La sécurité de demain dans le web d'aujourd'hui : mission impossible ?

@aeris, 06 octobre 2017

Aeris

Groupe cyber-terroriste individuel
auto-radicalisé sur le darknet digital

Mail / Jabber : aeris@imirhil.fr
Mastodon : aeris@social.imirhil.fr

Blog : https://blog.imirhil.fr/
Conférences : https://confs.imirhil.fr/

GPG : EFB7 4277 ECE4 E222
OTR : 5769 616D 2D3D AC72

Devops chez

Sommaire

- Pourquoi ?
- HTTPS
  - HSTS
  - HPKP
  - DNSSec - DANE/TLSA
- Contenu
  - Sub-Resource Integrity
  - Content Security Policy
  - Misc
- Conclusion

Pourquoi ?

10 ans en arrière :

- PC fixe
- RJ45

Pourquoi ?

10 ans en arrière :

- PC fixe
- RJ45

Aujourd'hui :

- Mobilité : 3G/4G ou Wifi
- MitM par le FAI (SFR, Bouygues, SwissCom...)
- Injection de contenu (companies aériennes...)
- Dictatures (Turquie, Egypte...)
- Surveillance de masse

Pourquoi ?

⇒ Réseaux non fiables

On n'est plus dans le réseau « Bisounours » d'il y a 10 ans…

- DroidSheep
- SSLStrip

⇒ Besoin de protections

Protection du tuyau : HTTPS

HTTP Strict Transport Security (HSTS)

RFC 6797 (novembre 2012 😳)

```
$ http --head https://imirhil.fr/ | grep ^Strict-Transport-Security:
Strict-Transport-Security: max-age=31536000; \
        includeSubDomains; preload;
```

En-tête HTTP = site HTTPS **only**

Conversion HTTP→HTTPS auto

« Trust On Firt Use » (TOFU)

Préchargement navigateurs https://hstspreload.org/

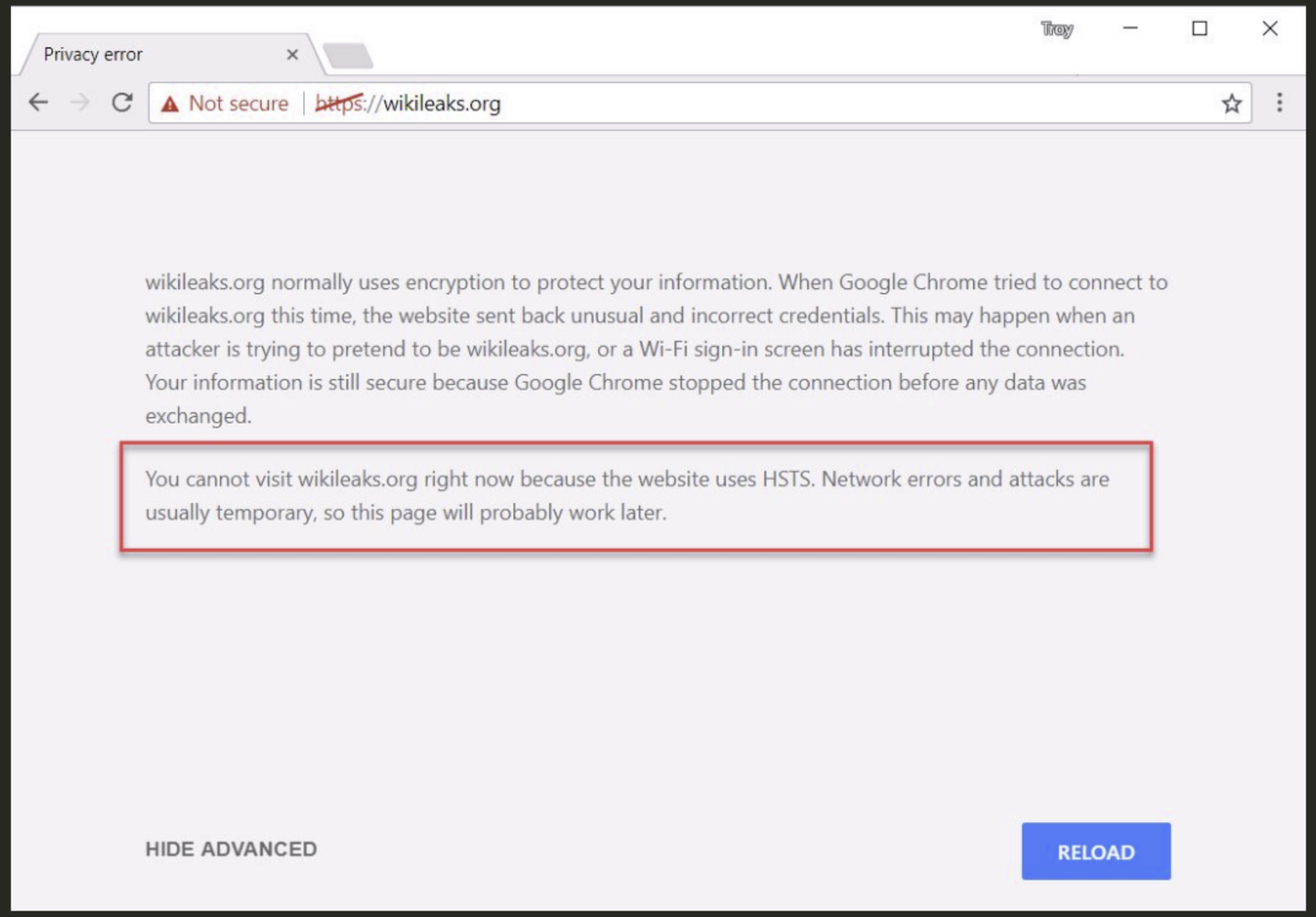
HTTP Strict Transport Security (HSTS)

