

How can the internet presentation of the lint list for the rust-clippy project be improved?

Fridtjof Stoldt

May 3, 2021

# Contents

<b>1</b>	<b>Introduction</b>	<b>1</b>
1.1	Problem . . . . .	1
1.2	Research question . . . . .	2
1.3	Goal . . . . .	2
1.4	Approach . . . . .	2
<b>2</b>	<b>Clippy's lint list</b>	<b>2</b>
2.1	Hosting . . . . .	2
2.2	Requirements . . . . .	3
2.2.1	Website functionality . . . . .	3
2.2.2	Requirements by the Rust Infrastructure Team . . . . .	3
<b>3</b>	<b>Fulfillment of requirements</b>	<b>4</b>
3.1	Repository requirements . . . . .	4
3.2	Hosting requirements . . . . .	4
3.3	Mozilla Observatory rating . . . . .	4
3.3.1	Scoring . . . . .	4
3.3.2	Measurement . . . . .	5
3.4	Summary . . . . .	5
<b>4</b>	<b>Analysis of missing response headers</b>	<b>5</b>
4.1	HTTP Strict-Transport-Security . . . . .	5
4.1.1	Preventable risks . . . . .	5
4.1.2	Importance for Clippy . . . . .	6
4.1.3	Configuration . . . . .	6
4.2	X-Frame-Options (XFO) . . . . .	6
4.2.1	Variations . . . . .	6
4.2.2	Importance for Clippy's lint list . . . . .	7
4.3	X-Content-Type-Options . . . . .	7
4.3.1	Importance for Clippy's lint list . . . . .	7
<b>5</b>	<b>Setting HTTP header fields</b>	<b>8</b>
5.1	GitHub Pages configuration . . . . .	8
5.2	HTML meta tag . . . . .	8
5.3	Content Delivery Network . . . . .	9
<b>6</b>	<b>Conclusion</b>	<b>10</b>
6.1	Summary . . . . .	10
6.2	Steps moving forward . . . . .	10
<b>7</b>	<b>Attachments</b>	<b>VI</b>

## List of Figures

## List of Tables

1	Mozilla Observatory analysis penalties for <i>rust-lang.github.io</i> from 2021-04-24 . . . . .	5
2	Determined values for the investigated HTTP header fields . . . . .	8

## Attachments

1	Mozilla Observatory output for <i>rust-lang.github.io</i> from 2021-04-24 . . . . .	VIII
2	The HTTP response header for <i>https://rust-lang.github.io/rust-clippy/master/index.html</i> from 2021-04-30 . . . . .	IX
3	The HTTP response header for <i>https://rust-lang.github.io/rust-clippy/master/lints.json</i> from 2021-04-30 . . . . .	IX
4	The HTTP response for the test page with <i>enfore HTTPS</i> enabled from 2021-04-30 . . .	X
5	Mozilla Observatory output for <i>rustup.rs</i> from 2021-05-01 . . . . .	XII

# 1 Introduction

Rust is a programming language that focusses on performance, security and reliability. The compiler is open source and dual-licensed under the Apache 2.0 and MIT license (Hoare and et al. 2019). Rust 1.0 the first stable version was announced in May 2015 (The Rust Core Team 2015). This release also marked the start of the *commitment to stability* which promises stability on future Rust stable releases (Turon and Matsakis 2014). This new commitment also introduced a 6-week release cycle as well as development channels for language users and early adapters (Turon and Matsakis 2014). The latest stable compiler version 1.51.0 has been released on 25 of March 2021 (The Rust Core Team 2021). Developers and teams within the project put high effort into open communication. This focussed is formalized in the official *Code of conduct* (The Rust Team 2021b). The language with its connected tools has attracted over 5900 individual contributors as of writing this (The Rust Team 2021a).

The Rust project consists out of several tools besides the compiler itself. These tools are seen as a vital part in automating parts of the development process and collaboration among teams. *Clippy* is the official linter for Rust and is being developed in the *rust-clippy* repository. The linter contains over 450 lints which span from complexity and style lints over to restriction lints which might be required by certificates (The Rust Clippy Developers 2021). Clippy is written in Rust itself and interfaces with the compiler directly. This direct connection enables the use of the existing lexer, parser and connected diagnostic tools and ensures that the project stays up to date with the latest compiler changes. Since 2018 Clippy is distributed as a component of the Rust installation itself (Lusby 2018).

## 1.1 Problem

Clippy maintains a website that contains documentation about all implemented lints. This list has the title *ALL the Clippy Lints* and will be referred to as *Clippy's lint list* or simply *lint list* in this paper. Diagnostic messages of the tool provide a suggestion and usually a small explanation with a reference to the website for a detailed lint documentation with examples. This makes Clippy's lint list the second point of contact for new users with the project itself. The lint list is also the only internet presentation of Clippy besides the GitHub repository inside the Rust organization.

Offering an online documentation gives a central point of reference that can be linked to and used in discussions. However, it also brings some responsibility when it comes to security and functionality. The *Rust Infrastructure Team*, a team inside the project with members that organize and manage the entire infrastructure, has therefore defined some guidelines for static websites (The Rust Infrastructure Team 2020). Clippy's lint list is static and should therefore follow these rules. A small review of these requirements has shown that not all of them might be fulfilled when it comes to security. Not having them fulfilled might give of a bad impression for new users and reduce the search engine rating.

A secondary problem is the initial load time of the lint list which is noticeably slower than most other websites in the Rust eco system. This aspect also influences the user experience and search engine rating. However, this will not be evaluated as part of this paper due to the fact that there has been some recent discussions on the topic inside the community to change the display of content completely which would void all research on this topic.

## 1.2 Research question

The described problem in 1.1 leads to the following research question: *Does Clippy's lint list fulfil all requirements and if not how can this be improved?*

## 1.3 Goal

The primary goal of this paper is to review which requirements are currently not met and possibly find a solution to fulfill them. These solutions should ideally be simple to implement in the form of a pull request in the GitHub repository or as a suggestion how to change the settings of the hosting provider.

