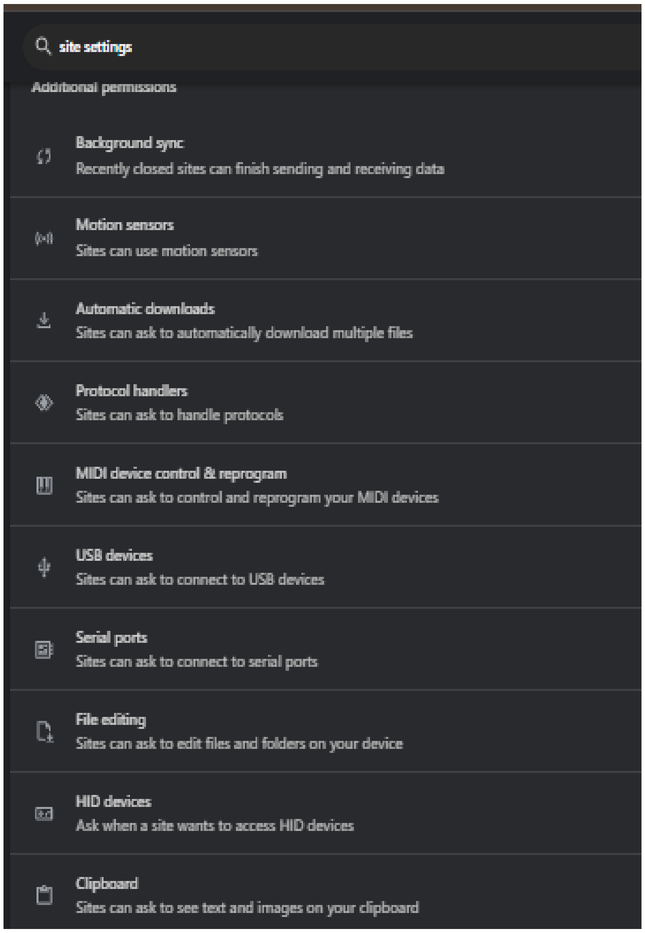
You and Google

Autofill and passwords

Privacy and security

Site settings

When I deep dived into i found many additional options like:



site settings

Additional permissions

Background sync
Recently closed sites can finish sending and receiving data

Motion sensors
Sites can use motion sensors

Automatic downloads
Sites can ask to automatically download multiple files

Protocol handlers
Sites can ask to handle protocols

MIDI device control & reprogram
Sites can ask to control and reprogram your MIDI devices

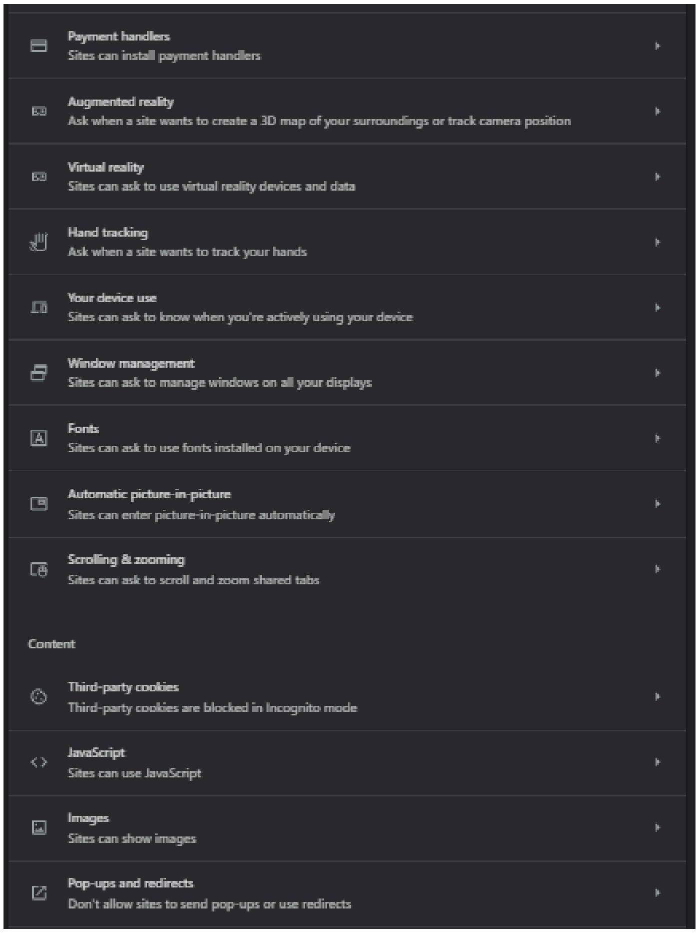
USB devices
Sites can ask to connect to USB devices

Serial ports
Sites can ask to connect to serial ports

File editing
Sites can ask to edit files and folders on your device

HID devices
Ask when a site wants to access HID devices

Clipboard
Sites can ask to see text and images on your clipboard



Payment handlers
Sites can install payment handlers

Augmented reality
Ask when a site wants to create a 3D map of your surroundings or track camera position