- ✅ Pas/peu de risque de mise-en-place
- Marche arrière difficile, surtout si preload

HTTP Strict Transport Security (HSTS)

- ✅ Pas/peu de risque de mise-en-place
- Marche arrière difficile, surtout si preload

À mettre en prod pour hier !



31/08/2017 : détournement DNS de Wikileaks

HTTP Public Key Pinning (HPKP)

RFC 7469 (avril 2015)

```
$ http --head https://imirhil.fr/ | grep ^Public-Key-Pins:
Public-Key-Pins: max-age=5184000; \
        pin-sha256="wdkD38iQQzxE7g0RpmN8VoaIqX7YmPWwoueD9Iqawfg="; \
        pin-sha256="EswdUzfH2N8sx6Nb4Vr9gamtNF5VWQxLWUG0gDIPVLw="
```

En-tête HTTP = certificat utilisé

Épingle CA, intermédiaire ou final

« Trust On Firt Use » (TOFU)

Backup obligatoire

HTTP Public Key Pinning (HPKP)

✅ Pas/peu de risque de mise-en-place

- Retour arrière difficile
- Bien maîtriser le rollover (erreur = injoignable)

HTTP Public Key Pinning (HPKP)

✅ Pas/peu de risque de mise-en-place

- Retour arrière difficile
- Bien maîtriser le rollover (erreur = injoignable)

⛔ (Très) risqué (sur un site réel…)

- Répartition de charge / CDN
- Incompréhension écosystème X.509

HTTP Public Key Pinning (HPKP)

✅ Pas/peu de risque de mise-en-place

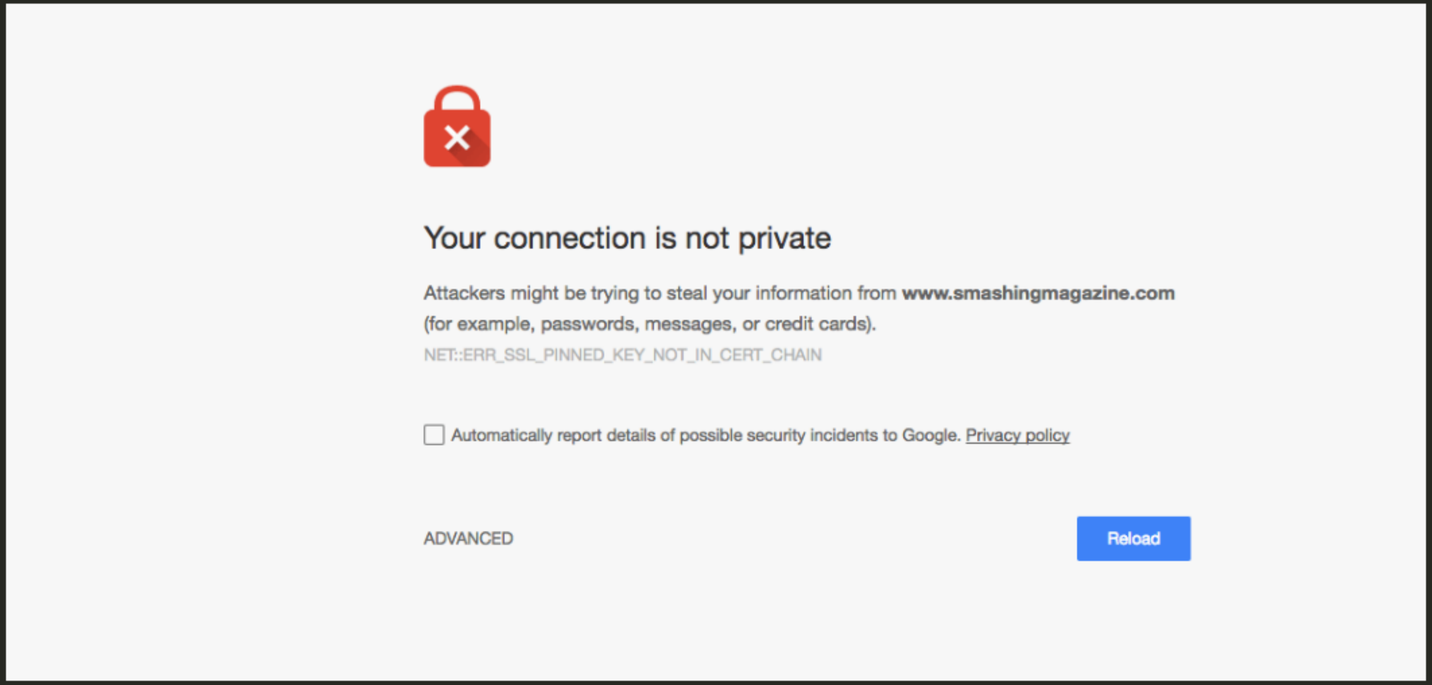
- Retour arrière difficile
- Bien maîtriser le rollover (erreur = injoignable)