## 1.4 Approach

The start of this paper will provide some context about the Clippy's lint list and the current hosting provider. It will then collect the requirements defined for that static websites, like Clippy's lint list, inside the Rust ecosystem.

The next chapter will then measure the current fulfillment of these collected requirements to deduct which topics should be further investigated. The following section will analyze the measurements and explain the technical importance behind them as well as evaluate the importance for Clippy.

Based in this work the author will try to find or develop solutions for unfulfilled requirements. This section might include some practical test to see if certain changes have the desired effects.

The assignment will conclude with a summary of the investigated topics and suggestions for further work that can be done on the topic.

# 2 Clippy's lint list

Chapter 1 gives an introduction of Clippy and the lint list which is being maintained by the contributors of the rust-clippy project. This section will provide relevant background information about the website and it hosting. It will then summarize the relevant requirements and conclude with an overview which aspects will be further investigated.

## 2.1 Hosting

Clippy's lint list is a static website centered around a HTML file which displays a json document with lint documentation and metadata. It additionally references resources by other projects but these two are the only once that are directly hosted in project. The website is automatically updated and deployed with every merged pull request.

The rust-clippy project has selected *GitHub Pages* as a hosting provider. GitHub Pages provides a simple way to host project websites directly from the repository itself. GitHub additionally provides a project domain which is made up of the name of the organization or username and a path to the project (GitHub Docs 2021a). For Clippy this domain is <https://rust-lang.github.io/rust-clippy/>. The use of this hosting adds no additional cost if the user or organization has a payed product plan, like *GitHub Pro* or *GitHub Team* (GitHub Docs 2021b). The later applies to the Rust Organization. GitHub Pages has soft limits when it comes to bandwidth usage, page site and amount of page updates per hour. The

documentation also states that the hosting should not be used directly for commercial purposes or sensitive and personal data (GitHub Docs 2021a).

## 2.2 Requirements

The research question specified in 1.2 focusses on requirements that are put on the lint list as a static website that is provided as a part of the Rust community. This part of the paper outlines these requirements.

### 2.2.1 Website functionality

The website has *functional requirements* which describe direct functionality and behavior that the website should provide (Sommerville 2010, p. 83ff). An example is the implemented search and filter feature. These requirements will not be listed as part of this work as they are not necessarily needed to fulfil the technical requirements defined in the Rust development documentation. However, it is noteworthy that this functionality should not be impacted by suggestions in this paper. This paragraph will be referenced again if a suggested solution could impact them. A list of requested and implemented functionality can be retrieved from the rust-clippy issue tracker.

### 2.2.2 Requirements by the Rust Infrastructure Team

The Rust Infrastructure team has created a set of guidelines that static websites affiliated with the Rust project should fulfill to be hosted and managed by them. Clippy is an official Rust project and the website itself presents static content, the guidelines therefor apply to the website. The requirements are as follows (The Rust Infrastructure Team 2020):

- "The website must be managed by a Rust team, or be officially affiliated with the project."
  - This point excludes community projects due to finite resources of the infrastructure team.
- "The website's content and build tooling must be hosted on a GitHub repository in either the rust-lang<sup>1</sup> or rust-lang-nursery<sup>2</sup> organizations."
  - The teams wants to be able to rebuild the website at any time. They therefor require it to be hosted in a GitHub repository that is also managed by them.
- "The website must be built and deployed with a CI service."
- "The website must reach an A+ grade on the Mozilla Observatory<sup>3</sup>."
  - This requirement focusses on user security as it ensures that multiple security features are enabled for the website. The referenced tool analyzes security features than can toggled through header fields in the HTTP response by the hosting provider. The target grade indicates that the website is configured correctly.
- "The website must be hosted on platforms vetted by the infra team."
  - The documentation recommends the usage of *GitHub Pages* or *Amazon AWS* in combination with *CloudFront* as a *content delivery network*. Other providers can be suggested and requested as long as they are deemed to be secure and reliable.

---

<sup>1</sup><<https://github.com/rust-lang>>

<sup>2</sup><<https://github.com/rust-lang-nursery>>

<sup>3</sup><<https://observatory.mozilla.org/>>

## 3 Fulfillment of requirements

The previous chapter has summarized the requirements that are put on Clippy's lint list and provided additional information and reasoning behind them. This section will investigate to which extend these are currently fulfilled. The goal is to identify key areas that could be improved.

### 3.1 Repository requirements

This first part evaluates the project and repository related requirements for the rust-clippy project. Clippy is as mentioned in 1 the official linter for the Rust language and deployed as part of the Rust installation. This makes Clippy an affiliated project to the Rust organization. The project repository is a part of the rust-lang organization on GitHub and therefor also satisfies the requirement of being managed by the Rust Infrastructure Team. Clippy therefor meets the project related requirements.

### 3.2 Hosting requirements

This section assesses the requirements connected to website hosting for Clippy. The project uses *continuous integration* to deploy the lint list with every merged pull request (The Rust Clippy Developers 2020). This ensures that the documentation is always up to date with current development. The content is hosted on GitHub Pages, this is a vetted and even suggested website host by the Rust Infrastructure Team. Clippy's lint list therefor fulfills all requirements in relation to deployment and content hosting.

### 3.3 Mozilla Observatory rating

*Mozilla Observatory* is a collection of tools that can analyze a website to determine which available security measures have been utilized by it (King and et al. 2018b). The scan is focussed on opt-in security options that are set in the HTTP response header, these will then instruct the client to enforce them (The Rust Infrastructure Team 2020). The Rust development documentation links to a free online interface<sup>4</sup> for the Mozilla Observatory that is provided by the Mozilla Foundation free of charge. The requirements in 4 state that a website should archive the grade A+.

#### 3.3.1 Scoring

The result of the analyzes is summarized in a single score with a corresponding grade. The score is calculated using a baseline. Each checked criteria can add bonus points or subtracted a penalty. This implementation is used to give different weight to specific configurations. The significance of these modifiers are based on how important the analyzed aspect for security. Scores can range from a minimum of 0 to a maximum of 135, the score of 100 already indicates that the website is configured correctly a higher score can be archived by gaining bonus points. A score of 100 and above corresponds to the grade A+ (King and et al. 2018a).

