

HTTPS bevorzugen

Wenn Sie die Verwendung von HTTPS auf Ihrer Webseite bevorzugen möchten, stehen Ihnen derzeit zwei Möglichkeiten zur Auswahl. Welche Methode Sie verwenden bleibt Ihnen überlassen, jedoch sollten Sie sich zunächst mit den Unterschieden und deren Konsequenzen vertraut machen.



Bevor Sie HTTPS-Verbindungen bevorzugen können, benötigen Sie ein Sicherheitszertifikat. Bitte lesen Sie dazu den Artikel [TLS \(HTTPS\)](#).

Mittels Redirect

HTTP bietet die Möglichkeit, im *Header* durch die Angabe einer *Location* auf einen anderen URI zu verweisen. Dies wird begleitet durch einen 30x Statuscode. Es gibt verschiedene Status Codes für Weiterleitungen unterschiedlicher Intention und technischer Spezifikation.

An dieser Stelle seien nur die beiden wichtigsten Statuscodes genannt:

| Statuscode | Bedeutung |
|-----------------|---|
| 301 (Permanent) | Die gesuchte Webseite ist dauerhaft unter einem neuen Ziel verfügbar. |
| 302 (Temporary) | Die gesuchte Webseite verweist temporär auf ein anderes Ziel. |



Diese Methode wurde nicht zur Erhöhung der Sicherheit, sondern als Möglichkeit der Umleitung auf ein anderes Ziel entworfen. Ein Angreifer kann diese Methode unter Umständen durch verschiedene Mechanismen aushebeln.

Mittels HSTS

Bei *HTTP Strict Transport Security (HSTS)* handelt es sich um einen Sicherheitsmechanismus, der vor Aushebelung der Verschlüsselung durch eine Downgrade-Attacke, sowie vor Session Hijacking schützen soll.

Unser Server sendet in diesem Fall mittels des HTTP response header *Strict-Transport-Security* dem Browser des Anwenders die Information, in Zukunft ausschließlich verschlüsselte Verbindungen für Ihre Domain zu nutzen. Der Parameter *max-age* legt fest, für welchen Zeitraum der Browser nur HTTPS-Verbindungen mit gültigem Sicherheitszertifikat für Ihre Domain akzeptiert. Optional lässt sich dies mit Hilfe des Parameter *includeSubDomains* auch auf alle Subdomains ausweiten.





Diese Methode wurde speziell zur Vermeidung sogenannter Downgrade- und Session Hijacking Attacken entworfen. Sollte Ihr Sicherheitszertifikat ungültig werden oder Sie aus einem anderen Grund auf HTTPS verzichten wollen, so genügt es nicht diese Option zu deaktivieren. Ein Webbrowser wird bis zum Ablauf des *max-age* Parameter nur HTTPS-Verbindungen mit gültigem Sicherheitszertifikat akzeptieren.

Konfigurationsbeispiel

Für beide Varianten finden Sie hier ein Konfigurationsbeispiel:

Konfiguration mittels Redirect

Schritt 1 Erstellen Sie eine Datei mit dem Namen *.htaccess* im Hauptverzeichnis Ihrer Domain. Bitte beachten Sie, dass diese Datei unter Umständen bereits existiert und mit Inhalten gefüllt ist (z.B. wenn Sie Wordpress verwenden).

Schritt 2 Füllen Sie die Datei mit dem folgenden Inhalt, um alle Anfragen permanent auf HTTPS weiterzuleiten. Sie können natürlich auch einen anderen Statuscode verwenden, indem Sie die Angabe *R=301* entsprechend abändern.

```
RewriteEngine On
RewriteCond %{HTTPS} on
RewriteRule (.*) http:// %{HTTP_HOST} %{REQUEST_URI} [R=301,L]
```

Konfiguration mittels HSTS

Schritt 1 Melden Sie sich am Webhostingsystem an und wählen Sie **Domains**

Schritt 2 Wählen Sie **SSL-Zertifikat verwalten**

| Name | Mount point | Document root | Redirect | Status | SSL status | Actions |
|------------------------|--------------|---------------|----------|--------|------------|---------|
| beispiel.de [Alt. URL] | /beispiel.de | /htdocs | N/A | Ok | Ok | |

Schritt 3 Aktivieren Sie HSTS.

Domains » Overview » Edit SSL certificate

[Logout](#)

EDIT SSL CERTIFICATE

| Certificate data | |
|---|---|
| Common name | beispiel.de |
| Status | Ok |
| HSTS (HTTP Strict Transport Security) | <input checked="" type="button"/> Yes <input type="button"/> No |
| HSTS max-age directive value | 31536000 Sec. |
| HSTS includeSubDomains directive <small>(?)</small> | <input type="button"/> Yes <input checked="" type="button"/> No |

From:

<https://doku.deltaweb.de/> - Deltaweb Dokumentation



Permanent link:

<https://doku.deltaweb.de/doku.php/public:imscp:ssl:hsts>

Last update: **2018/11/12 15:34**