CHAPTER

Understanding Browsers and Beyond

3

INFORMATION IN THIS CHAPTER

- Browser's basics
- Browser architecture
- Custom browsers
- Addons

INTRODUCTION

In first chapter we discussed a little about web browsers in general, then we moved on to put some light on different popular browsers such as Chrome and Firefox and also tried to simplify the process behind browsing. Now it's time to understand what exactly happens in background. You might think that why is this required. As we have gone through some of the details earlier in this book the reason to focus on browsers and discuss different aspects of it in details is because the majority of tools we will use in the course of this book are mainly web based and to communicate with those web-based tools we will use browsers a lot. That's why it is very important to understand the working of a browser and what exactly is going on in background when we do something in it. Learning the internal process of how browser operates will help us choosing and using it efficiently. Later we will also learn about ways to improve the functionalities of our daily browsers. Now without wasting much time on definitions and descriptions which we already covered, let's get to the point directly and that is "The secrets of browser operation."

BROWSER OPERATIONS

When we open a browser, we will generally find an address bar where we can insert the web address that we want to browse; a bookmark button to save the link for future use; a Show bookmark button, where we can see what all bookmark links we already have in the browser; back and forward button to browse pages accordingly; a home button to redirect from any page to the home page which has been already set in the browser and an options button to set all the browser settings such as to set home page, download location, proxy settings, and lots of other settings. The location of

Hacking Web Intelligence. http://dx.doi.org/10.1016/B978-0-12-801867-5.00003-3

these buttons might change with the versions to provide better user experience but somewhere in the interface of the browser you will find all these buttons for sure.

As all the browsers have quite similar user interfaces, with most of the functionalities common as discussed above but still there are some facilities and functionalities that make each browser unique. There are different popular browsers such as Chrome, Firefox, IE, Opera, and Safari but as discussed earlier in Chapter 1, we will focus mostly on two browsers which are also present in open source versions and they are Chrome and Firefox.

HISTORY OF BROWSERS

The first browser was written by Tim Berners-Lee in 1991 which only displayed text-based results. The first user-friendly commercial graphical browser was Mosaic. To standardize the web technology an organization was found named World Wide Web Consortium, also known as W3C in 1994. Almost all of the browsers came into the market in mid-1990s. Today browsers are much more powerful than they were in early 1990s. The technology has evolved rapidly from text only to multimedia and is still moving on, today browsers display different type of web resources such as video, images, documents along with HTML and CSS. How a browser will display these resources are specified by W3C.

BROWSER ARCHITECTURE

Browser architecture differs from browser to browser, so based on common components if we derive an architecture it will be something as follows.

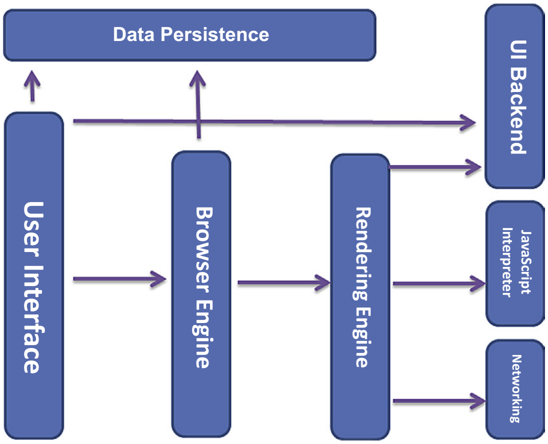


FIGURE 3.1

Browser architecture.

USER INTERFACE

The user interface here is what we have already discussed above. It's all about the buttons and bars to access the general features easily.

BROWSER ENGINE

It's the intermediate or combination of layout engine with render engine. Layout engine is nothing but the user interface.

RENDERING ENGINE

It's responsible for displaying the requested web resources by parsing the contents. By default it can parse html, xml, and images. It uses different plugins and/or extensions to display other type of data such as flash, PDF, etc.

There are different rendering engines such as Gecko, WebKit, and Trident. Most widely used rendering engine is WebKit or its variant version. Gecko and WebKit are open source rendering engines while Trident is not. Firefox uses Gecko, Safari uses WebKit, Internet Explorer uses Trident, Chrome and Opera uses Blink, which is a variant of WebKit. Different rendering engines use different algorithms and also have their different approaches to parse a particular request. The best example to support this statement is that you might have encountered some website which work with a particular browser because that website is designed compatible to that browser's rendering engine so in other browsers they don't work well.

NETWORKING

This is a major component of a browser. If it fails to work, all other activities will fail with it. The networking component can be described as socket manager which takes care of the resource fetching. It's a whole package which consists of application programming interfaces, optimization criteria, services, etc.

UI BACKEND

It provides user interface widgets, drawing different boxes, fonts, etc.

JAVASCRIPT INTERPRETER

Used to interpret and execute java script code.

DATA PERSISTENCE

It is a subsystem that stores all the data required to save in a browser such as session data. It includes bookmarks, cookies, caches, etc. As browsers store cookies which contain user's browsing details that are often used by marketing sites to push advertisement. Let's say we wanted to buy a headphone from some e-commerce site so we visited that site but never bought that. Then from our browsing data marketing sites will get this information and will start pushing advertisements at us of the same product may be from that same e-commerce site or others. This component definitely has its own importance.

ERROR TOLERANCE

All the browsers have traditional error tolerance to support well-known mistakes to avoid invalid syntax errors. Browsers have this unique feature to fix the invalid syntax that's why we never get any invalid syntax error on result. Though different browsers fix these errors in different way but anyhow all the browsers do it on or other way.

