

sslstrip und HSTS



Sven Schleier

OWASP Stammtisch München, 18. Februar 2014

sslstrip und HSTS

Sven Schleier

Der Angriff

Vorführung sslstrip

Vorstellung sslstrip

Die Gegenmaßnahme

HSTS-Header - Syntax

HSTS-Header - Details

Zertifikatswarnung - ohne HSTS

Zertifikatswarnung - mit HSTS

Adressierte Bedrohungen

Preloaded HSTS Sites

Implementierung in Browsern

Die Auswertung

BlackHat 2010

Vorgehensweise

Von 10/2012

Von 01/2014

Deutsche Seiten und Banken Seiten

HSTS - Die Lösung?

Referenzen

Inhaltsverzeichnis

Der Angriff

Die Gegenmaßnahme

Die Auswertung

HSTS - Die Lösung?

Referenzen

sslstrip und HSTS

Sven Schleier

Der Angriff

Vorführung sslstrip

Vorstellung sslstrip

Die
Gegenmaßnahme

HSTS-Header - Syntax

HSTS-Header - Details

Zertifikatswarnung - ohne
HSTS

Zertifikatswarnung - mit
HSTS

Adressierte Bedrohungen

Preloaded HSTS Sites

Implementierung in
Browsem

Die Auswertung

BlackHat 2010

Vorgehensweise

Von 10/2012

Von 01/2014

Deutsche Seiten und
Banken Seiten

HSTS - Die
Lösung?

Referenzen

Vorführung sslstrip

- ▶ Vorführung von sslstrip

sslstrip und HSTS

Sven Schleier

Der Angriff

Vorführung sslstrip

Vorstellung sslstrip

Die Gegenmaßnahme

HSTS-Header - Syntax

HSTS-Header - Details

Zertifikatswarnung - ohne HSTS

Zertifikatswarnung - mit HSTS

Adressierte Bedrohungen

Preloaded HSTS Sites

Implementierung in Browsern

Die Auswertung

BlackHat 2010

Vorgehensweise

Von 10/2012

Von 01/2014

Deutsche Seiten und Banken Seiten

HSTS - Die Lösung?

Referenzen

Vorführung sslstrip

- ▶ Vorführung von sslstrip
- ▶ # arpspoof -i <interface>-t <targetIP><gatewayIP>

sslstrip und HSTS

Sven Schleier

Der Angriff

Vorführung sslstrip

Vorstellung sslstrip

Die Gegenmaßnahme

HSTS-Header - Syntax

HSTS-Header - Details

Zertifikatswarnung - ohne HSTS

Zertifikatswarnung - mit HSTS

Adressierte Bedrohungen

Preloaded HSTS Sites

Implementierung in Browsern

Die Auswertung

BlackHat 2010

Vorgehensweise

Von 10/2012

Von 01/2014

Deutsche Seiten und Banken Seiten

HSTS - Die Lösung?

Referenzen

Vorführung sslstrip

- ▶ Vorführung von sslstrip
- ▶ # arpspoof -i <interface>-t <targetIP><gatewayIP>
- ▶ # iptables -t nat -A PREROUTING -p tcp
-destination-port 80 -j REDIRECT --to-port 10000

sslstrip und HSTS

Sven Schleier

Der Angriff

Vorführung sslstrip

Vorstellung sslstrip

Die Gegenmaßnahme

HSTS-Header - Syntax

HSTS-Header - Details

Zertifikatswarnung - ohne HSTS

Zertifikatswarnung - mit HSTS

Adressierte Bedrohungen

Preloaded HSTS Sites

Implementierung in Browsern

Die Auswertung

BlackHat 2010

Vorgehensweise

Von 10/2012

Von 01/2014

Deutsche Seiten und Banken Seiten

HSTS - Die Lösung?

