SECURITY ANALYSIS ON BROWSERS

Lilyana Petkova
University of Library and Study of Information Technology (ULSIT), Bulgaria,
lilyanapetkova92@gmail.com

Abstract: The evolution of the digital world brings up one constantly changing variable called cyber threat. The casual user must be aware of what possibly can get wrong while interacting in the cyber space. In best case scenario the user should follow the trends for being up-to-date with all present vulnerabilities. Most of the users are just users which makes them easy being attacked. Their lack of information or too professionally explained information on the attacks makes them refuse diving in more investigations. Which makes them incompetent to fight against possible attacks or at least dealing with the consequences.

The article is going to make a security analysis on the most used application interface that provides access to the cyber space: **browsers**. Browsers have grown in breadth and depth creating a complex architecture with many components which at some point as every software development comes up with errors. Those flaws allow the attackers to overcome all kind of security policies harming different endpoints: from hardware to software, into data. And in every case the losses of the end user are very serious.

In preparation of the article, the reported data covers the period from around 1989 until the first half of 2021 by illustrating the results into graphics. The data is collected through reports from the most popular worldwide insights like CVE and CVSS.

The most detailed analyses are on browsers like Google Chrome, Mozilla Firefox, and Safari as part of the research defines them as the most popular. In some points some of the other popular browsers are also reviewed but as the description of each of them is saying most of them are based on the three mentioned above.

In the recent years, browsers have integrated certain security header controls to support the web application security. Those headers leads the browser on how to behave when handling sensitive content and data of the application. Enabled in the application, browsers will prevent attacks automatically. But not all browsers support them! In previous research, the scope of the already available HTTP headers was fully described by definition and use. Therefore, this article will add some compatibility issues analysis.

Unfortunately, every day a new threat is coming up but being up-to-date with the latest updates always brings another level of security into the user's daily cyber activities. And as browsers are being the tool for accessing the cyber world, the goal of this article is to help choosing the right as part of the user secure browsing.

Keywords: browser, security, cyberattacks, vulnerability, web application.

1. INTRODUCTION

Being a user and a developer, the big question was always about the right browser to use. The market share provides us with different options which technically reviewed have their advantages and disadvantages.

With this article we want to provide an analyses of several browsers over the years and their vulnerability level according to international insights.

2. METHODOLOGY

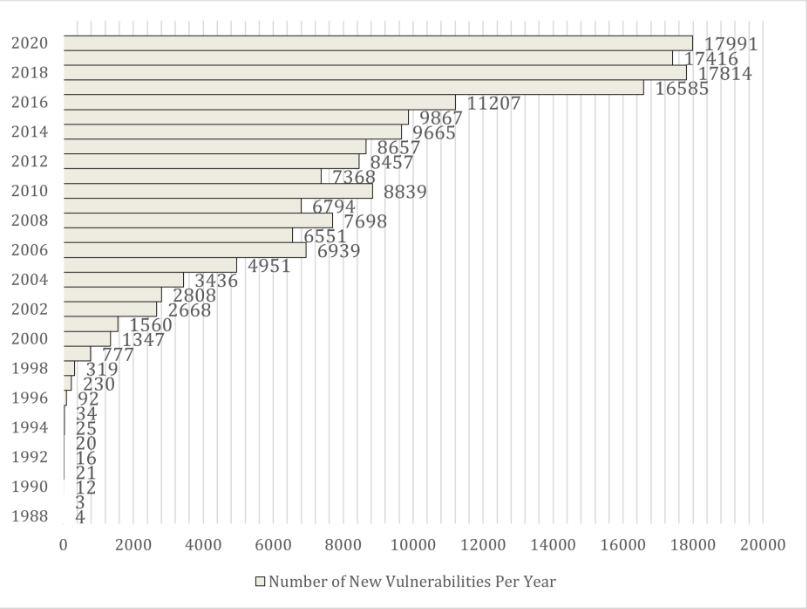
In preparation of the article, the reports begin with a comparison of the number of vulnerabilities per year for the period of 1989 up until 2021. During this period, the technological innovations passed through a lot of changes. Which makes us reduce this period for at least the last 15 years. The data is collected through reports from the most popular worldwide insights like CVE and CVSS. The analyses are on the following browsers: Google Chrome, Mozilla Firefox, and Safari which on personal opinion and as part of the research defines them as the most popular. Moreover, per description of all known browsers, most of them are based on the three mentioned above.