The observatory documentation notes that all websites are graded equally, this means certain graded configurations might be unimportant for the specific use case (King and et al. 2020).

---

<sup>4</sup><https://observatory.mozilla.org/>

### 3.3.2 Measurement

Scanning Clippy's lint list results in an overall grade of *C* with a score of 55/100. It is to note that the analysis cut of the path to the lint list and graded the domain itself. The results are therefor for the url `rust-lang.github.io` in general. The score was calculated using the baseline of 100 points and subtracting a penalty of 45 points. This sanction is the result of three failed tests that are shown in table 1.

No.	Score	Reason
1.	-20	HTTP Strict Transport Security (HSTS) header not implemented
2.	-20	X-Frame-Options (XFO) header not implemented
3.	-5	X-Content-Type-Options header not implemented

Table 1: Mozilla Observatory analysis penalties for *rust-lang.github.io* from 2021-04-24

The original scan output with all test results is included in attachment number 1.

### 3.4 Summary

The requirement evaluation has shown that Clippy's lint list fulfills all requirements with the exception of archiving a *A+* grade by the Mozilla Observatory rating engine. The actual grade is a *C* which is a result of three missing entires in the HTTP response header. The missing values are displayed in table 1.

## 4 Analysis of missing response headers

In it was determined that Clippy's lint list currently misses three HTTP response header fields to fulfill all requirements that have been defined in . This chapter will inspect each of this fields individually by explaining the technical background, evaluating the relevance for Clippy's use case and then suggest what each option should optimally be set to.

The observatory scan focuses on HTTP header which are set by the server behind the domain. The scan was therefor conducted for the domain `rust-lang.github.io`. Clippy's lint list is indirectly included in this result as well as documentation from other repositories inside the rust-lang organization. Further investigation will continue to focus on the context of Clippy's lint list however changes to the server could therefor also indirectly improve other sites.

### 4.1 HTTP Strict-Transport-Security

*Strict Transport Security* is a optional HTTP header field that instructs the client to only use encrypted connection for further requests. The instruction extends to all resources that are referenced by the requested result. It is therefor necessary that these resources hosts provide the option to download there resources over HTTPS (Hodges and et al. 2012, p. 6ff).

#### 4.1.1 Preventable risks

This header protects the user from *passive network attacks* where an attacker eavesdrop on the exchanged data. This can be used to collect personal information, passwords or browsing habits. A connection that is not encrypted is also vulnerable to *active network attack*. With this an attacker can impersonate



the actual site or deliver a modified version all together. An encrypted connection on the other hand can be used to request a certificate and validate that the content is delivered from the expected source. An additional advantage of this header is that it prevents accidental use of unencrypted connections by developers (Hodges and et al. 2012, p. 6ff).

#### 4.1.2 Importance for Clippy

Clippy's lint only displays publicly available information about lints in a easy accessible and searchable way. A passive network attack could therefor not collect any secret or personal information about the user. Except the fact that they visited the domain at all. However, this would still be possible with the header as the connected IP is not effected by it. The biggest threat could actually be an active network attack that injects a donation button into the website as several developers have expressed interest to donate to the Rust Foundation in general. This button would then forward the user to another page of the attacker to donate. However, the chance of this is probably negotiable due to the low traffic that Clippy's lint list actually receives. Such an attack would therefor be targeted an a specific user.

With all of this being said it has to be noted that all references to the website already include `https` at the start and a user has to deliberately enter the domain with `http` in front. Most browsers will then still recommend to use the encrypted connection or at least add a *not encrypted* notice next to the URL. All of this results in a very low risk. The header should still be set if the hosting provider provides a simple setting for this. Also due to the fact that the targeted A+ rating would require this field.

#### 4.1.3 Configuration

The header can take up to three arguments that configure which domains are included in this instruction and a duration for how long an encrypted connection should be forced (Hodges and et al. 2012, p. 14ff). Both Mozilla and the Rust development documentation recommends to define a duration of two years in the header field. This is equivalent to the value `"max-age=63072000"` (King 2018, `citerust-forge.static-websites`). This is therefor also the recommended value for Clippy's lint list.

### 4.2 X-Frame-Options (XFO)

This header was initially implemented by browsers as a non-standard HTTP header field as a new security measure to prevent the thread clickjacking. In 2013 the header was formalized by the *Internet Engineering Task Force (IETF)* in RFC7014. Clickjacking describes is the act of hijacking clicks of the user, this can be done by embedding a website that should be hijacks as a frame and than getting the user to unknowingly interact with that site. The XFO header field allows a host to specify that delivered content must not be displayed in a frame (Ross and Gondrom 2013, p. 3).

#### 4.2.1 Variations

The option can be set to three mutually exclusive values (Ross and Gondrom 2013, p. 4):

- *DENY*: Indicates that the content should not be displayed in any frame.
- *SAMEORIGIN*: Allows the display of the content inside a frame as long as it originated from the same origin as the frame.

- *ALLOW-FROM*: This prohibits the display of the content with the exception of the origins that are defined after the "ALLOW-FROM" value.

#### 4.2.2 Importance for Clippy's lint list

Clickhijacking is used to make a victim interacts with a different website to use the privileges or data that the user has saved on that site. Clippy's lint list provides the same data to everyone and the only user specific data is the selected color theme. An attacker has therefor nothing to gain with this attack. Adding the header would actually reduce flexibility from external users to embed the lint list in their own interface, even if the project at this point doesn't know of website doing so.

However, Clippy's lint list is just one site that's hosted under the domain, it should be investigated if other sites contain sensitive data that would require the header. This paper will still look into setting the header as it is required so receive a A+ grade by Mozilla Observatory. The goal will therefor be to set the header to *DENY* this can later be expanded to *SAMEORIGIN* or *ALLOW-FROM* if required.