THREADS

Almost every process is single threaded in all the browsers, however, network operations are multithreaded. It's done using 2–6 numbers of parallel threads. In Chrome the tab process is the main thread, while in other browsers like Firefox and Safari rendering process is the main thread.

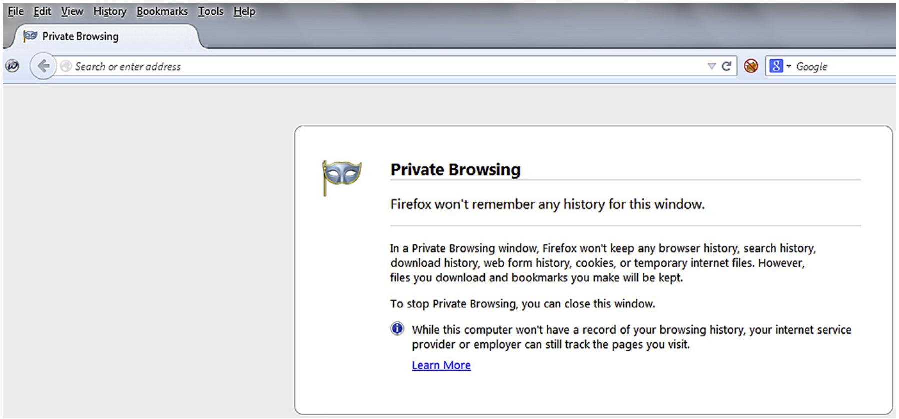
BROWSER FEATURES

Web browsing is a very simple and generic term that we all are aware of, but are we aware of its importance. A web browser opens a window for us to browse all the information available on the web. Browsers can be used for both the purposes, online browsing as well as offline browsing. Online browsing is that we do regularly with an internet connection. Offline browsing means opening local html contents in a browser. Modern browser also provides features to save html pages for offline browsing. These features allow a user to read or go through something later without any internet connection; we all have used this feature sometime during our browsing experience. When we save a page for offline view, sometime we might find that certain contents in a page are missing during offline browsing. The reason being that when we save a page it only saves direct media available for the page, but if a page contains resources from some other sites then those things will be found missing in offline view. Let's discuss some of the added functionalities provided by browsers.

PRIVATE BROWSING

Incognito is the term associated with Chrome for private browsing, whereas Firefox uses private browsing only as the term. It allows us to browse the internet without saving details of what we browse for that particular browsing session. We can use private browsing for online transactions, online shopping, opening official mails on public devices, and much more.

In Firefox and Chrome we can find this option near new window option. The shortcut key to open secure browsing in Firefox is Ctrl+Shift+P and for Chrome is Ctrl+Shift+N. The difference between normal browsing window and a private browsing window is that we get some kind of extra icon present in the title bar of the window. In Firefox it's a mask icon whereas in Chrome it's a detective icon. For the fancy features, browsers use these kinds of fancy icons.



Private Browsing

Firefox won't remember any history for this window.

In a Private Browsing window, Firefox won't keep any browser history, search history, download history, web form history, cookies, or temporary internet files. However, files you download and bookmarks you make will be kept.

To stop Private Browsing, you can close this window.

While this computer won't have a record of your browsing history, your internet service provider or employer can still track the pages you visit.

FIGURE 3.2

Firefox private browsing.

Private browsing will not save any visited pages details, form fill entries, search bar entries, passwords, download lists, cached files, temp files or cookies. Though the data downloaded or bookmarked during secure browsing will be saved in local system.

What private browsing does not provide?

It only helps user to be anonymous for local system while the internet service provider, network admin, or the web admin can keep track of the browsing details and it will also not protect a user from keyloggers or spywares.

There is always an option available to delete the data stored by a browser manually. We can simply click on clear recent history button and select what needs to be deleted and it's done.

AUTOCOMPLETE

Almost all browsers have this feature to configure it to save certain information such as form details and passwords. This feature has different names in different browsers or it is specific with different rendering engines. Some of the names are Password Autocomplete, Form Pre-filing, Form Autocomplete, Roboform, Remember password, etc.

Browsers provide user freedom to configure whether to save these information or not, if yes then whether to get some kind of prompt or not, what to be saved and in what type it should be saved.

In Firefox to avoid password storage, go to Menu → Options → Security → Uncheck "Remember passwords for sites," though we can store password in encrypted format using browser configuration.

In Chrome, go to Menu → Settings → Show advanced settings → Under Passwords and forms uncheck "Enable Auto-fill to fill out web forms in single click" and "Offer to save your web password."

Some web application treat this as a vulnerability or possible security risk so they used to add an attribute "autocomplete=off" in their form of the input box value that they do not want a browser to save, but nowadays most of the browsers either ignore it or have stopped supporting this attribute and save all the data or some based on browser configuration.

PROXY SETUP

Proxy setup feature is also an important feature provided by any browser. This feature allows a user to forward the requests made by a browser to an intermediate proxy.

Most of the companies use some sort of proxy device to avoid data leakage and those settings can be done in browser to limit or monitor the browsing process. Proxy options are also popularly used by penetration testers to capture the request and responses sent and received by a browser. They generally use some interception proxy tool and configure the settings in browser.

In day-to-day life also proxy setup can be used for anonymous browsing or browsing or visiting some pages that are country restricted. In that case a user just has to collect one proxy IP address and the port number of some other country where that site or content is available then setting up the same in a browser to visit those pages.

