FACULTY OF COMPUTER SYSTEMS AND SOFTWARE ENGINEERING

WEB BUCKLER

MINI PROJECT

BCN 3113 - ETHICAL HACKING

SEMESTER II - 17/18

NAME:	**NASRUL ARIF BIN ZAKRIA**
MATRIC NO:	**CB15060**
SECTION:	**01B**
LECTURER:	**DR. ABDULGHANI ALI AHMED**

INTRODUCTION

Web Buckler is a web extension that provides security in user browsing experience. “Buckler” came from famously used war shield, which is the small round shield with a handle by the forearm or hand. Web Buckler able to detect malicious web Uniform Resource Locator (URL) and inform the user regarding the web page. Web Buckler will alert the user and ask whether to proceed or to leave the site immediately. The objective of this extension is to prevent user from diving into malicious web pages such as phising web sites or web sites with malicious scripts that can steal confidential information.

USER MANUAL

Web Buckler is a web extension, thus it require a web browser to work. It is recommended for the user to use *Chrome* web browser to achieve full functionality of the extension. Using other browser is not guarantee for it to works depending on the browser support towards the configuration of Web Buckler. The manual will provide step by step of how to install Web Buckler and how it works.

1) DOWNLOAD THE WEB BUCKLER

- Download “Web Buckler” by going to the link below:
  - https://drive.google.com/open?id=17K1DEdV5-42wspWqMuLzYu7zA9TRSeCb

    OR
  - https://tinyurl.com/WebBuckler

2) UNZIP WEB BUCKLER

- Unzip “Web Buckler” using any zipping tools as shown in Figure 1.1.

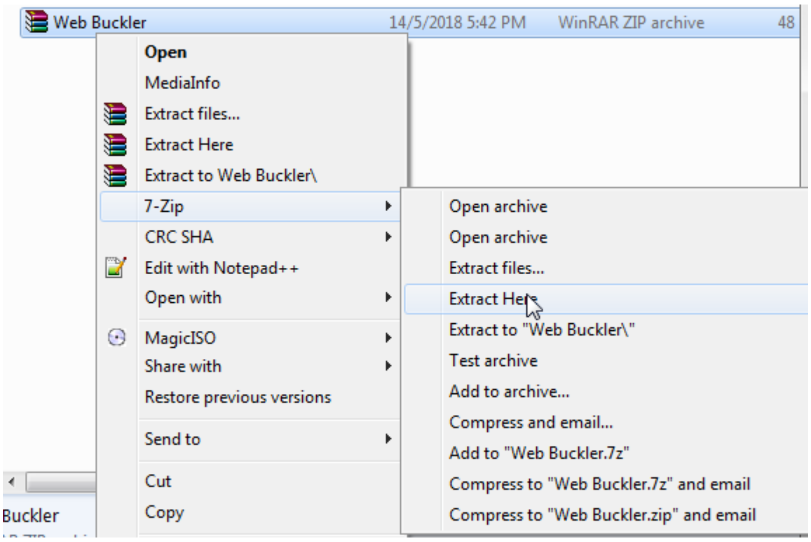


Figure 1.1

- If you don’t have any zipping tools, here is the link to download an open source zipping tools, there are many of zipping tools out there, but here is one of the commonly used.
    - https://www.7-zip.org/download.html

3) OPEN UP CHROME BROWSER

- It is recommended to use Chrome Browser for the extension to work properly.
- Open Chrome Browser, if you do not have it yet, below is the download link:
    - https://www.google.com/chrome/

4) LOAD THE EXTENSION

- In Chrome, click the **three dots** button on the top right corner of the browser window as in Figure 1.2.

