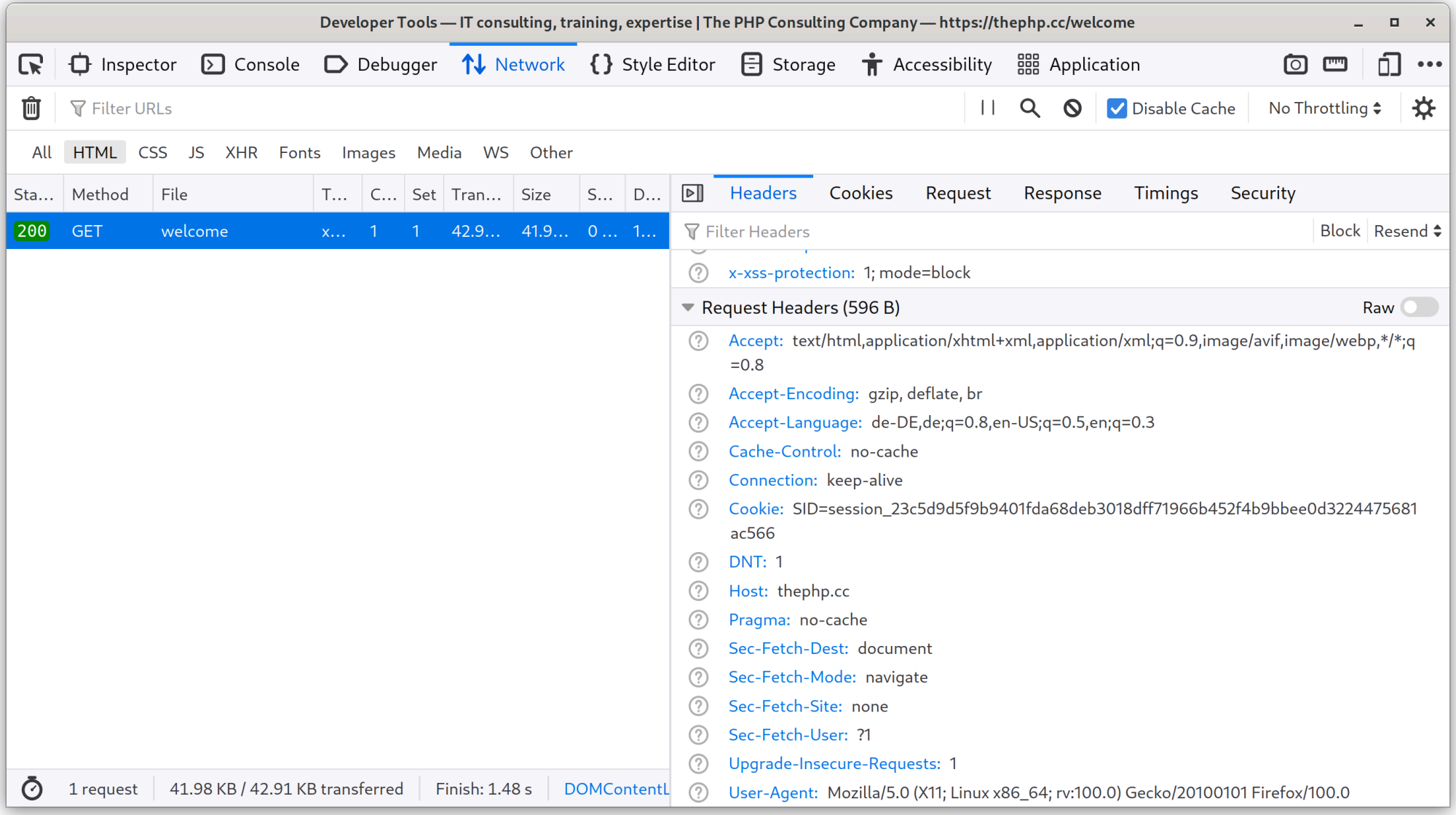