### 4.3 X-Content-Type-Options

In 2008 the *X-Content-Type-Options* HTTP header was initially implemented by Microsoft in Internet Explorer 8 to prevent attacks that abuse *MIME-sniffing* for attacks (Lawrence 2008b). HTTP includes a content-type header that indicate the type of content that is being delivered, these types are called *MIME* types. Most browsers have a mechanic called *MIME-sniffing* to determine what MIME type the received resource is in. This functionality is used for backwards compatibility with for example legacy servers that serve all content with the *text/plain* content type. MIME-Sniffing can determine that received data is in a different data type than specified and display it in the determined way. This would for instance render a HTML document that is send with the *text/plain* content-type if the text contains HTML elements (Lawrence 2008a).

The feature has however introduced some security concerns for content hosts. Attackers could create content like images that contain HTML text with scrips. The sniffing functionality could then falsely determine during the inspection that the received resource is a HTML document and then execute the contained script instead of showing an image (Lawrence 2008a). This lead to the introduction of the *X-Content-Type-Options* field that can be used to prevent such content sniffing (Lawrence 2008b).

The header can only be set to *nosniff* which disables the sniffing feature. It is supported by all major browsers (Bengtsson and et al. 2021).

#### 4.3.1 Importance for Clippy's lint list

This field can actually be of high importance to the project. Clippy like all Rust projects has a review policy that only allows the merge of changes if they have been reviewed by a project member. This type of attack especially focusses on hiding the malicious code inside an image, this could therefor also easily be overlooked during the review process. Additionally due to the fact that the project maintainers mainly focus on Rust and not the website.

This header requires that the *content-type* header is set correctly for content that is being delivered by the host. GitHub pages doesn't support the manual specification of the content type it instead uses a open

source database to determine the correct MIME type based on the file extension (GitHub Docs 2021a). Clippy's lint list is composed out of a *html* and a *json* which both are delivered with the correct content type as can be seen in attachment 2 and 3. The nosniff option can therefore be enabled without side effects.

## 5 Setting HTTP header fields

The analysis has shown that the aspects to improve can be split into two parts. First the addition of HTTP headers for security and secondly the optimization of the website content for faster loading times. These two will be investigated individually.

The measurement in chapter 4 has shown that three HTTP headers have not been set. The section 4 determined that they should be configured as defined in Table 2.

HTTP header field	Value	Reference
Strict-Transport-Security	max-age=63072000	See 4.1.3
X-Frame-Options	DENY	See 4.2
X-Content-Type-Options	nosniff	See 4.3

Table 2: Determined values for the investigated HTTP header fields

This chapter will investigate how these values can be set for Clippy's lint list.

### 5.1 GitHub Pages configuration

The GitHub Pages documentation does not contain any information if and how HTTP header can be set. There has been requests to support user defined HTTP headers in several places by the GitHub community. All of them have concluded with the answer that this is currently not possible (trante and et al. 2013, Laukenstein and Balter 2017, yawnoc and et al. 2021).

Searching in the documentation for the header functionality reveals that GitHub Pages provides an option called "Enforce HTTPS" (GitHub Docs 2021c). This option can be enabled for each hosted site, under the condition that the original `github.io` domain is used (GitHub Docs 2021c). Putting this setting to the test under a personal fork of the rust-clippy project reveals that the effect is limited. Requesting the project domain over HTTP results in a *301 Moved Permanently* responds that forwards the browser to the same domain using HTTPS. The Strict-Transport-Security header which could enforce this behavior by the client is not set. The responds for the test page is included in attachment 4. This forward message only works for the root project url, other resources and direct HTML pages can still be loaded without an encrypted connection. Clippy uses paths to display version specific documentation. This setting is therefore not helpful in enforcing HTTPS security for Clippy.

The GitHub Pages documentation currently does not contain any information regarding the other header options.

### 5.2 HTML meta tag

A discussion on the topic of setting HTTP header fields in GitHub Pages included suggestions to use a meta tag inside the main html file header (trante and et al. 2013). The meta tag is part of the living HTML standard defined by the *Web Hypertext Application Technology Working Group (WHATWG)*. It

can be used to add supplementary information for the client. The tag can contain a `http-equiv` attribute with a linked `content` attribute that can define values that would usually be set in the HTTP response header. The standard currently defines a set of fields that can be set with the meta attribute. The in focussed fields defined in Table 2 are not listed in the living standard (WHATWG 2021). However, clients can still deviate from this standard or support additional functionality that has not yet been specified.

Putting the meta tag to the test reveals that both Firefox and Chromium accept values for Strict-Transport-Security and X-Content-Type-Options. Assigning a value to X-Frame-Options produces a warning in the Chromium console with the message that this option is not supported and should be set as a HTTP header. After setting the meta tags both browsers take care to enforce HTTPS connections for all requested resources. Accessing a HTTP connection produces in both cases an error message indicating that mixed content is not allowed and the request has been blocked.

The meta tag can therefor be used to define Strict-Transport-Security and X-Content-Type-Options fields for individual websites and with that increase security. The max-time defined in the Strict-Transport-Security header also ensures that future accesses to the website will use HTTPS. This solution still has four drawbacks:

- The header to enforce HTTPS is only set during the loading of the page. An attacker could therefor still modify the page and remove the tag if they catch the initial request where HTTPS is not yet enforced.
- The meta tag to set these headers is not yet fully specified and can still change. The fact that Chromium and Firefox both accept these headers is an additional functionality.
- The X-Frame-Options header can not be set via a meta tag. This header is as discussed in 4.2 the least important for now but still relevant when it comes to the Mozilla Observatory rating.
- These meta tags are defined in HTML files, it will therefor not increase the Mozilla Observatory scoring and they have to be added to each project in each html file to ensure that they are enforces in the project.

### 5.3 Content Delivery Network

The Rust Infrastructure Team has noticed that some hosting providers have limitations when it comes to available configuration. The team has therefor setup a *CloudFront* account for rust projects (The Rust Infrastructure Team 2020). CloudFront is a *content delivery network (CDN)* provided by Amazon. It can be used to deliver content on a global scale by acting as an intermediary agent. Each content request is wired over the network, the network then saves the data in caches to speedup future access (Amazon Web Services 2021). Using a content delivery network enables the definition of custom behavior this can for example be used to define additional HTTP headers (The Rust Infrastructure Team 2020).