Virtual reality
Sites can ask to use virtual reality devices and data

Hand tracking
Ask when a site wants to track your hands

Your device use
Sites can ask to know when you're actively using your device

Window management
Sites can ask to manage windows on all your displays

Fonts
Sites can ask to use fonts installed on your device

Automatic picture-in-picture
Sites can enter picture-in-picture automatically

Scrolling & zooming
Sites can ask to scroll and zoom shared tabs

Content

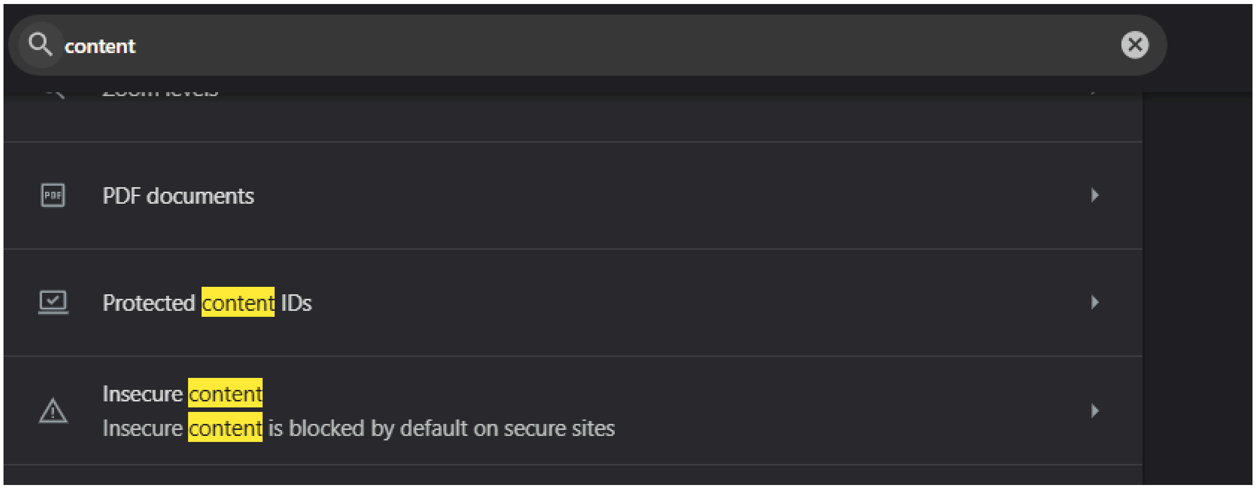
Third-party cookies
Third-party cookies are blocked in Incognito mode