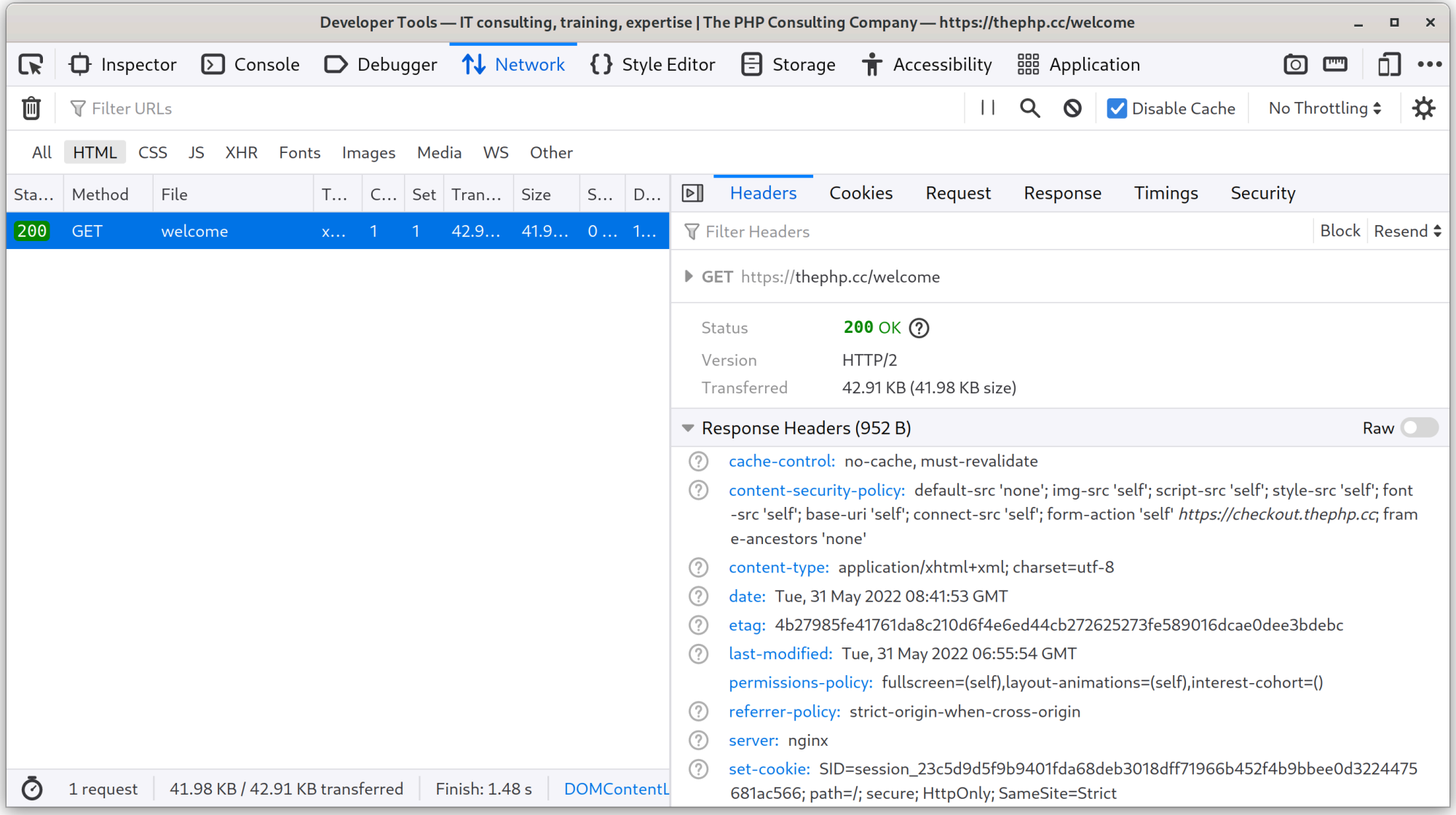
Arne Blankerts


