A Web Browser Plugin for Users' Security Awareness

Thomas Hoad
University of Southampton
Southampton, United Kingdom
tdh1g19@soton.ac.uk

Erisa Karafili
University of Southampton
Southampton, United Kingdom
e.karafili@soton.ac.uk

ABSTRACT

Browsing online continues to pose a risk to the users' privacy and security. There is a plethora of existing tools and solutions that aim at ensuring safe and private browsing but they are not used by the majority of the users due to the lack of ease of use or because they are too restrictive. In this work, we present a plugin for Google Chrome that aims to increase the users' security awareness regarding the visited websites. We aim to provide the user with simple and understandable information about the security of the visited website. We evaluated our tool through a usability analysis and compared it with existing well-known solutions. Our study showed that our plugin ranking was high in the ease of use, and in the middle range for clarity, information provided, and overall satisfaction. Overall, our study showed that the users would like to use a tool that has ease of use but that also provides some simple security information about the visited website.

CCS CONCEPTS

• **Information systems** → *Browsers*; • **Security and privacy** → **Browser security**.

KEYWORDS

google chrome, plugin, security awareness, usability study

Thomas Hoad and Erisa Karafili. . A Web Browser Plugin for Users' Security Awareness. In . , 7 pages.

1 INTRODUCTION

Browsing the internet has become a necessity for most people either for work or for leisure. In the meantime, websites continue to be a major security concern given the intentional and unintentional existence of vulnerabilities, implementation errors, and malicious content [14]. Thus, it is still important to protect the users while browsing online. Lately, we have seen an increase in the number of internet scanners, plugins, and browser features that aim to protect the security and privacy of users while browsing online [13]. Even though we are seeing an increase in the usage of mechanisms like ad-blockers, there is still a low usage of security tools while browsing. One of the issues for the low usage of these tools is that some of them require the users to have some technical skills. On the other hand, some of these tools might not provide a lot of information to the user and are too restrictive.

In this work, we introduce a web browser plugin for the Google Chrome browser that aims to provide security awareness to the users about the websites they are visiting. The goal of this work is to provide concise and useful information about the security of the visited website to the user, so they can make an informed decision of whether to continue or not their activities on the website, or the type of information they want to provide. We aim with our plugin to increase the security awareness of the users. Furthermore, we want to show that users want to use plugins that provide some information related to the security of the visited website.

Our solution can be launched by the user and states if the visited website is secure or not. In particular, it provides the information in two ways: through a security rating (that goes from A to F, where A stands for very secure, and decreases until very insecure for F), calculated on different information and tests performed on the website; and some clear and concise information about the security of the website and the results of the test ran on it. The security rating is provided through a color-coded ring, while the security information is clear concise text information with color-coded "passed" or "not passed" for the security tests performed on that domain.

We decided to develop a plugin that provides not only an easy-to-understand rating but also some further information so that the users can decide by themselves if they would like to continue browsing or not. We evaluated our plugin through a pilot usability study of 21 participants, who tested our plugin together with other similar existing solutions. The results of the usability study were promising and confirmed our intuition that users would like to use security tools that provide an intuitive security ranking score backed by security information about the website. Through the usability study, we also collected information about the experience of the user while using our plugin. The results were positive, and the users liked the idea of the security ring. We used the feedback to improve our plugin.

We build our solution as a Google Chrome extension that communicates with a Node.js server running in the background of the user's computer. The server will be used to compute the information from the extension and collect a database of results. The extension uses the Chrome Developer API to provide a suite of data collection tools to curate many first-party security tests, corroborated with third-party tests from the Google Safe Browsing API and the IPQualityScore API.

The main focus of our work is security plugins that deal with the security of the visited website. We will not explore the security of the plugins themselves [8, 12], their impact [6, 11], or ways to make them more secure. The aim of our work is not to provide a new plugin that competes with existing commercial solutions but rather to show what are the features required to increase their usability.

The paper is organized as follows. In Section 2 we provide an overview of the related work and existing solutions. We introduce our solution in Section 3 and perform an evaluation on the usability

of our plugin and provide the results in Section 4. We conclude and introduce some interesting future work in Section 5.

