Contents

List of Figures

List of Tables

Attachments

1 Introduction

Rust is a programming language that focusses on performance, security an 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 contributes 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 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 securely and functionality. The *Rust Infrastructure Team*, a team inside the project with members that organize and manage the entire infrastructure, has therefor defined some guidelines for static websites (The Rust Infrastructure team 2020). Clippy's lint list is static and should therefor 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: *How can the internet presentation of the lint list for the rust-clippy project 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

2.1 Hosting

2.2 Requirements

The goal of this work is to improve the impression of Clippy's lint list. This section of the document will set a list of requirements to focus on in further research for this paper. Requirements are usually split up into the following two groups (Sommerville 2010, p. 83ff):

- *Functional requirements* describe direct functionality and behavior that a system should provide. They can also be defined as negations, stating that a certain behavior should not happen. These requirements are usually documented in an abstract way to enable system users to understand them.
- *Non-functional requirements* are focussed on the characteristics of the system itself, an example might be the requirement to have a reliable and maintainable system. These requirements can include constraints that the system might have to take care of.

2.2.1 Implemented functionality

The topic of this assignment focusses on the perception and impression of Clippy's lint list as an entire system. The research question therefor puts a focus on non-functional requirements. The website itself is based on functional requirements and these should remain fulfilled even after the suggested changes. It

is therefor important to note them in some way or form while not taking focus of the key point of this paper. All requirements that have been implemented previously will therefor be summarized in the following functional requirement: *The functionality of the website should not be impacted by the implementation of new measures to improve the impression or usage.* This requirement covers functionality like the search feature, filter options and theming. The implementation of all of these has been completed at the point of writing this. A more extensive specification of the underlying requirements can be retrieved from the rust-clippy issue tracker.

2.2.2 Non-functional requirements (Maybe: Requirements by the Infra team)

The Rust Infrastructure team has created a set of guidelines that static websites affiliated with the Rust project should fulfill. Clippy is an official Rust project and the website itself presents static content, the guidelines therefor apply to the website.

These guidelines contain a *formal specification* that states: *"The website must reach an A+ grade on the Mozilla Observatory."* (The Rust Infrastructure team 2020). This specification is based on the requirement of security. The A+ grade ensures that all important headers have been set and that enhanced users privacy features should be enabled by the browser (The Rust Infrastructure team 2020). A secure website contributes to a trustful relation ship between the user and Clippy's lint list. It additionally improves the ranking in most search engines and therefor helps users to faster find the documentation they require.

The guidelines from the infrastructure team additionally contain some functional requirements that are not directly connected to the research question, they are also already fulfilled by the current setup. These are therefor included in the defined functional requirement.

3 Fulfillment of requirements

This chapter will measure the current fulfillment for the previously in 2.2 defined requirements. These results will then be used to identify the key aspects that need improvement. Additionally they will be used for comparison when testing suggestions.

3.1 Mozilla Observatory

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). These security is focussed on values that can be set in the HTTP header to indicate that opt-in security options should be enabled by the browser (**TODO**). The Rust development documentation links to a free online interface[1] for the Mozilla Observatory that is provided by the Mozilla Foundation free of charge.

3.1.1 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 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

[1] <https://observatory.mozilla.org/>

of 135, the score of 100 already indicates that the website is configured correctly a higher score can be archived by archiving bonuses. 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).

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 host itself. The results are therefor for *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.

3.3 Summary

There are missing headers!

4 Analysis of benchmark results

This chapter will inspect each identified technical problem from section 3. The inspection will first explain the technical background behind the problem and then identify the optimal configuration.

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 repositories by the *Rust Organization*. Further investigation will continue to focus on the context of Clippy's lint list however improvements to the server would directly improve other websites.

- TODO xFrednet 2021-04-29: Move section about clippy hosting to specification
- TODO xFrednet 2021-04-29: HTTP explanation/into header stuff

4.1 HTTP Strict-Transport-Security (HSTS)

HTTP Strict Transport Security (HSTS) is a optional HTTP header field that requests the client accessing the HTTP API to only use encrypted connection for further requests. The request to use and encrypted connection extends to all resources that are referenced by the requested result. It is therefor necessary that these resources also provide the option to connect via HTTPS (Hodges and et al. 2012, p. 6ff).

