ura

Case Study

HTTPS Everywhere Redesign

7th September 2019

A research study by **Ura Design**
Supported by **Open Technology Fund**

About

Ura Design

Ura is a digital agency focuses on visual communication solutions tailored for Open Source and Internet Freedom projects.

Ura is dedicated to Usability and User Experiences by keeping project's unique community consensus model in mind.

Ura was founded in 2016 in Albania to cater to the ever-rising demand for Usability and Design services in Open Source Software.

HTTPS Everywhere

HTTPS Everywhere is a Firefox, Chrome, and Opera extension that encrypts your communications with many major websites, making your browsing more secure.

HTTPS Everywhere is produced as a collaboration between The Tor Project and the Electronic Frontier Foundation.

Many sites on the web offer some limited support for encryption over HTTPS, but make it difficult to use. For instance, they may default to unencrypted HTTP, or fill encrypted pages with links that go back to the unencrypted site.

Table of Contents

Introduction

HTTPS Everywhere is a free and open-source browser extension for Google Chrome, Mozilla Firefox, Opera, Brave, and Firefox for Android, which is developed collaboratively by The Tor Project and the Electronic Frontier Foundation (EFF).

It automatically makes websites use a more secure HTTPS connection instead of HTTP if they support it. HTTPS Everywhere makes it possible to block and unblock all non-HTTPS browser connections with one click.

In an effort to improve user experience, HTTPS Everywhere went through a redesign phase. The process incorporated all core aspects of its UX design.

Our main objectives were: revamping the overall look and feel of the extension; improving its information architecture, consistency, language, usability; and rebuilding components in a standardized way.

We were committed to ensuring a smooth experience for everyone by following a user-centered design approach along the way.

Understanding the challenges

We started the redesign process by addressing the bigger picture first. We aimed to identify the underlying issues and challenges that we as designers face before starting to tackle specific usability issues.

Deciding priorities

Considering the fact that security-focused software often targets tech-savvy people, it tends to be intimidating for “average” users. Although HTTPS Everywhere is a security tool, its purpose is to ensure a secure connection and protect all; therefore, it targets a wide range of users.

Oftentimes, the “average user” is not interested in details on how HTTPS Everywhere works, they just want an easy way to set it up quickly and let it do its job in the background without wasting their time configuring the software.
Our challenge here was balancing out a simple interface with complex features.
We needed to find a way to keep the design understandable for “the average user,” yet intuitive for the “advanced user.” We decided to channel all our efforts into making the extension inclusive to all people despite their computer expertise, professional background or disabilities.

Leveraging the space

Since HTTPS Everywhere is an extension, the available space we had to work with was quite limiting. That meant we were restricted from using a lot of design practices that could otherwise help us make usability improvements. The challenge was to figure out a way to include all features, to prioritize and carefully place the most important ones, and to use a simple language that users can understand easily without needing any additional explanation.

Research

Throughout the redesign process, we UX research as an instrument to get closer to users. We decided to start with qualitative research, to then continue on with a quantitative approach. We conducted a few iterations of usability tests and also ran accessibility audits to make sure the whole user experience ties in smoothly.

Our research mainly focused on getting to know the users. We needed the perspective from first-time users to find out if they understood what HTTPS Everywhere does for them, if they understand its purpose, and if they find it useful? On the other hand, we also wanted to get feedback from regular users. How often do they use the tool? Do they find it helpful? And how do they perceive it compared to new users?

We analyzed the gathered information and used it to guide our decision-making throughout the redesign journey.

The research phase helped us tremendously in getting to know the users and tracking down all the pain points they've encountered while using HTTPS Everywhere. It also helped us get a feel for the overall experience users had when using the extension. In-person usability testing sessions allowed us to observe their reactions and emotions while accomplishing basic tasks that they would typically do to get the extension running or configuring it to suit their needs. It also gave us an insight into how users get help when they need it and made us reconsider new ways to offer help that is easily accessible.

Developing personas during this phase helped shape the design while keeping in mind our target users, which we had available to refer back to whenever we needed.

Survey

The survey questions were mostly focused on web security. We wanted to know more about participants' general understanding of security on the web and how the HTTPS Everywhere extension fits into it.
The survey included 12 questions, a mix of open and closed questions. We shared it on a few different platforms to target a diverse range of users, 34 people in total filled out the survey.

Hi. Your opinion is important to us! The information you provide will help us improve the HTTPS Everywhere experience on the desktop. The time estimated for this survey is 6 minutes.

1. How many hours per day do you spend browsing the internet?

- 1-5 hours
- 6-10 hours
- More than 10 hours

2. Which describes your computer/browser expertise best?

- Basic
- Intermediate
- Advanced

3. Which desktop browser do you usually use?

- Firefox
- Chrome
- Opera
- Other...

4. How concerned are you about your security while browsing?

- Not at all concerned
- A little bit concerned
- I am concerned
- Very concerned
- Other...

5. Is being on an HTTPS connection something you are aware of while browsing?

- Yes, most of the time
- Sometimes
- No, I forget about it
- I don't know what HTTPS is

6. How do you tell if a website you are currently using is secure and/or respects your privacy?

7. When a site requires sensitive information, e.g., your credit card, which steps do you take to ensure that the site is credible?

- ❏ Take a look at the FAQ section of the site
- ❏ Check which connection protocol the site is using
- ❏ Use an extension that enforces HTTPS connection on a site
- ❏ Read reviews about that site
- ❏ Try to contact the developers/maintainers/support
- ❏ Check the URL
- ❏ Check the certificate and see if it's valid and who issued it
- ❏ Add an extension that blocks non-secure websites
- ❏ Use other (non-HTTPS) extensions
- ❏ None of the above
- ❏ Other...