2 RELATED WORK

Let us have a look at some of the related work around identifying vulnerabilities in the browsed website, as it is a crucial step in protecting the users. The authors of [19] present a framework for identifying vulnerabilities using a collection of scanning plugins to analyze the source code that links up to a vulnerability database. The user can choose the plugins available and receive a log file of the findings at the end. Even though the presented tool is not optimal, and takes a long time to run, the authors argue that using a combination of scanning tools helps to improve the number of vulnerabilities found, and different plugins can cover the shortcomings of others. The authors of [5] focus on detecting visible security flaws in websites. They looked at over 200 different financial websites and found that 76% of them had at least one of the searched vulnerabilities.

The browsers themselves provide features that protect the users' security and privacy by restricting the actions of a website. The authors of [3] performed an analysis of the security of the Google Chrome extensions and concluded that privilege separation and permission would reduce the vulnerabilities in these features. The authors of [15] present a browser extension that allows users to select the best features for the website by improving security and privacy without compromising the functionality.

Users' security awareness of the visited website and the inserted data is important. The authors of [10] introduce a plugin for the Firefox browser that provides security information when the user enters particular data into the website. Their solution has the same goal as our work, raise the awareness of the users about the used website through an accessible plugin. While their focus is on the security of the inserted data, our work focuses on the overall website vulnerability. Currently, there are various solutions that provide some form of security awareness to the user about the visited website (see Section 2.1). These solutions are not always efficient, e.g., the authors in [22] showed that users did not understand toolbar warnings for phishing attacks, while the authors of [4] provide a study of web browsing active and passing phishing warnings and how to make them more effective.

It is important to notice that even though different security solutions exist for detecting web browsing vulnerabilities, not all users use or are familiar with them. A study on the usage of ad-blockers [9] showed that the US west coast states had an average of 25% prevalence usage of ad-blockers compared to southern states with a roughly 10% usage. Indicating that the more educated states/those with the best access to technology were more aware of their security online and accessible solutions would help in diminishing this gap. Other researchers have focused on analyzing the effectiveness of CAPTCHA usage, like the authors of [18]. In this work, they showed that different CAPTCHAs have different levels of utility and user experience satisfaction, but generally, the users liked to know a CAPTCHA was in place but did not like spending any time unlocking it.

2.1 Current Solutions

We looked at existing solutions for the web browsing security and awareness and identified the below tools. Mainly we noticed that there is no solution that provides high accessibility and clear relevant information about the website security. The found solutions were focused either on the accessibility or the informative side.

The most popular solution on the Chrome extension store is the Avast Online Security Checker [16], judging from the higher number of downloads, reviews, and its very high average rating. This solution is highly accessible as it is very easy to install and run on the browser. The plugin gives a very simple website rating (either good or bad) with a single line of text and a unique thumbs-up graphic, with no further information on how the rating was done. The second most popular Chrome extension is the WOT security scanner [17]. The WOT has the same level of accessibility as AVAST, but with a rating system based on users' reviews, where most websites do not have enough up-to-date reviews to make the rating reliable.

Another interesting solution is SSL Trust [21] which is a website-based tool. It takes time to scan a single website but it provides a good range of information for the scanned website, like network protocol checks, secure connection certificates, vulnerability detection, and malware and antivirus checks. Google Safe Browsing is a feature embedded into Chrome. It tells the user if the certificate, resources, and connections are secure. Its website version is the Google Transparency Report [7]. The website solution gives instant feedback, but like the extension solutions, it gives only a single indicator of whether a website is safe or not.

Pentest Tools [20] can be considered as an alternative to the above solutions. This set of tools is not very accessible but provides a good range of information. The website can analyze a URL to find possible vulnerabilities and provide an overall security assessment for users who may not understand the technical jargon. Browser Audit [2] is another solution that mainly focuses on the actual browsers' security information. IPQualityScore [1] is another third-party API that provides a similar solution. This API provides information about recent malware, phishing, and spamming attacks relating to that website.

3 OUR SOLUTION

We developed a Google Chrome plugin that can provide the user with useful information about the security of the visited URL. As with all the plugins, after the installation, once you visit a website you can run it by simply clicking on it. Our solution calculates the results about the security of the visited webpage and shows them in the popup window. The results are shown through a user-friendly interface that displays an intuitive colored ring, as shown in Fig. 1 with the rating of the websites that goes from A to F. The rating was calculated based on further information and tests performed. Our solution also provides the user with the extra information to increase the user's cyber-security awareness, as shown in Fig. 2, which includes overall information about the security of the website. The rating ring and grade are key features of the design as they made our solution readable and easy to understand.