JavaScript
Sites can use JavaScript

Images
Sites can show images

Pop-ups and redirects
Don't allow sites to send pop-ups or use redirects

When further investigated found these Insure content



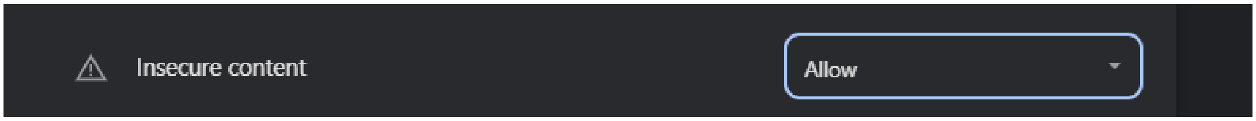
content

Zoom levels

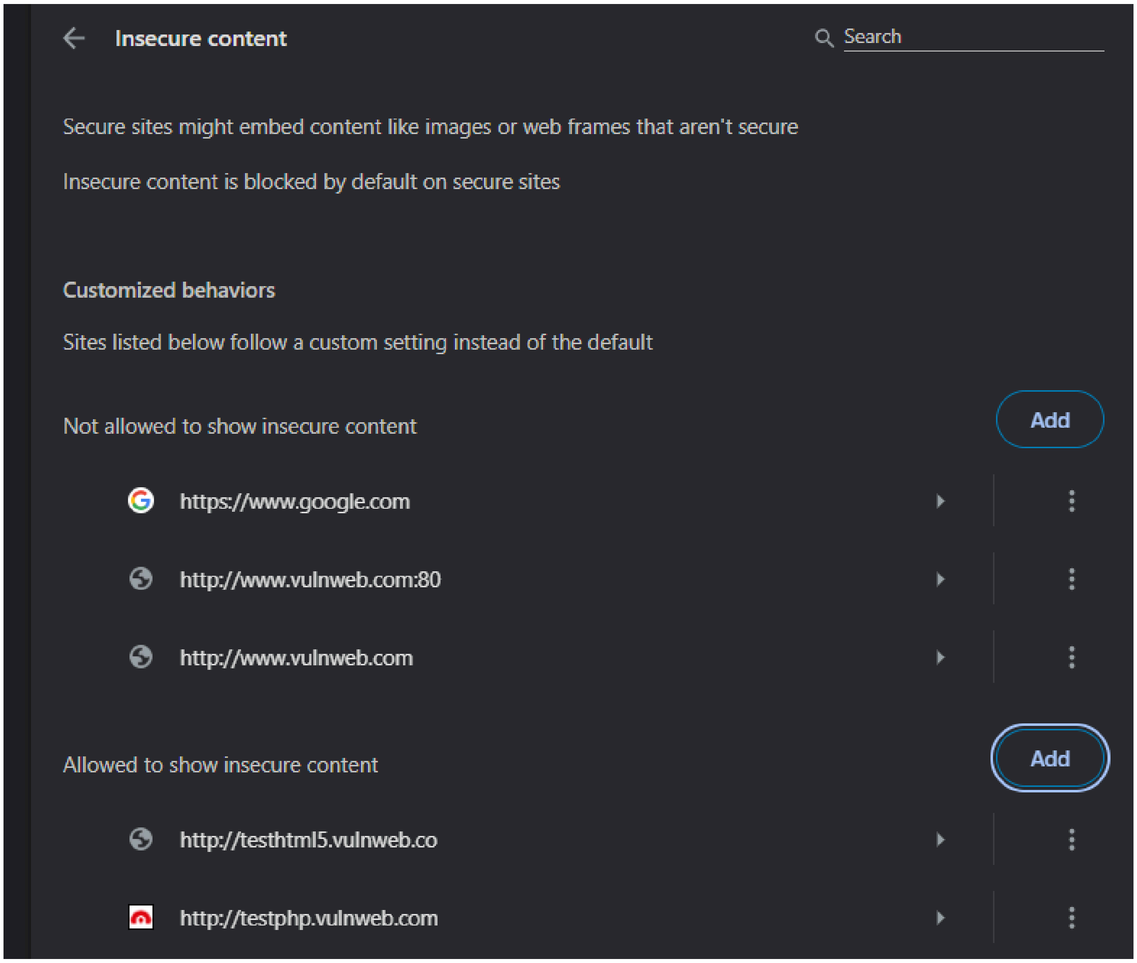
PDF documents

Protected content IDs

Insecure content
Insecure content is blocked by default on secure sites



Insecure content: Allow



Secure sites might embed content like images or web frames that aren't secure

Insecure content is blocked by default on secure sites

Customized behaviors

Sites listed below follow a custom setting instead of the default

Not allowed to show insecure content

https://www.google.com

http://www.vulnweb.com:80

http://www.vulnweb.com

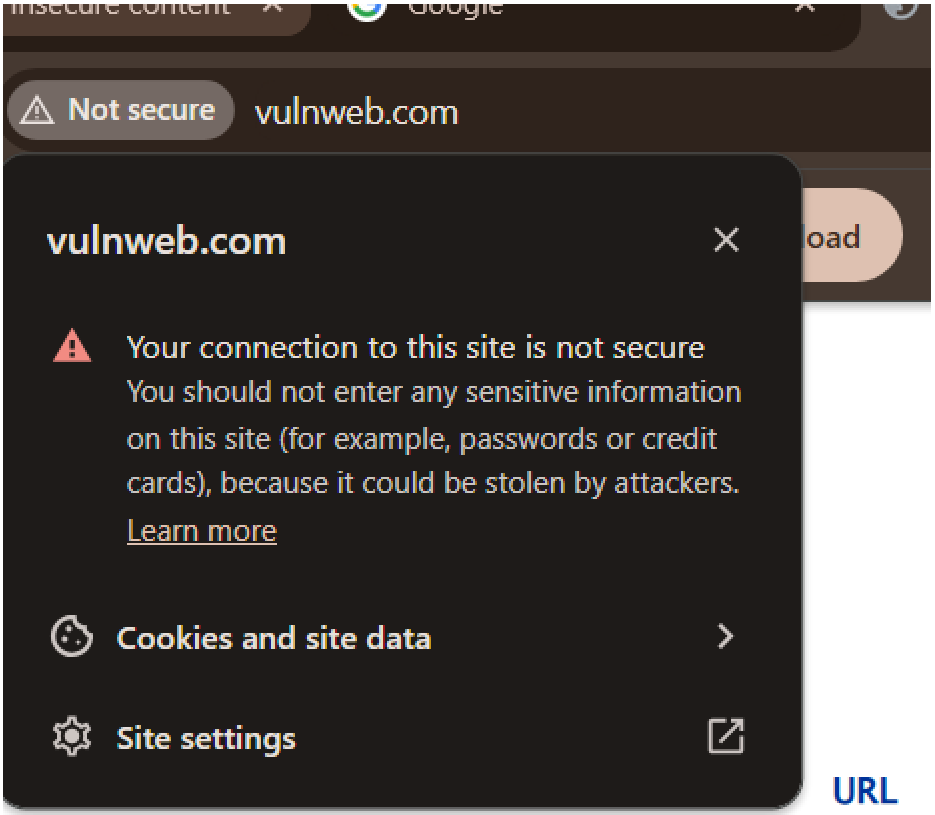
Allowed to show insecure content

http://testhtml5.vulnweb.co

http://testphp.vulnweb.com

I have visited few only “http” insecure website and tried to make it block and unblock

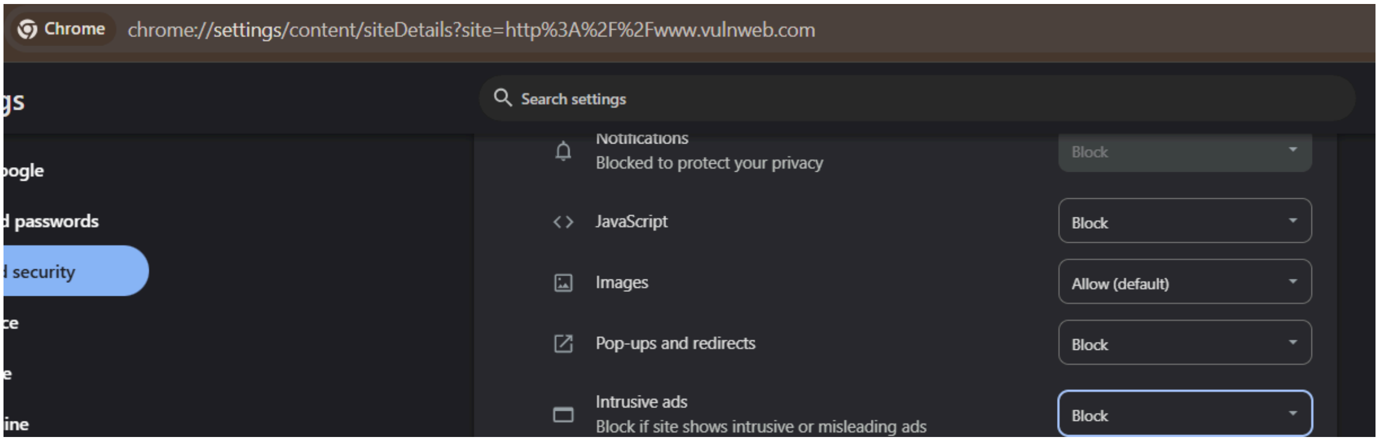
These kind of insecure website like below can contain malicious javascript code and execute in browser to hijack data and even compromise the computer system



vulnweb.com

Your connection to this site is not secure
You should not enter any sensitive information on this site (for example, passwords or credit cards), because it could be stolen by attackers. Learn more

Further went deeper on http://www.vulnweb.com/ abd blocked all the js, pop up and ads as well



chrome://settings/content/siteDetails?site=http%3A%2F%2Fwww.vulnweb.com

Notifications
Blocked to protect your privacy — Block

JavaScript — Block

Images — Allow (default)

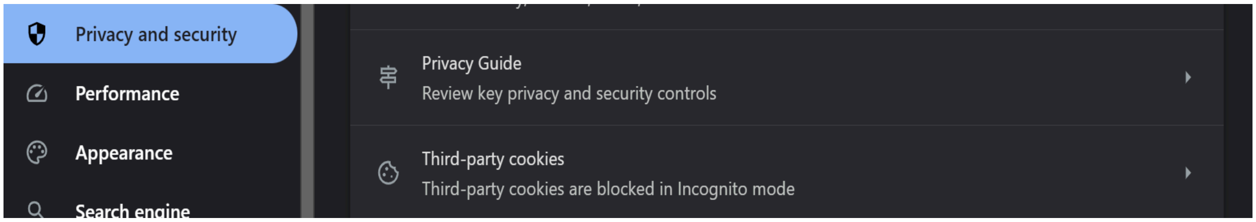
Pop-ups and redirects — Block

Intrusive ads
Block if site shows intrusive or misleading ads — Block

(ii) Enable/Disable Cookies

Cookies: store user data for websites. Disabling cookies can enhance privacy by limiting tracking, but it may also hinder website functionality. Blocking third-party cookies is a common compromise for enhanced privacy without disrupting user experience.