Proxy setup in Firefox

Go to Menu → Options → Advanced → Network → Connection Settings → Manual proxy configuration and add the proxy here.

Proxy setup in Chrome

Go to Menu → Settings → Show advanced settings → Under Network click on Change proxy settings → Click on LAN Settings → Check Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections.) and add your settings.

RAW BROWSERS

There are specific browsers available by default with specific operating systems, such as Internet Explorer for Windows and Safari for Mac. Almost all the browsers have their versions available for different operating system. But the widely used and popular browsers are not the one which comes preinstalled with operating system but the one which are open source and easily available for different operating systems, i.e., Mozilla Firefox and Google Chrome. Though Google Chrome was mostly used by Windows operating system, one of its open source version was generally found preinstalled in many Linux operating systems and is called Chromium. As the name itself has similarities with the Google Chrome browser, their features also do match with each other with a little difference.

As earlier we came across that there are different types of browser rendering engine like Gecko, WebKit, etc. and Chrome uses Blink the variant of WebKit so does Chromium. This project initially started in 2008 and now there are more than 35 updated versions. This is one of the popular browsers among the open source community. It is the concept behind Google Chrome window being used as the main process because Chromium project was made to make lightweight, fast, and efficient browser which can also be known as shell of the web by making its tab to be the main process. There are different other browsers released based on the Chromium project source code. Opera, Rockmelt, and Comodo Dragon are some of the well-known browsers based on Chromium.

Now one thing is clear from above paragraph that if a browser will be open source, then community will use that code to create different other browsers by adding some extra functionality as Comodo Group added some security and privacy feature in the Chromium and released it as Comodo Dragon. Similarly Firefox also has different custom versions. So let's consider the base version browser as Raw browser and other browsers as customized browser.

WHY CUSTOM VERSIONS?

The custom versions are being used for different purposes, to use the true power of functionalities of the Raw browser to the fullest or in simple words to make better use of the features available by the Raw browsers. The custom browsers can help us to serve our custom requirements. Let's say we want a browser which can help us being online 24/7 in social networking sites. We can either add different social network addons on the browser of our choice to make it happen or we can start from scratch and build a version of browser which contains the required functionalities. Similarly for other cases like if we are penetration testers or security analysts, we might want a browser to perform different application security tests so we can customize a browser for the same. A normal user might need a browser to be anonymous while browsing so that no one can keep track of what he/she is browsing, this can also be done by customizing a browser. There are already a number of customized browsers available in the market to serve these purposes and similarly we can also create such customized browser according to our desire. As the process is a bit complex to be included in this chapter and would require some technical background to understand we will not be discussing it, still knowing that it is possible to do so opens a new window, for people who would like this just take it as a self-learning project.

The Chromium project has its official website, http://www.chromium.org where we can find different documentations and help materials to customize the browser for different operating systems. Apart from Chromium it is maintained at sourceforge, http://www.sourceforge.net/projects/chromium. From here we can download the browser, download browser source code, subscribe to the mailing list to get updated news about the project, and submit bugs and feature requests.

If you are interested to customize Chromium, it will be a great kick start if you subscribe the mailing list as well as explore the documentation available in sourceforge. The first step to customize any browser is to get its source code. So how to get the source code of Chromium? It's quite easy, we just need to download the latest tar or zip version of the browser. Later by performing untar or unzip we will be able to get the source code along with the documentation details inside.

Now let's move on to discuss some already customized browsers and their functionalities.

SOME OF THE WELL-KNOWN CUSTOM BROWSERS

EPIC (https://www.epicbrowser.com/)

Epic is a privacy browser as its tagline describes itself with the line "We believe what you browse and search should always be private." It is made to extend the online privacy of a user. This browser is based on the Chromium project and developed by the Hidden Reflex group and is available for both for Windows and OSX.

On visiting their official website, we will get one paragraph with heading "Why privacy is important?", this paragraph contains some of the unique and effective reasons for it, one such is that when we browse the data collected from that can decide whether we are eligible to get a job, credit, or insurance. Epic was first developed based on Mozilla Firefox but later it was changed to the Chromium-based browser. It works quite similar to the secure browsing feature by Firefox and Chrome. It deletes every session data such as cookies, caches, and any other temporary data after exiting the browser. It removes the services provided by Chrome to send any kind of information to any particular server and it adds a no tracking header to avoid tracking by data collection companies. It also prefers SSL connection over browsing and also contains a proxy to hide user IP address. To avoid leak of the search preferences, Epic routes all the search details through a proxy.

Here we saw a customizing Chromium project, Epic which was developed as a privacy centric browser.

HconSTF (http://www.hcon.in/downloads.html)

HconSTF stands for Hcon security testing framework. It is a browser-based testing framework. With the package of different addons added in the browser, it allows a user to perform web application penetration testing, web exploit development, web malware analysis along with OSINT in a semiautomated fashion.

HconSTF has two variants; one is based on Firefox that is known as Fire base and the other based on Chromium that is known as Aqua base. The rendering engines are also different as per the base Raw browser. Fire base uses Gecko and Aqua base uses WebKit. Both the versions are loaded with tons of addons.

The core idea or inspiration of this project is taken from hackerfox but it's not quite similar to that. Hackerfox http://sourceforge.net/projects/hackfox/ is portable

Firefox with tons of addons loaded by Yangon Ethical Hacker Group. Hackerfox only contains addons, whereas HconSTF is a bit advanced than hackerfox and contains better toolset. This is available for Windows and all popular Linux versions for both 32 and 64 bit architecture operating systems. The installation process is very easy, just download the package and run it, no need to install anything. It has different code names for different versions. The first public version or V0.3 was known as “Hfox.” The next one known as “freedom” and the V0.5 is called “Prime.”

