Server Header Module Architecture

Integration Points

ⓒ HttpCodes
- …
- ○ ok(content, headers): Response
- ○ created(content, headers): Response

ⓒ BoilerplateResponses
- □ server_headers: ServerHeaders
- ○ success_response(): Response
- ○ error_response(): Response

ⓒ RuntimeManager
- ○ get(ServerHeaders): ServerHeaders
- ○ set(ServerHeaders, **kwargs): None

uses headers *depends on* *manages instance*

Server Header Module

ⓒ *«Final»* **ServerHeaders**
- □ disp: Disp
- □ host: str
- □ port: int
- □ app_name: str
- □ error: int
- □ success: int
- □ debug: bool

- ○ __init__(host, port, app_name, error, success, debug)

- □ _get_app_name_str(): str
- □ _base_security_headers(): Dict[str, str]

- ○ for_json(): Dict[str, str]
- ○ for_text(): Dict[str, str]
- ○ for_html(): Dict[str, str]
- ○ for_xml(): Dict[str, str]
- ○ for_form_data(): Dict[str, str]
- ○ for_streaming(): Dict[str, str]

- ○ for_css(): Dict[str, str]
- ○ for_javascript(): Dict[str, str]

- ○ for_image(): Dict[str, str]
- ○ for_video(): Dict[str, str]
- ○ for_audio(): Dict[str, str]

- ○ for_file(filename): Dict[str, str]
- ○ for_pdf(filename, inline): Dict[str, str]
- ○ for_csv(filename): Dict[str, str]

> All methods return:
> Dict[str, str] containing
> security + caching headers
>
> Base security always included
> Caching varies by content type

imports *generates* *strategy* *strategy* *strategy* *strategy*

ⓒ *«module»* **server_header_constants**
- ○ HEADER_APP_NAME: str
- ○ CACHE_CONTROL: str
- ○ PRAGMA: str
- ○ EXPIRES: str
- ○ CONTENT_DISPOSITION: str
- ○ ACCEPT_RANGES: str
- ○ REFERRER_POLICY: str
- ○ CONTENT_SECURITY_POLICY: str
- ○ CONTENT_TYPE: str
- ○ FRAME_OPTIONS: str
- ○ XSS_PROTECTION: str

Security Features

ⓒ Base Security
- ○ X-Content-Type-Options: nosniff
- ○ X-Frame-Options: DENY
- ○ X-XSS-Protection: 1; mode=block
- ○ Referrer-Policy: strict-origin-when-cross-origin
- ○ app_sender: <app_name>

> Applied to ALL responses
> Protects against:
> - MIME sniffing
> - Clickjacking
> - XSS attacks
> - Referrer leakage

generates (HTML only)

ⓒ HTML Security
- ○ Content-Security-Policy
- □ default-src 'self'
- □ script-src 'self' 'unsafe-inline' CDN
- □ style-src 'self' 'unsafe-inline'
- □ img-src 'self' data: https:
- □ font-src 'self' data:

Caching Strategies

ⓒ No Cache

Cache-Control: no-cache, no-store, must-revalidate
Pragma: no-cache
Expires: 0

- for_json()
- for_text()
- for_html()
- for_xml()
- for_form_data()
- for_streaming()

> For dynamic content that
> changes frequently:
> - API responses
> - User-specific data
> - Real-time updates

ⓒ Long Cache (1 year)

Cache-Control: public, max-age=31536000, immutable

- for_css()
- for_javascript()

> For versioned static assets:
> - app.v123.js
> - styles.abc456.css
>
> Immutable = never changes

ⓒ Medium Cache (24h)

Cache-Control: public, max-age=86400

- for_image()
- for_video()
- for_audio()

ⓒ Short Cache (1h)

Cache-Control: public, max-age=3600

- for_file()
- for_pdf()
- for_csv()