Package: agris (via r-universe)

March 13, 2025

Title Security for 'Ambiorix' Applications

Version 0.0.1.9000

Description Security middlewares for ` `Ambiorix" applications.

License GPL (>= 2)

Encoding UTF-8

Roxygen list(markdown = TRUE)

RoxygenNote 7.1.2

Depends R (>= 4.1.0)

Imports ambiorix (>= 1.0.2)

Config/pak/sysreqs make libssl-dev zlib1g-dev

Repository https://ambiorix-web.r-universe.dev

RemoteUrl https://github.com/ambiorix-web/agris

RemoteRef HEAD

RemoteSha 66c1d50d4febae359bbf73c5be83e261945ac677

Contents

`agris` *Agris Middlewares*

Description

Uses all agris middlewares.

Usage

```
agris()
```

Middlewares

- `use_content_security_policy()`
- `use_cross_origin_embedder_policy()`
- `use_cross_origin_opener_policy()`
- `use_cross_origin_resource_policy()`
- `use_dns_prefetch_control()`
- `use_frame_options()`
- `use_hide_powered_by()`
- `use_content_type_options()`
- `use_xss_protection()`
- `use_download_options()`
- `use_strict_transport_security()`
- `use_origin_agent_cluster()`
- `use_permitted_cross_domain_policies()`

`use_content_security_policy` *Use Content Security Policy*

Description

Adds relevant Content-Security-Policy headers.

Usage

```
use_content_security_policy()
```

Directives

- base-uri 'self';
- block-all-mixed-content;
- font-src 'self' https: data:;
- form-action 'self';
- frame-ancestors 'self';
- img-src 'self' data:;
- object-src 'none';
- style-src 'self' https: 'unsafe-inline';
- upgrade-insecure-requests

---

use_content_type_options

Content Type Options

Description

Sets the `X-Content-Type-Options` to `nosniff` (default).

Usage

```
use_content_type_options(value = "nosniff")
```

Arguments

`value`	Value to set.

---

use_cross_origin_embedder_policy

Cross Origin Embedder Policy

Description

Sets the `Cross-Origin-Embedder-Policy` to `require-corp` (default), so the document can only load resources from the same origin, or resources explicitly marked as loadable from another origin.

Usage

```
use_cross_origin_embedder_policy(policy = c("require-corp", "unsafe-none"))
```

Arguments

`policy`	Policy to set.

use_cross_origin_opener_policy *Cross Origin Opener Policy*

Description

Sets the `Cross-Origin-Opener-Policy` to `same-origin` (default).

Usage

```
use_cross_origin_opener_policy(
  policy = c("same-origin", "same-origin-allow-popups", "unsafe-nonce")
)
```

Arguments

`policy`	Policy to set.

use_cross_origin_resource_policy *Cross Origin Resource Policy*

Description

Sets the `Cross-Origin-Resource-Policy` to `same-origin` (default).

Usage

```
use_cross_origin_resource_policy(
  policy = c("same-origin", "same-site", "cross-origin")
)
```

Arguments

`policy`	Policy to set.

use_dns_prefetch_control *DNS Prefetch Control*

Description

Sets the `X-DNS-Prefetch-Control` header to on (default).

Usage

```
use_dns_prefetch_control(policy = c("on", "off"))
```

Arguments

`policy`	Policy to set.

use_download_options *Download Options*

Description

Sets to the `X-Download-Options` header to `noopen`, this is IE specific.

Usage

```
use_download_options()
```

use_frame_options *Frame Options*

Description

Sets `X-Frame-Options` header to `DENY` (default).

Usage

```
use_frame_options(policy = c("DENY", "SAMEORIGIN"))
```

Arguments

`policy`	Policy to set.

use_hide_powered_by *Powered By*

Description

Hides the `X-Powered-By` header. Someone may want to exploit vulnerabilities of R or ambiorix, hiding this provides less information to those people.

Usage

```
use_hide_powered_by(value = NA)
```

Arguments

`value`	Value to set the header to.

use_origin_agent_cluster *Origin Agent Cluster*

Description

Sets the `Origin-Agent-Cluster` to `true`. Mechanism to allow web applications to isolate their origins.

Usage

```
use_origin_agent_cluster(value = "?1")
```

Arguments

`value`	Value to set.

use_permitted_cross_domain_policies *Permitted Cross Domain Policies*

Description

Sets the `X-Permitted-Cross-Domain-Policies` header to `none`. Tells some clients (mostly Adobe products) your domain's policy for loading cross-domain content.

Usage

```
use_permitted_cross_domain_policies(
  policy = c("none", "master-only", "by-content-type", "all")
)
```

Arguments

`policy`	Policy to set.

use_referrer_policy *Referrer Policy*

Description

Sets the `Referrer-Policy` header to `no-referrer` (default). Controls how much referrer information (sent with the Referer header) should be included with requests.

Usage

```
use_referrer_policy(
  policy = c("no-referrer", "no-referrer-when-downgrade", "origin",
    "origin-when-cross-origin", "same-origin", "strict-origin",
    "strict-origin-when-cross-origin", "unsafe-url")
)
```

Arguments

`policy`	Policy to set.

use_strict_transport_security *Strict Transport Security*

Description

Sets the `Strict-Transport-Security` header, which nforms browsers that the site should only be accessed using HTTPS, and that any future attempts to access it using HTTP should automatically be converted to HTTPS.

Usage

```
use_strict_transport_security(
  max_age = 15552000,
  include_subdomains = FALSE,
  preload = FALSE
)
```

Arguments

`max_age`	The time, in seconds, that the browser should remember that a site is only to be accessed using HTTPS. Defaults to 6 months.
`include_subdomains`	Whether to apply this rule applies to all of the site's subdomains as well.
`preload`	Not part of specs, see MDN

use_xss_protection *XSS Protection*

Description

Sets the `X-XSS-Protection` header to `1; mode=block` to enable XSS filtering and rather than sanitizing the page, the browser will prevent rendering of the page if an attack is detected.

Usage

```
use_xss_protection(policy = "1; mode=block")
```

Arguments

`policy`	Policy to set.

Index