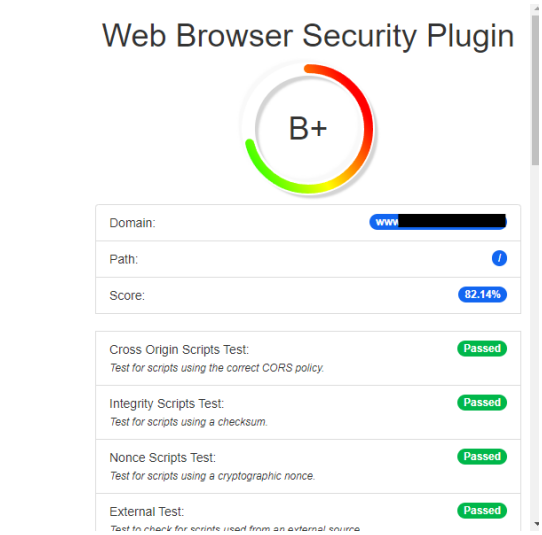

Figure 1: Plugin Main User Interface

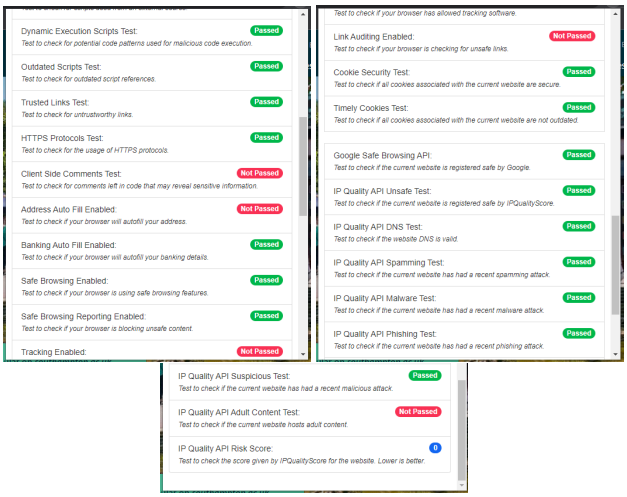

Figure 2: Information provided by the User Interface

3.1 Solution Architecture

Our plugin solution is composed of the client-side Chrome extension and the back-end server. The plugin architecture is shown in Fig. 3. The developed front end of the API consisted of a JSON manifest, a background JavaScript file, and an HTML file for the display. The client-side communicates with the server via web socket, sending JSON messages to each other. The server uses a web socket connection to communicate with an SQL database that stores the security information collected.

We show in Fig. 4 the entity-relationship diagram of our database. Every time a new scan of a website is completed, we automatically add the following records to the database, in case they do not exist in the table:

- A new domain;

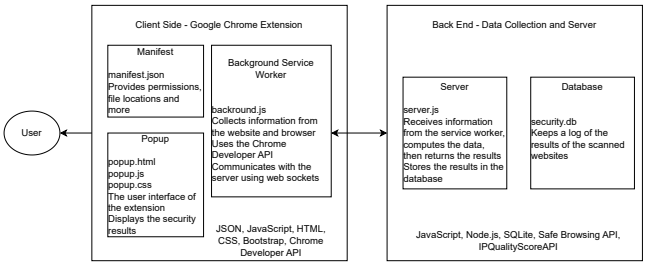

Figure 3: Plugin Architecture

- A new link - this record also contains the test results for that specific link;
- A new script - this record also contains the test results for that specific script;
- A domain entry with all the test results and a bit of background information;
- A link entry with the associated domain entry ID and link ID;
- A script entry with the associated domain entry ID and script ID.