⛔ (Très) risqué (sur un site réel…)

- Répartition de charge / CDN
- Incompréhension écosystème X.509

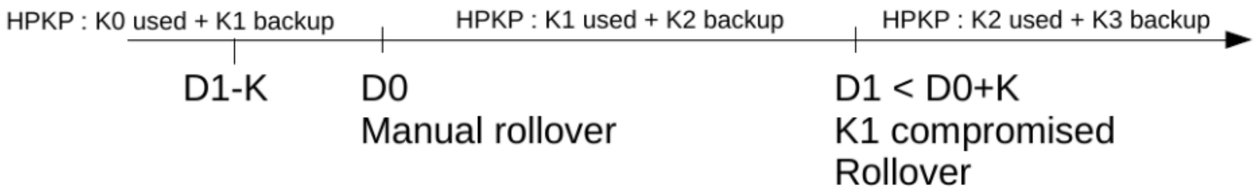
Devrait être en prod demain !

- Reprendre le contrôle de la chaîne de publication



21-25/10/2016 : erreur de déploiement Smash Magazine

HPKP expiration : K days



Visitors at D1 :

- last visit < D1-K : HPKP expired, OK
- D1-K < last visit < D0 : HPKP in memory K0 + K1, key in use K2, KO
- D0 < last visit : HPKP in memory K1 + K2, key in use K2, OK

You can rollover again with HPKP only at least K days after the last rollover !!!

Rollover

Simple chaîne / double chaîne

Sécurité proche du contenu lui-même

- sécurité ⇒ contenu : level noob
  - Accès aux entêtes = accès au contenu
- contenu ⇒ sécurité : level avancé
  - Backend proche du reverse

Simple chaîne / double chaîne

Sécurité proche du contenu lui-même

- sécurité ⇒ contenu : level noob
  - Accès aux entêtes = accès au contenu
- contenu ⇒ sécurité : level avancé
  - Backend proche du reverse

Nécessité d'une double chaîne

- accès au contenu sans accès à la sécurité
- accès à la sécurité sans accès au contenu

Simple chaîne / double chaîne

Sécurité proche du contenu lui-même

- sécurité ⇒ contenu : level noob
  - Accès aux entêtes = accès au contenu
- contenu ⇒ sécurité : level avancé
  - Backend proche du reverse

Nécessité d'une double chaîne

- accès au contenu sans accès à la sécurité
- accès à la sécurité sans accès au contenu

⇒ DNS

DNSSec

RFC 4033 (mars 2005 😳😳)