The user interface is very user-friendly and everything is perfectly organized. The author also provides a well-documented manual which contains all the details about the project including the release history, architecture, tools details, and settings with screenshots. The HconSTF contains addons, scripts, and search aggregator plugins. It also allows a user to update the addons and scripts by selecting update in respective places (Hmenu → settings → addons) but it does not allow a user to upgrade the framework. To upgrade the framework user need to check the official site of the project manually.

HconSTF covers tools in groups. The specified groups are

- Recon/mapping
- Editors/debuggers
- Exploitation/audit
- Request manipulation
- Anonymity
- Cryptography
- Database
- Scripting/automation
- Network utilities
- Reporting

The version 0.5 or “Prime” comes with some surprising package for the user such as integrated database (IDB). An IDB is used for different popular web attack payloads such as for cross-site scripting (XSS) and SQL Injection. Apart from this it facilitates a user by providing quick search links to get lots of search data and a large collection of bookmark to use for reference and research.

MANTRA (http://www.getmantra.com/)

Mantra is an Open Web Application Security Project (OWASP) project. It is a project quite similar to HconSTF but unlike HconSTF, it is fully dedicated to web application security testing. Simply stated it is a web application security testing framework based on top of browser. The earlier version came with the Firefox base but later its Chromium version also released which is also well known as MOC or Mantra on Chromium. Like other customized security framework browsers it also supports 32 and 64 bit operating system architecture of Windows, Linux as well as Macintosh. Mantra has an added feature that most other browser-based framework does not, i.e., it is available in nine different languages such as English, Portuguese, Russian, Arabic, Spanish, Turkish, French, Chinese simplified, and also in Chinese traditional. As it is very popular in the security community it comes by default installed in popular security operating systems such as Backtrack and Matriux.

It has security addons preinstalled and configured and with its simple yet user-friendly user interface, Mantra is an integral part of every web application pen tester's arsenal. The tools available in Mantra not only focus on web application testing but also on web services and network application penetration testing. It contains tools to switch user agent, manipulate cookie, manipulate parameters and their values, add proxy, and many more. FireCAT is also included in Mantra and that makes it more powerful tool (we will cover FireCAT in next topic separately).

Some of the popular tools groups are mentioned below:

- Information gathering
- Flagfox
- Passiverecon
- Wappalyzer
- Application audit
- Rest client
- Hackbar
- Dom inspector
- Editors
- Firebug
- Proxy
- Foxyproxy
- Network utilities
- Fireftp
- FireSSH
- Misc
- Event spy
- Session manager

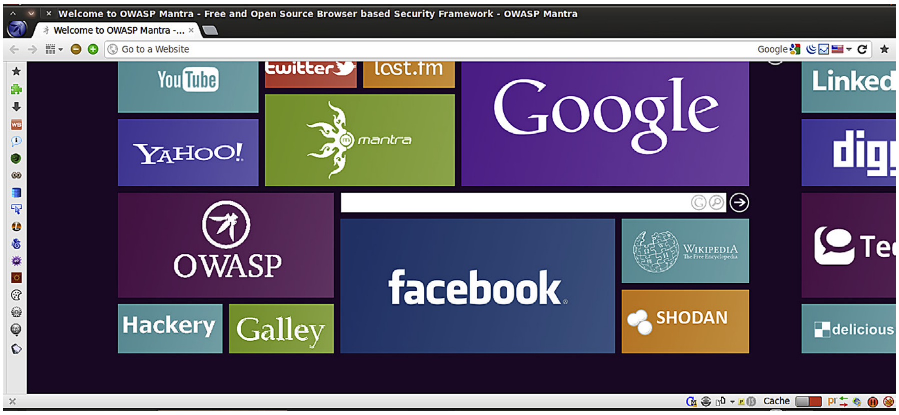


FIGURE 3.3

Mantra browser interface.

Apart from tools it also contains bookmarks. The bookmark is divided into two sections. First section is known as Hackery. It is a collection of different penetration testing links which will help a user in understanding and referring a particular attack. The other section contains gallery. It contains all the tools links that can be used for penetration testing.

We can download both the versions of Mantra from the following URL, http://www.getmantra.com/download.html or the individual download links are below. Where Mantra based on Firefox is available for different operating systems like Windows, Linux, and Macintosh whereas MOC is only available for Windows.

Mantra based on Firefox can be downloaded from http://www.getmantra.com/download.html.

Mantra based on Chromium can be downloaded from http://www.getmantra.com/mantra-on-chromium.html.

FireCAT (http://firecat.toolswatch.org/download.html)

FireCAT or Firefox Catalog for Auditing exTensions is a mind map collection of different security addons in a categorized manner. Now it's collaborated with OWASP Mantra project to provide one stop solutions to security addons based on browser customization. FireCAT contains seven different categories and more than 15 subcategories.

The categories and subcategories:

- Information gathering
  - Whois
  - Location info
  - Enumeration and fingerprint
  - Data mining
  - Googling and spidering
- Proxies and web utilities
- Editors
- Network utilities
  - Intrusion detection system
  - Sniffers
  - Wireless
  - Passwords
  - Protocols and applications
- Misc
  - Tweaks and hacks
  - Encryption/hashing
  - Antivirus and malware scanner
  - Antispoof
  - Antiphishing/pharming/jacking
- Automation
  - Logs and history
  - Backup/synchronization
  - Protection
- IT security related
- Application auditing

There is a category present “IT security related.” This one is an interesting category because it provides you plugins to collect information about the common vulnerabilities and exposures (CVEs) and exploits from various sources such as Open Sourced Vulnerability Database (OSDV), Packet storm, SecurityFocus, Exploit-DB, etc.