CloudFront is already used to provide the website for the Rust project *rustup* at *rustup.rs*<sup>5</sup>. That website archives the highest grade of A+ when evaluated with Mozilla Observatory. The rating is included in attachment number 5. However, the distribution over CloudFront requires the use of a domain as the direct access to GitHub Pages can not be intercepted via a CDN.

Using CloudFront, a different hosting or content provider would, as seen in the rustup website example,

---

<sup>5</sup><https://rustup.rs/>

improve the website rating to a possible grade of A+ if configured correctly. A valid configuration is also provided in the Rust development documentation (The Rust Infrastructure Team 2020). This is therefore a valid solution. However, using an additional new service like CloudFront would also add some additional complexity and use up resources of the Rust project in general. These are two disadvantages that have to be put into consideration when deciding for or against the usage.

## 6 Conclusion

### 6.1 Summary

This paper has summarized the technical requirements that the lint list of the rust-clippy project should fulfill in section 4. The main requirement put on the website is the goal of achieving an A+ rating by the rating engine Mozilla Observatory.

The assignment then continued in section 4 with an evaluation to which extent the requirement is currently fulfilled. This evaluation is done by using the previously mentioned tool. The results reveal that the evaluation and user security is impacted by the three following missing HTTP headers:

- Strict-Transport-Security
- X-Frame-Options
- X-Content-Type-Options

The following section 4 analyzed the security concern of the missing headers by explaining their behavior and reasoning behind them. This explanation was based on the formal specification and most relevant documentation. The paper then discussed the importance for Clippy's lint list and suggested an initial value that the specific field should be set to. The results of this evaluation have been summarized in table 2.

The 5th chapter then investigated how these header values could be set for the website. This included an investigation which settings are provided by the used hosting provider GitHub Pages. This is followed by evaluating the HTML meta tag as the author was unable to find a solution using the hosting provider's settings. It was determined that the meta tag could be used to specify values for Strict-Transport-Security and X-Content-Type-Options in the Firefox and Chromium browser even if this behavior is not part of the living standard. The last solution looked at the possibility to use a content delivery network to set these headers. It was determined that this last solution would work but add complexity to the hosting process and consume some additional resources.

### 6.2 Steps moving forward

The section 5 has concluded that the missing headers can be set with the use of a content delivery network. The next step is now to investigate if the added complexity and additional use of resources this would take are worth it as the website is currently operating to no additional cost to the project. Especially due to the fact that GitHub Pages is still a recommended hosting provider by the Rust Infrastructure Team.

If the decision is made to continue the use and deployment using GitHub pages then it might be worth to investigate the html meta tag a bit more. The use of the meta tag can address the two main security concerns in regard of the Strict-Transport-Security and X-Content-Type-Options header fields. Before

using this feature it has to be investigated if this usage is supported by all major browsers as it's not part of the living standard of HTML.

## References

- Amazon Web Services (2021). *Amazon CloudFront*. URL: <https://aws.amazon.com/cloudfront/> (visited on 2021-05-01).
- Bengtsson, Peter and et al. (2021-03). *X-Content-Type-Options*. URL: <https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Content-Type-Options> (visited on 2021-04-26).
- GitHub Docs (2021a). *About GitHub Pages*. URL: <https://docs.github.com/en/pages/getting-started-with-github-pages/about-github-pages> (visited on 2021-05-02).
- (2021b). *GitHub’s products*. URL: <https://docs.github.com/en/github/getting-started-with-github/githubs-products> (visited on 2021-05-02).
  - (2021c). *Securing your GitHub Pages site with HTTPS*. URL: <https://docs.github.com/en/pages/getting-started-with-github-pages/securing-your-github-pages-site-with-https> (visited on 2021-04-30).
- Hoare, Graydon and et al. (2019-01). *COPYRIGHT*. URL: <https://github.com/rust-lang/rust/blob/master/COPYRIGHT> (visited on 2021-04-20).
- Hodges, Jeff and et al. (2012-11). *RFC6797: HTTP Strict Transport Security (HSTS)*. Tech. rep. Internet Engineering Task Force (IETF). URL: <https://tools.ietf.org/html/rfc6797> (visited on 2021-04-25).
- King, April (2018-07). *Web Security Cheat Sheet*. URL: [https://infosec.mozilla.org/guidelines/web\\_security](https://infosec.mozilla.org/guidelines/web_security) (visited on 2021-05-03).
- King, April and et al. (2018a-01). *HTTP Observatory Scoring Methodology*. URL: <https://github.com/mozilla/http-observatory/blob/fa38ab4/httpobs/docs/scoring.md> (visited on 2021-04-24).
- (2018b-03). *Mozilla HTTP Observatory*. URL: <https://github.com/mozilla/http-observatory/blob/1bb1566/README.md> (visited on 2021-04-24).
  - (2020-10). *Frequently Asked Questions*. URL: <https://observatory.mozilla.org/faq/> (visited on 2021-04-24).
- Laukenstein, Binyamin and Ben Balter (2017-02). *[Github Pages] Modify headers, respect \_config.yml webrick headers*. URL: <https://github.com/github/pages-gem/issues/415> (visited on 2021-04-30).
- Lawrence, Eric (2008a-02). *IE8 Security Part V: Comprehensive Protection*. URL: <https://docs.microsoft.com/en-us/archive/blogs/ie/ie8-security-part-v-comprehensive-protection> (visited on 2021-04-29).
- (2008b-02). *IE8 Security Part VI: Beta 2 Update*. URL: <https://docs.microsoft.com/en-us/archive/blogs/ie/ie8-security-part-vi-beta-2-update> (visited on 2021-04-29).
- Lusby, Jane (2018-07). *Add clippy to the tools list #1461*. URL: <https://github.com/rust-lang/rustup/pull/1461> (visited on 2021-04-17).
- Ross, David and Tobias Gondrom (2013-10). *RFC7034: HTTP Header Field X-Frame-Options*. Tech. rep. Internet Engineering Task Force (IETF). URL: <https://tools.ietf.org/html/rfc7034> (visited on 2021-04-25).
- Sommerville, Ian (2010). *Software Engineering*. 9th edition. 501 Boylston Street, Suite 900, Boston, Massachusetts 02116: Pearson Education, Inc. ISBN: 978-0-13-703515-1.
- The Rust Clippy Developers (2020-10). *deploy.yml*. URL: <https://github.com/rust-lang/rust-clippy/blob/master/.github/workflows/deploy.yml> (visited on 2021-04-17).