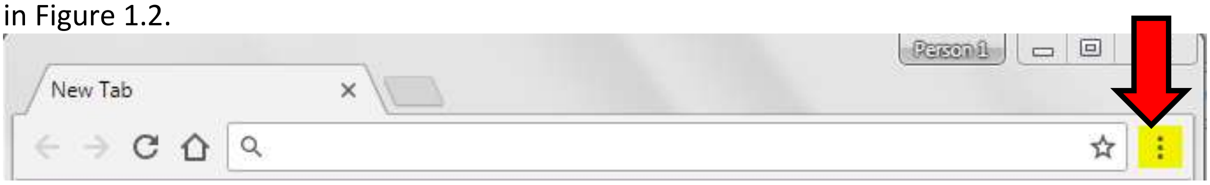


Figure 1.2

- When the button is clicked, a drop down menu will appear.
- Click on **More Tools > Extension** as shown in Figure 1.3.

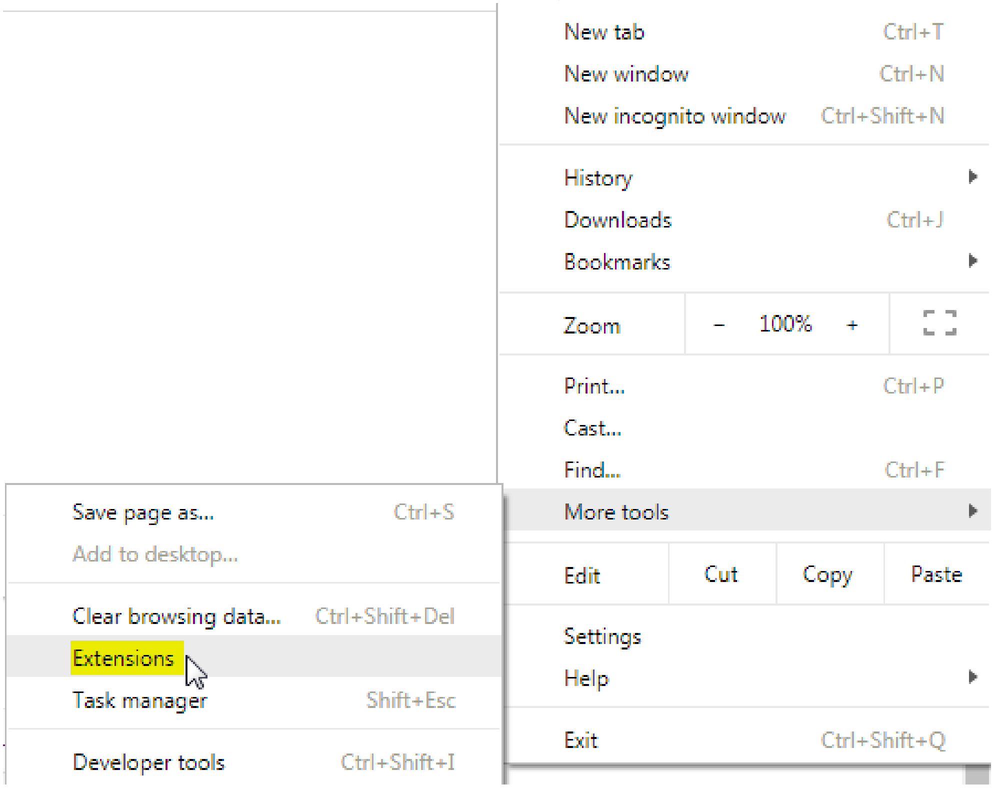


Figure 1.3

- The page will then redirect to **chrome://extensions**
- In **chrome://extensions** page, click the **Developer Mode** toggle as shown in Figure 1.4.