Referenzen

Vorführung sslstrip

- ▶ Vorführung von sslstrip
- ▶ # arpspoof -i <interface>-t <targetIP><gatewayIP>
- ▶ # iptables -t nat -A PREROUTING -p tcp
-destination-port 80 -j REDIRECT --to-port 10000
- ▶ # sslstrip.py -l 10000

sslstrip und HSTS

Sven Schleier

Der Angriff

Vorführung sslstrip

Vorstellung sslstrip

Die Gegenmaßnahme

HSTS-Header - Syntax

HSTS-Header - Details

Zertifikatswarnung - ohne HSTS

Zertifikatswarnung - mit HSTS

Adressierte Bedrohungen

Preloaded HSTS Sites

Implementierung in Browsern

Die Auswertung

BlackHat 2010

Vorgehensweise

Von 10/2012

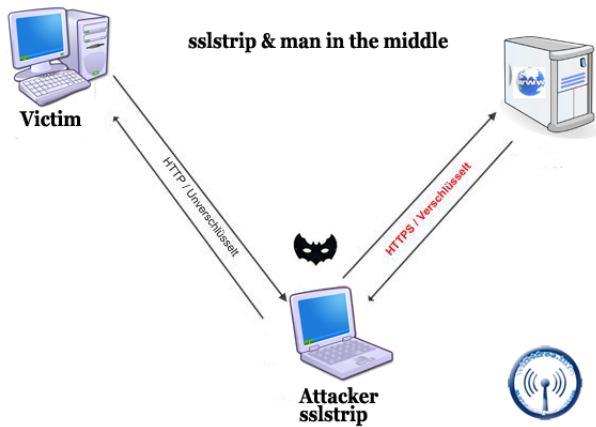
Von 01/2014

Deutsche Seiten und Banken Seiten

HSTS - Die Lösung?

Referenzen

sslstrip in Aktion [3]



Vorstellung sslstrip

- ▶ Moxie Marlinspike stellt das Tool sslstrip auf der Black Hat DC 2009 vor [4]
- ▶ sslstrip ist ein MitM Angriff der alle HTTPS:// Links mit HTTP:// austauscht [5]
- ▶ Dadurch wird der Aufbau einer SSL/TLS Verschlüsselung verhindert
- ▶ Kein Angriff auf die Verschlüsselung selbst



HSTS-Header - Syntax

```
GET /ServiceLogin HTTP/1.1
Host: accounts.google.com
...
```

```
HTTP/1.1 200 OK
...
```

```
Strict-Transport-Security: max-age
=10893354; includeSubDomains
```

Der Angriff

[Vorführung sslstrip](#)

[Vorstellung sslstrip](#)

Die Gegenmaßnahme

HSTS-Header - Syntax

[HSTS-Header - Details](#)

[Zertifikatswarnung - ohne HSTS](#)

[Zertifikatswarnung - mit HSTS](#)

[Adressierte Bedrohungen](#)

[Preloaded HSTS Sites](#)

[Implementierung in Browsern](#)

Die Auswertung

[BlackHat 2010](#)

[Vorgehensweise](#)

[Von 10/2012](#)

[Von 01/2014](#)

[Deutsche Seiten und Banken Seiten](#)

HSTS - Die Lösung?

Referenzen

HSTS-Header - Details

- ▶ HSTS ist in RFC 6797 beschrieben und ist im Moment ein Proposed Standard der IETF [2]
- ▶ max-age Direktive muss angegeben werden, include subdomains ist optional [8]
- ▶ Browser ruft nach setzen des Headers die Seite nur noch per HTTPS auf
- ▶ Zertifikatswarnungen können nicht mehr umgangen werden

sslstrip und HSTS

Sven Schleier

Der Angriff

Vorführung sslstrip

Vorstellung sslstrip

Die Gegenmaßnahme

HSTS-Header - Syntax

HSTS-Header - Details

Zertifikatswarnung - ohne HSTS

Zertifikatswarnung - mit HSTS

Adressierte Bedrohungen

Preloaded HSTS Sites

Implementierung in Browsern

Die Auswertung

BlackHat 2010

Vorgehensweise

Von 10/2012

Von 01/2014

Deutsche Seiten und Banken Seiten

HSTS - Die Lösung?

Referenzen

Zertifikatswarnung - ohne HSTS



Das Sicherheitszertifikat der Website ist nicht vertrauenswürdig!

Sie haben versucht, auf **localhost** zuzugreifen, der Server hat sich jedoch mit einem Zertifikat ausgewiesen, das von einer Entität ausgestellt wurde, der das Betriebssystem des Computers nicht vertraut. Dies bedeutet möglicherweise, dass der Server seine eigenen Sicherheitsinformationen erzeugt hat, auf die Google Chrome als Identitätsinformation nicht vertrauen kann, oder dass ein Hacker versucht, Ihre Kommunikation abzufangen.