ORYON C (http://sourceforge.net/projects/oryon/)

Oryon C portable is an open source intelligence framework based on Chromium browser meant for open source intelligence analysts and researchers. Like other customized browsers it also comes with lots of preinstalled tools and addons to support the OSINT investigation. It also contains links to different online tools for better reference and research. It is a project by “osintinsight” so some of the functions a user can only use after subscribing some package of OsintInsight.

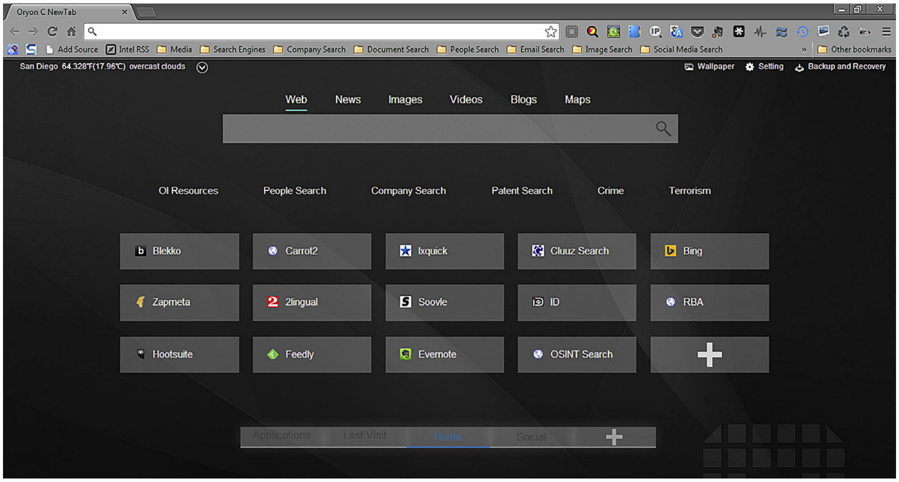


FIGURE 3.4

Oryon C browser interface.

It’s a straightaway use tool so no need to install Oryon C, just download and run it. It only supports Windows operating system 32 and 64 bit. The huge list of useful addons and categorized bookmarks makes it a must-have for any online investigator.

WhiteHat Aviator (https://www.whitehatsec.com/aviator/)

Though WhiteHat Aviator is not the one of its kind available but definitely it is a product of a reliable big brand security organization. WhiteHat Aviator is a private browsing browser. It’s quite similar to the Epic browser we discussed earlier in this chapter. It removes ads, eliminates online tracking to ensure a user to surf anonymously.

Like Epic browser Aviator is also based on Chromium. By default it runs in incognito or private browsing mode to allow a user to surf without storing any history, cookie, temporary file, or browsing preferences. It also disables autoplay of different media types, user has to allow a media such as flash in any page if he/she wants to see it. It also uses a private search engine duckduckgo to avoid string search preferences of the user.

Unlike Epic browser it is not open source, so open security community cannot audit the code or contribute much. Aviator is available for Windows as well as Macintosh operating system.

TOR BUNDLE (https//www.torproject.org/projects/torbrowser.html.en)

TOR or the onion routing project is very popular project. Most of us definitely have used, heard, or read about it somewhere some time. Though we will discuss about it in detail in a later chapter but for the time being let's discuss the basics about the tor browser bundle. Like Epic browser and Whitehat Aviator, tor browser is also a privacy centric browser. But the way it works is quite different from the other two. Through the tor application it uses the volunteer distributed relay network and bounces around before sending or receiving connection. It makes it difficult to backtrack the location of the user and provides privacy and anonymity to the user. Due to its proxy chaining type of concept it can be used to view the contents that are blocked for a particular location such as a country. The tor browser is available for different operating systems such as Windows, Linux, and Macintosh and can be used straightaway without installation. Tor browser or previously known as TBB or tor browser bundle is a customized browser based on Firefox. It contains tor button, tor launcher, tor proxy, HTTPS everywhere, NoScript, and lots of other addons. Like OWASP Mantra it is also available in 15 different languages.

CUSTOM BROWSER CATEGORY

As we came across different custom browsers, their base build, what rendering engine they use etc. Let's categorize them to understand their usability.

For easy understanding let's make three categories.

1. Penetration testing
2. OSINT
3. Privacy and anonymity

Under the first category we can find HconSTF, Mantra, FireCAT, whereas under OSINT category we can add HconSTF and Oryon C, likewise we can put Epic browser, Whitehat Aviator and tor browser under privacy and anonymity category. If we look at the core, what puts all these different browsers in different category, the answer will be the addons or the extensions. So by adding some similar functional addons we can create a customized browser for a specific purpose. If we want to create our own browser for some specific purposes we must keep this in mind.

PROS AND CONS OF EACH OF THESE BROWSERS

Let's start with the first browser we discussed and that is Epic browser. The advantage of using this browser is that it fully focuses on user privacy and anonymity. Apart from that it's open source and it can be used by all kind of users, technical as well as nontechnical. The only disadvantage is that the reliability factor. Is this browser does what it intends to do or does it do something else. As trust on the source is the key here. So either trust the source and use the product or use it then trust the product.