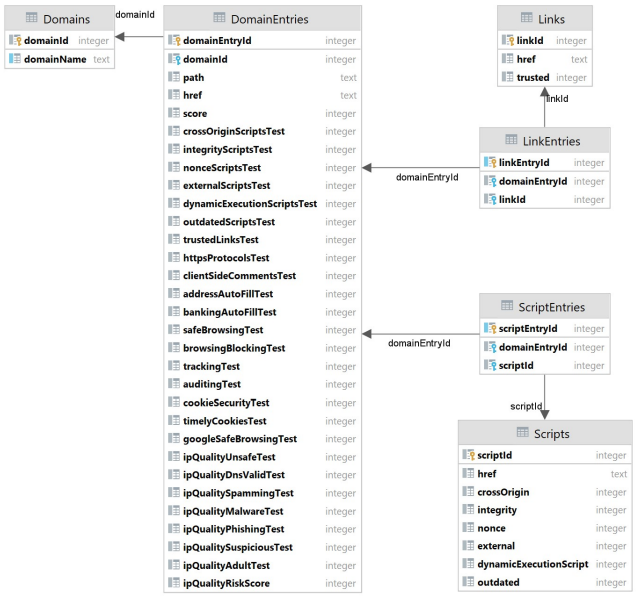

Figure 4: Plugin Database Structure

3.2 Implementation

We implemented a basic Chrome Extension, that required a manifest, a user interface, and a service worker. The data were collected every time a new website was loaded, refreshed or the active tab was changed. We collected the data through the built-in HTML commands for the window and document objects to collect information such as the path, domain, and URL protocol. We used the document objects to get the raw HTML of the website to be used

Address Auto Fill Test	Checks if addresses get auto-filled in forms. CVE-2012-3714CVE-2021-21177
Banking Auto Fill Test	Checks if the password information for a page gets auto-filled. CVE-2021-35527CVE-2022-0807
Safe Browsing Test	A measure of whether Google has safe browsing active. Prevents phishing/malware, active by default.
Browsing Blocking Test	It sends information to Google if a page is blocked, to discover malicious sites faster.
Tracking Test	If enabled, Google will ask websites not to track the user.
Auditing Test	Google will audit links on a page by pinging their requested destination.

Table 1: Performed Tests to the Browser Information

for the server scanning. Furthermore, we used also the Chrome Developer API to collect other data about the browser and the cookie data stored in the browser.

We collected information about the browser security every time we ran the service worker. This information does not provide the same level of results as the Browser Audit API, but it still provides a good overview of how Chrome itself tries to reduce risk. Below we provide parts of the API that are used to access this information. In Table 1, we present the performed tests, with information about what we were looking for and why.

- chrome.privacy.services.autofillAddressEnabled
- chrome.privacy.services.autofillCreditCardEnabled
- chrome.privacy.services.safeBrowsingEnabled
- chrome.privacy.services.safeBrowsingExtendedReportingEnabled
- chrome.privacy.services.doNotTrackEnabled
- chrome.privacy.services.hyperlinkAuditingEnabled

We then move on to collect cookie data from the browser, which usually has a lot of attributes that can be used to detect vulnerabilities. This data is filtered, to send to the server only information about the current domain.

We run various tests on: the scripts for the server, checking for different vulnerabilities; the cookies' security and their timeliness; and the HTTPS protocols, to check if the website uses the HTTPS protocol. We check if the website contains comments in the source code, as comments could contain sensitive or confidential information, and check if the links of the website directs to a secure location using HTTPS protocols. We used two third-party tools: Google Safe Browsing was used to know if the provided URL was considered safe by Google or not, while IPQualityScore provided further information e.g., valid DNS, URL associated to spamming, malware, viruses, or phishing attacks. After the various tests have been performed, the results are sent to the database to record the domain, scripts, and links with entries relating to all the associated files for each scan. Finally, our plugin calculates the results and shows them when the popup is opened. The results are shown through the security rating ring, and are split into three sections: overall information, first-party results, and third-party results. The results of each test are shown as either true or false. The score is calculated by counting the number of correct scores, getting a percentage, and then relating this information to an arbitrary grade to display.

3.3 Functionality Testing

We tested our solution on various websites to evaluate the provided results and answers. In particular, we present below a list of some of the websites that we used to test our plugin, with the rates provided by our solution and some explanations as to what we expected.

- University of XX website: We are fairly confident with the security of the website and is not a website you can log in to so there is a little avenue for an attack. Thus, in this case, we were expecting an A score, but the website did not passed some of the security tests. The provided grade was B+ while the score 82.14%.
- Twitter: A website with very high traffic and likely a very varied demographic. We were expecting it to be incredibly secure due to its popularity and reputation, but it did not passed all the security tests. The provided grade was B while the score 78.57%.
- cryptwalletimport.com: A website found using a fraudulent websites blacklist. Our solution rated it at a low C+ grade, as we were able to detect recent phishing activities. The provided grade was C+ while the score 67.86%.