Fahren Sie nicht fort, insbesondere wenn diese Warnung für diese Website vorher noch nie erschienen ist.

Trotzdem fortfahren

Zurück zu sicherer Website

► [Mehr Infos dazu](#)

Der Angriff

Vorführung sslstrip

Vorstellung sslstrip

Die Gegenmaßnahme

HSTS-Header - Syntax

HSTS-Header - Details

Zertifikatswarnung - ohne HSTS

Zertifikatswarnung - mit HSTS

Adressierte Bedrohungen

Preloaded HSTS Sites

Implementierung in Browsern

Die Auswertung

BlackHat 2010

Vorgehensweise

Von 10/2012

Von 01/2014

Deutsche Seiten und Banken Seiten

HSTS - Die Lösung?

Referenzen

Zertifikatswarnung - mit HSTS



Das Sicherheitszertifikat der Website ist nicht vertrauenswürdig!

Sie haben versucht, auf **localhost** zuzugreifen, der Server hat sich jedoch mit einem Zertifikat ausgewiesen, das von einer Entität ausgestellt wurde, der das Betriebssystem des Computers nicht vertraut. Dies bedeutet möglicherweise, dass der Server seine eigenen Sicherheitsinformationen erzeugt hat, auf die Google Chrome als Identitätsinformation nicht vertrauen kann, oder dass ein Hacker versucht, Ihre Kommunikation abzufangen.

Sie können nicht fortfahren, da der Betreiber der Website die Sicherheitsvorkehrungen für diese Domain erhöht hat.

Zurück

► [Mehr Infos dazu](#)

Der Angriff

Vorführung sslstrip

Vorstellung sslstrip

Die Gegenmaßnahme

HSTS-Header - Syntax

HSTS-Header - Details

Zertifikatswarnung - ohne HSTS

Zertifikatswarnung - mit HSTS

Adressierte Bedrohungen

Preloaded HSTS Sites

Implementierung in Browsern

Die Auswertung

BlackHat 2010

Vorgehensweise

Von 10/2012

Von 01/2014

Deutsche Seiten und Banken Seiten

HSTS - Die Lösung?

Referenzen

Adressierte Bedrohungen

- ▶ Passive Netzwerk Attacken
 - ▶ tcpdump (für Nerds)
 - ▶ Firesheep (einfachere Alternative)
 - ▶ Attacken werden unterstützt durch Setzen von falschen Bookmarks, HTTP Links in HTTPS-Applikationen
- ▶ Aktive Netzwerk Attacken
 - ▶ sslstrip
 - ▶ Rogue Access Point um MiTM-Angriffe auszuführen
- ▶ Web Site Entwicklung und Deployment Fehler
 - ▶ Mixed-Content
 - ▶ kaputte SSL-Zertifikate
- ▶ Phishing, Malware und Browser Schwachstellen weiterhin ausnutzbar

Der Angriff

[Vorführung sslstrip](#)

[Vorstellung sslstrip](#)

Die Gegenmaßnahme

[HSTS-Header - Syntax](#)

[HSTS-Header - Details](#)

[Zertifikatswarnung - ohne HSTS](#)

[Zertifikatswarnung - mit HSTS](#)

Adressierte Bedrohungen

[Preloaded HSTS Sites](#)

[Implementierung in Browsern](#)

Die Auswertung

[BlackHat 2010](#)

[Vorgehensweise](#)

[Von 10/2012](#)

[Von 01/2014](#)

[Deutsche Seiten und Banken Seiten](#)

HSTS - Die Lösung?

Referenzen

Preloaded HSTS Sites

- ▶ Die allererste Verbindung zur Webseite MUSS über eine gesicherte Verbindung erfolgen.
- ▶ Benutzer ist wieder verwundbar, z.B. nach Neuinstallation von Betriebssystem
- ▶ Fest verankerte Liste in Firefox und Chrome [6]
- ▶ HSTS out-of-the-box für Google, Paypal, Twitter usw.
- ▶ Jede Webseite kann auf die HSTS Preloaded List aufgenommen werden.

Der Angriff

Vorführung sslstrip

Vorstellung sslstrip

Die Gegenmaßnahme

HSTS-Header - Syntax

HSTS-Header - Details

Zertifikatswarnung - ohne HSTS

Zertifikatswarnung - mit HSTS

Adressierte Bedrohungen

Preloaded HSTS Sites

Implementierung in Browsern

Die Auswertung

BlackHat 2010

Vorgehensweise

Von 10/2012

Von 01/2014

Deutsche Seiten und Banken Seiten

HSTS - Die Lösung?