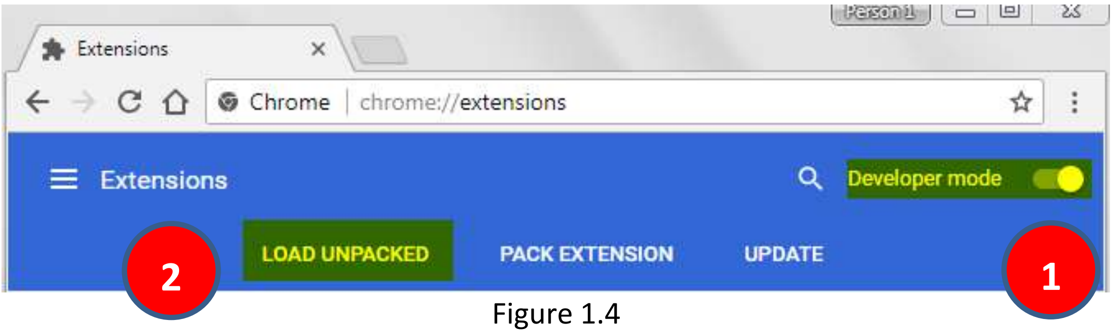
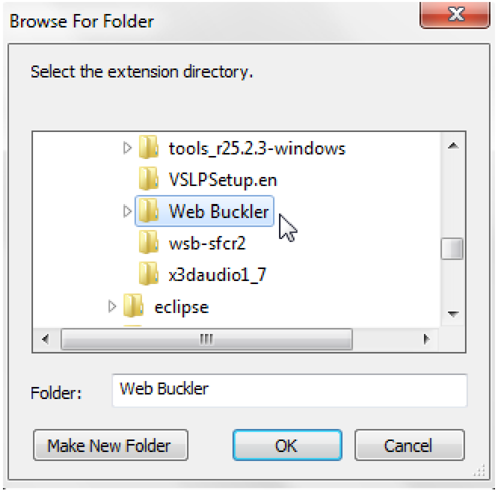


Figure 1.4

- Pressing **Developer Mode** will make the Chrome to assume that you are a developer so that you can test the extension outside the extension web store. If done correctly, three options **Load Unpacker**, **Pack Extension** and **Update** will appear.
- Click the **Load Unpacked** button and a small window explorer will appear for you to choose the folder containing Web Buckler.
- Find the directory (folder) that the Web Buckler is downloaded, click on the Web Buckler folder and click the **OK** button as shown in Figure 1.5.

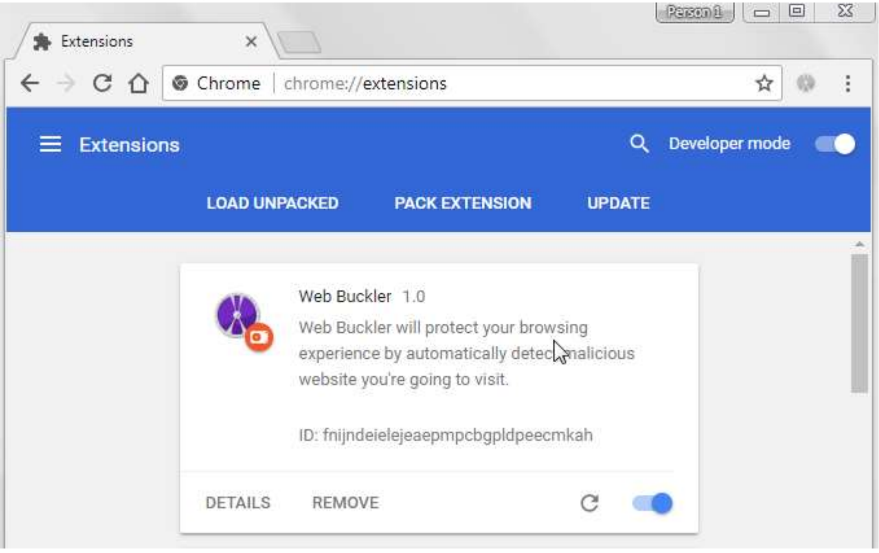

Browse For Folder

Select the extension directory.

Folder: Web Buckler

Figure 1.5

- If done correctly, the page will appear as shown in Figure 1.6.



Web Buckler 1.0

Web Buckler will protect your browsing experience by automatically detect malicious website you're going to visit.

