Browser Security

Robert Gabriel

R00102430

Task 1: (10 marks)

# Write a short note on the security features of one the Browser’s above.

Firefox is known for being one of the tightest web browsers on the web when it comes to security. Firefox uses a sandbox security model, (which separates running programs); it limits scripts from accessing data from other websites based on a system called same organ policy. It uses TLS to protect the communications of the users with web servers and using custom made cryptography when using HTTPS when visiting websites. In 2013, saw Firefox disable all 3rd party cookies by default. As of 2013 Firefox is ranked with the second highest security by default.

# Discuss what add-ons should be used to make the Browser more secure.

Adds ones for Firefox, are great as they add features and make the browsing on the web safer and easier. Some of the best ads on for Firefox privacy are :

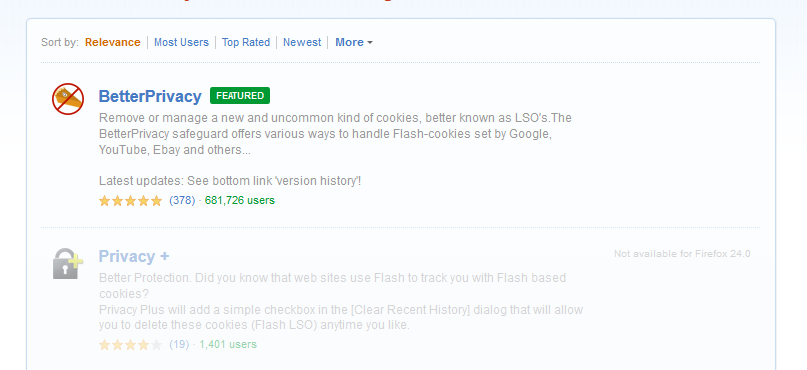
**Web of Trust (WOT**): WOT rates every site on the Internet for its security risk: green equals safe, amber equals worrisome and red means avoid like the plague. Simple, easy, and a must-have security measure.

**Better Privacy** – The Better Privacy Firefox add-on is designed to scrape away the most persistent tracking cookies that websites (and, especially, advertisers) use to profile your online activity.

**Torbutton** – For those that don’t know, Tor is a proxy surfing service that prevents even your ISP (or employer) from knowing exactly what web sites you’re visiting.

Give details of where you would go to download these add-ons.

• First, go to the Firefox Add-ons site and select the extension you would like to install.

****• Click on the Add to Firefox button and the Installation window will appear.

• After a brief countdown (takes about 5 seconds), the Install Now button will be active.

• Click on Install Now.

• Once Firefox restarts, you will now be able to use your add-on.

Task 2: (15 marks)

# Write a short note on each of the following Browser Security Checkers

## Shields Up

Shields Up is an online port scanning service created Gibson Research Corporation . The purpose of it is to alert the users of any ports that have been opened through their firewalls or through their NAT routers. The utility can scan the most common file sharing ports.

**It does the following tests.**

* File Sharing
* Common Ports
* All service ports
* Messengers spam
* Browser header

## Quays Browser Check,

Quays Browser Check is an open source service allowing anyone to scan their browser and ensure their browsers and plug-ins is secure and up-to-date.

## Browser Scope,

Browser scope is an open-source project for profiling web browsers and storing and aggregating crowd-sourced data about browser performance. Showing any flaws in the system.