4 EVALUATION

The main goal of our plugin is to inform the users about the security level of the visited website. In this section, we present the evaluation performed for our solution through our usability study. We provide below some more details on the usability study, its main results for our plugin. and some further information that came to light during the survey.

4.1 Usability Study

For our study, we recruited 21 users with different backgrounds, who took part in our study, tested our solution, and answered our survey. The users had different levels of education, different ages, as well as different level of security and technology experience. For the usability study, we also applied for ethical approval following the Institute guidelines (the approval is kept on file).

We divided the survey into four main parts: the consent and participation form, the internet browsing habits, usage of existing solutions, and rating of the existing solutions compared to our solution. In our survey (see Appendix A for details), we asked about the users' internet usage habits and their perception of safety whilst using their browser of choice. We wanted to capture people's opinions beforehand and then introduce the security extensions including our solution in order to understand how these solutions affected them and to capture the users' opinions. Along with our plugin, we showed other five existing solutions (Avast, WOT Scanner, SSL Trust, Google Sage Browsing, and Browser Audit). These solutions were picked as they are some of the most known and used ones.

We had one-to-one interviews with the users. We explained the study to our users, who would first fill out part of the survey related to internet browsing and usage of existing solutions. We then showed the users the different solutions, including our plugin, and asked them to try the various solutions by visiting websites of their choice as well as a list of other websites provided by us. All the solutions were already installed or opened (see Browser Audit) and ready to be used. At the end, we asked the users to finish the last part of the survey which asked them to rate all the solutions (including ours). In the survey, we also provided some screenshots for each of the tools, for the users to remember easily each of the solutions.

4.2 Main results

The results of our survey are provided below, where we present in Table 2 the calculated individual average rating made by the users for each of the seen solutions and the overall ranking of the tools with respect to their clarity, ease of use and information provided.

Our solution ranked best with respect to other Chrome extensions and had an average ranking with respect to clarity, ease of use, and provided information. Following the survey result, our solution does not compete on levels of information with SSL Trust and Browser Audit but it can provide a strong middle ground.

By analysing the results of our survey we can conclude that informative solutions are overall preferred over accessible solutions. Whilst accessible solutions ranked highly in the ease of use and clarity when it comes to the individual rating they fall significantly. Informative solutions often have to make significant trade-offs to achieve the required information. This can best be seen with SSL Trust which placed top in the information rankings yet 5th/6th in the clarity and ease of use rankings. From our results, we noticed that Browser Audit, which is a very unique solution, was ranked 1st on individual preference, and high for clarity and information provided.

In order to improve our solution, during the survey we asked the users to provide further feedback in terms of what they liked or disliked about our plugin and suggestions on how we could improve their experience in the usage of the plugin. The feedback was generally positive, e.g., a good number of users liked the security rating ring. Some of the comments we received were about the appearance of the tool, having more information about the tests, and the clarity of the scoring system. The majority of these comments were implemented in the final version of the tool, where we included more colour to make the test results clearer, added descriptions to the test so they are easier to understand, and improved the scoring system to reflect a more accurate grade.

4.3 Comparative Analysis

During our evaluation, we wanted to understand how our solution performed with respect to other similar tools. In particular, we compared it with similar solutions that focus more on the accessibility, by providing fewer results that are easier to understand by the users, like Avast and WOT. Both of them are Chrome browser extensions and as such have the same access to security information as our plugin. When analysing the results of the survey, we noticed that our solution had a higher rating when it comes to users' preference and information provided, and only second to Avast for ease of use, while the clarity was much lower than Avast but better than WOT.

The three factors we compared these plugins are the security rating, the breakdown of the score, and additional tools. For the first two, our solution provides a rating that you can differentiate between websites and is understandable for anyone at any level of technological proficiency. Avast gives you a thumbs up and WOT gives an equivalent rating with user reviews (that might be outdated and/or biased). Neither of these tools has a breakdown of how these results have been calculated, while we provide a host of tests that backup the provided score. We show a summary of this comparative analysis in Table 3.