8. Can you tell the difference between HTTP and HTTPS; what do you know about these terms?

9. Have you ever used HTTPS Everywhere?

- Yes
- No
- I don't know what HTTPS Everywhere is

10. Please describe briefly what you think HTTPS Everywhere does for you.

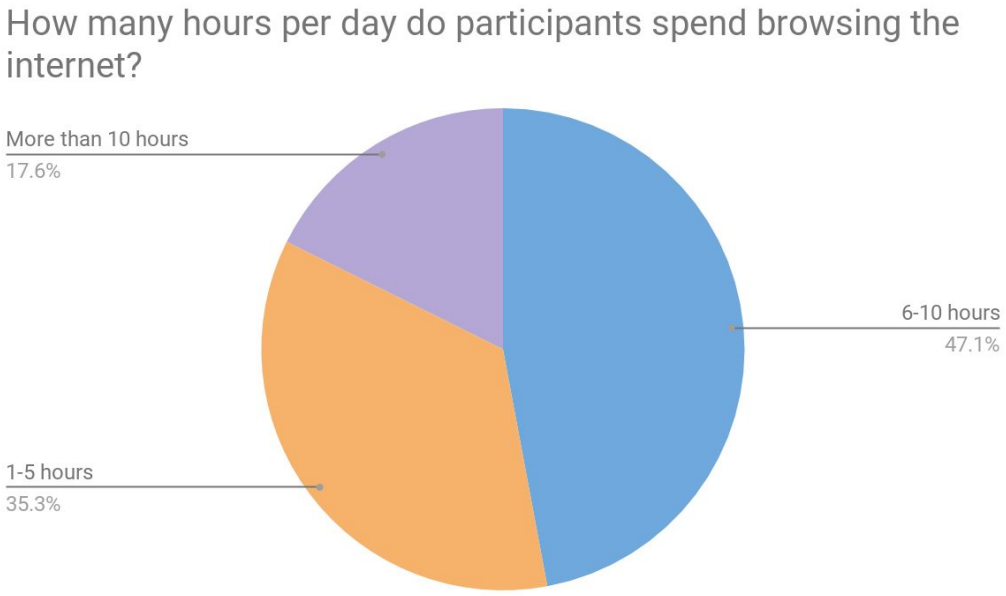
11. Which of these statements do you associate with HTTPS Everywhere?

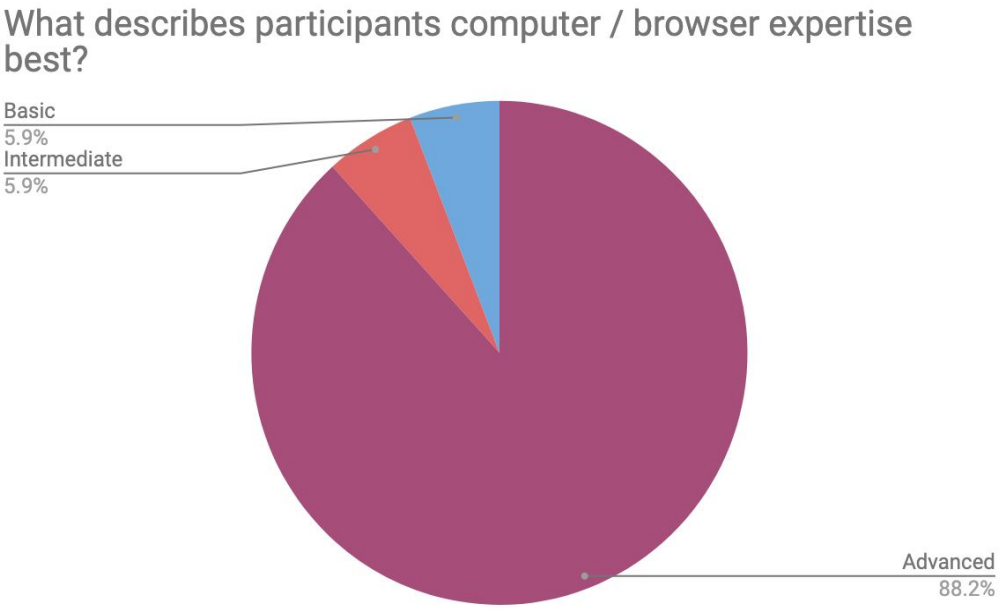
- ❏ Browser extension that blocks non-secure sites
- ❏ Browser extension that enforces sites to use HTTPS
- ❏ Browser extension that encrypts unencrypted site connections
- ❏ A protocol that indicates a secure connection
- ❏ Browser extension that blocks the non-secure elements of the site
- ❏ None of the above