3. RELEVANCE OF THE PROBLEM

The issue of security is huge which year by year can grow even more due to the never stop innovating Internet technologies, as seen in Chart 1. Number Of New Vulnerabilities From 1988-2020. For the past forty years, the number of vulnerabilities has grown exponentially. The reason can be defined as a 'development cycle' which brings the question 'who started it first – the attacker or the developer?'. But in conclusion, the hacker is just a developer from the 'dark side', which means that the never stop innovation has started a constant battle between the good and the bad in software development. (Petkova, 2021)

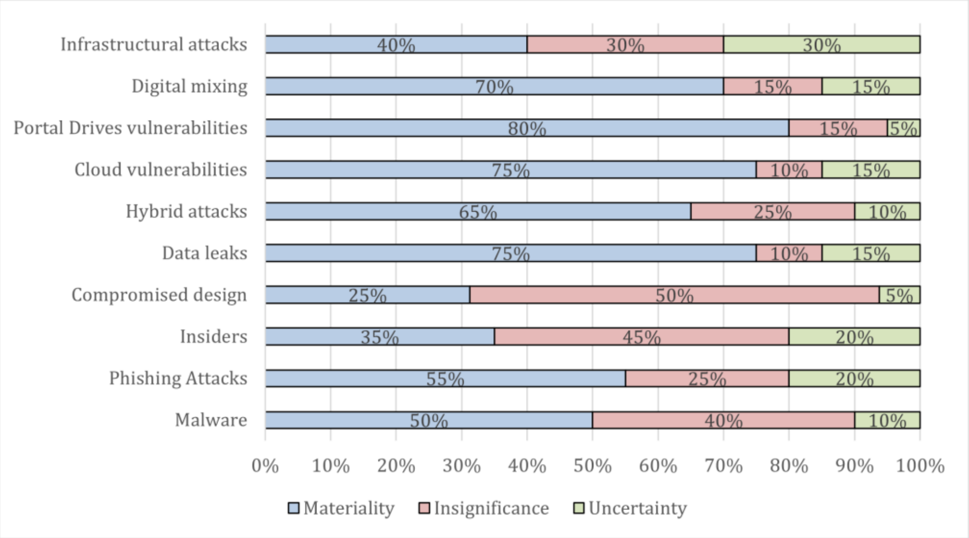
This means that the team must be continuously following the new “trends” in cyberattacks and never stop improving its skills to fight this “dark side” of the world of software development. (Arsov & Dimitrov, 2021)

Chart 1. Number Of New Vulnerabilities From 1988-202



Moreover, from Chart 2. Top 10 Cyber Threats for 2019 based on importance it can be concluded the importance of the attacked area. Which on the first view covers the entire software.

Chart 2. Top 10 Cyber Threats for 2019 based on importance



According to StatCounter, 50% of the internal-facing web applications vulnerabilities are considered high risk and around 32% on the internet-facing application. This tells us that more than 80% of web applications are vulnerable. Also, according to that report, 82% of the attacks in 2020 are critical, and only 6% with low risk. (StatCounter)