The advantage of using HconSTF is that it's a one stop solution for information security researchers. The only disadvantage it has is that it does not allow a user to upgrade it to the next level.

The advantage of OWASP Mantra is that it is available in different languages to support security community from the different parts of the world. It has only one disadvantage is that the light version or the MOC is only available for Windows, not for other operating systems like Linux or Macintosh.

The advantage of Oryon C is that it is very helpful in OSINT exercises, but there are different disadvantages like to use some of the modules a user need to subscribe and also it is only available for Windows.

The disadvantage of the Whitehat Aviator is that it is not open source and it does not have a version for Linux operating system.

TBB has the advantage is that it provides anonymity with a disadvantage like it only comes with one rendering engine Gecko.

As we already discussed these custom browser categories; based on category, user can choose which browser to use, but definitely the browsers for anonymity and privacy have larger scope as they do not belong to any single category of users. Any user who is concern about his/her online privacy can use these browsers. Like for e-shopping, netbanking, social networking as well as e-mailing, these browser can be helpful to all.

ADDONS

Browser addon, or in other terms browser extension or plugins are the same things but known differently in terms of different browsers. As in Firefox it's known as addon and in Chrome as extension. Though plugin is a different component from addons but still some use it as synonym for addon. In reality plugin can be a part of addon.

Browser addons are typically used to enhance the functionality of a browser. These are nothing but applications designed using web technology such as HTML, CSS, and JavaScript. Though due to difference in rendering engines the structure and code are different for different browser addons, but nowadays there are different tools and frameworks available to design a cross browser addon.

Addons are so popular that every web user might have used it already at some point or another. Some of the popular addons are YouTube downloader, Google translate in common and SOA client, Rest client, and hackbar in case of penetration testers.

We can install addon quite easily in both the browsers, Firefox as well as Chrome by simply clicking on install button. Addons are not always safe so choose them wisely so download from trusted sources and also after going through reviews. Sometimes we need to restart the browser to run a particular addon. Like other softwares, addons also keep on looking for their updates and update themselves automatically. Sometimes we might see that the addon is not compatible with the browser version that means there are two possibilities, (1) browser version is outdated, (2) addon is not updated to match with the requirements of latest browser installed. Sometime it's also possible that an addon might affect the performance of a browser and can even make the browser slow. So choose your addons wisely.

Let's discuss some common addons and extensions that are available for both Firefox as well as Chrome to serve in day-to-day life. Let's see what kind of addons are available and to serve what purpose.

We all use YouTube to watch video and share. Sometimes we also want to download some YouTube videos so for that a number of addons are available by installing which we do not need to install any other additional downloading software. Another major issue we feel while watching videos in YouTube is that the ads. Sometime we are allowed to skip the ads after 5 s and sometime we have to watch the full 20 s ad. That is pretty annoying so there are addons available to block ads on YouTube. Most of the people are addicted to social networking sites, we generally open one or all of these at least once every day. Social networks like Facebook, LinkedIn, Twitter are like part of our life now. Sometime we need to see the pictures of our friends or someone else in social networking sites and we need to click on the picture to zoom that. It wastes lots of valuable time, so if we want an addon to zoom all those for us when we point your mouse on the picture then there is addons available known as hoverzoom both in Firefox as well as Chrome.

There are different addons also available for chat notification, e-mail notification, news, weather. It looks like think there are addons available for almost everything, we just need to explore and definitely we will get one that will simplify our life. This is just for brainstorm, now let's discuss about some of the popular addons which will help us in various different important tasks.

SHODAN

It is a plugin available for Chrome. A user just has to install and forget about it. While we browse an application, it will collect information available about the particular site from its database and provide details such as what is the IP address of the website, who owns that IP, where is it hosted, along with open ports with popular services and some of the popular security vulnerability such as HeartBleed. This is definitely very helpful for penetration testers, if you haven't tried it yet, you must. The only limitation of this addon is that it will only show the results for the sites, for which information is already available in shodan sources. It generally won't show results for new sites and staging sites as its database might not contain information on them.

WAPPALYZER

It is also a popular addon available for both the browsers Firefox and Chrome. It uncovers the technology used by the web application. Similar to shodan, for wappalyzer also we simply need to install and forget, wappalyzer will show details about technology used while we browse a page. The way exactly wappalyzer works is that it collects information related to the technology and versions from the response header, source code, and other sources based on the signatures.

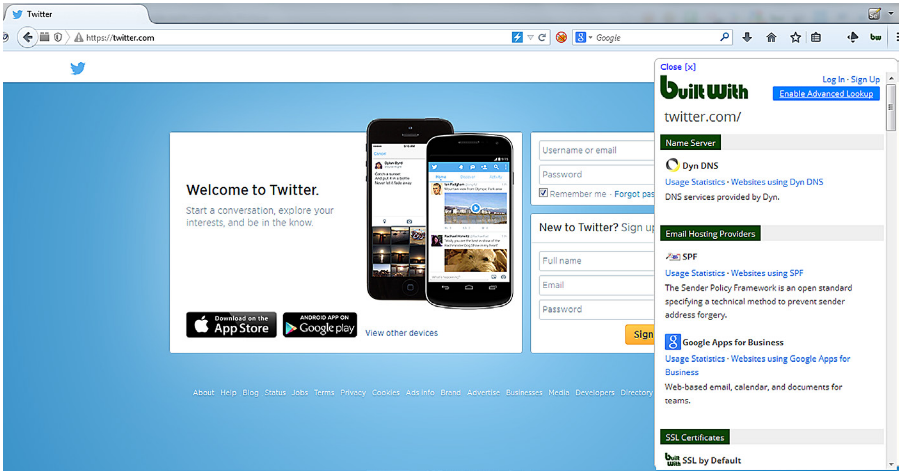
It identifies various different technologies such as CMS or content management systems, e-commerce platforms, web servers details, operating system details, JavaScript framework details, and many other things.