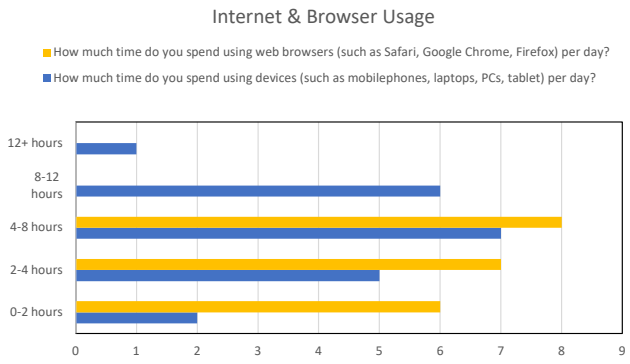

Figure 5: Internet and Browser Usage

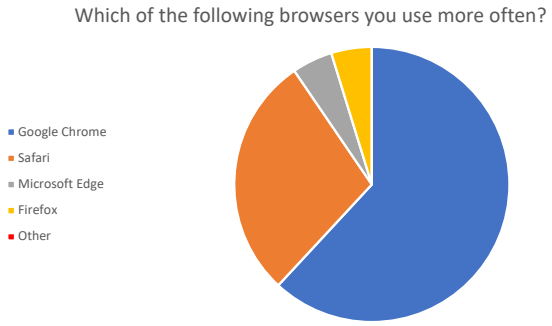

Figure 6: Popular Browser

4.4 Overview of further results of the survey

From the survey, we were able to collect some further information relating the users' browsing habits. In particular, we can see that most people spend many hours per day using the internet, an average of 6 hours for all devices and 4 hours for browsers (see Fig. 5). Google Chrome was one of the most popular browsers (see Fig. 6). In regards to security extensions, a very low number of the users that took the survey were using website security scanners (3 out of 21 users) and almost half of them (10 out of 21 users) were using ad blockers. We asked the users if they have used or heard of

Ranking	Clarity	Ease of Use	Information Provided	Individual Rating
1st	Avast	Avast	SSL Trust	Browser Audit - 4.19/5
2nd	Browser Audit	**Our Solution**	Browser Audit	SSL Trust - 4.0/5
3rd	Google Safe B	WOT Scanner	**Our Solution**	Google Safe B- 3.43/5
4th	**Our Solution**	Google Safe B	Avast Scanner	**Our Solution** - 3.43/5
5th	SSL Trust	Browser Audit	Google Safe B	Avast Scanner - 3.24/5
6th	WOT Scanner	SSL Trust	WOT Scanner	WOT Scanner - 2.14/5

Table 2: Ranking with respect to Clarity, Easy of Use, Information, and Individual Rating

Usability Tests	Our Solution	Avast	WOT
Average Rating	3.43	3.24	2.14
Clarity Ranking	4th	1st	6th
Easy of Use Ranking	2nd	1st	3rd
Information Ranking	3rd	4th	6th

Table 3: Comparison of Our Solution with Avast and WOT

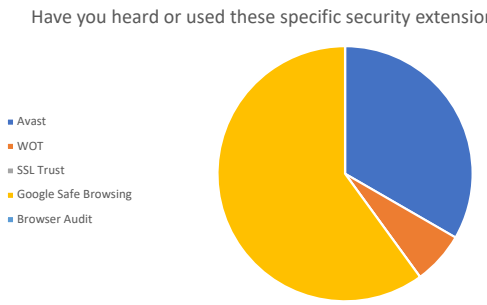

Figure 7: Other Security Extension

analysed security extensions and except for Google Safe Browsing, not many users had heard of any other existing security solutions (see Fig. 7).

5 CONCLUSION AND FUTURE WORK

Every day users spend a good part of their time browsing online. Not all of the visited websites are secure and some of them might have vulnerabilities or are used for malicious purposes. Knowing if a website is secure or not, and the vulnerabilities it suffers would allow the users to be more cautious during their browsing activity. Currently, some users are not aware of the existing solutions, or find them to difficult to use or understand.

In this work, we presented a solution, which is a web browser plugin for the Google Chrome browser. Our plugin provides an intuitive score security rating. It also provides further security related information as well as security tests performed on the website. We performed the evaluation of our plugin with a usability study where we compared our tool with other five existing solutions. Overall, our solution was in the middle ranking, on the higher bound for ease of use, and middle ranking for clarity and the quality of the information provided. Thus, surpassing some existing commercial solutions, despite the low resources spent on such plugin. We believe these good ranking results were due to the simplicity of the first feedback provided to the users (see Fig 1), thus, easily understandable by them; and the information provided about the tests that were passed or failed by the website (see Fig 2), thus, satisfying the users requests to know more on how the rating was calculated.