Arne Blankerts
Co-Founder, The PHP Consulting Company

Headers?


Developer Tools — IT consulting, training, expertise | The PHP Consulting Company — https://thephp.cc/welcome
Inspector
Console
Debugger
Network
Style Editor
Storage
Accessibility
Application
Filter URLs
Disable Cache
No Throttling
All
HTML
CSS
JS
XHR
Fonts
Images
Media
WS
Other
Sta…
Method
File
T…
C…
Set
Tran…
Size
S…
D…
200
GET
welcome
x…
1
1
42.9…
41.9…
0 …
1…
Headers
Cookies
Request
Response
Timings
Security
Filter Headers
Block
Resend
x-xss-protection: 1; mode=block
Request Headers (596 B)
Raw
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Encoding: gzip, deflate, br
Accept-Language: de-DE,de;q=0.8,en-US;q=0.5,en;q=0.3
Cache-Control: no-cache
Connection: keep-alive
Cookie: SID=session_23c5d9d5f9b9401fda68deb3018dff71966b452f4b9bbee0d3224475681ac566
DNT: 1
Host: thephp.cc
Pragma: no-cache
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:100.0) Gecko/20100101 Firefox/100.0
1 request
41.98 KB / 42.91 KB transferred
Finish: 1.48 s
DOMContentL


Developer Tools — IT consulting, training, expertise | The PHP Consulting Company — https://thephp.cc/welcome
Inspector
Console
Debugger
Network
Style Editor
Storage
Accessibility
Application
Filter URLs
Disable Cache
No Throttling
All
HTML
CSS
JS
XHR
Fonts
Images
Media
WS
Other
Sta…
Method
File
T…
C…
Set
Tran…
Size
S…
D…
200
GET
welcome
x…
1
1
42.9…
41.9…
0 …
1…
Headers
Cookies
Request
Response
Timings
Security
Filter Headers
Block
Resend
GET https://thephp.cc/welcome
Status
200 OK
Version
HTTP/2
Transferred
42.91 KB (41.98 KB size)
Response Headers (952 B)
Raw
cache-control: no-cache, must-revalidate
content-security-policy: default-src 'none'; img-src 'self'; script-src 'self'; style-src 'self'; font
-src 'self'; base-uri 'self'; connect-src 'self'; form-action 'self' https://checkout.thephp.cc; fram
e-ancestors 'none'
content-type: application/xhtml+xml; charset=utf-8
date: Tue, 31 May 2022 08:41:53 GMT
etag: 4b27985fe41761da8c210d6f4e6ed44cb272625273fe589016dcae0dee3bdebc
last-modified: Tue, 31 May 2022 06:55:54 GMT
permissions-policy: fullscreen=(self),layout-animations=(self),interest-cohort=()
referrer-policy: strict-origin-when-cross-origin
server: nginx
set-cookie: SID=session_23c5d9d5f9b9401fda68deb3018dff71966b452f4b9bbee0d3224475
681ac566; path=/; secure; HttpOnly; SameSite=Strict
1 request
41.98 KB / 42.91 KB transferred
Finish: 1.48 s
DOMContentL

Headers.

Headers are security relevant!

Headers are security relevant!

Well, some are.

Headers.

X-Frame-Options

X-Frame-Options

```
header('X-Frame-Options: DENY');
```

X-Frame-Options

```
header('X-Frame-Options: DENY');
```

```
header('X-Frame-Options: SAMEORIGIN');
```

X-Frame-Options

```
header('X-Frame-Options: DENY');
```

```
header('X-Frame-Options: SAMEORIGIN');
```

```
header('X-Frame-Options: ALLOW-FROM https://friend.example.org');
```