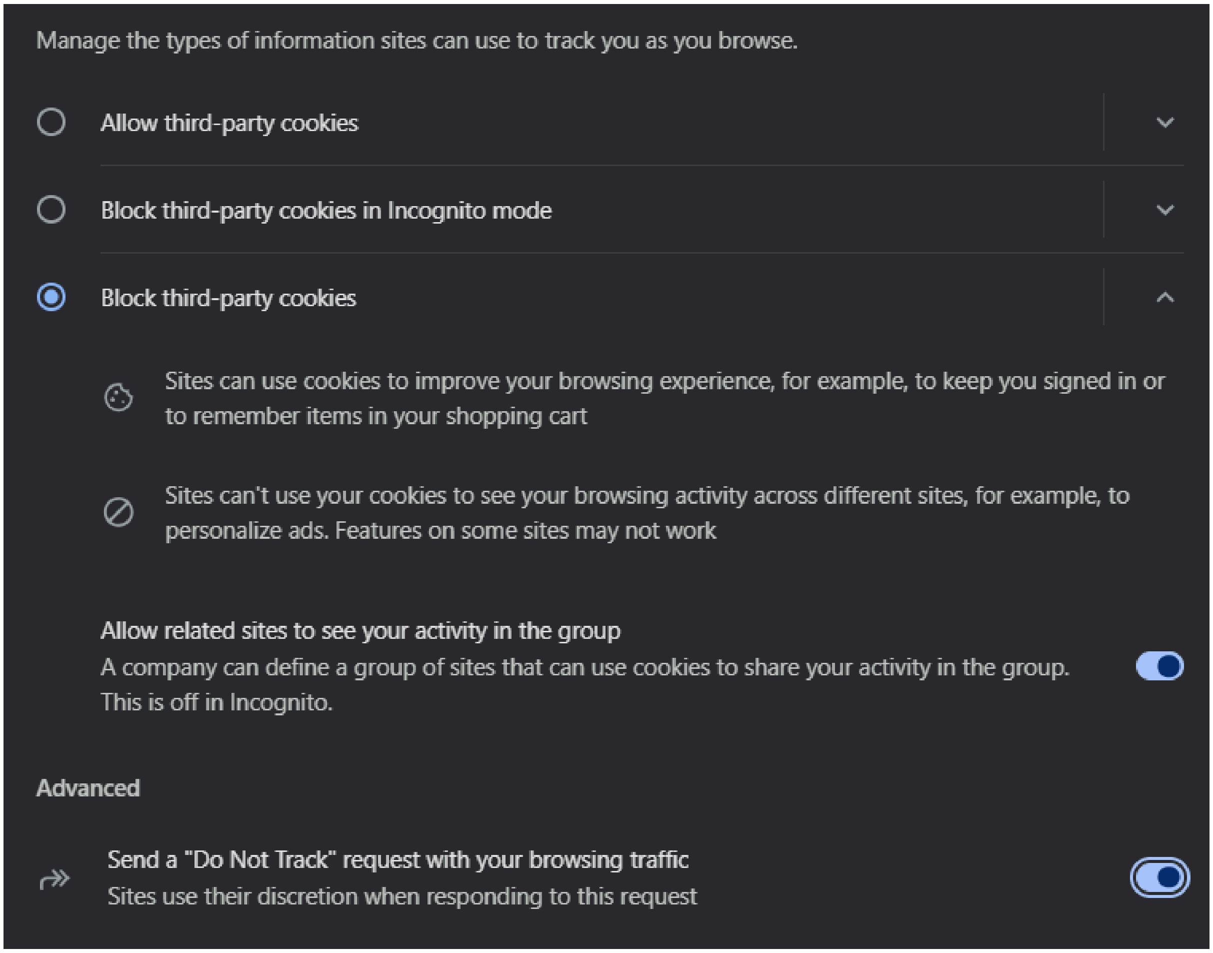
Steps : **Settings** > **Privacy and security** > **Cookies and other site data**.



Privacy Guide
Review key privacy and security controls

Third-party cookies
Third-party cookies are blocked in Incognito mode

To make it secure I have disabled all third party cookies also turn on “Do not track” in advance



Manage the types of information sites can use to track you as you browse.

○ Allow third-party cookies

○ Block third-party cookies in Incognito mode

● Block third-party cookies

Sites can use cookies to improve your browsing experience, for example, to keep you signed in or to remember items in your shopping cart

Sites can't use your cookies to see your browsing activity across different sites, for example, to personalize ads. Features on some sites may not work

Allow related sites to see your activity in the group
A company can define a group of sites that can use cookies to share your activity in the group. This is off in Incognito.

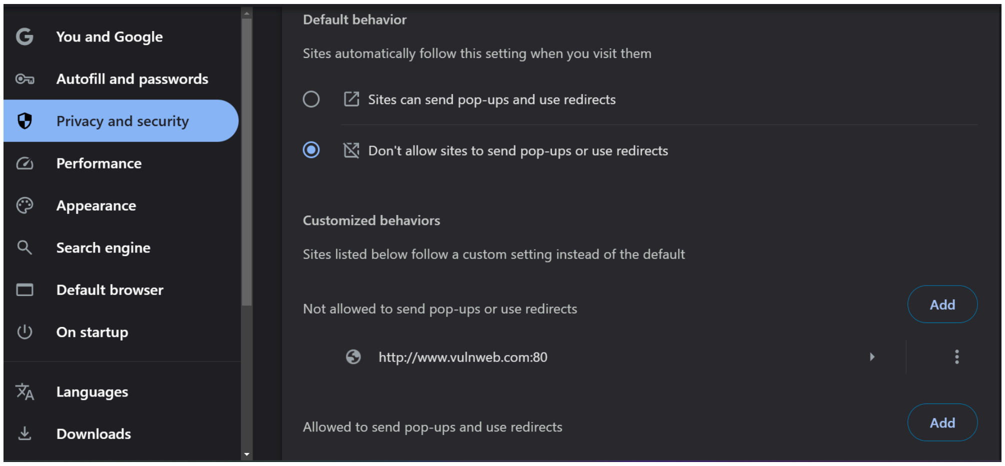
Advanced

Send a "Do Not Track" request with your browsing traffic
Sites use their discretion when responding to this request

(iii) Use of Pop-up Blocker

Pop-ups can be intrusive and sometimes deliver malware. Using a pop-up blocker helps to maintain a clean and secure browsing environment by preventing unsolicited windows.

