**Browser Extensions**

**Task: Identify and remove potentially harmful browser extensions**

**Objective:** Learn to spot and remote potentially harmful browser extensions.

**Tools:** Any web browser (Chrome, Firefox)

**Deliverables:** List of suspecious extensions found and removed (if any)

>>>

As in my browser i have only one extension I.e, shodan. It’s is an legitimate extension used to tell where the website is hosted (region) and who own the ip and what other service or ports are open.

Let’s assume an hypothetical situation where my browser has one extension which wasn’t installed by me and I don’t have any use with that, Let the extension be “Super Saver Deals” where it provides the coupons if there is any deals are running in a website, when i checked for permission it allowd, there are plenty of suspecious permission which are not required for the deals, they are:

**Read and change your Data:**

As it can read and change all your data on the website that you visit. It can see the all the typings in a web page (like: username, password, card details, ecc..). Also it can inject malicious code in a website which is a fake version of original.

**Access Your Browser History:**

It has no work to access my browser history, but It has access to visit it.

**Managing your Downloads:**

This can have the authority to download anything in your device.

**Read and Modify your Data:**

This can affect when you fill the details of your bitcoin withdrawl address, bank receiver address, etc..

**Communicate with Cooperating Website:**

It can communicate with their own malicious server and transfer the data to that server.

**Injecting Unwanted ads:**

It injects the unwanted ads in our webpage which may be injected to differernt malicious file.