It tested in the following areas:

* Post Message
* JSON. parse
* toStaticHTML
* httpOnly cookies
* X-Frame-Options
* X-Content-Type-Options
* Block reflected XSS
* Block location spoofing
* Block JSON hijacking
* Block XSS in CSS
* Origin header
* Strict Transport Security
* Block cross-origin CSS attacks
* Cross Origin Resource Sharing
* Block visited link sniffing
* Content Security Policy

Task 3: (5 marks)

## Use one of the above Browser Scanners to check the security of your browser.

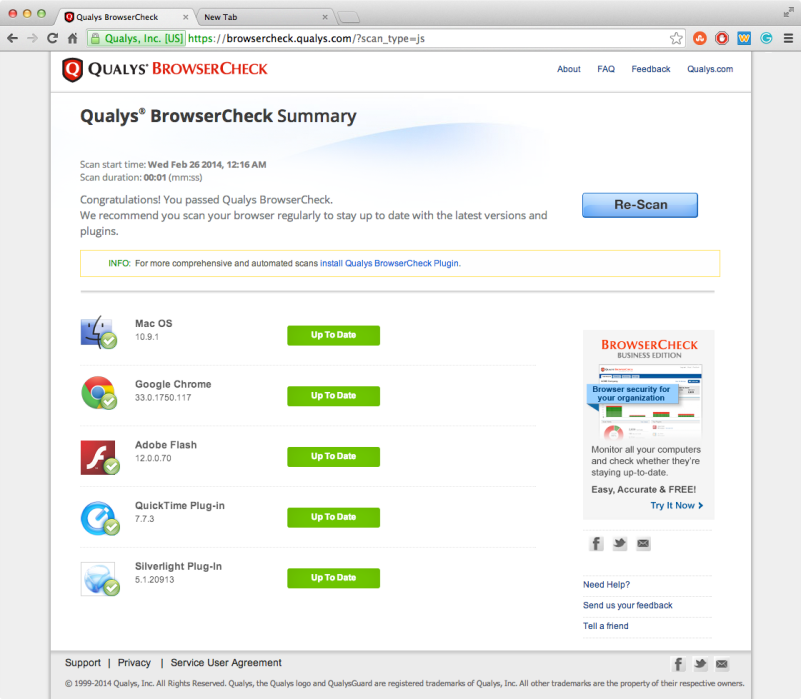
# Quays Browser Check

**Operation system**: Mac OS X

**Browser:** Chrome.

# No Plugin Scan

First, I went to https://browsercheck.qualys.com and I clicked on to the link that said "Launch a quick scan now.

After its run I got a list of all found plugins and setting..

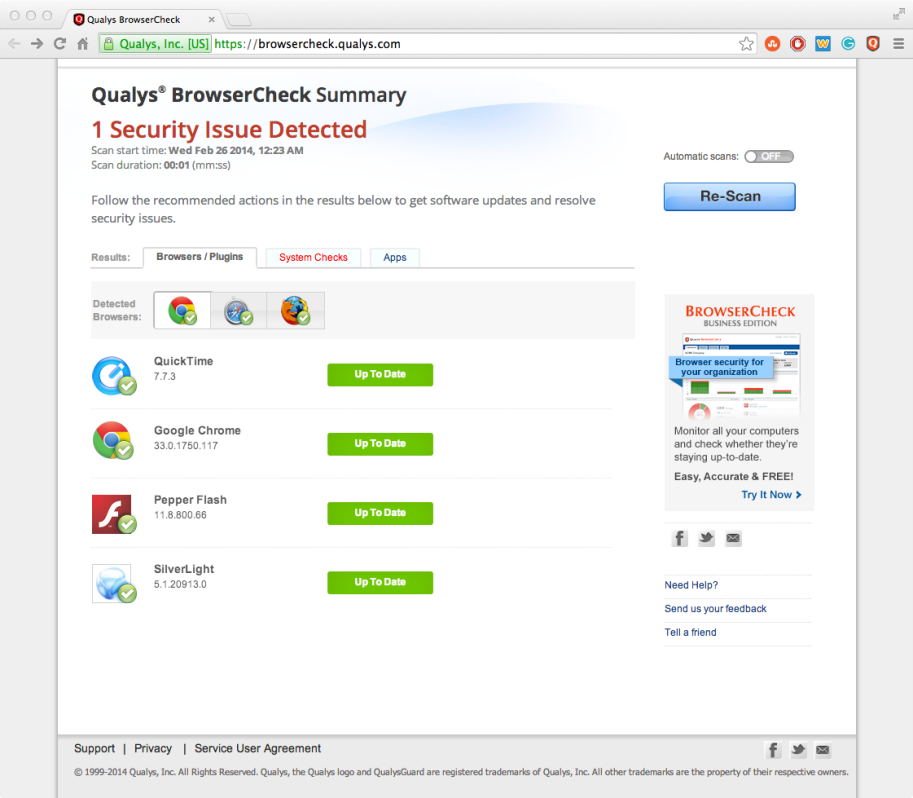
On the page it shows outdated plugs in and software in a red button with a fix it now. If an item found is up to date it will be in green. Clicking the button updates the plugin. It also checked if my browser is up to date as well. It didn’t give me much more than if chrome, Mac OS, flash and QuickTime where up to date.

