SecureNet

Web Application Security Untersuchung

Aktuelle Verbreitung von http Strict Transport Security (HSTS)

05.11.2012 - V1.1

Sven Schleier, SecureNet GmbH
Thomas Schreiber, SecureNet GmbH

Abstract

Das vorliegende Dokument gibt die Ergebnisse einer Untersuchung zur Verbreitung des HSTS Server Response-Headers unter den weltweit 1 Mio. meistbesuchten Websites, den darin enthaltenen rund 40.000 deutschen Websites sowie auf 424 deutschen Onlinebanking-Websites wieder. Die Untersuchung zeigt, dass diese wichtige Sicherheitsmaßnahme bisher noch kaum eingesetzt wird.

SecureNet GmbH - Frankfurter Ring 193a - D-80807 München
www.securenet.de - info (at) securenet.de

1 EINFÜHRUNG

Das Ausschalten der SSL-Verschlüsselung im Browser durch einen Man-in-the-Middle-Angriff (MitM) ist eine schwerwiegende Sicherheitslücke, die in ungeschützten Umgebungen (wie z.B. in öffentlichen WLANs) leicht ausgenutzt werden kann. Die Folge eines solchen Angriffes ist der komplette Verlust der Vertraulichkeit: Bankkonto-, Email- und Social Network-Zugangsdaten gelangen dabei ebenso in die Hände des Angreifers wie Kreditkartendaten oder vertrauliche Geschäftsinformationen. Der Angriff ist seit 2009 unter dem Namen SSL-Stripping bekannt (siehe [1]).

In Form eines HTTP-Headers existiert ein Schutzmechanismus, mit dem der Serverbetreiber die Gefahr der erfolgreichen Durchführung eines solchen Angriffs auf ein Minimum reduzieren kann.

Wir haben untersucht, wie hoch im Moment die Verbreitung dieses Headers (HSTS-Header oder `strict-transport-security`) ist. Die Untersuchung umfasst die gemäß „Alexa Top 1,000,000“-Liste (siehe [2], im Folgenden nur noch *Top1M*-Liste genannt) rund 40.000 meistbesuchten deutschen, sowie 1 Million internationalen Sites, sowie speziell das Onlinebanking-Login deutscher Banken.

Das Ergebnis der Erhebung ist erschreckend: Obwohl diese Schwachstelle seit 2009 bekannt ist und der Header mittlerweile von fast allen Browsern unterstützt wird, schützen international weniger als 0,5% und in Deutschland weniger als 0,2% der Websites ihr Benutzer in besagter Weise. Bei den deutschen Banken sind es ganze 7 von 424 Sites, die den Header einsetzen, jedoch außer einer alle in einer Weise, die so gut wie wirkungslos ist.

Im Folgenden werden die Ergebnisse präsentiert. Auf die Schwachstelle selbst und die konkreten Gegenmaßnahmen gehen wir in diesem Bericht nicht ein, dazu verweisen wir auf unser HSTS-Whitepaper (siehe [5]).

Schutzwirkung

Um den Benutzer vor oben beschriebenem Angriff zu schützen, muss der Server den HTTP-Header

`Strict-Transport-Security: max-age=`*Gültigkeitsdauer*`; includeSubDomains`

in der Response ausliefern. Der Browser wandelt nach Erhalt für den in der `max-age` Direktive in Sekunden angegebenen Zeitraum alle HTTP-Links auf den Host, von dem er den Header erhalten hat, in HTTPS-Links um. Der Benutzer ist damit in diesem Zeitraum vor dem Ausspähen vertraulicher Informationen und Manipulationen auf dem Übertragungsweg geschützt.

Die eingestellte Gültigkeitsdauer ist von großer Bedeutung für die Wirksamkeit des Schutzes: Ist diese kurz, so ist die Wahrscheinlichkeit entsprechend

hoch, dass der Schutz, der bei einem vorherigen Besuch „eingeschaltet“ worden ist, bereits abgelaufen ist, wenn der Benutzer in eine ungeschützte Umgebung gerät. Das Neusetzen des HSTS-Headers in der ungeschützten Umgebung ist dann unwirksam, da SSL-Stripping dies ebenfalls unterbindet.