4. BROWSERS MARKET SHARE

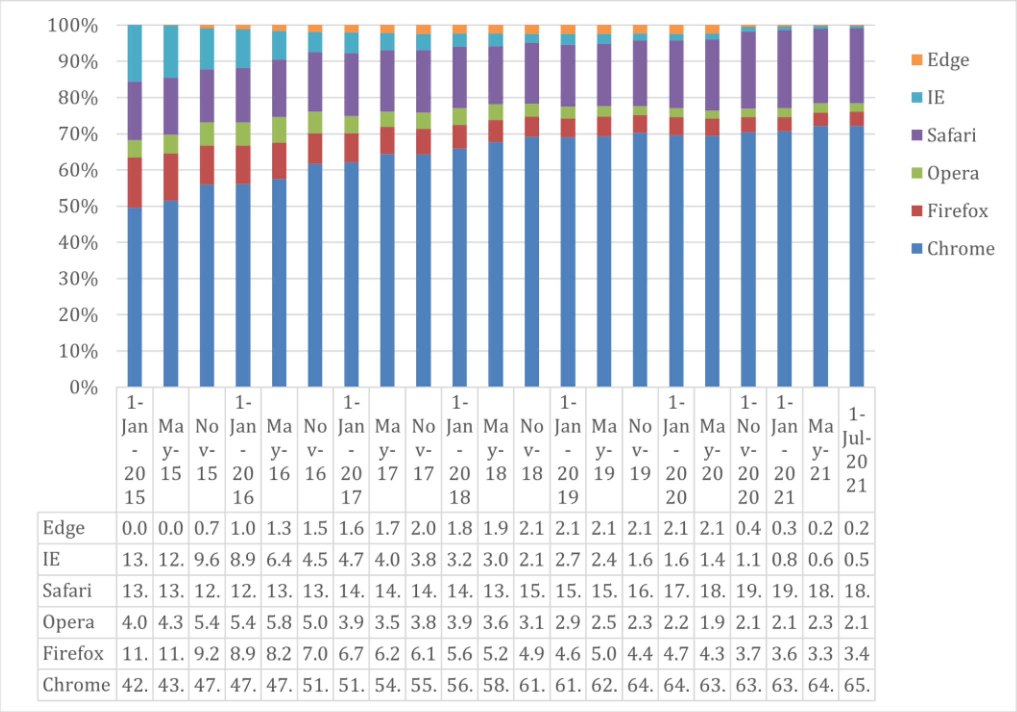
Web applications become a huge portal between different technologies in the different layers. For example, from a front-end perspective, the browsers cannot be controlled by the developers which come up questioning the browsers' security protection.

According to global analytical insights made from StatCounter (**https://gs.statcounter.com/**), the most used browser in 2021 is still Chrome followed by Safari. If see Chart 3. Browser Market Share from January 2015 to July

2021, the use of Chrome has increased by almost 20% for that period. Safari on the other hand has been consistently used during the selected period. (StatCounter)

Another significant difference is Internet Explorer whose use has been drastically decreased from around 15% to less than 1%. There are many reasons for that lack of enthusiasm of its use like frequently being vulnerable to some of the most critical attacks, lack of support, bad user experience. That's why in November 2020 Microsoft has announced that from August 17, 2021, this browser will be no longer supported.

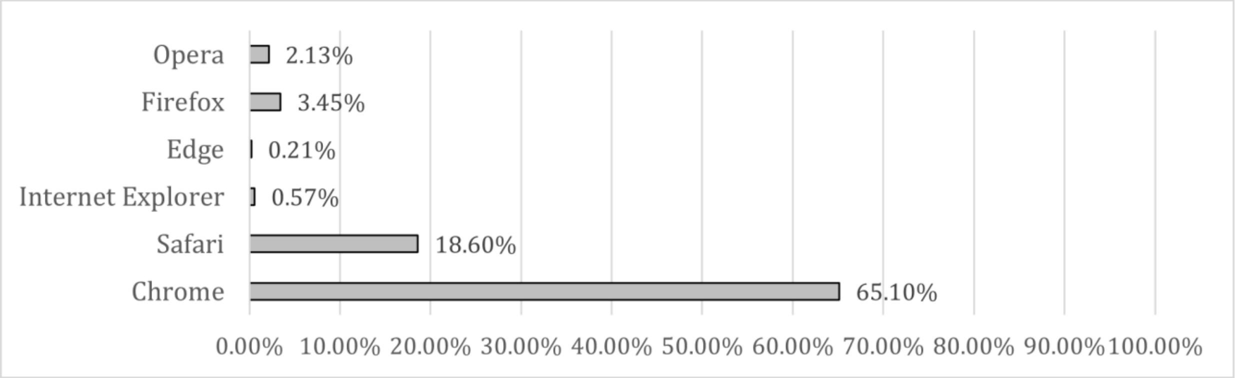
Chart 3. Browser Market Share from January 2015 to July 2021