X-Xss-Protection

X-Xss-Protection

```
header('X-Xss-Protection: 1; mode=block');
```

X-Content-Type-Options

X-Content-Type-Options

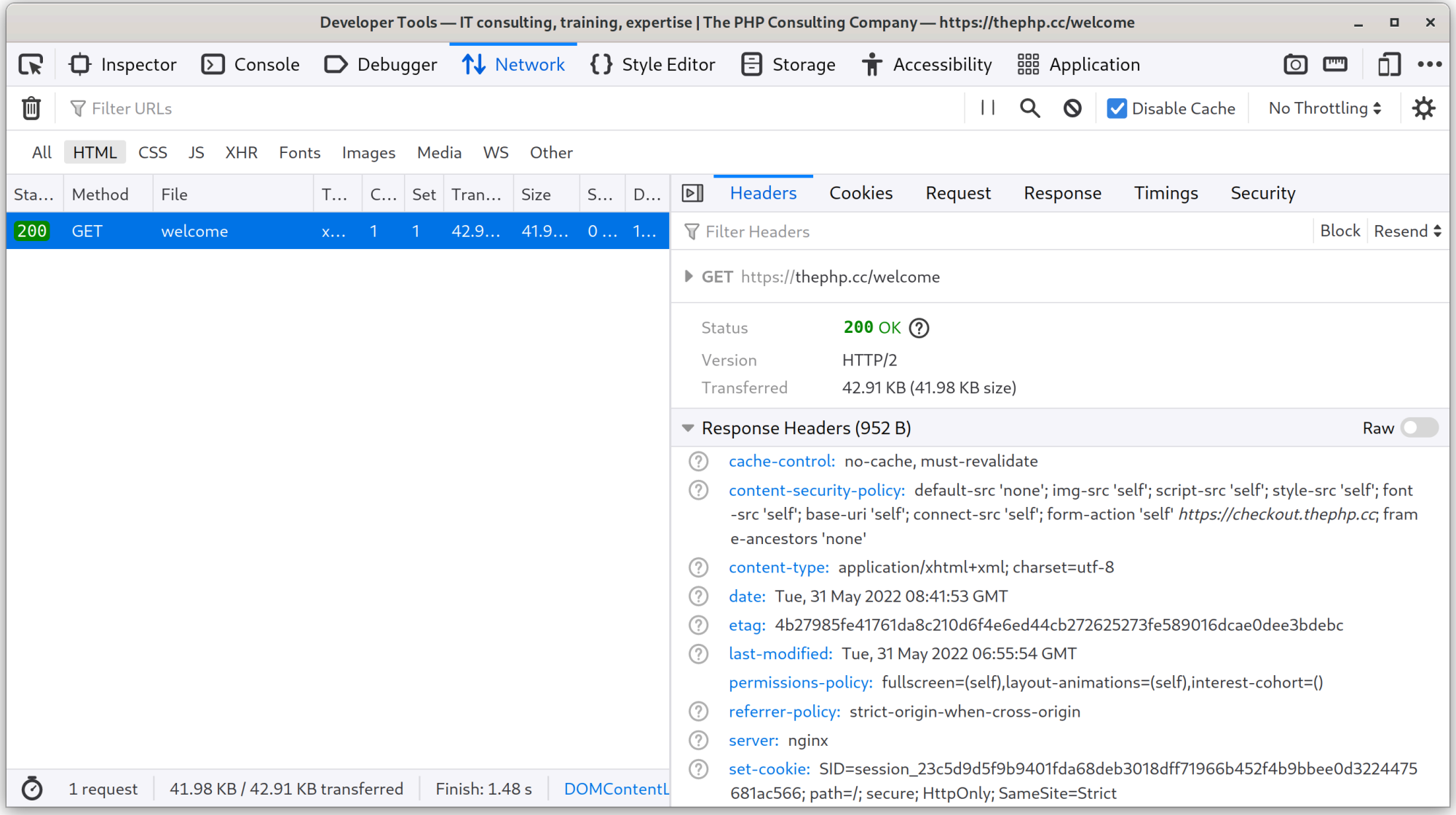
```
header('X-Content-Type-Options: nosniff');
```

