

# HTTP HEADER SECURITY

Meetup 16.08.2017 - Sergej Michel

# INHALT

- Transport Security Flags
  - HTTP Strict Transport Security
  - HTTP Public Key Pinning
  - Referrer Policy
- Web-Content Security Flags
  - X-Frame-Options
  - X-XSS-Protection
  - X-Content-Type-Options
  - Content-Security-Policy
- Cookie Security Flags

# WAS IST EIN HTTP HEADER?

# ANFRAGE-HEADER CLIENT

🔍

Inspektor

📄

Konsole

🐛

Debugger

{ }

Stilbearbeitung

⌚

Laufzeitanalyse

💾

Speicher

🔧

Netzwerkanalyse

📏

📏

📏

📏

📏

📏

🗑️

Alles

HTML

CSS

JS

XHR

Schriften

Grafiken

Medien

Flash

WebSockets

Sonstiges

🔄

Eine Anfrage, 7,13 KB (übertragen: 2,43 KB), 1,04 s

🔍 Adresser

Status	Metho...	Datei	Host	Ur	Kopfzeilen	Cookies	Parameter	Antwort	Zeit	S
200	GET	/	gramou.de	JS dc						

Angefragte Adresse: https://gramou.de/  
Anfragemethode: GET  
Externe Adresse: 85.214.106.124:443  
Status-Code: 200 OK [Weitere Informationen] Bearbeiten und erneut senden  
Version: HTTP/1.1

🔍 Kopfzeilen durchsuchen

▶ Antwortkopfzeilen (572 B)

▼ Anfragekopfzeilen (374 B)

Host: "gramou.de"  
User-Agent: "Mozilla/5.0 (Macintosh; Intel... Gecko/20100101 Firefox/54.0"  
Accept: "text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8"  
Accept-Language: "de,de-DE;q=0.8,en-US;q=0.5,en;q=0.3"  
Accept-Encoding: "gzip, deflate, br"  
Connection: "keep-alive"  
Upgrade-Insecure-Requests: "1"  
Cache-Control: "max-age=0"

# ANTWORT-HEADER SERVER

🔍

Inspektor

📄

Konsole

🐛

Debugger

{ }

Stilbearbeitung

🕒

Laufzeitanalyse

💾

Speicher

🌐

Netzwerkanalyse

🗑️

Alles

📄

HTML

📄

CSS

📄

JS

📄

XHR

📄

Schriften

📄

Grafiken

📄

Medien

📄

Flash

📄

WebSockets

📄

Sonstiges

🕒

Eine Anfrage, 7,13 KB (übertragen: 2,43 KB), 1,04 s

🔍

Adresse

# SECURITY SERVER-HEADER

Inspektor

Konsole

Debugger

Stilbearbeitung

Laufzeitanalyse

Speicher

Netzwerkanalyse

11 Anfragen, 1,38 MB (übertragen: 728,95 KB), 928 ms

Adressen durchsuchen

Status	Metho...	Datei	Host	Kopfzeilen	Cookies	Parameter	Antwort	Zeit	Sicherheit	Vorschau
200	GET	/	gramou.de	Angefragte Adresse: https://gramou.de/ Anfragemethode: GET Externe Adresse: 85.214.106.124:443 Status-Code: 200 OK [Weitere Informationen] Bearbeiten und erneut senden Kopfzeilen (unformatiert) Version: HTTP/1.1						
200	GET	bootstrap.min.css	gramou.de							
200	GET	bootstrap-theme.min.css	gramou.de							
200	GET	bootstrap.min.js	gramou.de							
200	GET	step1.png	gramou.de							
200	GET	step2.png	gramou.de							
200	GET	step3.png	gramou.de							
200	GET	step4.png	gramou.de							
200	GET	step5.png	gramou.de							
200	GET	bootstrap.min.css	gramou.de							
200	GET	bootstrap.min.css.map	gramou.de							

Kopfzeilen durchsuchen

Antwortkopfzeilen (573 B)