12. What do you think HTTPS Everywhere protects you against?

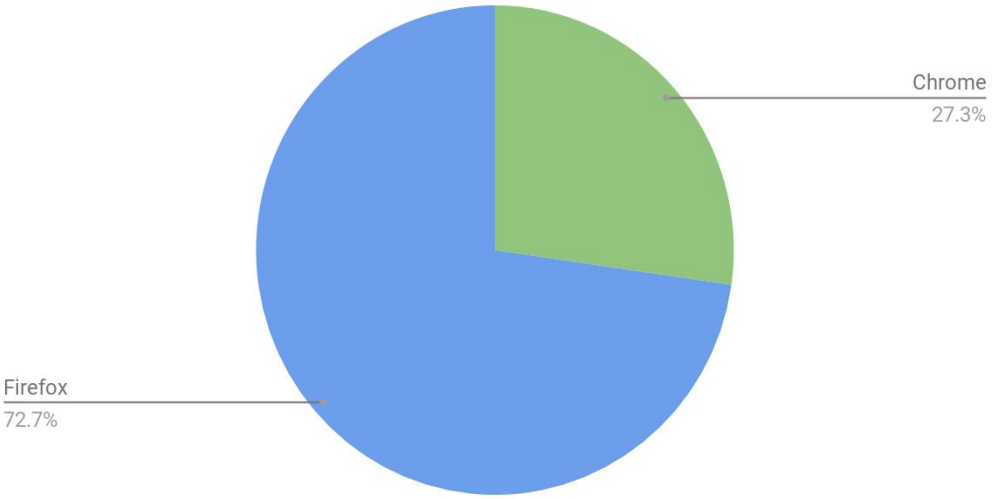
Results

Open questions

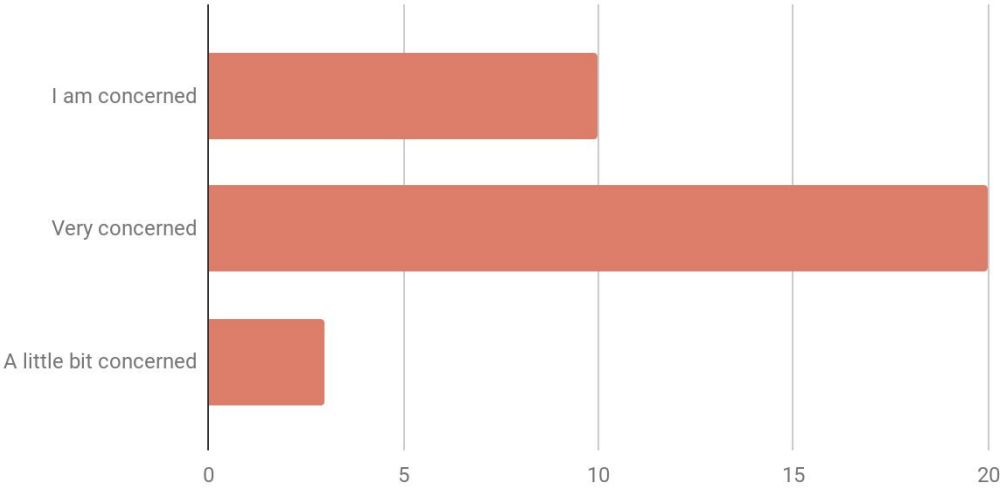


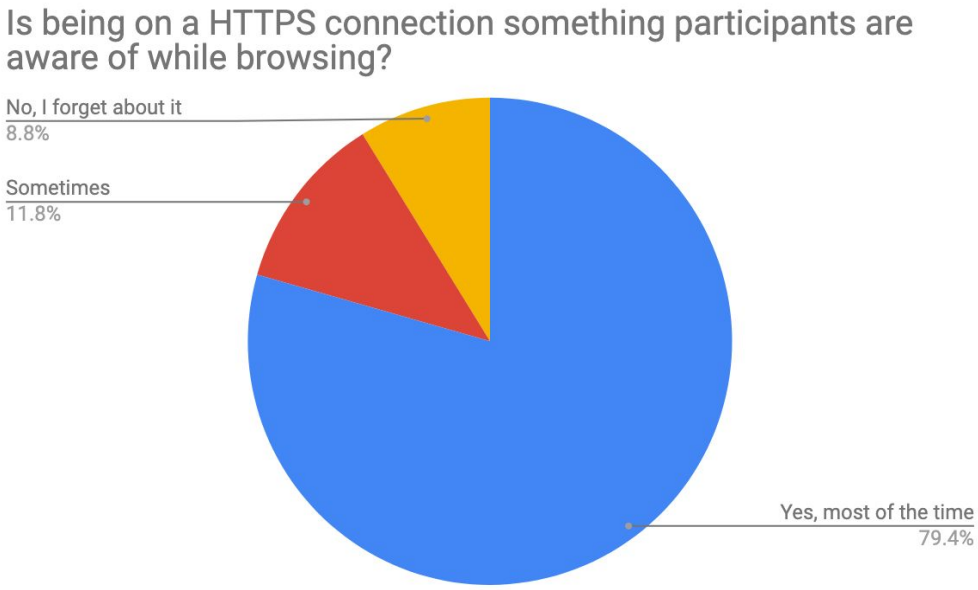


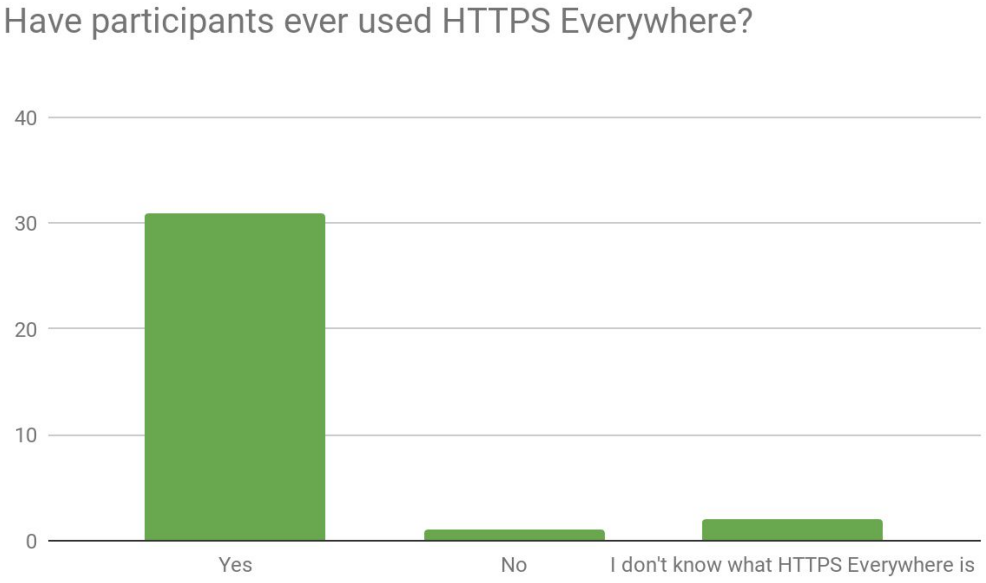
Which desktop browser do participants usually use?



How concerned are participants about their security while browsing?