	1-Jan-2015	May-15	Nov-15	1-Jan-2016	May-16	Nov-16	1-Jan-2017	May-17	Nov-17	1-Jan-2018	May-18	Nov-18	1-Jan-2019	May-19	Nov-19	1-Jan-2020	May-20	1-Nov-2020	1-Jan-2021	May-21	1-Jul-2021
Edge	0.0	0.0	0.7	1.0	1.3	1.5	1.6	1.7	2.0	1.8	1.9	2.1	2.1	2.1	2.1	2.1	2.1	0.4	0.3	0.2	0.2
IE	13.	12.	9.6	8.9	6.4	4.5	4.7	4.0	3.8	3.2	3.0	2.1	2.7	2.4	1.6	1.6	1.4	1.1	0.8	0.6	0.5
Safari	13.	13.	12.	12.	13.	13.	14.	14.	14.	14.	13.	15.	15.	15.	16.	17.	18.	19.	19.	18.	18.
Opera	4.0	4.3	5.4	5.4	5.8	5.0	3.9	3.5	3.8	3.9	3.6	3.1	2.9	2.5	2.3	2.2	1.9	2.1	2.1	2.3	2.1
Firefox	11.	11.	9.2	8.9	8.2	7.0	6.7	6.2	6.1	5.6	5.2	4.9	4.6	5.0	4.4	4.7	4.3	3.7	3.6	3.3	3.4
Chrome	42.	43.	47.	47.	47.	51.	51.	54.	55.	56.	58.	61.	61.	62.	64.	64.	63.	63.	63.	64.	65.

And when retrieving the data for the 2021 year from Chart 3. Browser Market Share from January 2015 to July 2021 there can be seen where it is a win for Chrome in Chart 4. Most Popular Web browsers in 2021.

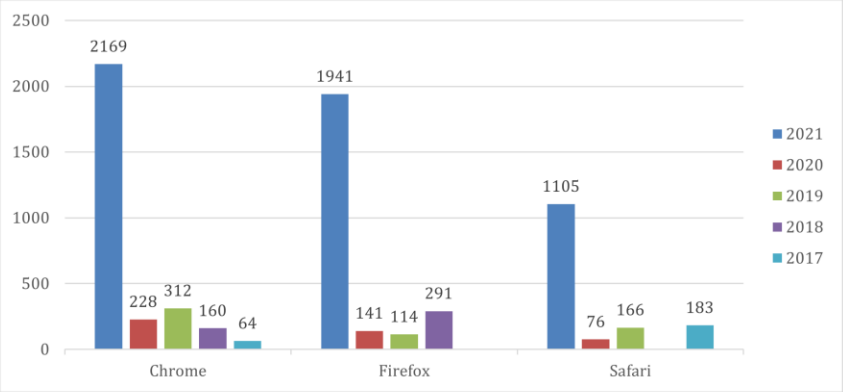
Chart 4. Most Popular Web browsers in 2021



But such popularity brings up a high vulnerability risk. According to CVE (Common Vulnerabilities and Exposures) reports from 2017 to 2021 (see Chart 5. Number of vulnerabilities in browsers for 2017-2021) for the top 50 products by total Number of "Distinct" Vulnerabilities on the most popular browsers (according to Chart 4. Most Popular Web browsers in 2021) Chrome is the browser that shows most errors in its software which provide hackers an opportunity to gain access to a system or network. (CVE details, n.d.)

This however does not mean that Chrome users are constantly facing dangerous attacks on their system, as Google continuously releases fixes to those bugs.

Chart 5. Number of vulnerabilities in browsers for 2017-2021



CVE also categorizes the vulnerabilities according to the weight of their damages from 0 to 9+. Where 0-1 are vulnerabilities with lower damage, and 9+ are those which can badly harm the system. And has a weighted average calculated with the following formula:

SUM((Cvss Range (*e.g: 2 for range 1-2*)) * (Number of vulnerabilities in that range)) / (Total number of vulnerabilities) (1)