So needed to install the plug in to get a better search.

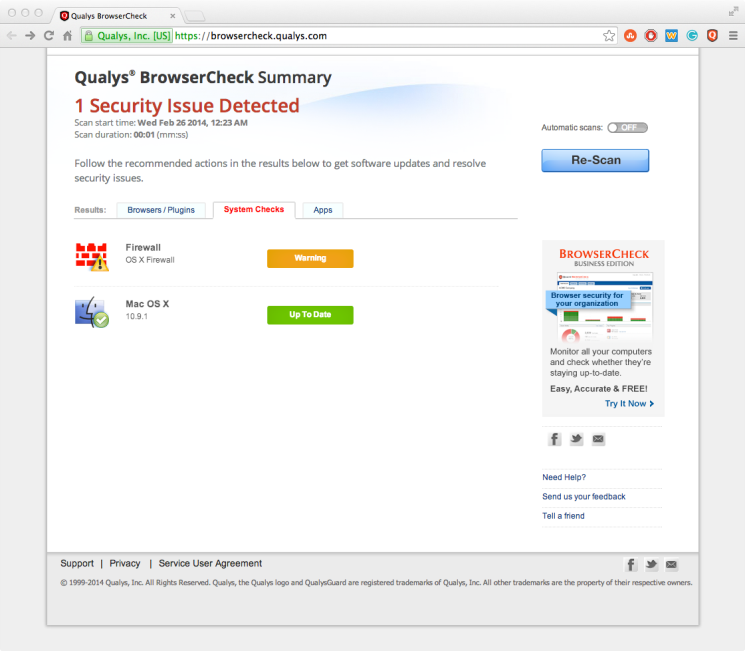
# Plugin installed Scan

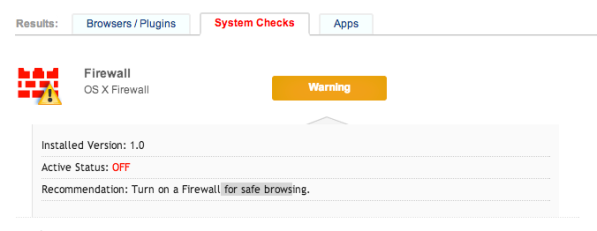
# Browser and Plugins

Below are the results it had for the installed Quays Browser Check plugin. It shows all browsers installed and if they're up to date. When I clicked on the browser, it showed more detail/ As you can see I had Chrome, Safari and Firefox which were all updated and safe. When I clicked on chrome it showed that all my plugs and if they were up to date.