Is being on a HTTPS connection something participants are aware of while browsing?
No, I forget about it
8.8%
Sometimes
11.8%
Yes, most of the time
79.4%


Have participants ever used HTTPS Everywhere?
40
30
20
10
0
Yes
No
I don't know what HTTPS Everywhere is

Closed questions

Question #6: *How do you tell if a website you are currently using is secure and/or respects your privacy?*

As we can notice from the chart #4, most users are concerned/very concerned about security and/or privacy; they are aware of it and try to make sure the connection is secure, and the site respects their privacy. From the answers collected, we can notice a pattern of methods that participants usually use to protect themselves.
The majority of users look for the “green padlock” in the left-hand corner of the URL and check if the site is connected through HTTPS. Some participants check the certificates, and some said that they use browser extensions to do that.

Privacy, on the other hand, seems to be trickier to check. Although some users mentioned that they read the terms of privacy, most of them didn’t know how to make sure that a site they are using is respecting their privacy.

Question #7: *When a site requires sensitive information, e.g., your credit card, which steps do you take to ensure that the site is credible?*

The majority of participants check the connection protocol to make sure it’s HTTPS, and they also use an extension to enforce HTTPS connection. In some cases, they also check the certificate to see if it's valid and verify who issued it.

Question #8: *Can you tell the difference between HTTP and HTTPS; what do you know about these terms?*

Users gave similar answers to this one. Some used more technical terms to describe it, while others chose a simpler way to do so. In short, they all agreed that HTTPS is the secure version of HTTP.

Question #10: *Please describe briefly what you think HTTPS Everywhere does for you.*

By looking at the chart that visualizes whether the participant has ever used the extension or not (chart at Question #9), we can see that most of the participants are familiar with it. They all described the extension's functionality in a similar way, something along these lines “HTTPS Everywhere enforces HTTPS connection.”

Two participants were not familiar with HTTPS Everywhere; their answers are a good chance to get the perspective of new users who are just introduced to the extension. This is how they answered the question:

- “I just read that it's an extension. Still, I don't think I would need it. If a feature is important enough, it should be the browser's default.”
- “It disables HTTP?”
- “It automatically makes websites use a more secure HTTPS connection instead of HTTP if they support it.”

Question #11: *Which of these statements do you associate with HTTPS Everywhere?*

This question aimed to reveal what was the user’s “first thought” was when HTTPS Everywhere was mentioned. The most common answer to this was: "It is a browser extension that enforces sites to use HTTPS."

Question #12: *What do you think HTTPS Everywhere protects you against?*

These answers give us a glimpse at the reasons why participants use HTTPS Everywhere. Some examples:

- “Man in the Middle attacks” *(a common answer)*
- “HTTPS Everywhere provides authentication of the website’s identity, connection, and data integrity, and encrypts all information shared between the website and a user (including any cookies exchanged), protecting the data from unauthorized viewing, tampering, or misuse.”
- “TLS/SSL stripping-web programming vulnerabilities on an HTTPS-enabled website.”
- “Surveillance. The addon, as far as I know, has no way of securing a site against non-requested packets”.

Participants gave very interesting and unique answers to the survey questions.
Although this is just a sample of opinions, we can extract some valuable conclusions regarding users’ understanding of web security and HTTPS Everywhere extension’s role in it.
The vast majority of users are concerned about their security on the web, but not all of them know how to protect themselves. They don’t know the steps they should

follow and signs they should pay attention to. Also, they often were unaware of what tools exist to help them on this path.

The survey definitely served its purpose in bringing light to misconceptions that users might have about HTTPS Everywhere. Especially on questions like “Please describe briefly what you think HTTPS Everywhere does for you” and “What do you think HTTPS Everywhere protects you against?” where all participants (new users and regular users) gave brief explanations on what the extension does or at least what they think it does to protect their security.

Judging from the responses, people do understand what the extension does for them. They might not understand the details of how it works, but they do know it helps them browse securely.

Personas

The survey laid out a solid foundation for developing personas. From the information previously gathered, we concluded three different categories of personas based on how much they are mindful of privacy. These categories are:

1. people who care a lot about privacy
2. people who care to some extent
3. people who don’t think about it that much

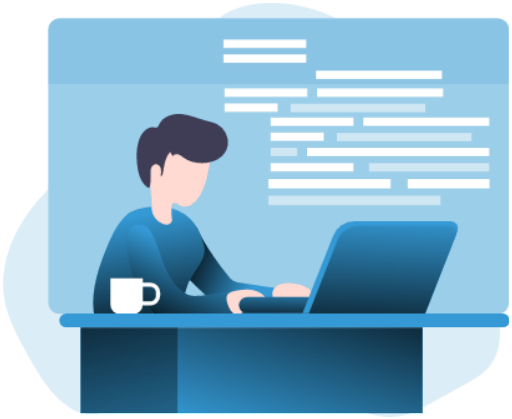
This conclusion is a derivative of many factors combined. For example, participants who spent 1-5 h or more than 10h using a browser are more likely to care about privacy than those who spend less time.

Name: Alexandra Gomez
Occupation: UX/UI Designer
Age: 32
Motivation:

- Uses a lot of web tools for her design work and productivity tools.
- Uses the web to do research

Name: Liam Davis
Occupation: Computer Science student
Age: 22
Motivation:

- Keen on security and privacy tools
- Uses Open Source software on a daily basis
- Uses the web to access study materials



Name: Keira Adams
Occupation: Financial Analyst
Age: 43
Motivation:

- Uses the web daily on her job
- Collaborates on documents with others
- Uses the web to access emails

Usability Testing

After completing the research phase, we started shaping the design. We decided to take an iterative approach to design. First, we did tentative design mockups and then tested them with participants' matching profiles with users extracted from persona development.

We conducted a 1:1 traditional Usability Testing. Participants were equipped with laptops and papers with the tasks that they needed to perform during the test. On traditional usability testing, typically only one participant at a time can enter the room and take the test. The test administrator was sitting next to the participant observing and taking notes. The session captured each participant's navigational choices, task completion rates, comments, overall satisfaction ratings, questions, and feedback. Testing did not include the download and installation process. HTTPS Everywhere extension was pre-downloaded and installed before the session started.