Steps: **Settings** > **Privacy and security** > **Site Settings** > **Pop-ups and redirects**.
Set this to **Blocked** for securing the browser, there are a lot of ads pop up which disturbs.



Default behavior

Sites automatically follow this setting when you visit them

○ Sites can send pop-ups and use redirects

● Don't allow sites to send pop-ups or use redirects

Customized behaviors

Sites listed below follow a custom setting instead of the default

Not allowed to send pop-ups or use redirects

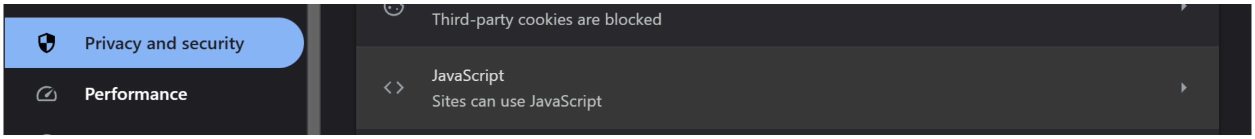
http://www.vulnweb.com:80

Allowed to send pop-ups and use redirects

(iv) Enable/Disable Scripts

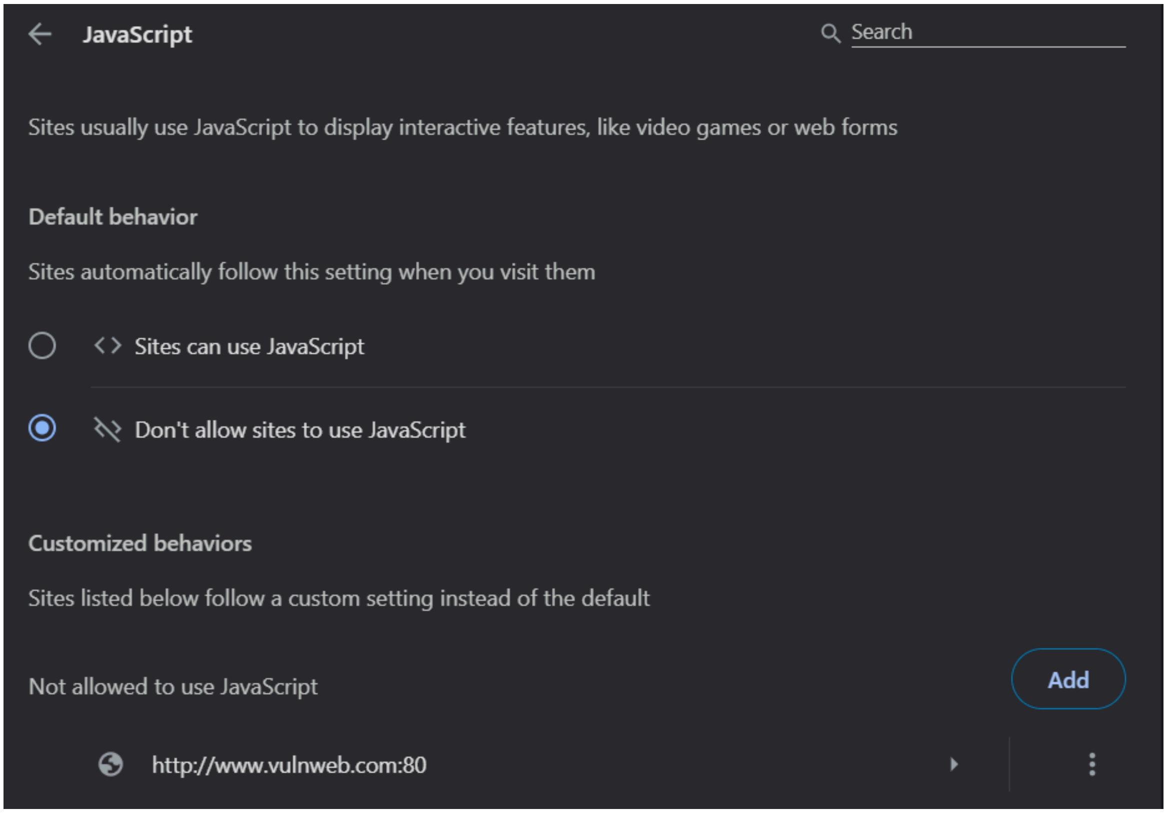
Scripts (like JavaScript) enhance website functionality but can be exploited for malicious activities. Disabling scripts by default and selectively enabling them increases security.
Hackers can inject malicious Scripts which can infect the computer and make it slow

Steps : **Settings** > **Privacy and security** > **Site Settings** > **JavaScript**



Third-party cookies are blocked

JavaScript
Sites can use JavaScript



JavaScript

Sites usually use JavaScript to display interactive features, like video games or web forms