Die Schutzwirkung des Headers wurde anhand des `max-age`-Wertes wie folgt bewertet:

max-age	Schutzgrad
bis 2.592.000 (30 Tage)	ungenügend
2.592.000 bis 30.758.400 (1 Jahr)	schlecht
30.758.400 (1 Jahr)	ausreichend (je höher desto sicherer)

Eine weitere Direktive des Headers legt fest, ob der Schutz sich auch auf Subdomains beziehen soll. In diesem Fall ist das Schlüsselwort `includeSubdomains` hinzuzufügen. Diese Direktive ist nicht in die Bewertung eingeflossen.

Vorgehen

Für die Untersuchung wurde ein Skript verwendet, das die im Folgenden genannten Websites gescannt und auf Vorhandensein des `strict-transport-security` Headers geprüft hat. Zusätzlich wurden die Werte für die Direktive `max-age` ausgewertet und es wurde auf die Direktive `includeSubDomains` geprüft.

Die der Untersuchung zugrunde liegende Top1M-Liste wird täglich neu durch Alexa erstellt und kann als CSV bezogen werden ([3]). Für diese Untersuchung wurde die am 05.10.2012 veröffentlichte Liste verwendet.

Der Test wurde in drei Kategorien aufgeteilt:

— Überprüfung aller Domains aus der Top1M-Liste

— Überprüfung aller darin enthaltenen de-Domains

— Überprüfung der Login-Seiten deutscher Bankenwebseiten

Die Scans wurden am 6. und 7.10.2012 sowie am 9. und 10.10.2012 durchgeführt.

Bei der Auswertung der Ergebnisse gehen wir von folgenden vereinfachenden Annahmen aus:

— Webserver, die keinen HTTPS-Zugang anbieten, beherbergen auch keine sonderlich schützenswerten Informationen. Sie werden daher von der Auswertung ausgenommen.

— Webserver, die einen HTTPS-Zugang anbieten, tun dies, weil sie entsprechend schützenswerte Informationen bereitstellen. HSTS-Schutz ist somit erforderlich.

— Bei Webservern, die ein fehlerhaftes Zertifikat ausliefern, handelt es sich um nicht ernsthaft produktiv eingesetzte Webserver. Diese wurden nicht in der Auswertung berücksichtigt.

Arbeitsweise des Skriptes

Das Skript ruft jede einzelne Domain aus der Top1M-Liste mit mehreren Requests auf. Die ersten beiden Requests sind per HTTPS ausgeführte HEAD-Requests, die lediglich die Headerinformation zurückliefern, wobei sowohl der www-Host als auch der leere Host berücksichtigt wurden:

```
https://<domain>
https://www.<domain>
```

Der Response-Header wird dann auf den `strict-transport-security`- Header und den in der `max-age`-Direktive gesetzten Wert überprüft.

Zusätzlich zu diesen beiden Aufrufen erfolgen 4 GET-Requests nach folgendem Schema:

```
https://<domain>
https://www.<domain>
http://<domain>
http://www.<domain>
```

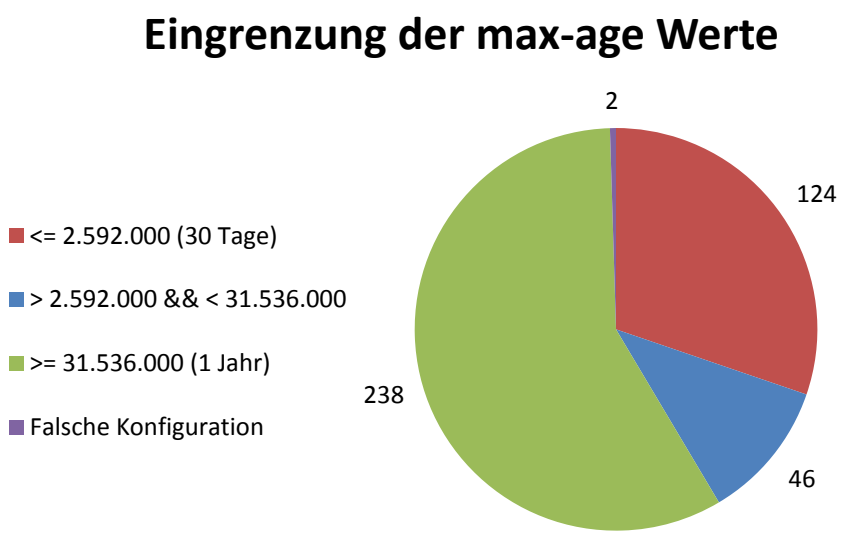
In der Response des Webservers wird daraufhin nach verschiedenen Link-Texten gesucht, unter anderem „Login“ oder „Signin“. Die URLs, die sich hinter diesen Link-Texten verbergen, werden dann wiederum mit einem HTTPS-Request aufgerufen und die hierauf folgende Response ebenfalls auf HSTS-Header überprüft.