We conducted 5 testing sessions per iteration. The time for completing the session, including the introduction and follow-up questions was 40 minutes. All participants accomplished tasks within the time limit. We gave each tester five tasks as in the following:

Scenario tasks

After all the bad news you've heard lately about sites being hacked and private information stolen, you want to make sure that the sites you visit are secure. You decide to use the HTTPS Everywhere extension to help you do that.

1. Make sure that the HTTPS Everywhere extension is functioning while you are browsing through the site.
2. Make sure you don't enter sites that don't use encryption.
3. Please disable the extension only for ura.design site.
4. Now, you would like to append a new rule that is not currently on your stable rules list.
5. Please find all the listed rules that you added manually.

Follow-up Questions

We extended the testing time and asked questions about specific tasks that the tester found more difficult to conduct. Questions like:

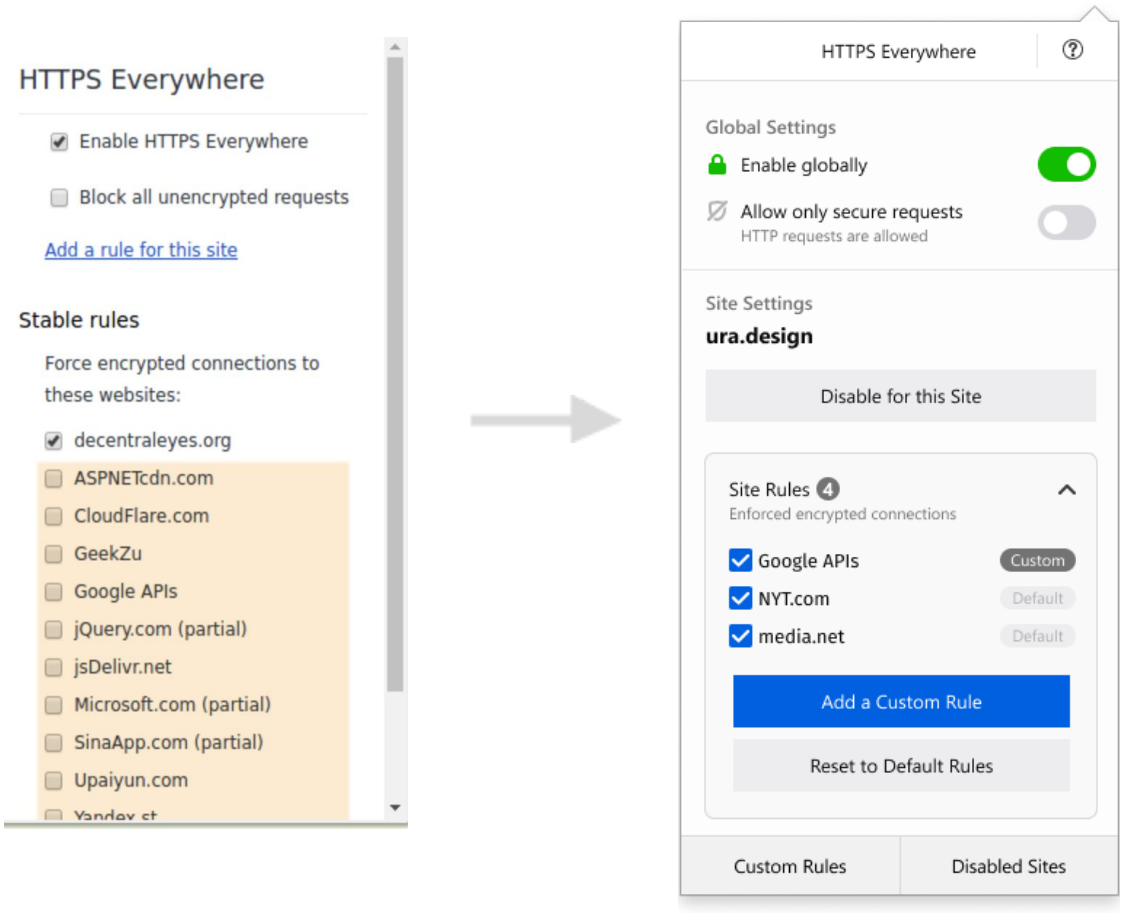
What were you thinking while completing this task?

Would it be more obvious for you to find this menu placed here?

Where did you expect to find this icon/menu?

How would it be more logical for you to accomplish this task?