Some of the types of technologies identified by wappalyzer are:

- Advertising networks
- Analytics platforms
- Content management system
- Databases
- E-commerce
- Issue trackers
- JavaScript frameworks
- Operating systems
- Programming languages
- Search engines
- Video players
- Wikis

BUILDWITH

Buildwith is similar to wappalyzer. It also identifies technologies used by a web applications based on signatures, using page source code, banner, cookie names, etc. While wappalyzer is open source, buildwith is not. The paid version of buildwith has way more features from its free version like contact information detection and subdomain detection, etc. which can be very helpful at times.


Twitter
https://twitter.com
Google
Welcome to Twitter.
Start a conversation, explore your interests, and be in the know.
Download on the App Store
ANDROID APP ON Google play
View other devices
Username or email
Password
☑ Remember me · Forgot pas
New to Twitter? Sign up
Full name
Email
Password
Sign
About Help Blog Status Jobs Terms Privacy Cookies Ads info Brand Advertise Businesses Media Developers Directory
Close [x]
BuiltWith
Log In · Sign Up
Enable Advanced Lookup

twitter.com/

Name Server

Dyn DNS

Usage Statistics · Websites using Dyn DNS

DNS services provided by Dyn.

Email Hosting Providers

SPF

Usage Statistics · Websites using SPF

The Sender Policy Framework is an open standard specifying a technical method to prevent sender address forgery.

Google Apps for Business

Usage Statistics · Websites using Google Apps for Business

Web-based email, calendar, and documents for teams.

SSL Certificates

SSL by Default

FIGURE 3.5

Buildwith identifying technologies on Twitter.

FOLLOW

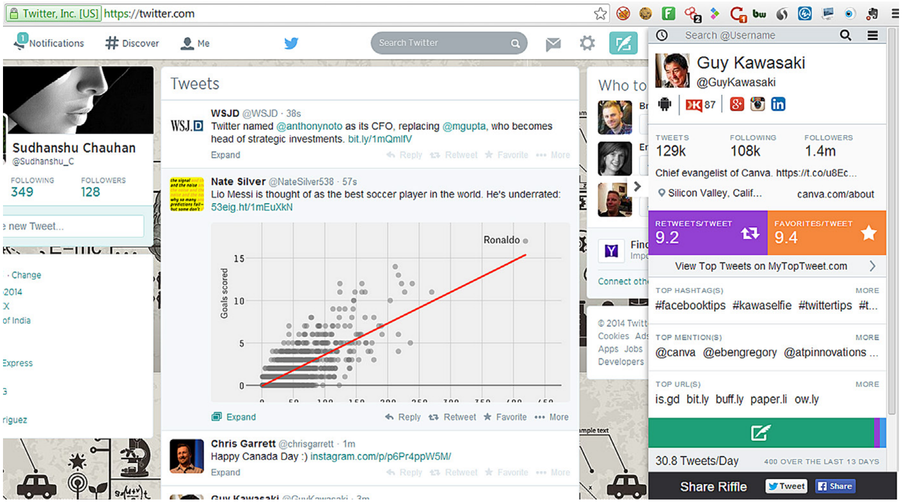
Follow.net is a competitive intelligence tool which helps us to stay updated by the online movement of our competitors and can be accessed using the browser addon provided by it. The major difficulty faced to keep track of the competitor is that we have to waste lots of time visiting their websites, blogs, tweets, YouTube channel, etc. After visiting lots of website we don't have a structured data from that we can understand the trend being followed. So here is follow.net that do most of these and much more for us and provides us report on how our competitor is trending on the web. It collects information from various sources such as alexa, Twitter, keyword-spy, etc. It will also send us a notification related to our competitors, if something new comes up. The simple addon of follow provides a complete interface to browse through all this information in an efficient manner.

So if we are starting a business want to learn the success mantra of your competitor then it is a must-have. The follow.net addon is available for both Firefox as well as Chrome browser.

RIFFLE

Riffle by CrowdRiff is a social analytics addon. It's focused on the popular microblogging site Twitter. It provides us with a smart Twitter dashboard which displays useful analytical data about a Twitter user of our choice.

It provides us the helpful information to create a popular account by giving reference to some influential tweets and accounts who posted them. It also provides quick insight about a Twitter user so that it will help us to understand and reply to that particular user in a particular way.



WSJD @WSJD · 38s
Twitter named @anthonynoto as its CFO, replacing @mgupta, who becomes head of strategic investments. bit.ly/1mQmlfV

Nate Silver @NateSilver538 · 57s
Lio Messi is thought of as the best soccer player in the world. He's underrated: 53eig.ht/1mEuXkN

Chris Garrett @chrisgarrett · 1m
Happy Canada Day :) instagram.com/p/p6Pr4ppW5M/

Guy Kawasaki
@GuyKawasaki
87

TWEETS	FOLLOWING	FOLLOWERS
129k	108k	1.4m

Chief evangelist of Canva. https://t.co/u8Ec...
Silicon Valley, Calif... canva.com/about

RETWEETS/TWEET 9.2
FAVORITES/TWEET 9.4

View Top Tweets on MyTopTweet.com

TOP HASHTAG(S) MORE
#facebooktips #kawaselfie #twittertips #t...