Our usability study confirmed that some users are not aware of the existing solutions that provide information about the security of the visited website or find some of the existing solutions to be difficult to use or not very informative. We gather also further information about the users' preferences, where it emerged that the users would prefer an informative solution rather than an accessible one. We believe that a trade-off like our solution would provide the best results from both sides and be preferable by current users.

There are different interesting future directions. One would be to further develop and test the plugin by removing some of the dependencies from third-party tools. Other research directions would be to extend the plugin to other browsers and to extend the usability study.

REFERENCES

[1] IP Quality Score API. 2023. *Malicious URL Scanner.* https://www.ipqualityscore.com/threat-feeds/malicious-url-scanner
[2] Browser Audit. 2023. *How secure is your browser?* https://browseraudit.com/
[3] Nicholas Carlini, Adrienne Porter Felt, and David Wagner. 2012. An Evaluation of the Google Chrome Extension Security Architecture. In *21st USENIX Security Symposium (USENIX Security 12).* 97–111.
[4] Serge Egelman, Lorrie Faith Cranor, and Jason Hong. 2008. You've Been Warned: An Empirical Study of the Effectiveness of Web Browser Phishing Warnings. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems.* 1065–1074.
[5] Laura Falk, Atul Prakash, and Kevin Borders. 2008. Analyzing Websites for User-Visible Security Design Flaws. In *Proceedings of the 4th Symposium on Usable Privacy and Security.* 117–126.
[6] José Carlos Coelho Martins da Fonseca and Marco Paulo Amorim Vieira. 2014. A Practical Experience on the Impact of Plugins in Web Security. In *2014 IEEE 33rd International Symposium on Reliable Distributed Systems.* 21–30. https://doi.org/10.1109/SRDS.2014.20
[7] Google. 2023. *Google Safe Browsing and Transparency Report.* https://transparencyreport.google.com/safe-browsing/search?hl=en_GB
[8] Teemu Koskinen, Petri Ihantola, and Ville Karavirta. 2012. Quality of WordPress Plug-Ins: An Overview of Security and User Ratings. In *2012 International Conference on Privacy, Security, Risk and Trust and 2012 International Confernece on Social Computing.* 834–837. https://doi.org/10.1109/SocialCom-PASSAT.2012.31
[9] Matthew Malloy, Mark McNamara, Aaron Cahn, and Paul Barford. 2016. Ad Blockers: Global Prevalence and Impact. In *Proceedings of the 2016 Internet Measurement Conference.* 119–125.
[10] Max-Emanuel Maurer, Alexander De Luca, and Sylvia Kempe. 2011. Using Data Type Based Security Alert Dialogs to Raise Online Security Awareness. In *Proceedings of the Seventh Symposium on Usable Privacy and Security (SOUPS '11).*
[11] Daniel T. Murphy, Minhaz F. Zibran, and Farjana Z. Eishita. 2021. Plugins to Detect Vulnerable Plugins: An Empirical Assessment of the Security Scanner Plugins for WordPress. In *2021 IEEE/ACIS 19th International Conference on Software Engineering Research, Management and Applications (SERA).* 39–44. https://doi.org/10.1109/SERA51205.2021.9509274

[12] Paulo Jorge Costa Nunes, José Fonseca, and Marco Vieira. 2015. phpSAFE: A Security Analysis Tool for OOP Web Application Plugins. In *2015 45th Annual IEEE/IFIP International Conference on Dependable Systems and Networks*. 299–306. https://doi.org/10.1109/DSN.2015.16
[13] Ignacio Redondo and Gloria Aznar. 2023. Whitelist or Leave Our Website! Advances in the Understanding of User Response to Anti-Ad-Blockers. *Informatics* 10, 1 (2023).
[14] Jahanzeb Shahid, Muhammad Khurram Hameed, Ibrahim Tariq Javed, Kashif Naseer Qureshi, Moazam Ali, and Noel Crespi. 2022. A Comparative Study of Web Application Security Parameters: Current Trends and Future Directions. *Applied Sciences* 12, 8 (2022).
[15] Peter Snyder, Cynthia Taylor, and Chris Kanich. 2017. Most Websites Don't Need to Vibrate: A Cost-Benefit Approach to Improving Browser Security. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security (CCS '17)*. 179–194.
[16] Chrome Web Store. 2023. *Avast Online Security Plugin*. https://chrome.google.com/webstore/detail/avast-online-security/gomekmidlodglbbmalcneegieacbdmki?hl=en
[17] Chrome Web Store. 2023. *WOT Website Security and Browsing Protection*. https://chrome.google.com/webstore/detail/wot-website-security-brow/bhmmomiinigofkjcapegjjndpbikblnp
[18] Nitirat Tanthavech and Apichaya Nimkoompai. 2019. CAPTCHA: Impact of Website Security on User Experience. In *Proceedings of the 2019 4th International Conference on Intelligent Information Technology*. 37–41.
[19] Nguyen Duc Thai and Nguyen Huu Hieu. 2019. A Framework for Website Security Assessment. In *Proceedings of the 7th International Conference on Computer and Communications Management (ICCCM '19)*. 153–157.
[20] Pentest Tools. 2023. *Website Vulnerability Scanner*. https://pentest-tools.com/website-vulnerability-scanning/website-scanner
[21] SSL Trust. 2023. *SSL Trust Website Safety and Security Check Website*. https://www.ssltrust.co.uk/ssl-tools/website-security-check
[22] Min Wu, Robert C. Miller, and Simson L. Garfinkel. 2006. Do Security Toolbars Actually Prevent Phishing Attacks?. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. 601–610.