- The Rust Clippy Developers (2021-03). *Clippy*. URL: <https://github.com/rust-lang/rust-clippy/blob/7fcd1/README.md> (visited on 2021-04-17).
- The Rust Core Team (2015-05). *Announcing Rust 1.0*. URL: <https://blog.rust-lang.org/2015/05/15/Rust-1.0.html> (visited on 2021-04-17).
- (2021-03). *Announcing Rust 1.51.0*. URL: <https://blog.rust-lang.org/2021/03/25/Rust-1.51.0.html> (visited on 2021-04-17).
- The Rust Infrastructure Team (2020-03). *Rust Infrastructure hosting for static websites*. URL: <https://forge.rust-lang.org/infra/guidelines/static-websites.html> (visited on 2021-04-24).
- The Rust Team (2021a-04). *All-time Contributors*. URL: <https://thanks.rust-lang.org/rust/all-time/> (visited on 2021-04-20).
- (2021b). *Code of conduct*. URL: <https://www.rust-lang.org/policies/code-of-conduct> (visited on 2021-04-20).
- trante and et al. (2013-02). *Github pages, HTTP headers*. Last time updated on 2019-06-18. URL: <https://stackoverflow.com/questions/14798589/github-pages-http-headers> (visited on 2021-04-30).
- Turon, Aaron and Niko Matsakis (2014-10). *Stability as a Deliverable*. URL: <https://blog.rust-lang.org/2014/10/30/Stability.html> (visited on 2021-04-20).
- WHATWG (2021-04). *HTML Living Standard*. Tech. rep. Web Hypertext Application Technology Working Group (WHATWG). URL: <https://html.spec.whatwg.org/multipage/semantics.html> (visited on 2021-05-01).
- yawnoc and et al. (2021-04). [Feature request] *Set HTTP header to opt out of FLoC in GitHub Pages*. URL: <https://github.com/community/t/feature-request-set-http-header-to-opt-out-of-floc-in-github-pages/174978> (visited on 2021-04-30).



## 7 Attachments

```
1 {
2   "content—security—policy": {
3     "expectation": "csp—implemented—with—no—unsafe",
4     "name": "content—security—policy",
5     "output": {
6       "data": {
7         "connect—src": [
8           "'self'"
9         ],
10        "default—src": [
11          "'none'"
12        ],
13        "img—src": [
14          "data:"
15        ],
16        "style—src": [
17          "'unsafe—inline'"
18        ]
19      },
20      "http": true,
21      "meta": true,
22      "policy": {
23        "antiClickjacking": false,
24        "defaultNone": true,
25        "insecureBaseUri": true,
26        "insecureFormAction": true,
27        "insecureSchemeActive": false,
28        "insecureSchemePassive": false,
29        "strictDynamic": false,
30        "unsafeEval": false,
31        "unsafeInline": false,
32        "unsafeInlineStyle": true,
33        "unsafeObjects": false
34      }
35    },
36    "pass": true,
37    "result": "csp—implemented—with—unsafe—inline—in—style—src—only",
38    "score_description": "Content Security Policy (CSP) implemented with unsafe sources inside style—src. This includes 'unsafe—inline', data: or overly broad sources such as
39      ↪ https:.",
40    "score_modifier": 0
41  },
42  "contribute": {
43    "expectation": "contribute—json—only—required—on—mozilla—properties",
44    "name": "contribute",
45    "output": {
46      "data": null
47    },
48    "pass": true,
49    "result": "contribute—json—only—required—on—mozilla—properties",
50    "score_description": "Contribute.json isn't required on websites that don't belong to Mozilla",
51    "score_modifier": 0
52  },
53  "cookies": {
54    "expectation": "cookies—secure—with—httponly—sessions",
55    "name": "cookies",
56    "output": {
57      "data": null,
58      "sameSite": null
59    },
60    "pass": true,
61    "result": "cookies—not—found",
62    "score_description": "No cookies detected",
63    "score_modifier": 0
64  },
65  "cross—origin—resource—sharing": {
66    "expectation": "cross—origin—resource—sharing—not—implemented",
67    "name": "cross—origin—resource—sharing",
68    "output": {
69      "data": {
70        "acao": "*",
71        "clientaccesspolicy": null,
72        "crossdomain": null
73      }
74    },
75    "pass": true,
76    "result": "cross—origin—resource—sharing—implemented—with—public—access",
77    "score_description": "Public content is visible via cross—origin resource sharing (CORS) Access—Control—Allow—Origin header",
78    "score_modifier": 0
79  },
80  "public—key—pinning": {
81    "expectation": "hpkp—not—implemented",
```

```

81     "name": "public-key-pinning",
82     "output": {
83         "data": null,
84         "includeSubDomains": false,
85         "max-age": null,
86         "numPins": null,
87         "preloaded": false
88     },
89     "pass": true,
90     "result": "hpkp-not-implemented",
91     "score_description": "HTTP Public Key Pinning (HPKP) header not implemented",
92     "score_modifier": 0
93 },
94 "redirection": {
95     "expectation": "redirection-to-https",
96     "name": "redirection",
97     "output": {
98         "destination": null,
99         "redirects": true,
100         "route": [
101             "http://rust-lang.github.io/",
102             "https://rust-lang.github.io/"
103         ],
104         "status_code": null
105     },
106     "pass": true,
107     "result": "redirection-to-https",
108     "score_description": "Initial redirection is to HTTPS on same host, final destination is HTTPS",
109     "score_modifier": 0
110 },
111 "referrer-policy": {
112     "expectation": "referrer-policy-private",
113     "name": "referrer-policy",
114     "output": {
115         "data": null,
116         "http": false,
117         "meta": false
118     },
119     "pass": true,
120     "result": "referrer-policy-not-implemented",
121     "score_description": "Referrer-Policy header not implemented",
122     "score_modifier": 0
123 },
124 "strict-transport-security": {
125     "expectation": "hsts-implemented-max-age-at-least-six-months",
126     "name": "strict-transport-security",
127     "output": {
128         "data": null,
129         "includeSubDomains": false,
130         "max-age": null,
131         "preload": false,
132         "preloaded": false
133     },
134     "pass": false,
135     "result": "hsts-not-implemented",
136     "score_description": "HTTP Strict Transport Security (HSTS) header not implemented",
137     "score_modifier": -20
138 },
139 "subresource-integrity": {
140     "expectation": "sri-implemented-and-external-scripts-loaded-securely",
141     "name": "subresource-integrity",
142     "output": {
143         "data": {}
144     },
145     "pass": true,
146     "result": "sri-not-implemented-but-no-scripts-loaded",
147     "score_description": "Subresource Integrity (SRI) is not needed since site contains no script tags",
148     "score_modifier": 0
149 },
150 "x-content-type-options": {
151     "expectation": "x-content-type-options-nosniff",
152     "name": "x-content-type-options",
153     "output": {
154         "data": null
155     },
156     "pass": false,
157     "result": "x-content-type-options-not-implemented",
158     "score_description": "X-Content-Type-Options header not implemented",
159     "score_modifier": -5
160 },
161 "x-frame-options": {
162     "expectation": "x-frame-options-sameorigin-or-deny",
163     "name": "x-frame-options",