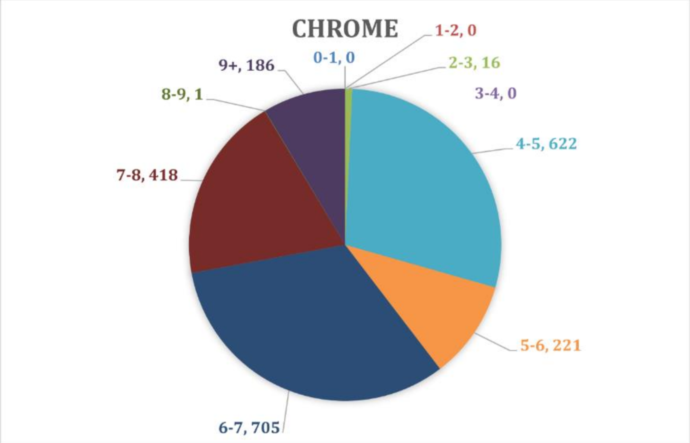
With the help of that equation, we are going to provide a calculation for the three selected browser on the weighted average.

4.1. CHROME

Google Chrome is a free web browser of Google created for “making the work in Internet faster, easier and safer with minimal design” based on the open-source Chromium (*which most of the new browsers are based on*). (US CERT)

As seen on Chart 6. Percentage of total vulnerabilities weight on Chrome 19% of the vulnerabilities on Chrome browser are with the highest risk on the system. 33% from the vulnerabilities very serious and 29% not so. And only 1% cannot seriously damage the system.

Chart 6. Percentage of total vulnerabilities weight on Chrome



And according to CVE, the total average weight is calculated to be around 6.7249. In Table 1. Weighted average of the vulnerabilities on Chrome validates the presented result from CVE according to Equation (1) where the total number of vulnerabilities is 2169 as visible from Chart 5. Number of vulnerabilities in most popular browsers for 2017-2021.

Table1. Weighted average of the vulnerabilities on Chrome

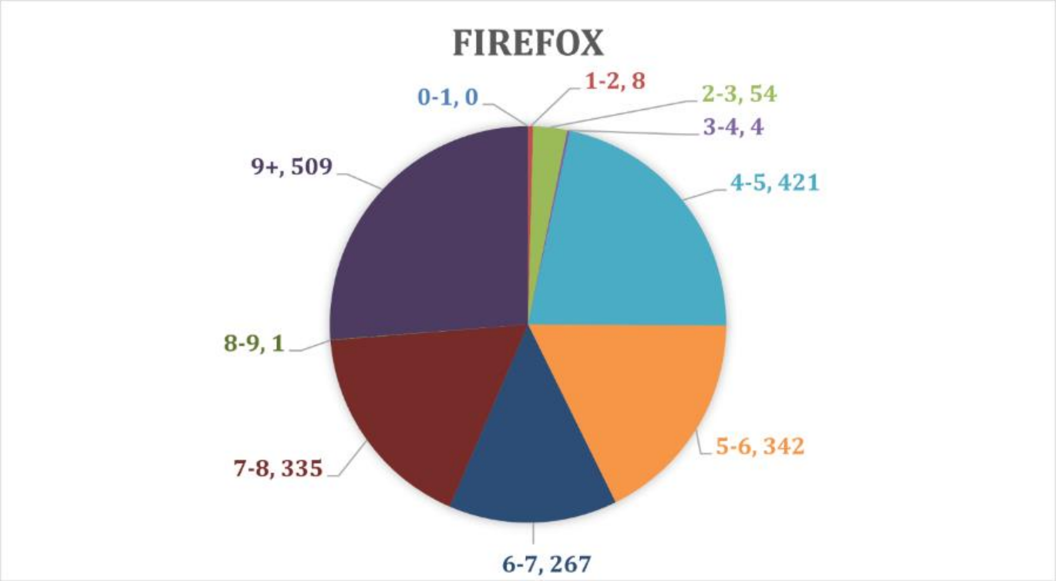
Range	Formula = Range * (Number of vulnerabilities in that range)) / (Total number of vulnerabilities)	Result
0-1	(1*0)/2169	0
1-2	(2*0)/2169	0
2-3	(3*1)/2169	0.0013
3-4	(4*0)/2169	0
4-5	(5*622)/2169	1.4338
5-6	(6*221)/2169	0.6113
6-7	(7*705)/2169	2.2752
7-8	(8*418)/2169	1.5417
8-9	(9*1)/2169	0.0041
9+	(10*186)/2169	0.8575
Total	~6.7249	

4.2. MOZILLA FIREFOX

Mozilla Firefox, or usually called Firefox, is an open-source browser based on Mozilla Application Suite. (US CERT)

With similar statistics, seen on Chart 7. Percentage of total vulnerabilities weight on Firefox that around 26% of the vulnerabilities on Firefox browser are with the highest risk on the system. 14% from the vulnerabilities very serious and 22% not so. And only 3% cannot seriously damage the system.