Signature cryptographique de la chaîne DNS

DNSSec

```
└─> $ dig imirhil.fr +dnssec +trace

; <<>> DiG 9.10.3-P4-Debian <<>> imirhil.fr +dnssec +trace
;; global options: +cmd
.                       482017  IN      NS      a.root-servers.net.
.                       482017  IN      RRSIG   NS 8 0 518400 20170901050000 20170819040000 15768 . UBnghhnvvCHstU94
RqeO9Hk8GsP/ujuTdPI/3mcUK2Kb/HQF8Q55aeaF dsgBh5QLxSFGLeTd4dXNl6GaMMeiLar4r3mFagEiEvHqrxumvOgCLksa dg4fZjbU975LTpjmoY
hkdvlz8RV/fokyznOO2skbaBI9fNjdfBoVcD29 AVvPnMKmlgV3Qam+KFiKOc30PGkVqLz3fa9irij+YvCq8IbHqLt2bFfX FaPXZnXcG8vB8aDjolvE
ovuReKfETKJhlahTJYgOpIPDNTLLrE0WkxIO XdiiGVYCRzxwFX7HsyQas/SJCpsH48P1iJ5EEQAsDg6H5ZQDatEaRRix OLyttw==
;; Received 525 bytes from 127.0.0.1#53(127.0.0.1) in 0 ms

fr.                     172800  IN      NS      d.ext.nic.fr.
fr.                     86400   IN      DS      9392 8 2 BAE7AB5D1604A18AB4DBDE018A3C12142E4EDBECE8AFC0E207901886 B2
DD2292
fr.                     86400   IN      DS      35095 8 2 23C6CAADC9927EE98061F2B52C9B8DA6B53F3F648F814A4A86A0FAF9 8
43E2C4E
fr.                     86400   IN      RRSIG   DS 8 1 86400 20170901170000 20170819160000 15768 . bl/AnC+AxeXinXn2e
I1M7ow9cmS6I2k5w563S5o/4ZDf8ePfAbEUOEXI 9Bf34XSVpZi9qmnpgewTaMulU0eMKZVqRBbQVuvzRJIXbuBUMWXDb6LJ Ek2fIl/IKw7NSE901yc
ua1lxTg/xMhPP5rj66OODIhxlgTn7L1P2mi8A SgDibiQ2dNO1bYkbSSIbPqfv4O65bETlhigwIGiNlU7QqiYP2Tjx8Zu0 RnPztT/MkMRPSr2/NB1on
+oY+Bw8FXnS8ltXrOmwIwKTpJuFs7XvF7gD x6w3OHuxZDeKv50RWAFyafIQKgteHH9G7/OkIUYwslUYzmPt+XTkll14 YRaVvw==
;; Received 730 bytes from 192.58.128.30#53(j.root-servers.net) in 51 ms

imirhil.fr.             172800  IN      NS      nssec.online.net.
imirhil.fr.             172800  IN      NS      tatooine.imirhil.fr.
imirhil.fr.             172800  IN      DS      7480 8 2 66AFFDB43AE010A81A770FB37A6BD03153295309E8D150DB0C836A58 4B
357290
imirhil.fr.             172800  IN      RRSIG   DS 8 2 172800 20171015063022 20170816063022 8235 fr. D+CRJ5H6tDv4OpI
6jq3LAS9e5VrlyLckdzXMAzpvQdgcqPD4z2WHv7hN ys4qc3UQXCf77gyYTuRL8eke7EbEw/tDYmvQJgXVZCv4dbi9ThpzNFK0 F28c8Wl4D1S2AQi2+
ZuS4N0ZAOQ+vJuybStI9oXF17xQhrN4ejue676N 5xg=
;; Received 318 bytes from 193.176.144.22#53(e.ext.nic.fr) in 48 ms

imirhil.fr.             3600    IN      A       163.172.46.173
imirhil.fr.             3600    IN      RRSIG   A 8 2 3600 20170901081048 20170818102922 45070 imirhil.fr. DZ3Qhe8jp
0Tq6s9VYxpAlhquc8fIW+10lLGOMAG07HeAFdV1WKjCH4+S Yoy227vmUgJkMu0Vx9K37CBS9fleAvK5V1i/LqdWBp0GWQzrRwv8XBgO +AnfmBRWjbD
AAuWOWeXY4KURzE/g8F3oYuaqVgjumAgDVC8VjACj7gbQ ziQ=
imirhil.fr.             604800  IN      NS      tatooine.imirhil.fr.
imirhil.fr.             604800  IN      NS      nssec.online.net.
imirhil.fr.             604800  IN      RRSIG   NS 8 2 604800 20170901060802 20170818042922 45070 imirhil.fr. cdWyOt
NFBBTLMrUCiex7649za4Zv5gonyQNRkYJumK2j98tqzF26ac+x QjkCls4e2xyrOvH/kZVfTdfluiL7IDskT8F4fjqC0og8s96p5Z6WOTTf eR9GdcId
TuZkRRcGaeiCQkBEM3mh2yIzey5zhRchFKl97ev1Rzo1Ik7p cZQ=
;; Received 832 bytes from 62.210.16.8#53(nssec.online.net) in 36 ms
```

DNSSec

- ✅ Pas/peu de risque de mise-en-place
- Fournit par le registre / OpenDNSSec

DNSSec

✅ Pas/peu de risque de mise-en-place

- Fournit par le registre / OpenDNSSec

💔 Peu déployé

- Peu de support côté visiteur (FAI)
- Faire les choses bien
  - PKI / stealth master DNS
  - résolveur local

DNSSec

⛔ L'enfer (sur un site réel)

- Externalisation du DNS
- Pas d'infra de gestion clef privée

DNSSec

⛔ L'enfer (sur un site réel)

- Externalisation du DNS
- Pas d'infra de gestion clef privée

Devrait être en prod après-demain

- Problème du support côté utilisateur
- 31/08/2017 : détournement DNS Wikileaks

DANE/TLSA

RFC 6698 (août 2012 😳), nécessite DNSSec

Comme HPKP, mais version DNS (plus TOFU, pas que HTTPS)

```
$ dig TLSA _443._tcp.imirhil.fr +short
1 1 2 16acc40419cef98984bf<snip>41f685c53e4911341451
```

- Usage :
  - 0/PKIX-TA = CA+X.509, 1/PKIX-EE = cert + X.509
  - 2/DANE-TA = CA, 3/DANE-EE = cert (💗 autosigné !!!)
- Sélecteur : 0 = cert, 1 = clef publique
- Correspondance : 0 = complet, 1 = SHA-256, 2 = SHA-512

DANE/TLSA

✅ Pas de risque de mise-en-place

- Bien maîtriser le rollover (erreur = injoignable)
- Facilement corrigeable (minus TTL)
- Facilement révocable (minus TTL)

💔 Peu déployé

- DNSSec…
- Pas/peu/plus de support côté navigateur
  - extension Firefox (< v57)

DANE/TLSA

⛔ Risqué (sur un site réel...)