Da oft nur Loginbereiche auf einer Webseite per HTTPS verschlüsselt sind und diese häufig nicht direkt auf der Startseite platziert sind, wurde diese tiefergehende Überprüfung mit in das Skript aufgenommen. So können auch diese Seiten automatisiert auf den HSTS Header überprüfen.

2 ERGEBNISSE

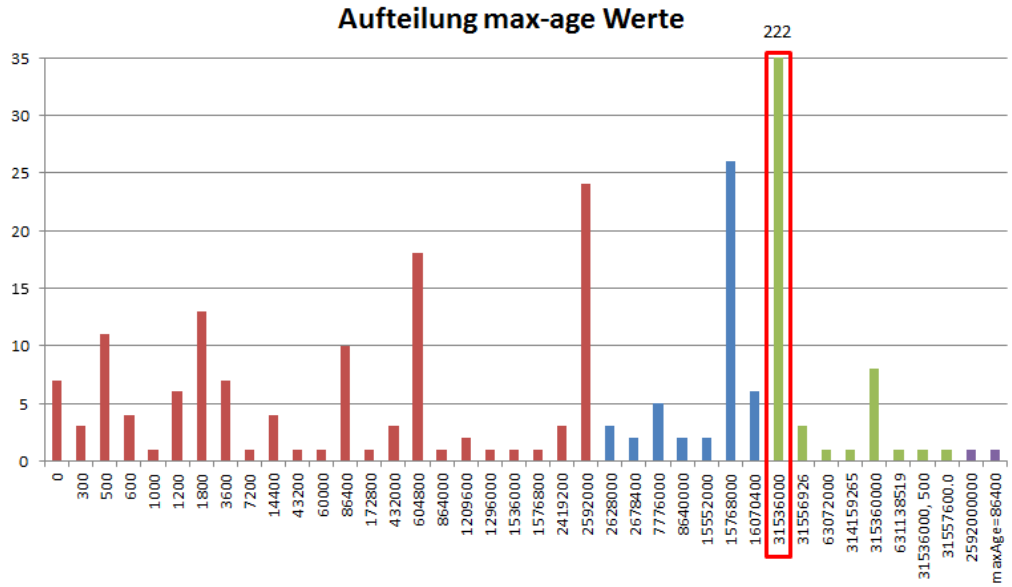
Internationale Sites

Rund 10% der Top1M-Liste bedienen das HTTPS-Protokoll. 410 dieser rund 100.000 HTTPS-Websites liefern die HSTS-Direktive im Header aus.



Der gemessene Wertebereich für den `max-age`-Parameter reichte von 300 bis 631.138.519 Sekunden, d.h. von 5 Minuten bis 7304,8 Tagen oder 20 Jahren. Insgesamt wurde achtmal der Wert 0 für `max-age` ausgeliefert, was die HSTS-Einstellung zurücksetzt und somit SSL-Stripping-Angriffe nicht mehr verhindern kann.

In der folgenden Auswertung der einzelnen `max-age`-Werte, wurde der empfohlene Mindestwert von 1 Jahr (31.536.000) rot hervorgehoben.



Der häufigste Wert für `max-age` ist 31.536.000 (1 Jahr). Er wird von 222 Websites verwendet.

100 Webseiten definieren einen Wert, der unter 30 Tagen liegt, und davon wiederum 69 Webseiten einen Wert, der sogar nur 24 Stunden oder kleiner ist.

Bewertung

Die Verbreitung von HSTS unter den 10 % der 1 Mio. weltweit meistbesuchten Websites, die auch einen HTTPS-Zugang anbieten, liegt bei ganzen 0,4 %. Einen als ausreichend anzusehenden Schutz bieten sogar nur 0,25 % der Websites.

de-Domains

Für die Untersuchung der deutschen Websites wurden alle de-Domains aus der Top1M-Liste berücksichtigt. Die Zahl beläuft sich auf 39.270, von denen 6.206 Sites auch das HTTPS-Protokoll anbieten.