Default behavior

Sites automatically follow this setting when you visit them

○ Sites can use JavaScript

● Don't allow sites to use JavaScript

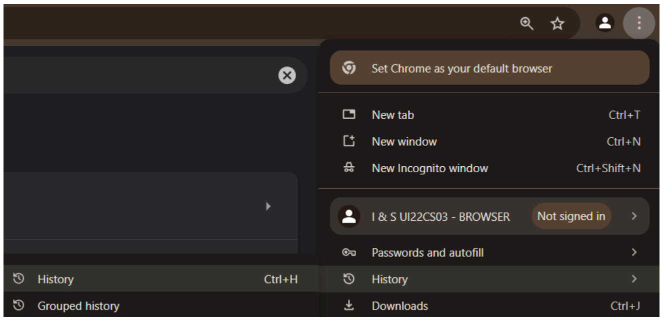
Customized behaviors

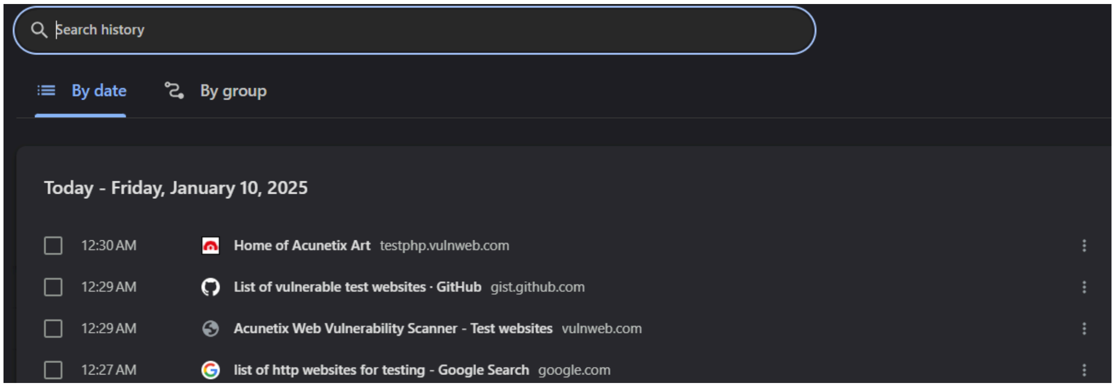
Sites listed below follow a custom setting instead of the default

Not allowed to use JavaScript

http://www.vulnweb.com:80

(v) Browsing History



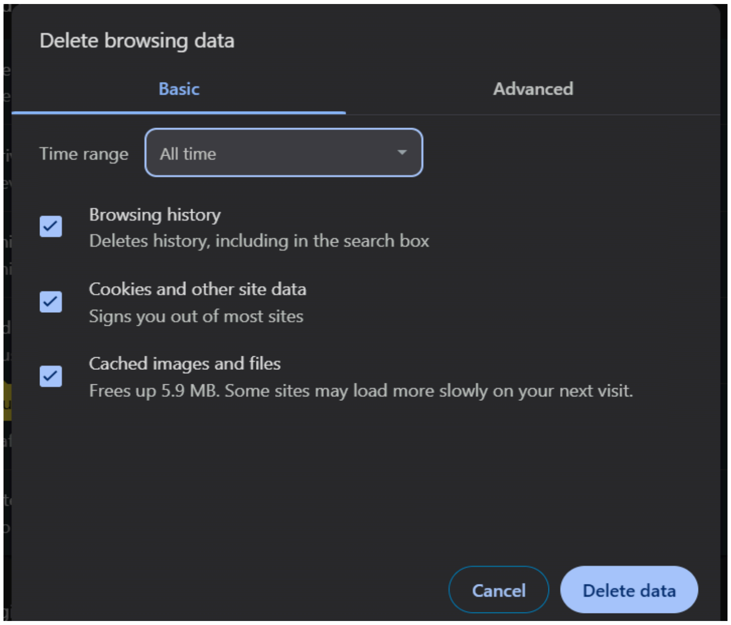


Today - Friday, January 10, 2025

```
□ 12:30 AM   Home of Acunetix Art  testphp.vulnweb.com
□ 12:29 AM   List of vulnerable test websites · GitHub  gist.github.com
□ 12:29 AM   Acunetix Web Vulnerability Scanner - Test websites  vulnweb.com
□ 12:27 AM   list of http websites for testing - Google Search  google.com
```

To Clear the history

Steps: **Settings** > **Privacy and security** > **Clear browsing data**.