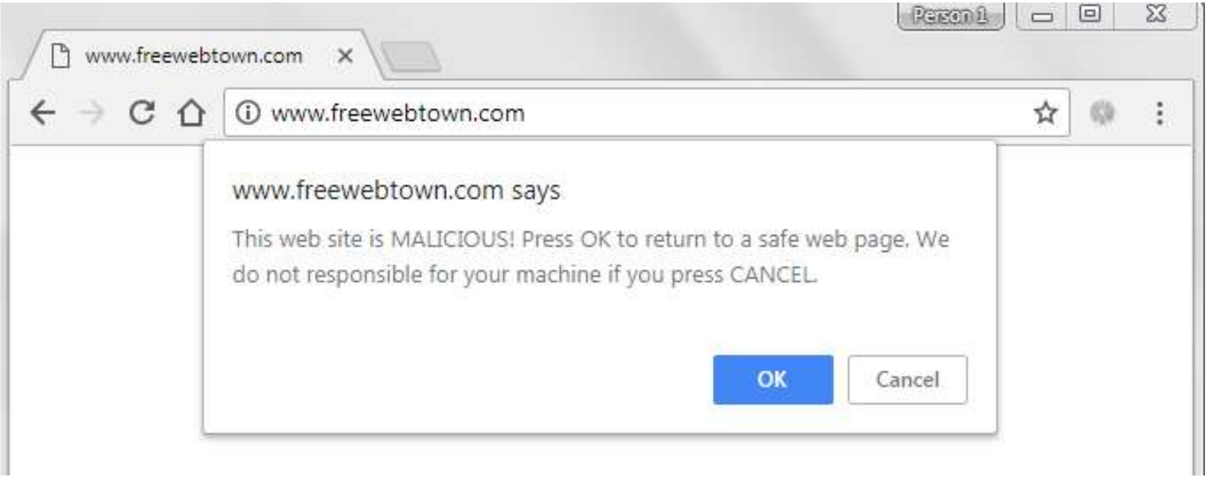
ID: fnijndeielejeaepmpcbgpldpeecmkah

Figure 1.6

- Now that the Web Buckler appears in the extension page, we can assume it is finished installing.

5) HOW IT WORKS

- If you happen to enter any site listed in the blacklist database, an alert will appear telling you to go to leave the page immediately to the safe zone or if you choose not, then anything happened to you is your responsibility. Example of malicious website is shown in Figure 1.7.



www.freewebtown.com says

This web site is MALICIOUS! Press OK to return to a safe web page. We do not responsible for your machine if you press CANCEL.

Figure 1.7

- Web Buckler also detect the URL from solicited symbols such as:
  - Blank space - “ “
  - “<>”
  - “[]”
  - “{}”
  - “|”
  - “\”
  - “^”

CODES

Codes below are used to get the URL or Domain of the website visited.

```
var domain = window.location.hostname;
var url = window.location.href;
```

Codes below are used to store the list of Malware domain, Normal domain and Buffer domain (first time visit with no suspicious activity). Using Chrome Storage to store in the Local Storage in which the list will remain even when the Computer is shut down.

```
//listA object to store list of malware URL, listB object to store list of trusted URL
var listA, listB;
var listBuffer;

//to get the list of malware URL from chrome localstorage
chrome.storage.local.get("malwareList", function(items){
    listA = items;
});

//to get the list of trusted URL from chrome localstorage
chrome.storage.local.get("normalList", function(items){
    listB = items;
});

//to get the list of trusted URL from chrome localstorage
chrome.storage.local.get("bufferList", function(items){
    listBuffer = items;
});
```

Codes below are used to get the URL or Domain of the website visited.

```
var domain = window.location.hostname;
var url = window.location.href;
```

First it will check if list has existed before, else it will initiate the list

```
//init list
    if(malwareList == null)
        initiateMalwareList();

    if(normalList == null)
```

```
        initiateNormalList();

    if(bufferList == null)
        initiateBufferList();
```