X-Content-Type-Options: "nosniff"

X-Frame-Options: "sameorigin"

x-xss-protection: "1;mode=block"

Content-Security-Policy: "default-src 'self';"

Strict-Transport-Security: "max-age=63072000; includeSubdomains;"

referrer-policy: "same-origin"

Content-Length: "2489"

Keep-Alive: "timeout=5, max=100"

Connection: "Keep-Alive"

Content-Type: "text/html; charset=UTF-8"

# WAS IST EIN HTTP SECURITY HEADER?

- Browserseitiger Schutz
- Security Header Mode:
  - Persistent
  - Pro Request
- Unterstützung der Header ist browserabhängig
- Entbindet nicht von serverseitiger Security
- HTTP Security Header stehen im Server-Antwort-Header

# TRANSPORT SECURITY FLAGS



# HTTP STRICT TRANSPORT SECURITY (HSTS)



# HTTP STRICT TRANSPORT SECURITY (HSTS)

```
Strict-Transport-Security: max-age=63072000;  
includeSubDomains; preload
```

# HSTS FUNKTIONSWEISE

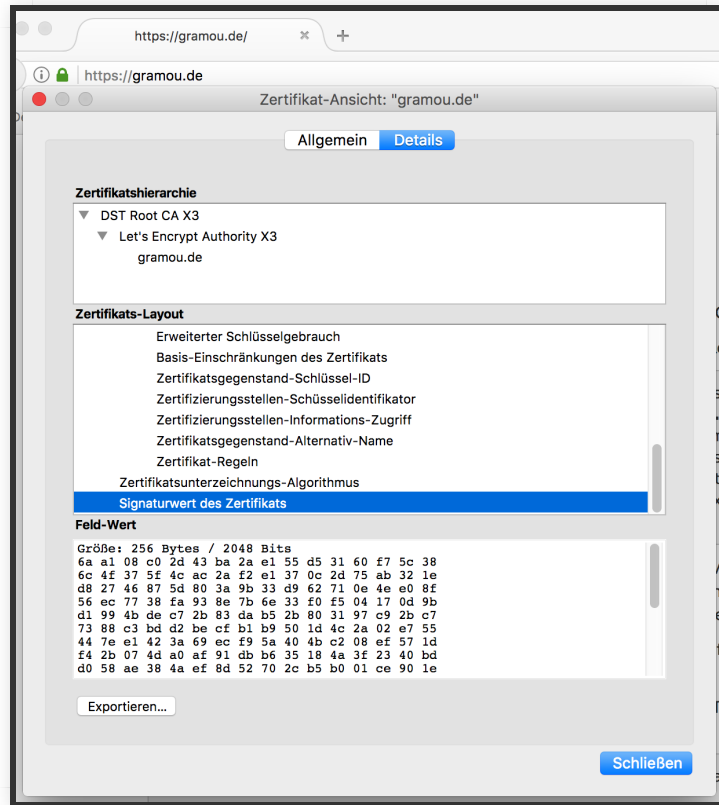
- Der Server setzt den HSTS Header für eine Domain
- Persistent im Browser
- Alle HTTP Anfragen im Browser auf die HSTS-Domain werden auf HTTPS umgeleitet
- Kein HTTP mehr möglich

```
Strict-Transport-Security: max-age=63072000;  
includeSubDomains; preload
```

# WAS MUSS MAN BEIM SETZEN VON HSTS BEACHTEN?

- HTTP Webseiten werden ausgesperrt
- Nebenwirkung: Evercookie

# HTTP PUBLIC KEY PINNING



# HTTP PUBLIC KEY PINNING

- Der Server setzt den HPKP Header für eine Domain
- Persistent im Browser
- Verwendung von anderen validen Zertifikaten nicht möglich
- Achtung! Self-Denial-Of-Service möglich

```
Public-Key-Pins: max-age=1296000;  
includeSubDomains;  
pin-sha256="WoiWRyIOVNa9ihaBciRSC7XHjliYS9VwUGOIud4PB18=";  
pin-sha256="YLh1dUR9y6Kja30RrAn7JKnbQG/uEtLMkBgFF2Fuihg=";  
pin-sha256="P0NdsLTMT6LSwXLUSEHnlvg4WxtWb5rIJhfZMyeXUE0="
```