Referenzen

Implementierung in Browsern [1]

► Show options ■ = Supported ■ = Not supported ■ = Partially supported ■ = Support unknown

Strict Transport Security - other **-Usage stats:** **Global**
 Support: 53.94%

Declare that a website is only accessible over a secure connection (HTTPS).

Show all versions	IE	Firefox	Chrome	Safari	Opera	iOS Safari	Opera Mini	Android Browser	Blackberry Browser	IE Mobile
								2.1		
								2.2		
						3.2		2.3		
						4.0-4.1		3.0		
						4.2-4.3		4.0		
	8.0			5.1		5.0-5.1		4.1		
	9.0			6.0				4.2-4.3		
	10.0	26.0	31.0	6.1		6.0-6.1		4.3	7.0	
Current	11.0	27.0	32.0	7.0	19.0	7.0	5.0-7.0	4.4	10.0	10.0
Near future		28.0	33.0		20.0					
Farther future		29.0	34.0		21.0					
3 versions ahead		30.0	35.0							

Notes Known issues (0) Resources (3) Feedback [Edit on GitHub](#)

The HTTP header is 'Strict-Transport-Security'.

Der Angriff

- Vorführung sslstrip
- Vorstellung sslstrip

Die Gegenmaßnahme

- HSTS-Header - Syntax
- HSTS-Header - Details
- Zertifikatswarnung - ohne HSTS
- Zertifikatswarnung - mit HSTS
- Adressierte Bedrohungen
- Preloaded HSTS Sites

Implementierung in Browsern

Die Auswertung

- BlackHat 2010
- Vorgehensweise
- Von 10/2012
- Von 01/2014
- Deutsche Seiten und Banken Seiten

HSTS - Die Lösung?

Referenzen

Auswertung von 2010 - Qualys SSL Labs

Strict Transport Security (STS)

Only **12** trusted sites seem to support Strict Transport Security (STS)

- Supported by further 3 untrusted sites
- STS allows sites to say that they do not want plain-text traffic
- Just send a Strict-Transport-Security response header from the SSL portion of the site
- Supported in Chrome and Firefox with NoScript
- Internet draft
<http://tools.ietf.org/html/draft-hodges-strict-transport-sec>

Sites that support STS
secure.greputar.com
secure.information.com
www.aodet.com
www.datamerica.com
www.defcon.org
www.elanex.biz
www.feistyduck.com
www.paypal.com
www.squareup.com
www.sslabs.com
www.strongspace.com
www.volpescanner.com

sslstrip und HSTS

Sven Schleier

Der Angriff

Vorführung sslstrip
Vorstellung sslstrip

Die Gegenmaßnahme

HSTS-Header - Syntax
HSTS-Header - Details
Zertifikatswarnung - ohne HSTS
Zertifikatswarnung - mit HSTS
Adressierte Bedrohungen
Preloaded HSTS Sites
Implementierung in Browsern

Die Auswertung

BlackHat 2010
Vorgehensweise
Von 10/2012
Von 01/2014
Deutsche Seiten und Banken Seiten

HSTS - Die Lösung?

Referenzen

Vorgehensweise

- ▶ Grundlage ist die Alexa Top 1 Millionen
- ▶ Perl-Skript das an alle Domains einen HEAD-Request ausführt
- ▶ Zusätzlich GET-Request, der in Response nach Links mit password, login usw. sucht