X-Powered-By

X-Powered-By

```
expose_php = off
```

Server


Developer Tools — IT consulting, training, expertise | The PHP Consulting Company — https://thephp.cc/welcome
Inspector
Console
Debugger
Network
Style Editor
Storage
Accessibility
Application
Filter URLs
Disable Cache
No Throttling
All
HTML
CSS
JS
XHR
Fonts
Images
Media
WS
Other
Sta…
Method
File
T…
C…
Set
Tran…
Size
S…
D…
200
GET
welcome
x…
1
1
42.9…
41.9…
0 …
1…
Headers
Cookies
Request
Response
Timings
Security
Filter Headers
Block
Resend
GET https://thephp.cc/welcome
Status
200 OK
Version
HTTP/2
Transferred
42.91 KB (41.98 KB size)
Response Headers (952 B)
Raw
cache-control: no-cache, must-revalidate
content-security-policy: default-src 'none'; img-src 'self'; script-src 'self'; style-src 'self'; font
-src 'self'; base-uri 'self'; connect-src 'self'; form-action 'self' https://checkout.thephp.cc; fram
e-ancestors 'none'
content-type: application/xhtml+xml; charset=utf-8
date: Tue, 31 May 2022 08:41:53 GMT
etag: 4b27985fe41761da8c210d6f4e6ed44cb272625273fe589016dcae0dee3bdebc
last-modified: Tue, 31 May 2022 06:55:54 GMT
permissions-policy: fullscreen=(self),layout-animations=(self),interest-cohort=()
referrer-policy: strict-origin-when-cross-origin
server: nginx
set-cookie: SID=session_23c5d9d5f9b9401fda68deb3018dff71966b452f4b9bbee0d3224475
681ac566; path=/; secure; HttpOnly; SameSite=Strict
1 request
41.98 KB / 42.91 KB transferred
Finish: 1.48 s
DOMContentL

NGINX

```
server { server_tokens off; }
```

Apache

```
ServerSignature Off
ServerTokens Prod
```

Secure Cookies

Secure Cookies

```
header('set-cookie: SID=e3dc5....9032; path=/; secure; HttpOnly; SameSite=Strict');
```

Cookie Prefixes

Cookie Prefixes

```
header('set-cookie: __Secure-SID=e3dc5....9032; path=/; secure; HttpOnly; SameSite=Strict');
```

Cookie Prefixes

```
header('set-cookie: __Secure-SID=e3dc5....9032; path=/; secure; HttpOnly; SameSite=Strict');
```

```
header('set-cookie: __Host-SID=e3dc5....9032; path=/; secure; HttpOnly; SameSite=Strict');
```

Referrer-Policy

Referrer-Policy

```
header('Referrer-Policy: strict-origin-when-cross-origin');
```

Referrer-Policy

no-referrer (or empty string)

Referrer-Policy

no-referrer-when-downgrade

Referrer-Policy

same-origin

Referrer-Policy

origin

Referrer-Policy

strict-origin

Referrer-Policy

origin-when-cross-origin

Referrer-Policy

strict-origin-when-cross-origin

Referrer-Policy

unsafe-url

Strict-Transport-Security

Strict-Transport-Security

```
header('Strict-Transport-Security: max-age=63072000; includeSubDomains');
```

Strict-Transport-Security - Preload

Strict-Transport-Security - Preload

```
header('Strict-Transport-Security: max-age=63072000; includeSubDomains; preload');
```

Permissions-Policy

Permissions-Policy

```
header('Permissions-Policy: fullscreen=(self),layout-animations=(self)');
```

Content-Security-Policy

Content-Security-Policy

```
header("Content-Security-Policy: default-src 'none'; img-src 'self'; style-src 'self';");
```

Cross Origin Resource Sharing (CORS)

Cross Origin Resource Sharing (CORS)

- Access-Control-Allow-Origin: *
- Access-Control-Allow-Origin: https://example.org

CORS - Preflight

Request

- Access-Control-Request-Method: POST
- Access-Control-Request-Headers: Content-Type

CORS - Preflight

Response

- Access-Control-Allow-Origin: https://foo.example
- Access-Control-Allow-Methods: POST, GET, OPTIONS
- Access-Control-Allow-Headers: Content-Type
- Access-Control-Max-Age: 86400

Links.

- https://tools.ietf.org/html/draft-ietf-httpbis-cookie-prefixes-00
- https://hstspreload.org/
- https://securityheaders.com/
- https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP
- https://report-uri.com/home/analyse
- https://report-uri.com/home/generate
- https://www.w3.org/TR/referrer-policy/
- https://www.permissionspolicy.com/
- https://developer.mozilla.org/en-US/docs/Web/HTTP/CORS

Thank you.

https://thephp.cc arne@thephp.cc @arneblankerts