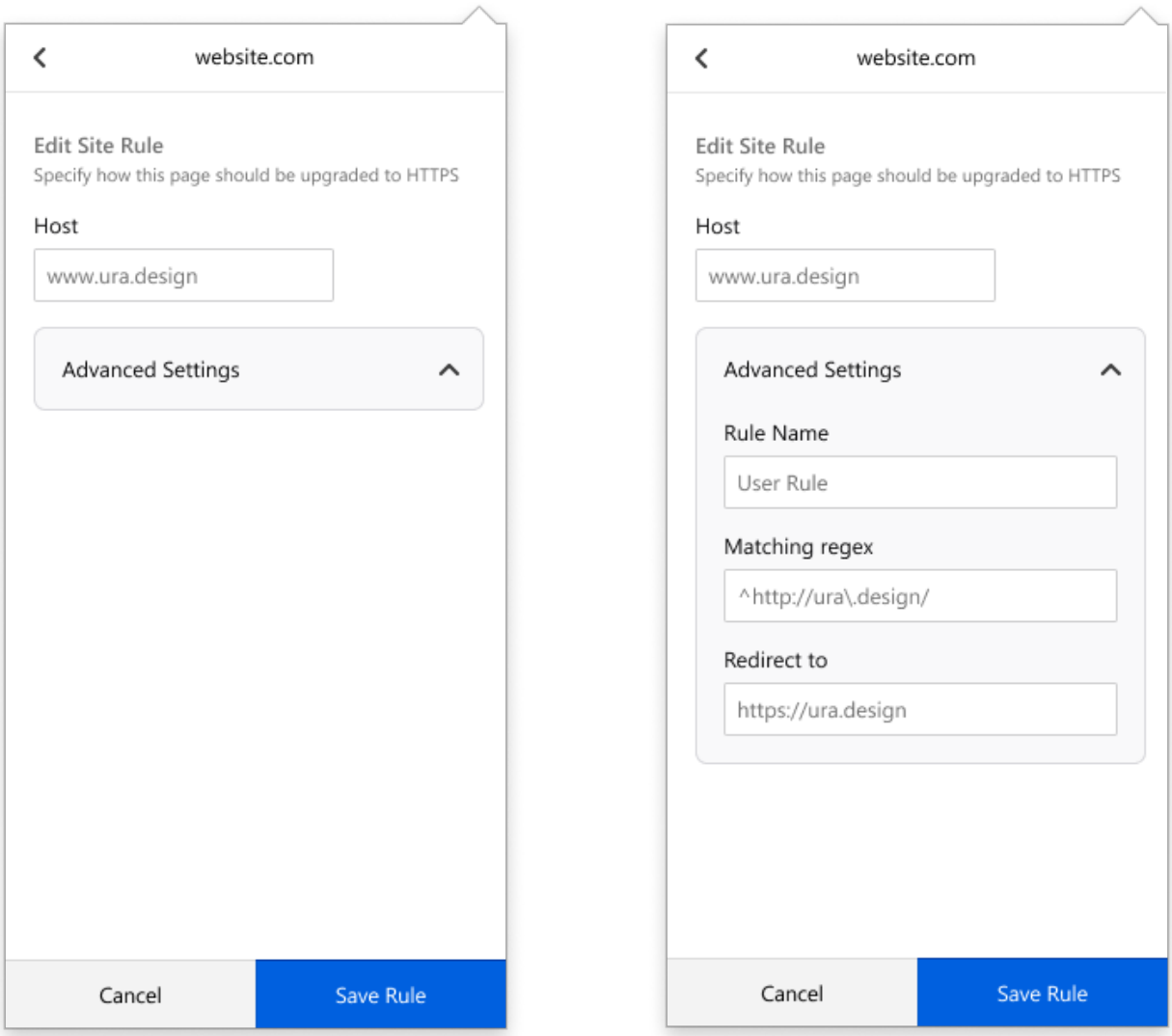
Iteration 1



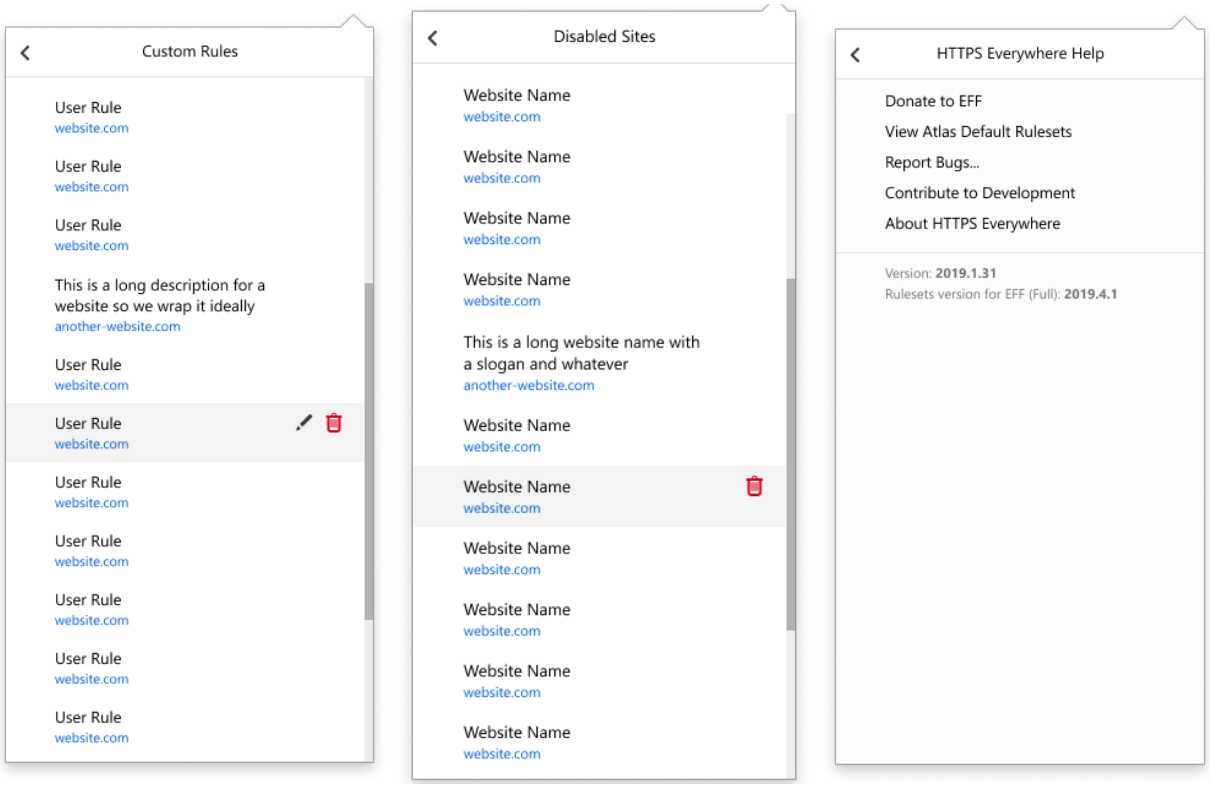
The user testing sessions we conducted allowed us to observe the most commonly used features of the extension. We started the first iteration with the main objective to gather all these features in one place, where they would be easily accessible. This results in saving time and avoiding frustration.