- Répartition de charge / CDN
- Incompréhension écosystème X.509

DANE/TLSA

⛔ Risqué (sur un site réel…)

- Répartition de charge / CDN
- Incompréhension écosystème X.509

Devrait être en prod dans un mois

- Problème du support côté utilisateur
- Reprise de contrôle de la chaîne de publication

Protection du contenu

Sub-Resource Integrity (SRI)

W3C Candidate recommendation (novembre 2015)
W3C Proposed recommendation (mai 2016)
W3C Recommendation (juin 2016)

```
<link rel="stylesheet" href="https://cdn.example.com/style.css"
        integrity="sha384-+/M6kredJcxdsqkczBUjMLvqyHb1K/
                   JThDXWsBVxMEeZHEaMKEOEct339VItX1zB">
<script src="https://exemple.com/exemple-framework.js"
        integrity="sha384-oqVuAfXRKap7fdgcCY5uykM6+R9GqQ
                   8K/uxy9rx7HNQlGYl1kPzQho1wx4JwY8wC"
```

Bloque les modifications à la volée (MitM)

Bloque les compromissions (Wordpress…)

Sub-Resource Integrity (SRI)

- ✅ Pas de risque de mise-en-place

Sub-Resource Integrity (SRI)

✅ Pas de risque de mise-en-place

⛔ Risqué (sur un site réel…)

- Répartition de charge / CDN
- Pas de maîtrise des ressources

Sub-Resource Integrity (SRI)

✅ Pas de risque de mise-en-place

⛔ Risqué (sur un site réel…)

- Répartition de charge / CDN
- Pas de maîtrise des ressources

Devrait être en prod demain !

- Reprendre le contrôle de la chaîne de publication

Content Security Policy (CSP)

W3C lvl1 Candidate Recommendation (novembre 2012 😳)
W3C lvl2 Candidate Recommendation (février 2015)
W3C lvl2 Proposed Recommendation (novembre 2016)
W3C lvl2 Recommendation (décembre 2016)
W3C lvl3 Working Draft (septembre 2016)

```
$ http --head https://imirhil.fr/ | grep ^Content-Security-Policy:
Content-Security-Policy: default-src 'none'; style-src 'self';
        script-src 'self'; img-src 'self'; font-src 'self';
```

Indique ce qui est chargeable dans la page, et à partir d'où

Content Security Policy (CSP)

Contenu

- default-src
- img-src
- style-src
- script-src
- font-src
- media-src
- connect-src

Origine

- none
- self
- unsafe-inline
- unsafe-eval
- data:
- hostname

Content Security Policy (CSP)

- ✅ Peu de risque de mise-en-place
- JS & CSS inline

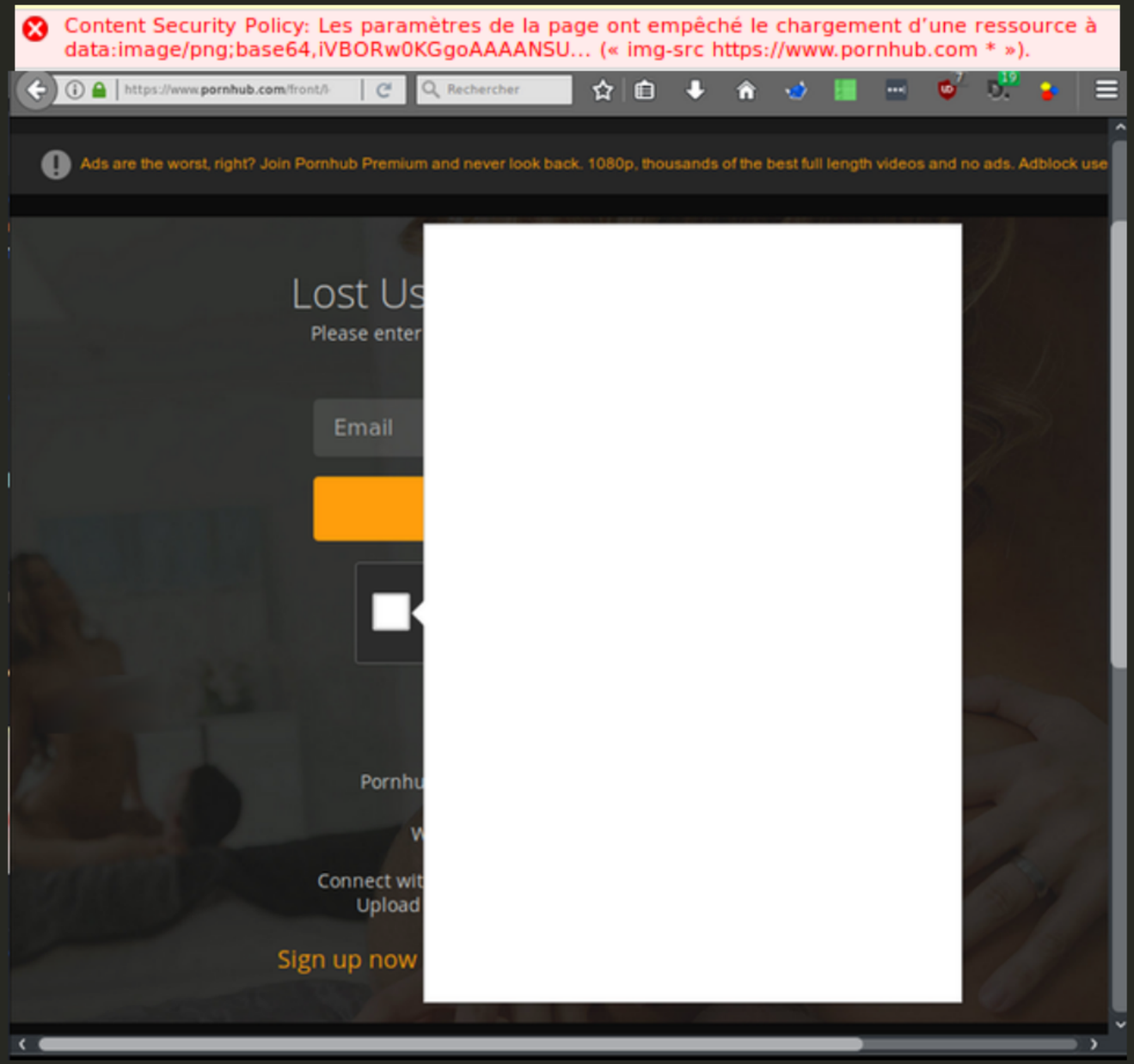
Content Security Policy (CSP)