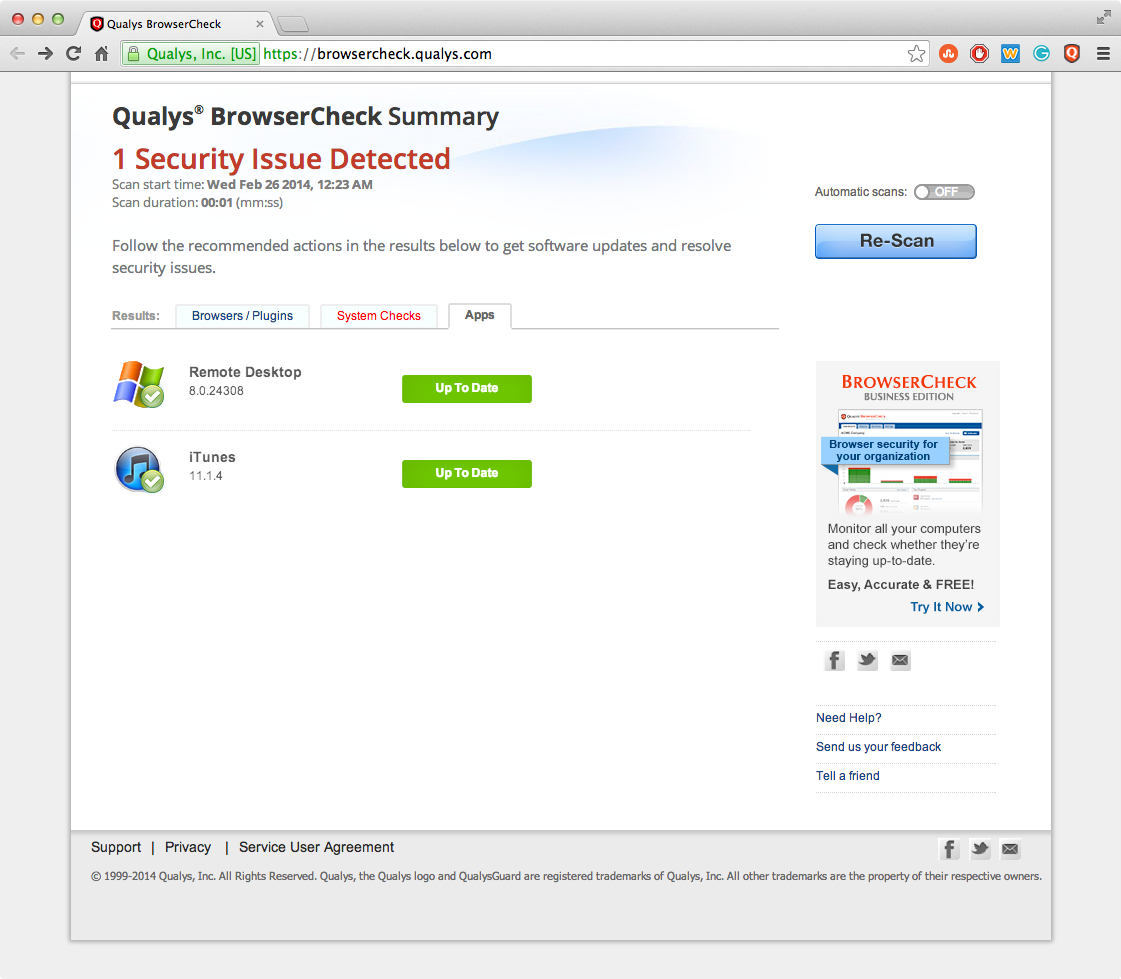
# System Check

The second screen is the System check, which checks over my Operating system and security setting ( antivirus and firewall). As you can see the operation system is up to date and perfect while the firewall isn't all that safe. When I clicked on the warning it showed me why it was bad. That the firewall was turned off. This is an easy fix and makes my computer safer too. I didn’t know this was a problem until I ran the software.



# Apps

Last but not least was the Apps section, this is the area that lists any apps that use or access 3rd party software, such as remote desktop and iTunes. These were all up to date and secure. This is great for me. It should be noted I use these machines a lot of web developers. If there was a problem, it would alert me to update the software.



This is great software that showed me all the problems I could have with my system. I was pretty safe with my settings beside the firewall. I didn't know it was turned off, but is now fixed. ☺.

I would highly rate this software for everyone to check their system. 10/10.