sslstrip und HSTS

Sven Schleier

Der Angriff

Vorführung sslstrip

Vorstellung sslstrip

Die Gegenmaßnahme

HSTS-Header - Syntax

HSTS-Header - Details

Zertifikatswarnung - ohne HSTS

Zertifikatswarnung - mit HSTS

Adressierte Bedrohungen

Preloaded HSTS Sites

Implementierung in Browsern

Die Auswertung

BlackHat 2010

Vorgehensweise

Von 10/2012

Von 01/2014

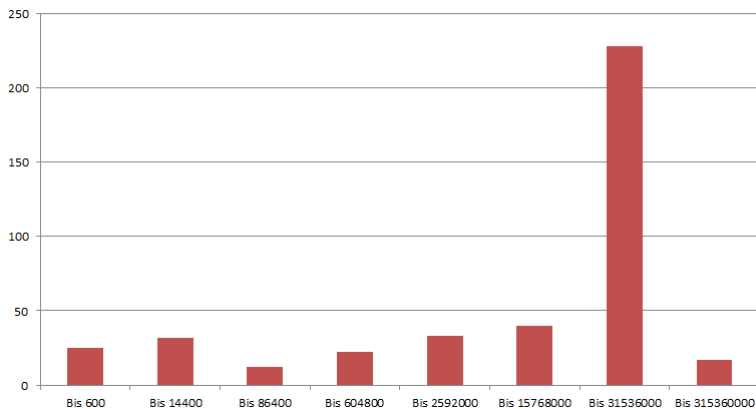
Deutsche Seiten und Banken Seiten

HSTS - Die Lösung?

Referenzen

Auswertung von Oktober 2012 [7]

Aufteilung max-age Werte



Der Angriff

Vorführung sslstrip
Vorstellung sslstrip

Die Gegenmaßnahme

HSTS-Header - Syntax
HSTS-Header - Details
Zertifikatswarnung - ohne HSTS
Zertifikatswarnung - mit HSTS
Adressierte Bedrohungen
Preloaded HSTS Sites
Implementierung in Browsern

Die Auswertung

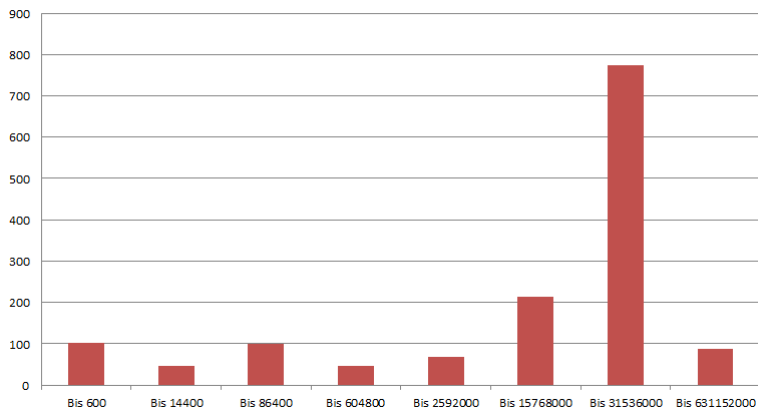
BlackHat 2010
Vorgehensweise
Von 10/2012
Von 01/2014
Deutsche Seiten und Banken Seiten

HSTS - Die Lösung?

Referenzen

Auswertung von Januar 2014

Aufteilung max-age Werte



Der Angriff

Vorführung sslstrip
Vorstellung sslstrip

Die Gegenmaßnahme

HSTS-Header - Syntax
HSTS-Header - Details
Zertifikatswarnung - ohne HSTS
Zertifikatswarnung - mit HSTS
Adressierte Bedrohungen
Preloaded HSTS Sites
Implementierung in Browsern

Die Auswertung

BlackHat 2010
Vorgehensweise
Von 10/2012
Von 01/2014
Deutsche Seiten und Banken Seiten

HSTS - Die Lösung?

Referenzen

Verbreitung von HSTS bei Banken und Deutschen Webseiten

- ▶ Deutsche Seiten (insgesamt 40471 deutsche Seiten aus Alexa Top 1 Millionen)
 - ▶ Oktober 2012: 12 Seiten mit HSTS Header
 - ▶ Februar 2014: 112 Seiten mit HSTS Header
- ▶ Bank Webseiten (insgesamt 423 Webseiten von deutschen Banken)
 - ▶ Oktober 2012: 4 Seiten mit HSTS Header
 - ▶ Februar 2014: 7 Seiten mit HSTS Header

HSTS - Die Lösung?

- ▶ HSTS ist nur ein kleiner Baustein zur Sicherstellung einer sicheren Verbindung über SSL/TLS
- ▶ HTTPS Everywhere von EFF
- ▶ Preloaded Lists in Firefox und Chrome [6]
- ▶ Certificate Pinning
- ▶ Awareness bei Benutzern (Bookmarks setzen, auf das 'Schloss' achten usw.)

sslstrip und HSTS

Sven Schleier

Der Angriff

[Vorführung sslstrip](#)

[Vorstellung sslstrip](#)

Die Gegenmaßnahme

[HSTS-Header - Syntax](#)

[HSTS-Header - Details](#)

[Zertifikatswarnung - ohne HSTS](#)

[Zertifikatswarnung - mit HSTS](#)

[Adressierte Bedrohungen](#)

[Preloaded HSTS Sites](#)

[Implementierung in Browsern](#)

Die Auswertung

[BlackHat 2010](#)

[Vorgehensweise](#)

[Von 10/2012](#)

[Von 01/2014](#)

[Deutsche Seiten und Banken Seiten](#)

HSTS - Die Lösung?

