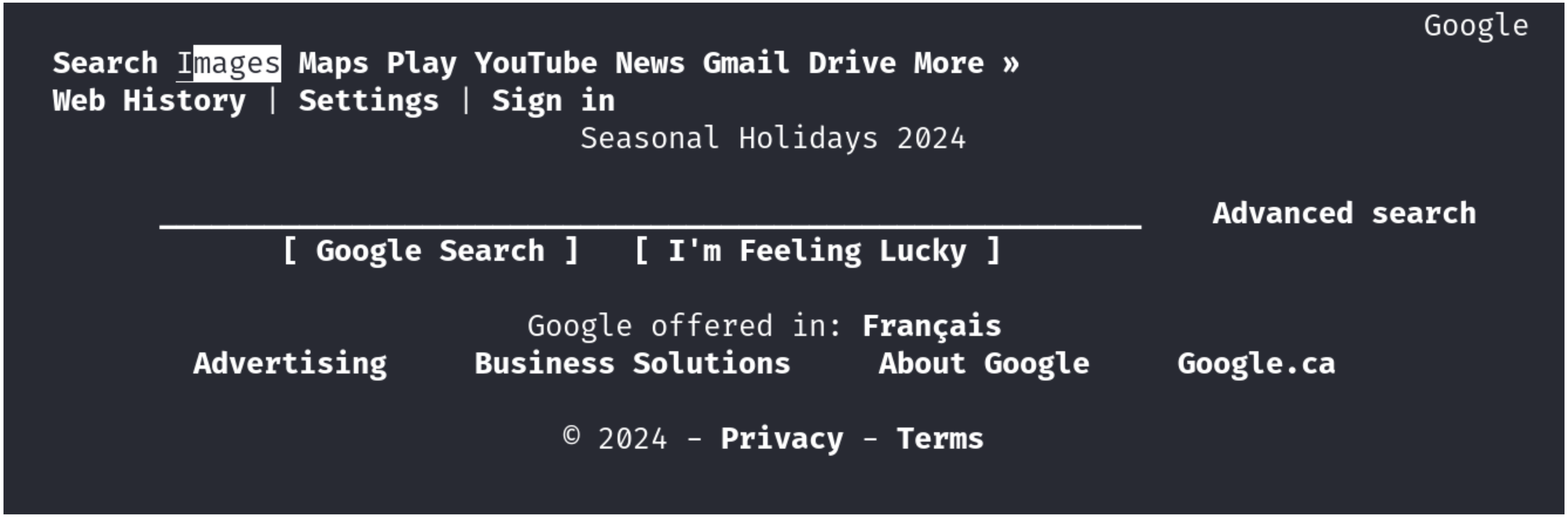
Node JS OS Command Injection

Node JS is a runtime environment which allows JavaScript to be used to write many different types of applications, including software for running webservers

Node JS OS Command Injection

Node JS web apps can be vulnerable to OS command injection if they're written insecurely, particularly if the app fails to sanitize user input

Privilege Escalation
Sudo Links

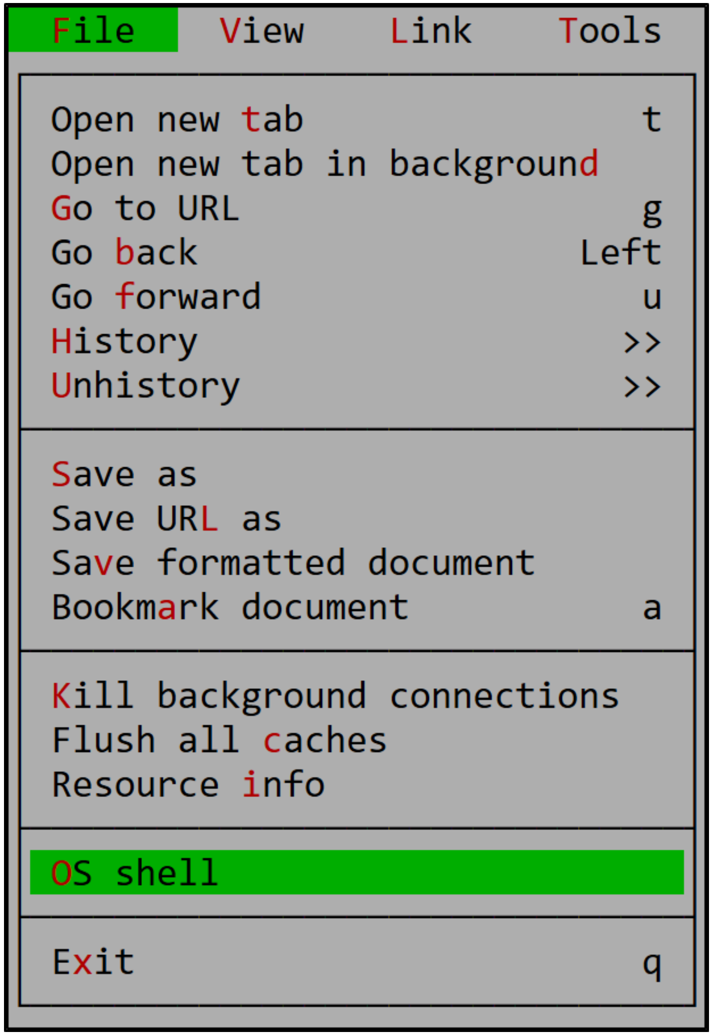


```
                                                                        Google
  Search Images Maps Play YouTube News Gmail Drive More »
  Web History | Settings | Sign in
                            Seasonal Holidays 2024

        ____________________________________________________    Advanced search
              [ Google Search ]   [ I'm Feeling Lucky ]

                         Google offered in: Français
        Advertising     Business Solutions     About Google     Google.ca

                          © 2024 - Privacy - Terms
```

The ELinks program, which uses the Links command in Linux, is a text-based web browser that can be used from the command line interface

Privilege Escalation
Sudo Links

We have sudo access to the Links binary. Links is a text-based web browser, but more importantly, we can open an OS shell while using the Links program, which, when combined with sudo, is a privileged shell


File
View
Link
Tools
Open new tab t
Open new tab in background
Go to URL g
Go back Left
Go forward u
History >>
Unhistory >>
Save as
Save URL as
Save formatted document
Bookmark document a
Kill background connections
Flush all caches
Resource info
OS shell
Exit q