4.1.1 Risks

The specification references three threads that can be prevented using this header (Hodges and et al. 2012, p. 6ff):

1. Using an unencryped connection allows attackers to eavesdrop on the exchanged data. This is a *passive network attack* and can be used to collect personal information, passwords or browsing habits.
2. A HTTPS connection requires a certificate that has to be signed by a certification authority. This certificate intern lists the owner or organization. This can be used to validate that the displayed content really originates from the expected source and with that prevent attackers from creating a fake website copy to steal otherwise secure information.
3. Forcing the use of HTTPS additionally ensures that mistakes like referencing ressources via HTTP links will be corrected by the requesting client

4.1.2 Importance for Clippy

Clippy's lint 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 of personal information about the user. Except the fact that they visited the domain at all. However, this would however also be possible with the header as the connected IP is not effected by it. This also extends to the third thread of accidentally not requesting unencrypted resources, this can currently still happen but would not be detrimental.

The second thread of modification of the website is the relevant thread in this case. An attacker could for instance inject a donation button as several developers have expressed interest to donate to the Rust Foundation itself. This button would then forward the user to another page of the attacker to donate.

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.

4.2 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 withe the correct content type as can be seen in attachment 2 and 3. The nosniff option can therefor 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 3 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
`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 GutHub Pages provides an option called "Enforce HTTPS" (GitHub Docs 2021b). This option can be enabled for each hosted site, under the condition that the original `github.io` domain is used (GitHub Docs 2021b). 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 therefor not helpful in enforcing HTTPS security for Clippy.

The GutHub 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 GutHub 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[2]. That website

[2] `<https://rustup.rs/>`

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, 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 therefor 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 as summarized the technical requirements that the lint list of the rust-clippy project should fulfill in section 2.2. The main requirement put on the website is the goal of archiving A+ rating by the rating engine Mozilla Observatory.

The assignment then continued in section 3 with an evaluation to which extend 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 than discussed the importance for Clippy's lint list and suggested a initial value that the specific field should be set to. The results of this evaluation have been summarized in table 2.

The 5 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 providers 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 the Strict-Transport-Security and X-Content-Type-Options header fields. Before using this feature it haas 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#mime-types-on-github-pages (visited on 2021-04-30).

– (2021b). *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 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 (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).

The Rust Core Team (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.community/t/feature-request-set-http-header-to-opt-out-of-floc-in-github-pages/174978 (visited on 2021-04-30).