Referenzen

Ende...

► Noch Fragen?

sslstrip und HSTS

Sven Schleier

Der Angriff

Vorführung sslstrip

Vorstellung sslstrip

Die
Gegenmaßnahme

HSTS-Header - Syntax

HSTS-Header - Details

Zertifikatswarnung - ohne
HSTS

Zertifikatswarnung - mit
HSTS

Adressierte Bedrohungen

Preloaded HSTS Sites

Implementierung in
Browsem

Die Auswertung

BlackHat 2010

Vorgehensweise

Von 10/2012

Von 01/2014

Deutsche Seiten und
Banken Seiten

HSTS - Die
Lösung?

Referenzen

Referenzen I

- [1] caniuse.com.
aktuelle verbreitung von hsts in browsern.
<http://caniuse.com/#search=hsts>, February 2014.
- [2] IETF.
rfc 6797.
<https://tools.ietf.org/html/rfc6797>, November 2012.
- [3] jahfire.
Abbildung zu sslstrip angriff.
<http://forum.wifi4free.info/bilder/backtrack/ettercapsslstriphttpspwsnif/sslstrip.png>,
February 2014.

Der Angriff

Vorführung sslstrip

Vorstellung sslstrip

Die Gegenmaßnahme

HSTS-Header - Syntax

HSTS-Header - Details

Zertifikatswarnung - ohne HSTS

Zertifikatswarnung - mit HSTS

Adressierte Bedrohungen

Preloaded HSTS Sites

Implementierung in Browsern

Die Auswertung

BlackHat 2010

Vorgehensweise

Von 10/2012

Von 01/2014

Deutsche Seiten und Banken Seiten

HSTS - Die Lösung?

Referenzen II

- [4] Moxie Marlinspike.
blackhat präsentation von sslstrip.
<https://www.blackhat.com/presentations/bh-dc-09/Marlinspike/BlackHat-DC-09-Marlinspike-Defeating-SSL.pdf>,
August 2009.
- [5] Moxie Marlinspike.
sslstrip projekt.
<http://www.thoughtcrime.org/software/sslstrip/>,
February 2014.

sslstrip und HSTS

Sven Schleier

Der Angriff

Vorführung sslstrip

Vorstellung sslstrip

Die Gegenmaßnahme

HSTS-Header - Syntax

HSTS-Header - Details

Zertifikatswarnung - ohne HSTS

Zertifikatswarnung - mit HSTS

Adressierte Bedrohungen

Preloaded HSTS Sites

Implementierung in Browsern

Die Auswertung

BlackHat 2010

Vorgehensweise

Von 10/2012

Von 01/2014

Deutsche Seiten und Banken Seiten

HSTS - Die Lösung?

Referenzen

Referenzen III

- [6] The Chromium Projects.
preloaded lists in chrome und firefox.
<http://dev.chromium.org/sts>, February 2014.
- [7] Sven Schleier und Thomas Schreiber.
Hsts verbreitung.
http://www.securenet.de/fileadmin/papers/HTTP_Strict_Transport_Security_HSTS_Verbreitung.pdf, November 2012.
- [8] Sven Schleier und Thomas Schreiber.
Hsts whitepaper.
http://www.securenet.de/fileadmin/papers/HTTP_Strict_Transport_Security_HSTS_Whitepaper.pdf, November 2012.

Der Angriff

Vorführung sslstrip

Vorstellung sslstrip

Die Gegenmaßnahme

HSTS-Header - Syntax

HSTS-Header - Details

Zertifikatswarnung - ohne HSTS

Zertifikatswarnung - mit HSTS

Adressierte Bedrohungen

Preloaded HSTS Sites

Implementierung in Browsern

Die Auswertung

BlackHat 2010

Vorgehensweise

Von 10/2012

Von 01/2014

Deutsche Seiten und Banken Seiten

HSTS - Die Lösung?