# REFERRER POLICY

# REFERRER POLICY

- Verhindert z.B. webseitenübergreifend Information Disclosure
- Beispiel für Information Disclosure: Session-Information im Server-Log

```
referrer-policy: same-origin
```



# WEB-CONTENT SECURITY FLAGS

# X-FRAME-OPTIONS

- Verhindert Clickjacking

```
X-Frame-Options: DENY
```

# X-XSS-PROTECTION

- Verhindert einfache XSS-Angriffe

```
X-XSS-Protection: 1; mode=block
```

# X-CONTENT-TYPE-OPTIONS

- Verhindert das Laden von JavaScript oder CSS mit falschem Mime-Type

```
X-Content-Type-Options: nosniff
```

# CONTENT SECURITY POLICY (CSP)

- Verhindert das XSS und andere Angriffe

```
# Disable unsafe inline/eval, only load resources  
# from same origin,  
# also disables the execution of plugins
```

```
Content-Security-Policy: default-src 'self'; object-src 'none'
```

# CONTENT SECURITY POLICY (CSP)

```
# Pre-existing site that uses too much inline  
# code to fix but wants to ensure resources are  
# loaded only over https and disable plugins
```

```
Content-Security-Policy: default-src https: 'unsafe-eval'  
'unsafe-inline'; object-src 'none'
```

# CONTENT SECURITY POLICY (CSP)


```
# Disable the use of unsafe inline/eval,  
# allow everything else except plugin execution  
  
Content-Security-Policy: default-src *; object-src 'none'
```

# COOKIE SECURITY FLAGS

- Das HttpOnly-Flag verhindert das Auslesen des Cookies mittels JavaScript
- Das Secure-Flag verhindert das Senden des Cookies über HTTP

```
Set-Cookie: YOURSESSION=6F42313; Secure; HttpOnly
```





Host:	gramou.de
Scan ID #:	4304848
Start Time:	August 13, 2017 10:19 PM
Duration:	4 seconds
Score:	115/100
Tests Passed:	11/11

🚩🚩🚩 We don't have any! 🚩🚩🚩

Make sure to check back occasionally to ensure that your website is keeping up with the latest in web security standards.

In the meantime, thanks for for everything you're doing to keep the internet a safe, secure, and private place!

## Test Scores

Test	Pass	Score	Explanation	
<a href="#">Content Security Policy</a>	✓	+5	Content Security Policy (CSP) implemented without 'unsafe-inline' or 'unsafe-eval'	👍
<a href="#">Cookies</a>	=	0	No cookies detected	👍
<a href="#">Cross-origin Resource Sharing</a>	✓	0	Content is not visible via cross-origin resource sharing (CORS) files or headers	👍
<a href="#">HTTP Public Key Pinning</a>	=	0	HTTP Public Key Pinning (HPKP) header not implemented (optional)	👍
<a href="#">HTTP Strict Transport Security</a>	✓	0	HTTP Strict Transport Security (HSTS) header set to a minimum of six months (15768000)	👍
<a href="#">Redirection</a>	✓	0	Initial redirection is to https on same host, final destination is https	👍
<a href="#">Referrer Policy</a>	✓	+5	Referrer-Policy header set to "no-referrer", "same-origin", "strict-origin" or "strict-origin-when-cross-origin"	👍
<a href="#">Subresource Integrity</a>	✓	+5	Subresource Integrity (SRI) is implemented and all scripts are loaded from a similar origin	👍
<a href="#">X-Content-Type-Options</a>	✓	0	X-Content-Type-Options header set to "nosniff"	👍
<a href="#">X-Frame-Options</a>	✓	0	X-Frame-Options (XFO) header set to SAMEORIGIN or DENY	👍
<a href="#">X-XSS-Protection</a>	✓	0	X-XSS-Protection header set to "1; mode=block"	👍