Chart 7. Percentage of total vulnerabilities weight on Firefox



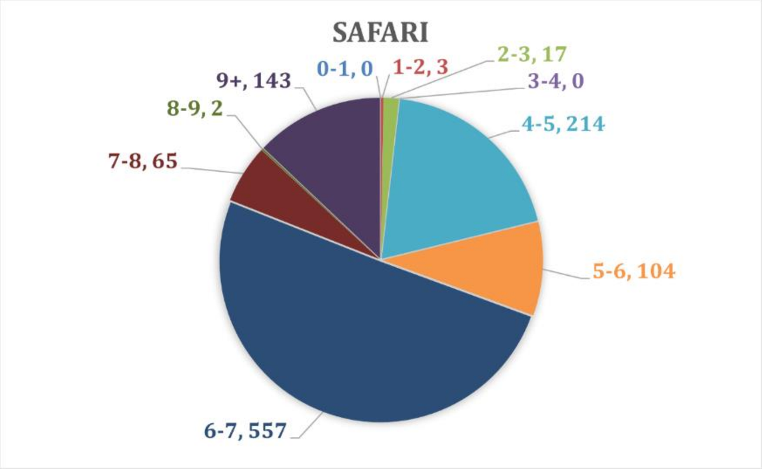
The total average weight of the vulnerabilities on Firefox is calculated to be around 7.2118 where the total number of vulnerabilities is 1941 (see Chart 5. Number of vulnerabilities in most popular browsers for 2017-2021).

4.3. SAFARI

Safari is a browser specifically built for Apple devices. It is built on JavaScript which according to Apple makes it the fastest and battery sufficiency browser. (US CERT)

With similar statistics, seen on Chart 9. Percentage of total vulnerabilities weight on Safari that around 13% of the vulnerabilities on Firefox browsers are with the highest risk on the system. 50% from the vulnerabilities very serious and 19% not so. And only 2% cannot seriously damage the system. And according to CVE, the total average weight is calculated to be 6.8938 where the total number of vulnerabilities is 1105 (see Chart 6. Number of vulnerabilities in most popular browsers for 2017-2021).

Chart 8. Percentage of total vulnerabilities weight on Safari



To summarize the highest risk in the most damageable vulnerabilities is Firefox followed by Chrome. But Safari is more vulnerable to average damages by 50/100 from all vulnerabilities.

5. CONCLUSION

Choosing the right browser can help a lot on the battlefield of security against attacks. In this article, we presented the results of the already reviewed during the entire scope of the research - attacks and security steps for protecting against them. As browsers are being the actual field where those battles are fought, with the analyses we are hoping of giving more clearness on the best browser to work on. Even thought there is no full security due to the constant technology innovations, the better one is the one which can constantly provide updates on the security level.

REFERENCES

Arsov, N., & Dimitrov, W. (2021). SECURITY ANALYSIS OF BROWSERS. *Proceedings Knowledge Society and 21st Century*. Sofia: UNIBIT.

CERT/CC. Secure Coding website. (n.d.). Retrieved from http://www.cert.org/secure-coding/

CVE details. (n.d.). Retrieved from https://www.cvedetails.com/.

Petkova, L. (2021). CYBERSECURITY TRENDS. *V INTERNATIONAL SCIENTIFIC CONFERENCE – CONFSEC*. Borovets, Bulgaria.

StatCounter. (n.d.). Retrieved from https://gs.statcounter.com/.

US CERT. (n.d.). Securing Your Web Browser. Retrieved from https://us-cert.cisa.gov/publications/securing-your-web-browser