This group of functions is to initiate list if the system does not have any list before. Malware list is taken from https://www.malwaredomainlist.com/hostslist/hosts.txt.

```
function initiateMalwareList (){
    var content, ret, blacklist;

    $.get("https://www.malwaredomainlist.com/hostslist/hosts.txt", function(data, status){
            content = data;
      ret = content.replace('#               MalwareDomainList.com Hosts List           #','');
      ret = ret.replace('#   http://www.malwaredomainlist.com/hostslist/hosts.txt   #','');
      blacklist = ret.replace('#         Last updated: Tue, 03 Apr 18 20:39:48 +0000      #','');
            chrome.storage.local.set({ "malwareList": blacklist }, function(items){
                console.log(items);
            });
        });
}

//
function initiateNormalList(){
    var whitelist;

    whitelist = "www.facebook.com www.google.com www.instagram.com";
    chrome.storage.local.set({ "normalList": whitelist }, function(items){
        console.log(items);
    });
}

function initiateBufferList(){
    var buffer;

    buffer = "empty";
    chrome.storage.local.set({ "bufferList": buffer }, function(items){
        console.log(items);
    });
}
```

Below is the main core of the extension where it will first check the unsolicited symbol, then the normal list, then the malware list, then check if the URL has been visited at least once or if the URL never had been visited before.

```
if(contains(url, malwareSymbol))
    {
        if(confirm("THIS SITE IS SUSPICIOUS, IT MAY CONTAINS MALICIOUS ELEMENTS! CONTINUE?")){

        }
        else
        {
            window.location.assign("https://www.google.com");
        }
        malwareList = malwareList + "\n" + url;
        updateMalwareList(malwareList);

        console.log("ENTERED SUSPICIOUS");
    }
    else if(normalList.includes(domain.replace("http",""))) //check if domain from normal list
    {
        console.log("ENTERED SAFE");
    }
    else if(malwareList.includes(domain.replace("http",""))) //check if domain from blacklist
    {
        if(confirm("This web site is MALICIOUS! Press OK to return to a safe web page. We do not responsible for your machine if you press CANCEL."))
        {
            window.location.assign("https://www.google.com");
        }
        else
        {
            if(confirm("Are you sure? Press OK to proceed to MALICIOUS web site. CANCEL to go back to safe web page."))
            {

            }
            else
            {
                window.location.assign("https://www.google.com");
            }
        }
        console.log("ENTERED MALWARE");
    }
```

```
        else if(bufferList.includes(domain.replace("http",""))) //check if domain was accessed atleast once
        {
                bufferList = bufferList.replace(domain,"");
                normalList = normalList + " " + domain;
                updateNormalList(normalList);
                updateBufferList(bufferList);
                console.log("ENTERED NORMAL ATTEMPT 2");
        }
        else //all non suspicious domain will be stored in buffer for once
        {
                bufferList = bufferList + " " + domain;
                updateBufferList(bufferList);
                console.log("ENTERED NORMAL ATTEMPT 1");
        }
```

The way of checking if the URL contains certain criteria is through the function:

```
function contains(target, pattern){
  var value = 0;
  pattern.forEach(function(word){
    value = value + target.includes(word);
  });
  return (value === 1)
}
```

The way of checking if the URL matches any of list is through javascript String.includes() method.

CONCLUSION

Web Buckler can be use to prevent user from accessing malicious sites that can attack the user using various type of technique such as phishing, client-side scripting and etc. It is important to ensure the prevention of entering such sites. Even a small suspicious symbol in the URL should be taken into account as attack can happen in many unnoticed ways.

REFERENCE

http://www.ietf.org/rfc/rfc3986.txt - RFC3986 Uniform Resource Identifier

http://www.ietf.org/rfc/rfc2396.txt - RFC2396 Uniform Resource Identifier

https://stackoverflow.com/questions/695438 - Safe Characters for Friendly URL

https://developer.chrome.com/apps/storage - Chrome Storage API Documentation

http://www.malwaredomainlist.com/hostslist/hosts.txt - List of Malware Domain

https://www.w3schools.com/jquery/default.asp - JQuery Documentation

https://developer.mozilla.org/en-US/Add-ons/WebExtensions - Web Extension Documentation