```

```

164     "output": {
165         "data": null
166     },
167     "pass": false,
168     "result": "x-frame-options-not-implemented",
169     "score_description": "X-Frame-Options (XFO) header not implemented",
170     "score_modifier": -20
171 },
172 "x-xss-protection": {
173     "expectation": "x-xss-protection-1-mode-block",
174     "name": "x-xss-protection",
175     "output": {
176         "data": null
177     },
178     "pass": true,
179     "result": "x-xss-protection-not-needed-due-to-csp",
180     "score_description": "X-XSS-Protection header not needed due to strong Content Security Policy (CSP) header",
181     "score_modifier": 0
182 }
183 }

```

Attachment 1: Mozilla Observatory output for `rust-lang.github.io` from 2021-04-24

```
1 HTTP/1.1 200 OK
2 Date: Fri, 30 Apr 2021 19:08:24 GMT
3 Via: 1.1 varnish
4 Cache-Control: max-age=600
5 Expires: Fri, 30 Apr 2021 19:18:25 GMT
6 Age: 0
7 X-Served-By: cache-fra19138-FRA
8 X-Cache: MISS
9 X-Cache-Hits: 0
10 X-Timer: S1619809705.954395,VS0,VE90
11 Vary: Accept-Encoding
12 X-Fastly-Request-ID: 941e117097d3830dfbc28eda40096862241b1bcc
13 Server: GitHub.com
14 Content-Type: text/html; charset=utf-8
15 permissions-policy: interest-cohort=()
16 Last-Modified: Mon, 26 Apr 2021 21:40:11 GMT
17 Access-Control-Allow-Origin: *
18 ETag: W/"6087333b-4a05"
19 Content-Encoding: gzip
20 x-proxy-cache: MISS
21 X-GitHub-Request-Id: CB52:4B29:333A3A:3A24C8:608C3FC5
22 Content-Length: 4722
23 Accept-Ranges: bytes
```

Attachment 2: The HTTP response header for <https://rust-lang.github.io/rust-clippy/master/index.html> from 2021-04-30

```
1 HTTP/1.1 200 OK
2 Date: Fri, 30 Apr 2021 19:08:25 GMT
3 Via: 1.1 varnish
4 Cache-Control: max-age=600
5 Expires: Fri, 30 Apr 2021 19:18:25 GMT
6 Age: 0
7 X-Served-By: cache-fra19138-FRA
8 X-Cache: MISS
9 X-Cache-Hits: 0
10 X-Timer: S1619809705.316870,VS0,VE94
11 Vary: Accept-Encoding
12 X-Fastly-Request-ID: 30deedad3daffa933d4f55f7174a69c2fd13ffa3
13 Server: GitHub.com
14 Content-Type: application/json; charset=utf-8
15 permissions-policy: interest-cohort=()
16 Last-Modified: Mon, 26 Apr 2021 21:40:11 GMT
17 Access-Control-Allow-Origin: *
18 ETag: W/"6087333b-4ec5f"
19 Content-Encoding: gzip
20 x-proxy-cache: MISS
21 X-GitHub-Request-Id: 98EA:29DE:BE987C:C3D1A8:608C3FC5
22 Content-Length: 80925
23 Accept-Ranges: bytes
```

Attachment 3: The HTTP response header for <https://rust-lang.github.io/rust-clippy/master/lints.json> from 2021-04-30

```
1 HTTP/1.1 301 Moved Permanently
2 Server: GitHub.com
3 Content-Type: text/html
4 permissions-policy: interest-cohort=()
5 Location: https://xfrednet.github.io/rust-clippy/
6 X-GitHub-Request-Id: 3620:3A01:104182F:110536D:608C3D70
7 Content-Length: 162
8 Accept-Ranges: bytes
9 Date: Fri, 30 Apr 2021 17:25:04 GMT
10 Via: 1.1 varnish
11 Age: 0
12 X-Served-By: cache-fra19120-FRA
13 X-Cache: MISS
14 X-Cache-Hits: 0
15 X-Timer: S1619803505.769013,VS0,VE87
16 Vary: Accept-Encoding
17 X-Fastly-Request-ID: b837829c5922d053b087ff1e129d92f5b470a120
```