We decided that the “Site Settings” screen should be the main screen which contains all the important features and the user can easily navigate through.
The screen is split into two sections: “Global Settings” and “Site Settings”.
Global Settings contains the two main features of HTTPS Everywhere. Here the user can enable/disable the extension globally and control the allowance of requests.
Site Settings includes all the features that are specifically related to the site the user is visiting currently. Here they can control the rules applied to the site and disable them only for that site if they choose to. The toggle menu lists the applied rules, each rule is

labeled as “Custom” or “Default” in distinct colors. The user can also add a custom rule , reset to defaults or disable HTTPS Everywhere only for the visited site. In addition, they can also see a list of all custom rules if they wish to. The user can now access the disabled sites from the main screen; this feature was previously placed on add-on settings.



The site settings are now separated on a different screen, where user can edit site settings while specifying how they wish the page to be upgraded to HTTPS.
The basic view of the screen has a toggle menu to not confuse the user. When expanded, user can access the advanced settings and edit them before saving the new rule.



Users can access a list of all custom rules that they've added before and edit or delete each one. We also created a separate screen to show all the disabled sites.

On the previous version of HTTPS Everywhere, the disabled sites could only be accessed through add on settings on the browser. This option was hard to notice so the users ignored it most of the time. We decided that disabled sites need to be accessed easily, so we created a different screen where the user can find listed all the disabled sites, their names and URL and they can also have the option to delete them.

Through "HTTPS Everywhere Help" screen, user can view All default rules, report bugs, learn more on how to contribute to development or learn more about HTTPS Everywhere.

We used heatmap tables to visualize how each iteration performed and keep track of improvements.

How to read the map:

1. Scenario tasks (from the usability test) are arranged in rows
2. Test participants are arranged in columns (P1-5)
3. The colored blocks represent each tester's difficulty with each scenario task

G Green blocks represent the ability of the participant to accomplish the tasks with little or no difficulty.

Y Yellow blocks indicate the tasks that the tester had significant difficulties in accomplishing.

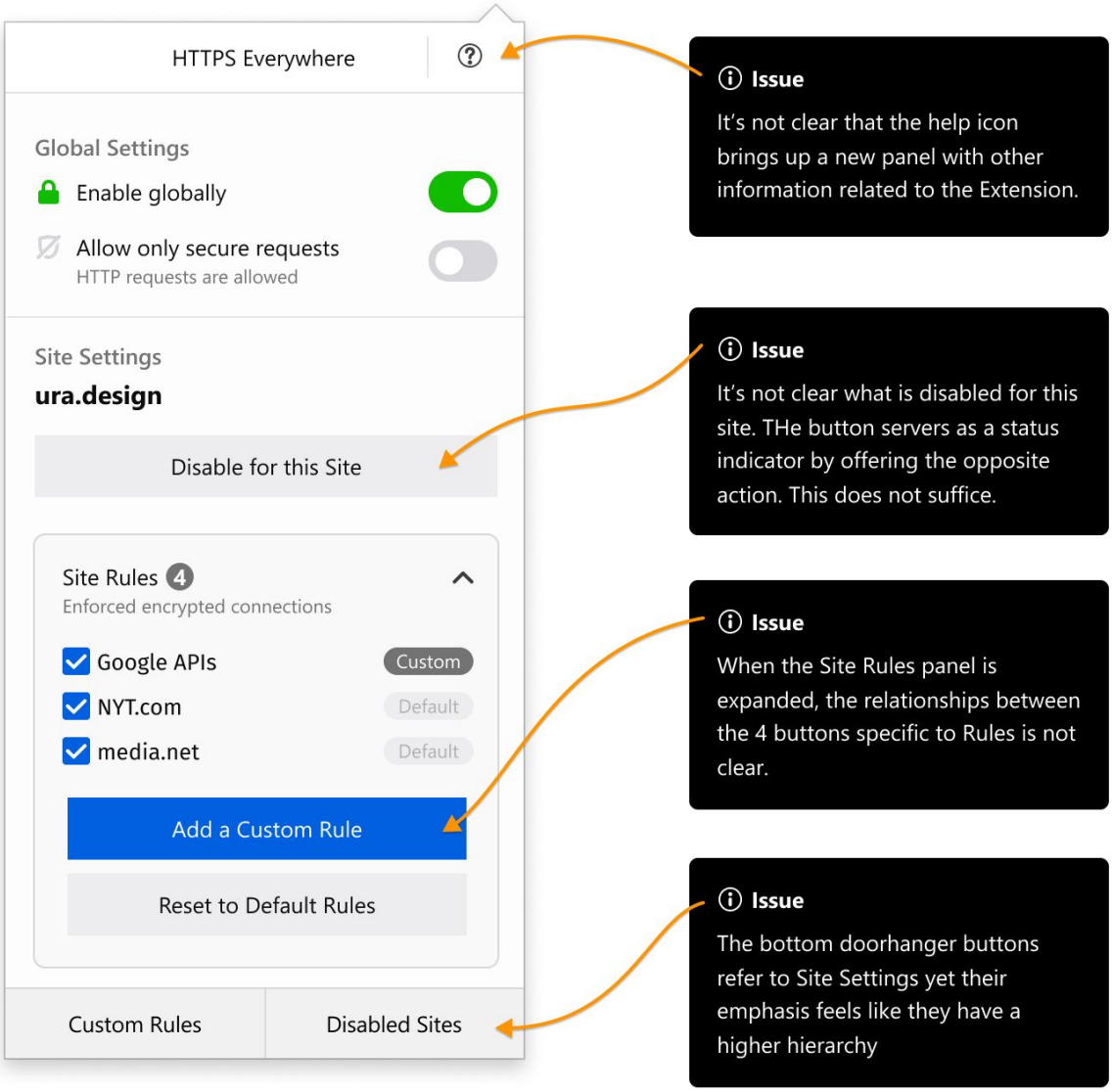
R Red blocks indicate that testers experienced extreme difficulty or where testers completed the tasks incorrectly.

B Black blocks indicate tasks the tester was unable to complete.