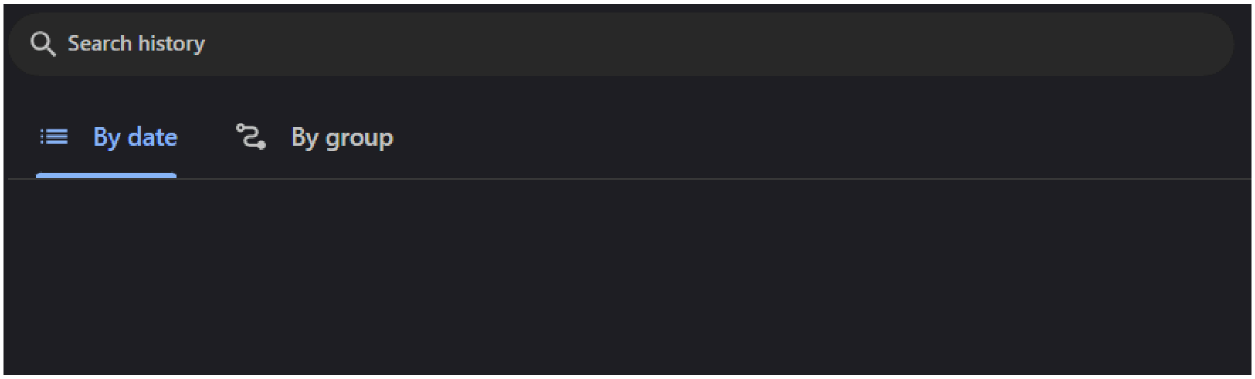


Time range: All time

☑ Browsing history
Deletes history, including in the search box

☑ Cookies and other site data
Signs you out of most sites

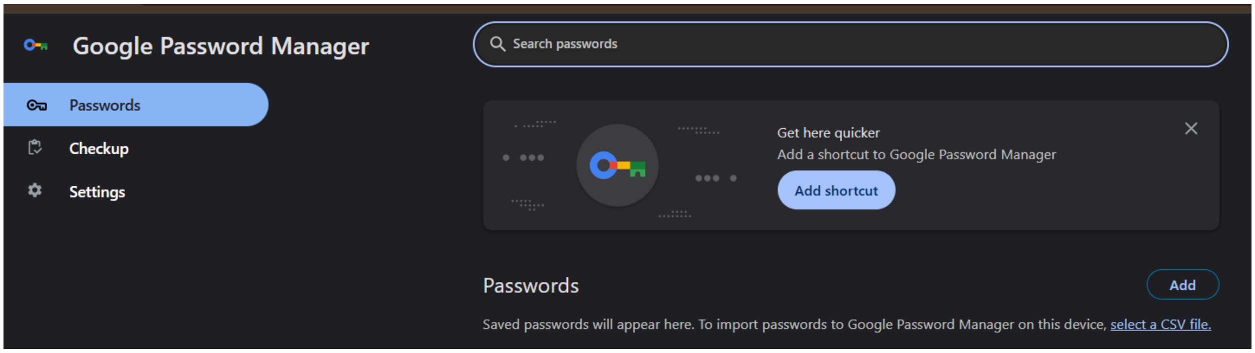
☑ Cached images and files
Frees up 5.9 MB. Some sites may load more slowly on your next visit.



(vi) Saving Passwords/Master Password

Saving passwords in the browser can be convenient but poses a security risk if the browser is compromised. Using a master password or a dedicated password manager enhances the security of stored credentials.

Steps : **Settings** > **Autofill** > **Passwords**



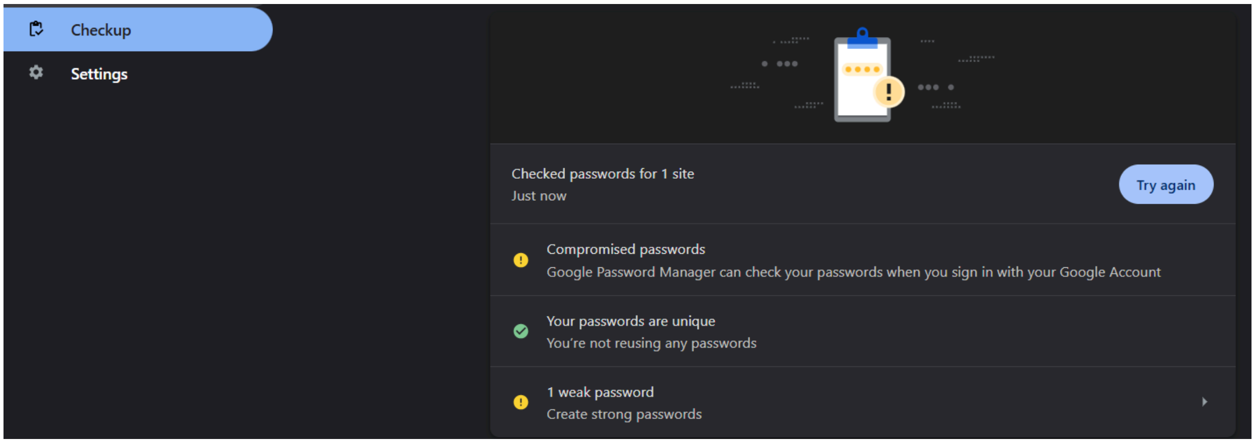
Saved passwords will appear here. To import passwords to Google Password Manager on this device, select a CSV file.

Google Password Manager : It encrypts passwords using your Google account credentials, ensuring that your data is secure. Passwords are stored in Google's cloud, accessible only to you.

Auto-fill and Auto-save: The manager automatically fills in passwords for websites and apps you use, streamlining the login process. It also prompts to save new passwords, reducing the need to remember them.

Password Sync Across Devices:Google Password Manager syncs passwords across all devices where you're signed into your Google account, providing seamless access whether on your phone, tablet, or computer.

Password Checkup: This feature alerts users if any saved passwords have been compromised in data breaches. It also suggests stronger alternatives for weak or reused passwords.

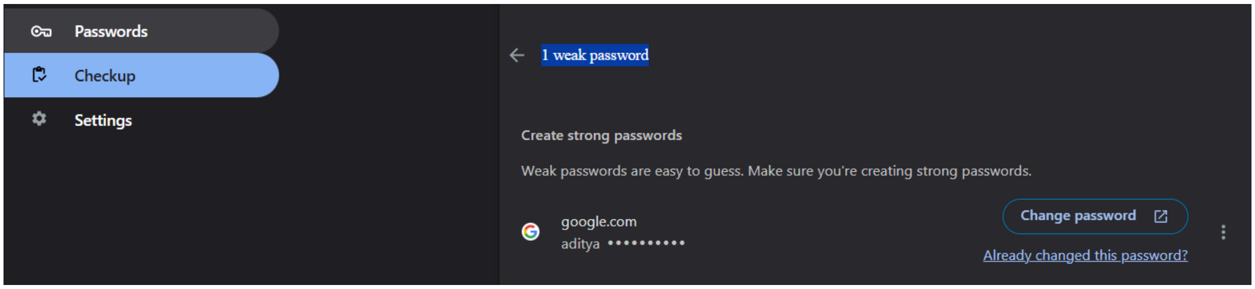


Checked passwords for 1 site
Just now

Compromised passwords
Google Password Manager can check your passwords when you sign in with your Google Account

Your passwords are unique
You're not reusing any passwords

1 weak password
Create strong passwords



1 weak password

Create strong passwords

Weak passwords are easy to guess. Make sure you're creating strong passwords.

google.com
aditya ••••••••••

From above I can observe that in checkup password, it uses string methods and dictionary to evaluate is that password strong, medium or weak.