TOP MENTION(S) MORE
@canva @ebengregory @atpinnovations ...

TOP URL(S) MORE
is.gd bit.ly buff.ly paper.li ow.ly

30.8 Tweets/Day 400 OVER THE LAST 13 DAYS

Share Riffle Tweet Share

FIGURE 3.6

Riffle interface integrated into the browser.

Some of the key feature provided by this extension is that it helps in tweet source tracking, activity breakdown, engagement assessments, etc. with a clean user interface. It's a must-have for power users of Twitter.

WhoWorks.at

Similar to Riffle a Twitter focused addon, we have whoworks.at a LinkedIn specific addon. Let's take a scenario where we are salespersons and we need to gather information about the key influential persons of a company, so how do we proceed. We will go to LinkedIn, search for that particular company and then find the 1st degree, 2nd degree, or 3rd degree connections. Based on their title we might want to add them to discuss business. This is the old fashion way. Now there is another way to do the same in a more automated manner. Now let's install whoworks.at extension on Chrome, visit the company website that we are interested in and let the extension show us the 1st degree, 2nd degree, and 3rd degree connections from that company along with details such as recent hires, promotions, or title changes.

This is the power of whoworks.at, it finds the connections for us when we visit a website and saves us a lot of time.

ONETAB

Onetab is an addon or extension available for both the browsers Firefox as well as Chrome. It provides us solution for tab management. It helps us to make a list of tabs that are open in our browser and aggregate them under a single tab, especially in Google Chrome as we already learned that it is a tab centric browser. The tab is the main thread in Chrome so by using onetab we can save lot of memory because it converts tabs into a list, which we can later restore one by one or all at a time as per our wish.

SALESLOFT

Most of the sales people must have used it, if not they need to. It's simply a dream addon for salespersons. It allows to create a prospecting list from browsing profiles from different social networks for leads focusing on a particular segment of market. It allows a user to run specific search based on title, organization, or industry name. Some of the popular features are it allows to gather contact information from a prospect from LinkedIn. Contact information contains name, e-mail id, and phone number. We are allowed to add any result as a prospector by single click. Import prospects from LinkedIn and export it to excel or Google spreadsheets. It also allows to synchronize the data directly with salesforce.com

It is a one stop free and lightweight solution for every sales person. Use it and enhance your lead generation with its semiautomated approach.

PROJECT NAPTHA

We all know how it's nearly impossible to copy the text present in any image, one method is that we type it manually but that is definitely a bizarre experience. So here is the solution, Project Naptha. It is an awesome addon which provides us freedom to copy, highlight, edit, and also translate available text on any image present on the web using its advanced OCR technology. It's available for Google Chrome.

TINEYE

Tineye is a reverse image search engine, so its addon is also used for same. As we enter keywords in search engines to get the required result, Tineye can be used to search for a particular picture in the Tineye database. It has a large amount of images indexed in its database. The myth behind the image identification technology is that it creates a unique signature for each and every image it indexes in its database. When user search for a picture it starts comparing that signature, and most of the time it gives exact result. Apart from exact result it also gives similar results. Another great feature of Tineye is that it can search for cropped, resized, and edited images and give almost exact result. Tineye is available for both the browsers Firefox as well as Chrome.

REVEYE

Reveye is quite similar to Tineye. This addon is only available for Chrome. It works very simple. It gives a user result of reverse image search based on results provided by Google reverse image search as well as Tineye reverse image search.

CONTACTMONKEY

Contactmonkey is a very useful addon for all professionals, especially sales. It helps us to track our e-mails. Using this simple addon we can identify if the person we have sent an e-mail has opened it or not and at what time. This can help us to identify whether our mails are being read or are simply filling up the spam folder and also what is the best time to contact a person. Though the free version has some limitations yet it is very useful.

If you want to improve your user experience of Google Chrome browser this list by digital inspiration is a must to look at. The list contains some of the Chrome extensions and apps list which will enhance Chrome features and also enhance user experience. Following is the URL where you can get the list, http://digitalinspiration.com/google-Chrome.

BOOKMARK

Bookmark is a common feature of every browser. It allows us to save a website's URL under a name for later use. Most of the time while browsing we get different interesting pages but due to lack of time we cannot go through all those pages at that time. There bookmark help us to save those links for future use.

There are popularly two ways to save the bookmark:

1. By clicking on bookmark button when we are on the page that needs to bookmark.
2. By clicking on ctrl+d when we are in the page that needs to bookmark.

We can even import and as well as export bookmarks from one browser to another. We can also create a new folder for a list of bookmarks. In Firefox we need to go to show all bookmark link or click on ctrl+shift+B where we will get all those options directly or by right clicking on that page. Similarly for Chrome we need to go to bookmark manager. There also we will find all the options on the page itself or otherwise we need to right click on that page to get those options.

THREATS POSED BY BROWSERS

As we discussed browsers are a great tool which allows us to access the web and the availability of various addons simply enhances its functionalities. This wide usage of browsers also present a huge threat. Browsers being one of the most widely used softwares are the favorite attack vector of many cyber attackers. Attackers try to exploit most of the client side vulnerabilities using browser only, starting from phishing, cookie theft, session hijacking, cross-site scripting, and lots of others. Similarly browsers are one of the biggest actors which play a role in identity leakage. So use your browser wisely. In later chapters we will discuss about some methods to stay secure and anonymous online. For now let's move to our next chapter where we will learn about various types of unconventional but useful search engines.