Iteration 1	**P1**	**P2**	**P3**	**P4**	**P5**
1. Enable HTTPSE globally	G	G	G	G	Y
2. Block HTTP requests	Y	G	G	Y	G
3. Disable HTTPSE for a specific site	Y	G	G	Y	Y
4. Add a rule	Y	R	R	Y	R
5. View custom rules	Y	Y	Y	Y	G

Iteration 2

Although the first iteration resulted in a big improvement, we can notice from the heatmap that there were still issues we needed to tackle. On the second iteration, we decided to refresh the overall look and deal with the usability issues from the previous iteration.



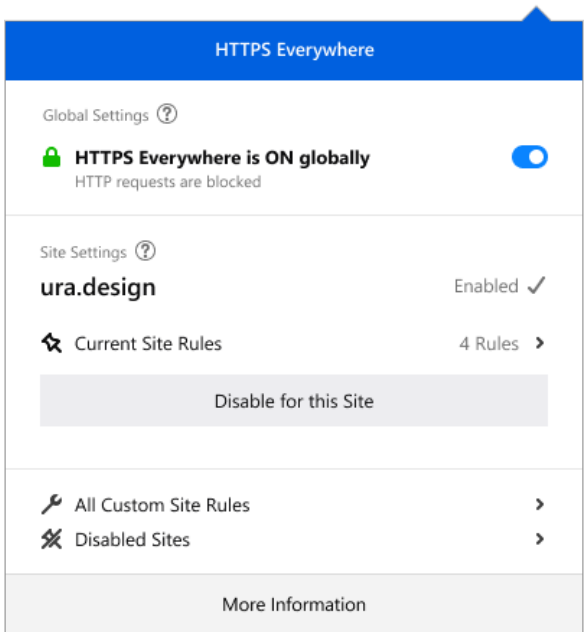
We included helpers that explain to the user what "Site Settings" and "Global Settings" are since there seemed to be a lot of confusion regarding these terms.

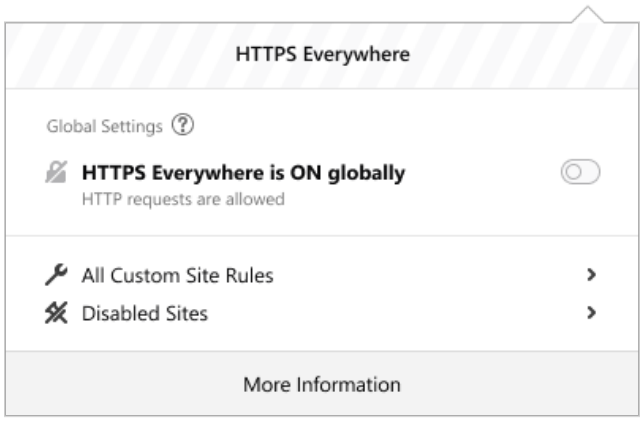
We also decluttered the main screen. In the previous round, we noticed that having a lot of buttons ("Disable for this Site" button, "Add a Custom Rule" button, "Reset to Default" button) on a small screen was confusing. The buttons were competing for the user's attention. We decided to prioritize the most used feature "Disable for this site" so that it is easily accessible and hide the buttons on Site rules screen, as these are

not used as often.

We also added clear indicators that show the state for the current site. Changing the background color of the button was not intuitive enough so we added a greyed out background for the whole section(see screenshot below). The user can now clearly see when HTTPS Everywhere is disabled for a specific site and can choose to enable it right away.

We also included a “More Information” button that helps the user understand more about the extension on the bottom because the “?” icon on the header did not perform well on the usability testing sessions. The icon didn’t give a clear direction that the user can click on it to access another panel which gives more information about the extension.





Main improvements:

- The blue colored header bar indicates that HTTPS Everywhere is enabled.
- The current site domain stands out due to the improved typographic hierarchy.
- The current site rules are nested in another panel which declutters the main view
- The list of customs rules and disabled sites is now separated from the current site settings with a lower emphasis.
- String clearly shows the current state in one option instead of two

- Small status indicators are very helpful in showing whether HTTPS Everywhere is enabled for the current site.

We also improved the browser status icon to make clear indications on what each of them means.

Full letter in blue color indicates that HTTPS Everywhere is enabled globally

Strike-through grayed out logo letter indicates that HTTPS Everywhere is currently disabled

Strike-through grayed out logo letter with a small dot indicates that HTTPS Everywhere is disabled for the current site, but is enabled globally.

Iteration 2

	P1	P2	P3	P4	P5
1. Enable HTTPSE globally	G	Y	G	G	G
2. Block HTTP requests	Y	G	G	Y	G
3. Disable HTTPSE for a specific site	G	G	G	Y	Y
4. Add a rule	Y	R	R	Y	G
5. View custom rules	Y	Y	Y	Y	G

Iteration 3

The third iteration was the final one, where we mostly polished the design and tackled some small usability issues, encountered on the previous iteration of user testing. These issues mostly being language simplification, iconography and information architecture.

Conclusion

Deciding our priorities in the very beginning gave us a clear direction of the design path we needed to follow. Our approach to redesigning the extension allowed us to completely transform the design without compromising the extension's functionality. Knowing the users is definitely the key to good user experience and starting the redesign phase with UX research helped us nail that aspect. Usability testing gave us a different perspective and helped us craft the design with diversity in mind.

Designing for a browser extension is quite challenging considering the limited space they offer but we managed to use the space wisely while being mindful to not overcrowd it.

The iterative designing and testing offered us flexibility and gave us space to improve.

Acknowledgments

Ura Team Members who worked on this study:

Renata Gegaj	Usability Researcher
Elio Qoshi	Creative Lead
Anxhelo Lushka	Frontend Designer

We also want to thank **Glenn Sorrentino** who independently conducted the first UX Audit for HTTPS Everywhere prior to this Usability Study.

This research has been made possible by **Open Tech Fund** which kindly funded this work.

Licensing