7 Attachments


```
{
    "content-security-policy": {
        "expectation": "csp-implemented-with-no-unsafe",
        "name": "content-security-policy",
        "output": {
            "data": {
                "connect-src": [
                    "'self'"
                ],
                "default-src": [
                    "'none'"
                ],
                "img-src": [
                    "data:"
                ],
                "style-src": [
                    "'unsafe-inline'"
                ]
            },
            "http": true,
            "meta": true,
            "policy": {
                "antiClickjacking": false,
                "defaultNone": true,
                "insecureBaseUri": true,
                "insecureFormAction": true,
                "insecureSchemeActive": false,
                "insecureSchemePassive": false,
                "strictDynamic": false,
                "unsafeEval": false,
                "unsafeInline": false,
                "unsafeInlineStyle": true,
                "unsafeObjects": false
            }
        },
        "pass": true,
        "result": "csp-implemented-with-unsafe-inline-in-style-src-only",
        "score_description": "Content Security Policy (CSP) implemented with unsafe sources inside style-src. This includes 'unsafe-inline', data: or overly broad sources such as https:.",
        "score_modifier": 0
    },
    "contribute": {
        "expectation": "contribute-json-only-required-on-mozilla-properties",
        "name": "contribute",
        "output": {
            "data": null
        },
        "pass": true,
        "result": "contribute-json-only-required-on-mozilla-properties",
        "score_description": "Contribute.json isn't required on websites that don't belong to Mozilla",
        "score_modifier": 0
    },
    "cookies": {
        "expectation": "cookies-secure-with-httponly-sessions",
        "name": "cookies",
        "output": {
            "data": null,
            "sameSite": null
        },
        "pass": true,
        "result": "cookies-not-found",
        "score_description": "No cookies detected",
        "score_modifier": 0
    },
    "cross-origin-resource-sharing": {
        "expectation": "cross-origin-resource-sharing-not-implemented",
        "name": "cross-origin-resource-sharing",
        "output": {
            "data": {
                "acao": "*",
                "clientaccesspolicy": null,
                "crossdomain": null
            }
        },
        "pass": true,
        "result": "cross-origin-resource-sharing-implemented-with-public-access",
        "score_description": "Public content is visible via cross-origin resource sharing (CORS) Access-Control-Allow-Origin header",
        "score_modifier": 0
    },
    "public-key-pinning": {
        "expectation": "hpkp-not-implemented",
```

```
        "name": "public-key-pinning",
        "output": {
            "data": null,
            "includeSubDomains": false,
            "max-age": null,
            "numPins": null,
            "preloaded": false
        },
        "pass": true,
        "result": "hpkp-not-implemented",
        "score_description": "HTTP Public Key Pinning (HPKP) header not implemented",
        "score_modifier": 0
    },
    "redirection": {
        "expectation": "redirection-to-https",
        "name": "redirection",
        "output": {
            "destination": null,
            "redirects": true,
            "route": [
                "http://rust-lang.github.io/",
                "https://rust-lang.github.io/"
            ],
            "status_code": null
        },
        "pass": true,
        "result": "redirection-to-https",
        "score_description": "Initial redirection is to HTTPS on same host, final destination is HTTPS",
        "score_modifier": 0
    },
    "referrer-policy": {
        "expectation": "referrer-policy-private",
        "name": "referrer-policy",
        "output": {
            "data": null,
            "http": false,
            "meta": false
        },
        "pass": true,
        "result": "referrer-policy-not-implemented",
        "score_description": "Referrer-Policy header not implemented",
        "score_modifier": 0
    },
    "strict-transport-security": {
        "expectation": "hsts-implemented-max-age-at-least-six-months",
        "name": "strict-transport-security",
        "output": {
            "data": null,
            "includeSubDomains": false,
            "max-age": null,
            "preload": false,
            "preloaded": false
        },
        "pass": false,
        "result": "hsts-not-implemented",
        "score_description": "HTTP Strict Transport Security (HSTS) header not implemented",
        "score_modifier": -20
    },
    "subresource-integrity": {
        "expectation": "sri-implemented-and-external-scripts-loaded-securely",
        "name": "subresource-integrity",
        "output": {
            "data": {}
        },
        "pass": true,
        "result": "sri-not-implemented-but-no-scripts-loaded",
        "score_description": "Subresource Integrity (SRI) is not needed since site contains no script tags",
        "score_modifier": 0
    },
    "x-content-type-options": {
        "expectation": "x-content-type-options-nosniff",
        "name": "x-content-type-options",
        "output": {
            "data": null
        },
        "pass": false,
        "result": "x-content-type-options-not-implemented",
        "score_description": "X-Content-Type-Options header not implemented",
        "score_modifier": -5
    },
    "x-frame-options": {
        "expectation": "x-frame-options-sameorigin-or-deny",
        "name": "x-frame-options",
```

```
        "output": {
            "data": null
        },
        "pass": false,
        "result": "x-frame-options-not-implemented",
        "score_description": "X-Frame-Options (XFO) header not implemented",
        "score_modifier": -20
    },
    "x-xss-protection": {
        "expectation": "x-xss-protection-1-mode-block",
        "name": "x-xss-protection",
        "output": {
            "data": null
        },
        "pass": true,
        "result": "x-xss-protection-not-needed-due-to-csp",
        "score_description": "X-XSS-Protection header not needed due to strong Content Security Policy (CSP) header",
        "score_modifier": 0
    }
}
```