A WEB BROWSER SECURITY SURVEY

We provide here the main parts of the Survey of our Usability Study introduced in Section 4.

Internet Browsing Habits

(1) Roughly how often do you spend browsing using devices (such as mobile phones, laptops, or PCs) per day?
- 0 to 2 hours
- 2 to 4 hours
- 4 to 8 hours
- 8 to 12 hours
- 12+ hours

(2) Roughly how often do you spend browsing using browsers (such Safari, Google Chrome or Firefox) per day?
- 0 to 2 hours
- 2 to 4 hours
- 4 to 8 hours
- 8 to 12 hours
- 12+ hours

(3) Which of these browsers have you used before?
- Google Chrome
- Safari
- Microsoft Edge/Internet Explorer
- Firefox
- Other

(4) On a scale of 1 to 5 how safe do you feel whilst using devices such as mobile phones, laptops, or PCs?
- 1-5 (1 very unsafe, 5 very safe)

(5) On a scale of 1 to 5 how safe do you feel whilst using web browsers such as Safari, Goggle Chrome or Firefox?
- 1-5 (1 very unsafe, 5 very safe)

(6) Do you use either of these kinds of security extensions? (Leave blank if you use neither.)
- Website Security Checkers
- As Blockers

(7) Have you ever heard of or used these specific security extensions?
- Avast Online Security Checker
- WOT Website Security and Browsing Protection
- SSL Trust
- Google Safe Browsing
- Browser Audit

(8) Are there any other security extensions that you use? Feel free to include as little or as much details as you like

Rating of the shown solutions

The following questions were asked after the user tried all six solutions. Please note that we asked for feedback for each of the solutions after their evaluation in the survey. For the sake of space, we removed all the feedback questions below.

(9) Solution A - Avast Security Scanner. How well do you think this solution provides a reliable security overview of the current website?
- 1-5 (1 very poorly, 5 very well)

(10) Solution B - WOT Website Security and Browser Protection. How well do you think this solution provides a reliable security overview of the current website?
- 1-5 (1 very poorly, 5 very well)

(11) Solution C - Web Browser Security Plugin. How well do you think this solution provides a reliable security overview of the current website?
- 1-5 (1 very poorly, 5 very well)

(12) Solution D - SSL Trust. How well do you think this solution provides a reliable security overview of the current website?
- 1-5 (1 very poorly, 5 very well)

(13) Solution E - Google Safe Browsing. How well do you think this solution provides a reliable security overview of the current website?
- 1-5 (1 very poorly, 5 very well)

(14) Solution F - Browser Audit. How well do you think this solution provides a reliable security overview of the current website?
- 1-5 (1 very poorly, 5 very well)

(15) How would you rank these security solutions in terms of how much information they provide?
- Solution A - Avast Security
- Solution B - WOT Website Security and Browser Protection
- Solution C - Web Browser Security Plugin
- Solution D - SSL Trust
- Solution E - Google Safe Browsing
- Solution F - Browser Audit

(16) How would you rank these security solutions in terms of how easy they are to understand? (all six solutions are provided as in Question 15)

(17) How would you rank these security solutions in terms of ease of use (all six solutions are provided as in Question 15)