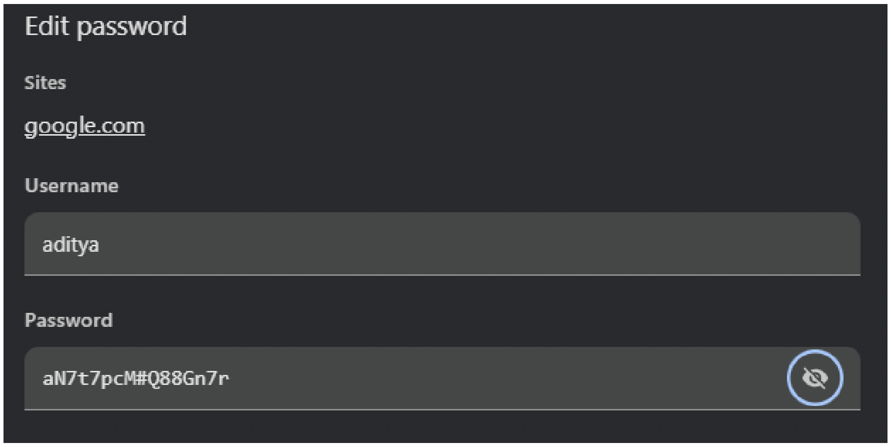
Importance of Strong Passwords

A strong password is a critical aspect of digital security. It acts as the first line of defense against unauthorized access to your accounts. Here are the key characteristics and importance of a strong password:

1. **Length**:
   - A strong password should be at least 12-16 characters long. Longer passwords are harder to crack through brute-force attacks.
2. **Complexity**:
   - Use a mix of uppercase and lowercase letters, numbers, and special characters. This complexity makes it difficult for attackers to guess the password.
3. **Uniqueness**:
   - Each account should have a unique password. This prevents a breach of one account from compromising others.
4. **Avoid Common Patterns**:
   - Avoid easily guessable patterns like "password123," "admin," or sequential numbers. Use random combinations instead.
5. **Memorability**:

- ○ While the password should be complex, it should also be memorable or managed using a password manager. Avoid writing it down or storing it in unsecured locations.

Let's set a strong password: **aN7t7pcM#Q88Gn7r**



Edit password

Sites

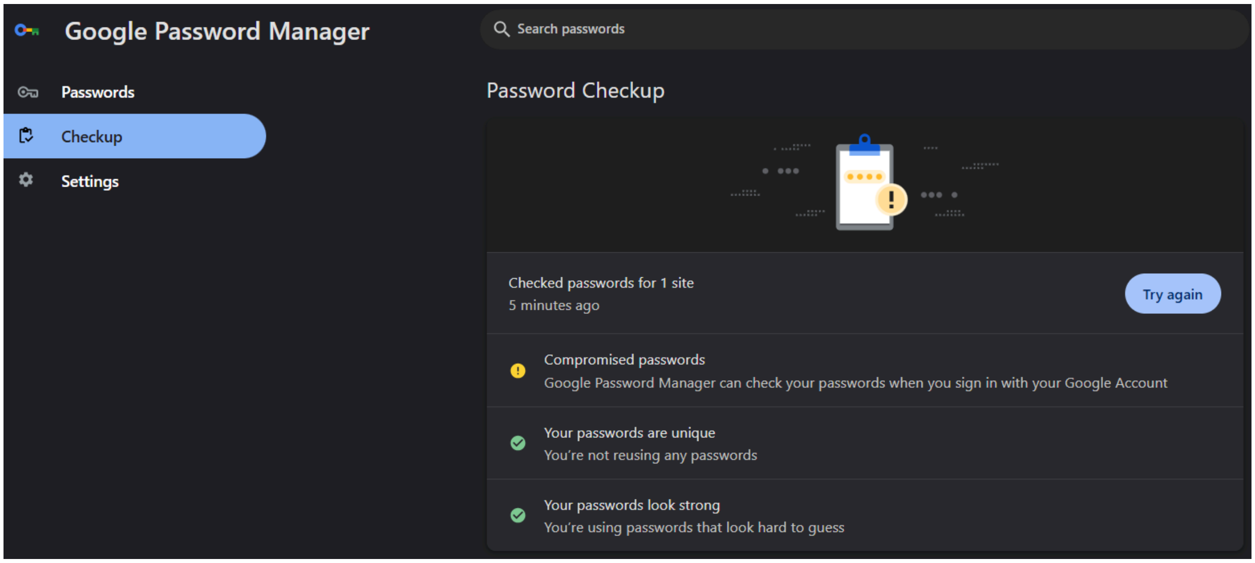
google.com

Username

aditya

Password

aN7t7pcM#Q88Gn7r



Password Checkup

Checked passwords for 1 site
5 minutes ago

Compromised passwords
Google Password Manager can check your passwords when you sign in with your Google Account

Your passwords are unique
You're not reusing any passwords

Your passwords look strong
You're using passwords that look hard to guess

Observations

(i) Trusted Sites/Blocked Sites

Managing trusted and blocked sites allowed me to control website interactions with my browser. I observed that marking trusted sites provided a seamless browsing experience, while blocking suspicious or harmful sites effectively reduced exposure to potential security threats.

(ii) Enabling or Disabling Cookies

Enabling cookies improved website functionality by remembering login details and preferences. However, disabling third-party cookies significantly enhanced privacy by reducing tracking and limiting the collection of personal data by advertisers and third-party services.

(iii) Use of Pop-up Blocker

Using the pop-up blocker drastically reduced intrusive advertisements and prevented accidental clicks on potentially malicious pop-ups. This improved my browsing experience by eliminating distractions and mitigating security risks.

(iv) Enabling or Disabling Scripts

Disabling scripts by default helped minimize the risk of malicious code execution, but it also restricted certain website functionalities. Selectively enabling scripts for trusted sites maintained a balance between security and usability.

(v) Browsing History

Managing and clearing browsing history helped protect my privacy, especially on shared or public devices. Regularly deleting history and cached data reduced the chances of sensitive information being accessed by unauthorized users.

(vi) Saving Passwords/Master Password

Using the password manager streamlined password storage and retrieval. The master password feature provided an additional layer of security, ensuring that stored credentials remained protected from unauthorized access.

Conclusion

This exercise provided valuable insights into various browser security settings and their impact on privacy and security. By effectively managing trusted sites, cookies, pop-ups, scripts, browsing history, and passwords, I was able to enhance my online safety and protect sensitive information. This experience emphasized the importance of regularly reviewing and adjusting browser settings to strike a balance between functionality and security, ultimately fostering a safer and more private browsing environment.