# KONFIGURATIONSBEISPIEL APACHE

```
Header set X-Content-Type-Options: "nosniff"  
Header set X-Frame-Options: "sameorigin"  
Header set X-XSS-Protection 1;mode=block  
Header set Content-Security-Policy "default-src 'self';"  
Header set Strict-Transport-Security "max-age=63072000; includeSubDomains"  
Header set Referrer-Policy "same-origin"
```

```
LoadModule headers_module /usr/lib/apache2/modules/mod_headers.so  
Header edit Set-Cookie ^(.*)$ $1;HttpOnly;Secure
```

Sicher

https://wiki.mozilla.org/Security/Guidelines/Web\_Security#HTTP\_Public\_Key\_Pinning

Page

Discussion

Read

Vl

lla wiki

e  
leases  
es  
anges  
loads  
ages  
age

Contribute  
ds meeting  
meetings  
ute to Mozilla  
Reps  
adors  
Wiki  
Mozilla

## Security/Guidelines/Web Security

< Security | Guidelines

Contents [hide]

1 Cheat Sheet

2 Transport Layer Security (TLS/SSL)

2.1 HTTPS

2.2 HTTP Strict Transport Security

2.3 HTTP Redirections

2.4 HTTP Public Key Pinning

2.5 Resource Loading

3 Content Security Policy

4 contribute.json

5 Cookies

6 Cross-origin Resource Sharing

7 CSRF Prevention

8 Referrer Policy

9 robots.txt

10 Subresource Integrity

11 X-Content-Type-Options

12 X-Frame-Options

13 X-XSS-Protection

14 Version History

The goal of this document is to help operational teams with creating secure w deployments are expected to follow the recommendations below. Use of these strongly encouraged.


The Enterprise Information Security (EIS) team maintains this document as a r changing landscape of web security. Changes are reviewed and merged by the various Operational teams.

Updates to this page should be submitted to the [source repository on github](#)

STATUS: 

READY

# MOZILLA GUIDELINES WEB SECURITY

 [https://wiki.mozilla.org/Security/Guidelines/Web\\_Security#HTTP\\_Public\\_Key\\_Pinning](https://wiki.mozilla.org/Security/Guidelines/Web_Security#HTTP_Public_Key_Pinning)

## Web Security Cheat Sheet

Guideline	Security Benefit	Implementation Difficulty	Order <sup>†</sup>	Requirements
HTTPS	MAXIMUM	MEDIUM		Mandatory
Public Key Pinning	LOW	MAXIMUM	--	Mandatory for maximum risk sites only
Redirections from HTTP	MAXIMUM	LOW	3	Mandatory
Resource Loading	MAXIMUM	LOW	2	Mandatory for all websites
Strict Transport Security	HIGH	LOW	4	Mandatory for all websites
TLS Configuration	MEDIUM	MEDIUM	1	Mandatory
Content Security Policy	HIGH	HIGH	10	Mandatory for new websites Recommended for existing websites
Cookies	HIGH	MEDIUM	7	Mandatory for all new websites Recommended for existing websites
contribute.json	LOW	LOW	9	Mandatory for all new Mozilla websites Recommended for existing Mozilla sites
Cross-origin Resource Sharing	HIGH	LOW	11	Mandatory
Cross-site Request Forgery Tokenization	HIGH	UNKNOWN	6	Varies
Referrer Policy	LOW	LOW	12	Recommended for all websites
robots.txt	LOW	LOW	14	Optional
Subresource Integrity	MEDIUM	MEDIUM	15	Recommended <sup>‡</sup>
X-Content-Type-Options	LOW	LOW	8	Recommended for all websites
X-Frame-Options	HIGH	LOW	5	Mandatory for all websites
X-XSS-Protection	LOW	MEDIUM	13	Mandatory for all new websites Recommended for existing websites

# ZUSAMMENFASSUNG

# FRAGEN?