✅ Peu de risque de mise-en-place

- JS & CSS inline

⛔ Risqué (sur un site réel…)

- Répartition de charge / CDN
- Pas de maîtrise des ressources
- 🤮 Publicité, tracking…



18/06/2017 : PornHub

Divers

Frames ✅

```
Content-Security-Policy: frame-ancestors 'none'
X-Frame-Options: DENY
```

Cross-origin Resource Sharing (CORS) ✅

```
Access-Control-Allow-Origin: <origin>
```

Cookies ✅ / ⚠️

```
Set-Cookie: Foo=Bar; Path=/; Secure; HttpOnly
```

Content type options ✅

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

Referer ✅ / ⚠️

```
Referrer-Policy: same-origin

<meta http-equiv="Referrer-Policy"
        content="no-referrer, strict-origin-when-cross-origin">
```

XSS Protection ✅

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

Comment vérifier

Recommandations Mozilla

https://wiki.mozilla.org/Security/Guidelines/Web_Security

Guideline	Security Benefit	Implementation Difficulty	Order†	Requirements	Notes
HTTPS	MAXIMUM	MEDIUM		Mandatory	Sites should use HTTPS (or other secure protocols) for all communications
TLS Configuration	MEDIUM	MEDIUM	1	Mandatory	Use the most secure Mozilla TLS configuration for your user base, typically Intermediate
Resource Loading	MAXIMUM	LOW	2	Mandatory for all websites	Both passive and active resources should be loaded through protocols using TLS, such as HTTPS
Redirections from HTTP	MAXIMUM	LOW	3	Mandatory	Websites must redirect to HTTPS, API endpoints should disable HTTP entirely
Strict Transport Security	HIGH	LOW	4	Mandatory for all websites	Minimum allowed time period of six months
X-Frame-Options	HIGH	LOW	5	Mandatory for all websites	Websites that don't use DENY or SAMEORIGIN must employ clickjacking defenses
Cross-site Request Forgery Tokenization	HIGH	UNKNOWN	6	Varies	Mandatory for websites that allow destructive changes Unnecessary for all other websites Most application frameworks have built-in CSRF tokenization to ease implementation
Cookies	HIGH	MEDIUM	7	Mandatory for all new websites Recommended for existing websites	All cookies must be set with the Secure flag, and set as restrictively as possible
X-Content-Type-Options	LOW	LOW	8	Recommended for all websites	Websites should verify that they are setting the proper MIME types for all resources
contribute.json	LOW	LOW	9	Mandatory for all new Mozilla websites Recommended for existing Mozilla sites	Mozilla sites should serve contribute.json and keep contact information up-to-date
Content Security Policy	HIGH	HIGH	10	Mandatory for new websites Recommended for existing websites	Disabling inline script is the greatest concern for CSP implementation
Cross-origin Resource Sharing	HIGH	LOW	11	Mandatory	Origin sharing headers and files should not be present, except for specific use cases
Referrer Policy	LOW	LOW	12	Recommended for all websites	Improves privacy for users, prevents the leaking of internal URLs via `Referer` header
X-XSS-Protection	LOW	MEDIUM	13	Mandatory for all new websites Recommended for existing websites	Manual testing should be done for existing websites, prior to implementation
robots.txt	LOW	LOW	14	Optional	Websites that implement robots.txt must use it only for noted purposes
Subresource Integrity	MEDIUM	MEDIUM	15	Recommended‡	‡ Only for websites that load JavaScript or stylesheets from foreign origins
Public Key Pinning	LOW	MAXIMUM	--	Mandatory for maximum risk sites only	Not recommended for most sites

