Validate the SameSite cookie option #1051

New issue

Closed bobjflong wants to merge 3 commits into `rack:master` from `bobjflong:BL/validatesamesite`

Conversation 11 Commits 3 Checks 0 Files changed 2 +50 −9

bobjflong commented on 17 Apr 2016 — Contributor

The draft spec for the SameSite option mentions two configuration options: Strict & Lax. This commit introduces validation of the associated same_site attribute.

The main motivation for validating this value is ensuring that awry option values don't cause unexpected behaviour. As this is a sensitive security option, I think validation is warranted.

The main drawback of validating the option value is that Rack won't immediately support new options.

`Validate the SameSite cookie option` … 56d56bc

jeremy commented on 17 Apr 2016 — Member

👍 to validate the attribute value now that it's required by spec, too. This changed in draft 7. Draft 6 assumed Strict then downgraded to Lax; draft 7 treats the entire cookie as invalid and ignores it unless the attribute value is Strict or Lax.

Looks like this came up @ https://bugs.chromium.org/p/chromium/issues/detail?id=600983

/cc **@mastahyeti**

jeremy commented on 17 Apr 2016 — Member

Ref #1033

jeremy commented on 17 Apr 2016 — Member

Draft 7 is a little confusing now. It allows SameSite with no attribute value in 3.1 and says that cookies with an invalid SameSite value should be treated as Strict in 3.2, yet 4.1 makes it clear that User Agents must ignore cookies with a SameSite attribute whose value is not Strict or Lax.

3.1

> samesite-av = "SameSite" / "SameSite=" samesite-value

3.2

> If the "SameSite" attribute's value is "Strict", or if the value is invalid, the cookie will only be sent along with "same-site" requests.

4.1

> 1. If "cookie-av"'s "attribute-value" is not a case-sensitive match for "Strict" or "Lax", ignore the "cookie-av".

/cc **@mikewest**

jeremy reviewed on 17 Apr 2016 — View changes

`lib/rack/utils.rb` Outdated

```
255 +              unless ["Lax", "Strict"].include?(same_site_rule)
256 +                raise ArgumentError, "Unrecognized cookie header value for SameSite option: #{same_site_ru
257 +              end
258 +              "; SameSite=#{same_site_rule}"
255 259          else
256 260            "; SameSite"
257 261          end
```

jeremy on 17 Apr 2016 — Member

We can dial this back to a stricter whitelist now that the spec requires valid values, e.g.

```
same_site =
  case value[:same_site]
  when false, nil
    nil
  when :lax, 'Lax'
    '; SameSite=Lax'.freeze
  when true, :strict, 'Strict'
    '; SameSite=Strict'.freeze
  else
    raise ArgumentError, "Invalid SameSite value: #{value[:same_site].inspect}"
  end
```

bobjflong on 17 Apr 2016 — Author Contributor

cool 👍 added the uppercase symbols too

`simpler whitelist for SameSite options` fc96b0a

jeremy reviewed on 17 Apr 2016 — View changes

`test/spec_response.rb` Outdated

```
120 -    response.set_cookie "foo", {:value => "bar", :same_site => Object.new}
121 -    response["Set-Cookie"].must_equal "foo=bar; SameSite"
122 -  end
123 -
124 118    it "can set SameSite cookies with string value" do
125 119      response = Rack::Response.new
126 120      response.set_cookie "foo", {:value => "bar", :same_site => "Lax"}
```

jeremy on 17 Apr 2016 — Member

Let's add specific test coverage for the allowed values, too.

bobjflong on 17 Apr 2016 — Author Contributor

done!

bobjflong force-pushed the `bobjflong:BL/validatesamesite` branch from `591eeb8` to `56f4016` on 17 Apr 2016

`spec coverage for all allowed SameSite options` 8a14474

bobjflong force-pushed the `bobjflong:BL/validatesamesite` branch from `56f4016` to `8a14474` on 17 Apr 2016

mikewest mentioned this pull request on 17 Apr 2016

3.1 and 3.2 disagree with 4.1 mikewest/internetdrafts#11 — Closed

mikewest commented on 17 Apr 2016

@jeremy: Thanks! Looks like it's time for an -08 draft. :)

The text in 4.1 is what I intended throughout, and matches Chrome's behavior in 51: `SameSite` and `SameSite=Blah` both cause the cookie to be ignored (which gives us some options for extensibility in the future, and feature-detection in the present). I'll adjust the document accordingly in mikewest/internetdrafts#11.

👍 1

jeremy commented on 18 Apr 2016 — Member

Merged @ `f0f828c`. Thanks **@bobjflong**!

jeremy closed this on 18 Apr 2016

reedloden commented on 18 Apr 2016 • edited

Could we get a new `rack` release that includes `SameSite` support? :)

Also, doesn't this need to be backported to `1-6-stable` (as per #1037)?

👍 1

jeremy commented on 18 Apr 2016 — Member

Backported @ `6712b86`

bobjflong mentioned this pull request on 2 May 2016

Add laxSameSiteSessions and strictSameSiteSessions yesodweb/yesod#1226 — Merged

jeremy mentioned this pull request on 1 Nov 2018

Add SameSite to Cookies rails/rails#28297 — Closed

ashawley mentioned this pull request on 4 Feb

Add support for SameSite cookie to 1.4.7 #1547 — Closed

Reviewers: No reviews

Assignees: No one assigned

Labels: None yet

Projects: None yet

Milestone: No milestone

Linked issues: Successfully merging this pull request may close these issues. None yet

4 participants