12 der HTTPS-Sites lieferten eine gültige HSTS-Direktive im Header aus, wobei aber nur 5 Sites die Minimalanforderung von 30 Tagen Gültigkeit erfüllten. 3 Domains hatten zusätzlich das `includeSubDomains`-Attribut gesetzt.

Der gemessene Wertebereich für `max-age` reichte von 600 bis 31.536.000 Sekunden, d.h. von 10 Minuten bis 365 Tage.

Bewertung

Die Verbreitung von HSTS unter den 6.209 meistbesuchten deutschen Websites mit HTTPS-Zugang liegt bei knapp unter 0,2 %. Nur 3 Websites haben das HSTS so konfiguriert, dass es als ausreichend sicher anzusehen ist.

Bankenwebseiten

Zusätzlich zu den automatisierten Auswertungen erfolgte eine manuelle Auswertung von deutschen Banken-Webseiten und deren Onlinebanking-Login.

Die Bankenliste für den Test wurde folgendermaßen zusammengestellt:

Aus der Top1M-Liste wurden alle de-Domains extrahiert, die "bank" oder "sparkasse" enthielten. Die resultierende Liste wurde manuell bereinigt und mit einem Bankenverzeichnis des Bankenverbandes (siehe [4]) abgeglichen. Am Ende enthielt die Liste 424 Bankendomains, darunter 190 Internetauftritte der Sparkassen und 79 der Volks- und Raiffeisenbanken.

Es konnten 7 Onlinebanking-Sites mit gesetztem HSTS-Header gefunden werden. Das `includeSubDomains`-Attribut fand in keinem Fall eine Verwendung.

Der gemessene Wertebereich für `max-age` reichte von 3.600 bis 31.536.000 Sekunden, d.h. von einer Stunde bis 365 Tagen.

Bewertung

Lediglich eine einzige deutsche Bank schützt ihre Kunden ausreichend vor dem Ausspähen der (Zugangs-)Daten in unsicherer Umgebung. 6 weitere senden zwar ebenfalls den HSTS-Header aus, allerdings mit einer weitgehend wirkungslosen Konfiguration.

3 FAZIT

Offenbar sind die Gefahren, die von SSL-Stripping-Angriffen ausgehen, noch so gut wie unbekannt. Anders ist es nicht zu erklären, dass im deutschen Online-Banking nur in einem einzigen Fall der HSTS-Header mit einer ausreichend sicheren Einstellung verwendet wird und auch außerhalb des Bankensektors auf deutschen und internationalen Websites ein Schutz vor SSL-Stripping nur in Einzelfällen anzutreffen ist.

Angesichts der breiten Angriffsfläche kann jedem Betreiber von HTTPS-geschützten Websites nur dringend empfohlen werden, den HSTS-Schutz einzuschalten. Die Einrichtung ist in den meisten Fällen trivial und frei von Seiteneffekten. Eine ausführliche Behandlung von HSTS findet sich u. a. in [5] und [6].

4 QUELLEN

[1] sslstrip
http://www.thoughtcrime.org/software/sslstrip/

[2] Alexa Topsites
http://www.alexa.com/topsites

[3] Alexa „Top 1,000,000 Sites“ als CSV-Datei
http://s3.amazonaws.com/alexa-static/top-1m.csv.zip

[4] Liste der 100 größten deutschen Kreditinstitute
http://www.bankenverband.de/service/statistik-service/banken/strukturdaten-die-100-groesten-deutschen-kreditinstitute

[5] HTTP Strict Transport Security Whitepaper, SecureNet
http://www.securenet.de/fileadmin/papers/HTTP_Strict_Transport_Security_HSTS_Whitepaper.pdf

[6] HTTP Strict Transport Security, OWASP
https://www.owasp.org/index.php/HTTP_Strict_Transport_Security

5 ÄNDERUNGSHISTORIE

5.11.2012	V1.1	Korrektur der Tabelle auf S. 3: max-age Werte waren teilweise falsch berechnet
2.11.2012	V1.0	Initiales Release

Über SecureNet

Die SecureNet GmbH ist Softwarehaus und Rundum-Dienstleister für Web Application Security. Seit 8 Jahren führt SecureNet Penetrationstests, Codeanalysen sowie umfassende Beratung zum Aufbau der Softwaresicherheit durch und gibt in Best-Practice-Seminaren die Erfahrungen an Entwickler, Sicherheits- und Fachverantwortliche weiter.

www.securenet.de