Recommandations Mozilla

https://observatory.mozilla.org/

HTTP Observatory | TLS Observatory | SSH Observatory (Beta) | Third-party Tests

Scan Summary

A+

Host:	imirhil.fr
Scan ID #:	4343341
Start Time:	August 20, 2017 2:35 PM
Duration:	12 seconds
Score:	125/100
Tests Passed:	11/11

Recommended Change

Initiate Rescan

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
Content Security Policy	✔	+10	Content Security Policy (CSP) implemented with `default-src 'none'` and no `'unsafe'`
Cookies	–	0	No cookies detected
Cross-origin Resource Sharing	✔	0	Content is not visible via cross-origin resource sharing (CORS) files or headers
HTTP Public Key Pinning	✔	+5	HTTP Public Key Pinning (HPKP) header set to a minimum of 15 days (1296000)
HTTP Strict Transport Security	✔	+5	Preloaded via the HTTP Strict Transport Security (HSTS) preloading process
Redirection	✔	0	All hosts redirected to are in the HTTP Strict Transport Security (HSTS) preload list
Referrer Policy	✔	+5	Referrer-Policy header set to `"no-referrer"`, `"same-origin"`, `"strict-origin"` or `"strict-origin-when-cross-origin"`
Subresource Integrity	–	0	Subresource Integrity (SRI) is not needed since site contains no script tags
X-Content-Type-Options	✔	0	X-Content-Type-Options header set to `"nosniff"`
X-Frame-Options	✔	0	X-Frame-Options (XFO) header set to `SAMEORIGIN` or `DENY`
X-XSS-Protection	✔	0	X-XSS-Protection header set to `"1; mode=block"`

Recommandations Mozilla

https://observatory.mozilla.org/

HTTP Observatory | TLS Observatory | SSH Observatory (Beta) | Third-party Tests

Scan Summary

F

Host:	www.caisse-epargne.fr
Scan ID #:	4343362
Start Time:	August 20, 2017 2:59 PM
Duration:	11 seconds
Score:	15/100
Tests Passed:	5/11

Recommended Change

Initiate Rescan

Fantastic work using HTTPS! Did you know that you can ensure users never visit your site over HTTP accidentally?

HTTP Strict Transport Security tells web browsers to only access your site over HTTPS in the future, even if the user attempts to visit over HTTP or clicks an `http://` link.

- Mozilla Web Security Guidelines (HSTS)
- MDN on HTTP Strict Transport Security

Once you've successfully completed your change, click Initiate Rescan for the next piece of advice.

Test Scores

Test	Pass	Score	Explanation
Content Security Policy	✗	-25	Content Security Policy (CSP) header not implemented
Cookies	✗	-20	Cookies set without using the `Secure` flag or set over http
Cross-origin Resource Sharing	✓	0	Content is not visible via cross-origin resource sharing (CORS) files or headers
HTTP Public Key Pinning	–	0	HTTP Public Key Pinning (HPKP) header not implemented (optional)
HTTP Strict Transport Security	✗	-20	HTTP Strict Transport Security (HSTS) header not implemented
Redirection	✓	0	Initial redirection is to https on same host, final destination is https
Referrer Policy	–	0	Referrer-Policy header not implemented (optional)
Subresource Integrity	✗	-5	Subresource Integrity (SRI) not implemented, but all external scripts are loaded over https
X-Content-Type-Options	✗	-5	X-Content-Type-Options header not implemented
X-Frame-Options	✓	0	X-Frame-Options (XFO) header uses `ALLOW-FROM` uri directive
X-XSS-Protection	✗	-10	X-XSS-Protection header not implemented

Conclusion

Conclusion

~~Futures~~ technos sécurité = enfer dans le web actuel

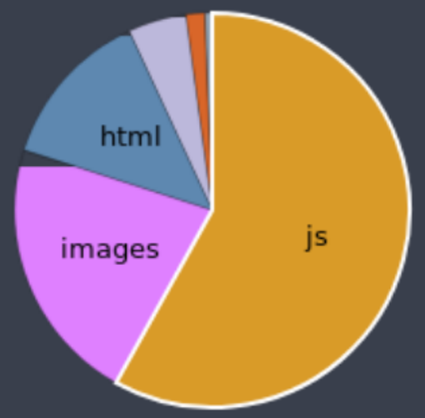
- Perte de contrôle du contenu
  - CDN
  - Contenus tiers
  - (Multiples) prestataires
- Perte de contrôle de la technique
  - (Multiples) prestataires
  - Externalisation / SaaS / « cloud »
  - (Non) formation
  - (Non) accompagnement

Un exemple dans la vraie vie

Le Figaro

```
dig NS lefigaro.fr +short
dns2.sdv.fr.
dns1.sdv.fr.

dig NS f1g.fr +short
ns3.nameshield.net.
obs.ns1.fr.
ns2.observatoiredesmarques.fr.
```



Avec mise en cache [En savoir plus]