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

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

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


```
{
    "content-security-policy": {
        "expectation": "csp-implemented-with-no-unsafe",
        "name": "content-security-policy",
        "output": {
            "data": {
                "default-src": [
                    "'none'"
                ],
                "font-src": [
                    "'self'"
                ],
                "img-src": [
                    "'self'",
                    "https://www.rust-lang.org"
                ],
                "script-src": [
                    "'self'"
                ],
                "style-src": [
                    "'self'"
                ]
            },
            "http": true,
            "meta": false,
            "policy": {
                "antiClickjacking": false,
                "defaultNone": true,
                "insecureBaseUri": true,
                "insecureFormAction": true,
                "insecureSchemeActive": false,
                "insecureSchemePassive": false,
                "strictDynamic": false,
                "unsafeEval": false,
                "unsafeInline": false,
                "unsafeInlineStyle": false,
                "unsafeObjects": false
            }
        },
        "pass": true,
        "result": "csp-implemented-with-no-unsafe-default-src-none",
        "score_description": "Content Security Policy (CSP) implemented with default-src 'none' and no 'unsafe'",
        "score_modifier": 10
    },
    "contribute": {
        "expectation": "contribute-json-only-required-on-mozilla-properties",
        "name": "contribute",
        "output": {
            "data": null
        },
        "pass": true,
        "result": "contribute-json-only-required-on-mozilla-properties",
        "score_description": "Contribute.json isn't required on websites that don't belong to Mozilla",
        "score_modifier": 0
    },
```

```
    "cookies": {
        "expectation": "cookies-secure-with-httponly-sessions",
        "name": "cookies",
        "output": {
            "data": null,
            "sameSite": null
        },
        "pass": true,
        "result": "cookies-not-found",
        "score_description": "No cookies detected",
        "score_modifier": 0
    },
    "cross-origin-resource-sharing": {
        "expectation": "cross-origin-resource-sharing-not-implemented",
        "name": "cross-origin-resource-sharing",
        "output": {
            "data": {
                "acao": null,
                "clientaccesspolicy": null,
                "crossdomain": null
            }
        },
        "pass": true,
        "result": "cross-origin-resource-sharing-not-implemented",
        "score_description": "Content is not visible via cross-origin resource sharing (CORS) files or headers",
        "score_modifier": 0
    },
    "public-key-pinning": {
        "expectation": "hpkp-not-implemented",
        "name": "public-key-pinning",
        "output": {
            "data": null,
            "includeSubDomains": false,
            "max-age": null,
            "numPins": null,
            "preloaded": false
        },
        "pass": true,
        "result": "hpkp-not-implemented",
        "score_description": "HTTP Public Key Pinning (HPKP) header not implemented",
        "score_modifier": 0
    },
    "redirection": {
        "expectation": "redirection-to-https",
        "name": "redirection",
        "output": {
            "destination": "https://rustup.rs/",
            "redirects": true,
            "route": [
                "http://rustup.rs/",
                "https://rustup.rs/"
            ],
            "status_code": 200
        },
        "pass": true,
        "result": "redirection-to-https",
        "score_description": "Initial redirection is to HTTPS on same host, final destination is HTTPS",
        "score_modifier": 0
    },
    "referrer-policy": {
        "expectation": "referrer-policy-private",
        "name": "referrer-policy",
        "output": {
            "data": "no-referrer, strict-origin-when-cross-origin",
            "http": true,
            "meta": false
        },
        "pass": true,
        "result": "referrer-policy-private",
        "score_description": "Referrer-Policy header set to \"no-referrer\", \"same-origin\", \"strict-origin\" or \"strict-origin-when-cross-origin\"",
        "score_modifier": 5
    },
    "strict-transport-security": {
        "expectation": "hsts-implemented-max-age-at-least-six-months",
        "name": "strict-transport-security",
        "output": {
            "data": "max-age=63072000; includeSubDomains",
            "includeSubDomains": true,
            "max-age": 63072000,
            "preload": false,
            "preloaded": false
        },
        "pass": true,
```

```
        "result": "hsts-implemented-max-age-at-least-six-months",
        "score_description": "HTTP Strict Transport Security (HSTS) header set to a minimum of six months (15768000)",
        "score_modifier": 0
    },
    "subresource-integrity": {
        "expectation": "sri-implemented-and-external-scripts-loaded-securely",
        "name": "subresource-integrity",
        "output": {
            "data": {}
        },
        "pass": true,
        "result": "sri-not-implemented-but-all-scripts-loaded-from-secure-origin",
        "score_description": "Subresource Integrity (SRI) not implemented, but all scripts are loaded from a similar origin",
        "score_modifier": 0
    },
    "x-content-type-options": {
        "expectation": "x-content-type-options-nosniff",
        "name": "x-content-type-options",
        "output": {
            "data": "nosniff"
        },
        "pass": true,
        "result": "x-content-type-options-nosniff",
        "score_description": "X-Content-Type-Options header set to \"nosniff\"",
        "score_modifier": 0
    },
    "x-frame-options": {
        "expectation": "x-frame-options-sameorigin-or-deny",
        "name": "x-frame-options",
        "output": {
            "data": "DENY"
        },
        "pass": true,
        "result": "x-frame-options-sameorigin-or-deny",
        "score_description": "X-Frame-Options (XFO) header set to SAMEORIGIN or DENY",
        "score_modifier": 0
    },
    "x-xss-protection": {
        "expectation": "x-xss-protection-1-mode-block",
        "name": "x-xss-protection",
        "output": {
            "data": "1; mode=block"
        },
        "pass": true,
        "result": "x-xss-protection-enabled-mode-block",
        "score_description": "X-XSS-Protection header set to \"1; mode=block\"",
        "score_modifier": 0
    }
}
```


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