Attachment 4: The HTTP response for the test page with *enfore HTTPS* enabled from 2021-04-30

```
1 {
2   "content-security-policy": {
3     "expectation": "csp-implemented-with-no-unsafe",
4     "name": "content-security-policy",
5     "output": {
6       "data": {
7         "default-src": [
8           "none"
9         ],
10        "font-src": [
11          "self"
12        ],
13        "img-src": [
14          "self",
15          "https://www.rust-lang.org"
16        ],
17        "script-src": [
18          "self"
19        ],
20        "style-src": [
21          "self"
22        ]
23      },
24      "http": true,
25      "meta": false,
26      "policy": {
27        "antiClickjacking": false,
28        "defaultNone": true,
29        "insecureBaseUri": true,
30        "insecureFormAction": true,
31        "insecureSchemeActive": false,
32        "insecureSchemePassive": false,
33        "strictDynamic": false,
34        "unsafeEval": false,
35        "unsafeInline": false,
36        "unsafeInlineStyle": false,
37        "unsafeObjects": false
38      }
39    },
40    "pass": true,
41    "result": "csp-implemented-with-no-unsafe-default-src-none",
42    "score_description": "Content Security Policy (CSP) implemented with default-src 'none' and no 'unsafe'",
43    "score_modifier": 10
44  },
45  "contribute": {
46    "expectation": "contribute-json-only-required-on-mozilla-properties",
47    "name": "contribute",
48    "output": {
49      "data": null
50    },
51    "pass": true,
52    "result": "contribute-json-only-required-on-mozilla-properties",
53    "score_description": "Contribute.json isn't required on websites that don't belong to Mozilla",
54    "score_modifier": 0
55  },
56 }
```

```

56     "cookies": {
57         "expectation": "cookies—secure—with—httponly—sessions",
58         "name": "cookies",
59         "output": {
60             "data": null,
61             "sameSite": null
62         },
63         "pass": true,
64         "result": "cookies—not—found",
65         "score_description": "No cookies detected",
66         "score_modifier": 0
67     },
68     "cross—origin—resource—sharing": {
69         "expectation": "cross—origin—resource—sharing—not—implemented",
70         "name": "cross—origin—resource—sharing",
71         "output": {
72             "data": {
73                 "acao": null,
74                 "clientaccesspolicy": null,
75                 "crossdomain": null
76             }
77         },
78         "pass": true,
79         "result": "cross—origin—resource—sharing—not—implemented",
80         "score_description": "Content is not visible via cross—origin resource sharing (CORS) files or headers",
81         "score_modifier": 0
82     },
83     "public—key—pinning": {
84         "expectation": "hpkp—not—implemented",
85         "name": "public—key—pinning",
86         "output": {
87             "data": null,
88             "includeSubDomains": false,
89             "max—age": null,
90             "numPins": null,
91             "preloaded": false
92         },
93         "pass": true,
94         "result": "hpkp—not—implemented",
95         "score_description": "HTTP Public Key Pinning (HPKP) header not implemented",
96         "score_modifier": 0
97     },
98     "redirection": {
99         "expectation": "redirection—to—https",
100         "name": "redirection",
101         "output": {
102             "destination": "https://rustup.rs/",
103             "redirects": true,
104             "route": [
105                 "http://rustup.rs/",
106                 "https://rustup.rs/"
107             ],
108             "status_code": 200
109         },
110         "pass": true,
111         "result": "redirection—to—https",
112         "score_description": "Initial redirection is to HTTPS on same host, final destination is HTTPS",
113         "score_modifier": 0
114     },
115     "referrer—policy": {
116         "expectation": "referrer—policy—private",
117         "name": "referrer—policy",
118         "output": {
119             "data": "no—referrer, strict—origin—when—cross—origin",
120             "http": true,
121             "meta": false
122         },
123         "pass": true,
124         "result": "referrer—policy—private",
125         "score_description": "Referrer—Policy header set to \"no—referrer\", \"same—origin\", \"strict—origin\" or \"strict—origin—when—cross—origin\"",
126         "score_modifier": 5
127     },
128     "strict—transport—security": {
129         "expectation": "hsts—implemented—max—age—at—least—six—months",
130         "name": "strict—transport—security",
131         "output": {
132             "data": "max—age=63072000; includeSubDomains",
133             "includeSubDomains": true,
134             "max—age": 63072000,
135             "preload": false,
136             "preloaded": false
137         },
138         "pass": true,

```

```

139     "result": "hsts-implemented-max-age-at-least-six-months",
140     "score_description": "HTTP Strict Transport Security (HSTS) header set to a minimum of six months (15768000)",
141     "score_modifier": 0
142 },
143 "subresource-integrity": {
144     "expectation": "sri-implemented-and-external-scripts-loaded-securely",
145     "name": "subresource-integrity",
146     "output": {
147         "data": {}
148     },
149     "pass": true,
150     "result": "sri-not-implemented-but-all-scripts-loaded-from-secure-origin",
151     "score_description": "Subresource Integrity (SRI) not implemented, but all scripts are loaded from a similar origin",
152     "score_modifier": 0
153 },
154 "x-content-type-options": {
155     "expectation": "x-content-type-options-nosniff",
156     "name": "x-content-type-options",
157     "output": {
158         "data": "nosniff"
159     },
160     "pass": true,
161     "result": "x-content-type-options-nosniff",
162     "score_description": "X-Content-Type-Options header set to \"nosniff\"",
163     "score_modifier": 0
164 },
165 "x-frame-options": {
166     "expectation": "x-frame-options-sameorigin-or-deny",
167     "name": "x-frame-options",
168     "output": {
169         "data": "DENY"
170     },
171     "pass": true,
172     "result": "x-frame-options-sameorigin-or-deny",
173     "score_description": "X-Frame-Options (XFO) header set to SAMEORIGIN or DENY",
174     "score_modifier": 0
175 },
176 "x-xss-protection": {
177     "expectation": "x-xss-protection-1-mode-block",
178     "name": "x-xss-protection",
179     "output": {
180         "data": "1; mode=block"
181     },
182     "pass": true,
183     "result": "x-xss-protection-enabled-mode-block",
184     "score_description": "X-XSS-Protection header set to \"1; mode=block\"",
185     "score_modifier": 0
186 }
187 }

```

Attachment 5: Mozilla Observatory output for rustup.rs from 2021-05-01