	Type	Taille	Transfert	Temps
45	js	2 233,87 Ko	759,02 Ko	7,31 s
84	images	840,03 Ko	809,08 Ko	16,28 s
7	html	506,96 Ko	101,73 Ko	0,69 s
9	fonts	183,27 Ko	183,27 Ko	1,86 s
6	xhr	58,53 Ko	15,56 Ko	0,91 s
4	other	23,58 Ko	6,90 Ko	0,71 s

Réponses mises en cache : 0
Nombre de requêtes : 155
Taille : 3 846,24 Ko
Taille du transfert : 1 875,56 Ko
Durée : 27,77 secondes

lefigaro.fr	Tout	Cookie	CSS	Image	Plugin	Script	XHR	Frame	Autre
Domaine de la page									
lefigaro.fr	6								
bourse.lefigaro.fr							1		
plus.lefigaro.fr			2			1			
sport24.lefigaro.fr				10					
tvmag.lefigaro.fr							1		
www.lefigaro.fr	8			2		1	5		
basilic.io									
foglio.basilic.io						1			
cloudflare.com									
cdnjs.cloudflare.com						2			
d3utgaucctw1fm.cloudfront.net							1		
f1g.fr									
a.f1g.fr			14	5		19	6		
i.f1g.fr				73					
facebook.com									
www.facebook.com				2					
facebook.net									
connect.facebook.net						4			

lefigaro.fr								
Tout	Cookie	CSS	Image	Plugin	Script	XHR	Frame	Autre
google.com								
www.google.com			1					
google.fr								
www.google.fr			1					
ajax.googleapis.com					2			
fonts.googleapis.com		2						
kxcdn.com								
actorssl-5637.kxcdn.com					1			
leguide.com								
cimg.leguide.com			2					
csimg.leguide.com			16					
shoppingbox.leguide.com			1		1		1	
zebestof.com								
cdn.zebestof.com					1			
dpm.zebestof.com			1		1		1	
adnxs.com								
acdn.adnxs.com					2			
ib.adnxs.com						1		
chartbeat.com								

lefigaro.fr								
Tout	Cookie	CSS	Image	Plugin	Script	XHR	Frame	Autre
beacon.krxd.net			2		2			
cdn.krxd.net					8		2	
newrelic.com								
js-agent.newrelic.com					1			
nxtck.com					3			
outbrain.com								
amplifypixel.outbrain.com			2					
images.outbrain.com			8					
log.outbrain.com					2			
odb.outbrain.com					2			
widgets.outbrain.com			2		4		2	
scorecardresearch.com								
sb.scorecardresearch.com			2		1			
taboola.com								
trc.taboola.com			1					
weborama.fr								
cstatic.weborama.fr							1	
xiti.com								
logc111.xiti.com			2					

Certificate exchanged. Reason to be careful! (tweetdeck.twitter.com)

Alert: Hostname has changed. Take a look if that's okay.

Warning: This certificate wasn't due yet. If this site regularly uses more than one certificate, you may want to activate the 'CA only' option in the details.

Old Certification Hierarchy:

View Old Certificate

- DigiCert High Assurance EV Root CA
  - DigiCert SHA2 High Assurance Server CA
    - tweetdeck.twitter.com

New Certification Hierarchy:

View New Certificate

- DigiCert High Assurance EV Root CA
  - DigiCert SHA2 High Assurance Server CA
    - tweetdeck.com

Issued To:

Common Name (CN):	- tweetdeck.twitter.com + tweetdeck.com
Organization (O):	Twitter, Inc.
Organizational Unit (OU):	- Twitter Security + LON3 Point of Presence
MD5 Fingerprint:	- + undefined
SHA1 Fingerprint:	- 7F:93:A2:E3:90:1B:27:64:5C:A6:DC:28:59:97:93:CC:BF:9A:FE:46 + 65:5D:2F:BF:0E:EB:0C:F4:17:FA:79:0B:20:72:7D:BA:5C:AB:FD:FC
SHA256 Fingerprint:	- + 6E:CE:D0:12:EF:EF:26:BF:DA:E9:B6:DA:23:BF:0C:F7:68:D7:13:FE:F5:55:A2:31:C2:7E:B4:6C:E3:07:AF

Validity:

Issued On:	- 2015-05-20 02:00:00 (824 days ago) + 2015-01-21 01:00:00 (943 days ago)
Expires On:	- 2018-05-24 14:00:00 (277 days ahead) + 2018-01-24 13:59:59 (157 days ahead)
Stored Since:	2015-09-05 23:52:38 (715 days ago)

Apparently Issued By:

Common Name (CN):	DigiCert SHA2 High Assurance Server CA
Organization (O):	DigiCert Inc
Organizational Unit (OU):	www.digicert.com

☐ Too many pop-ups? Try checking authority only for this domain

Ignore this website | Reject | Accept

Twitter

La sécurité ~~de demain~~ d'hier
dans le web d'aujourd'hui :
mission impossible ?

La sécurité ~~de demain~~ d'hier
dans le web d'aujourd'hui :
mission impossible ?

Nécessite un web responsable !

Question ?