

web et sécurité

TP03+04

Réaliser Par : Guettouche Islam

1. Coté client

Exercice 1

L'état des cookies <http://www.google.fr> sur **Firefox**:

Cookies

Filtrer les éléments

Filtrer les valeurs

https://www.google.fr

Stockage de session

Stockage cache

Indexed DB

Stockage local

Nom	Domaine	Chemin	Expire le	Dernier accès le	Valeur	HttpOnly
1P_JAR	.google.fr	/	Thu, 14 Dec 2017 14:40:1...	Tue, 14 Nov 2017 14:40:1...	2017-11-14-14	false
CONSENT	.google.fr	/	Sun, 10 Jan 2038 07:59:59...	Tue, 14 Nov 2017 14:39:3...	YES+FR.fr+V8	false
DV	www.google.fr	/	Tue, 14 Nov 2017 14:50:1...	Tue, 14 Nov 2017 14:40:1...	A7UtYESDo3sfIO0rziNe...	false
NID	.google.fr	/	Sun, 13 May 2018 14:40:1...	Tue, 14 Nov 2017 14:40:1...	117=CFBGxuDDiP5yH5k...	true
OGPC	.google.fr	/	Sat, 13 Jan 2018 14:21:17 ...	Tue, 14 Nov 2017 14:39:3...	5061821-1:	false
OGP	.google.fr	/	Sat, 13 Jan 2018 14:21:21 ...	Tue, 14 Nov 2017 14:39:3...	-5061821:	false
SNID	.google.fr	/verify	Thu, 08 Jun 2017 14:02:17...	Wed, 07 Dec 2016 14:02:1...	91=jFyTmmuuxGk6j8G...	true

▼ Données

▼ 1P_JAR : "2017-11-14-14"

CreationTime: "Tue, 14 Nov 2017 14:20:58 GMT"

Domain: ".google.fr"

Expires: "Thu, 14 Dec 2017 14:40:17 GMT"

HostOnly: false

HttpOnly: false

LastAccessed: "Tue, 14 Nov 2017 14:40:17 GMT"

Path: "/"

Secure: false

▼ Valeur analysée

▼

1P_JAR : 1978

L'état des cookies <https://www.amazon.fr/> sur **Firefox**:

Cookies

https://images-eu.ssl-images-amazon.com

https://aax-eu.amazon-adsystem.com

https://www.amazon.fr

Stockage de session

Stockage cache

Indexed DB

Stockage local

+ ↺

Filtrer les éléments

📄

Filtrer les valeurs

Nom	Domaine	Chemin	Expire le	Dernier accès le	Valeur	HttpOnly
csm-hit	www.amazon.fr	/	Tue, 21 Nov 2017 14:32:0...	Tue, 14 Nov 2017 14:47:3...	Y2R4VHWBT9V...	false
lc-acbfr	.amazon.fr	/	Mon, 31 Dec 2035 23:00:0...	Tue, 14 Nov 2017 14:40:4...	fr_FR	false
session-id-time	.amazon.fr	/	Tue, 01 Jan 2036 08:00:01...	Tue, 14 Nov 2017 14:40:0...	20827872011	false
session-id	.amazon.fr	/	Tue, 01 Jan 2036 08:00:01...	Tue, 14 Nov 2017 14:40:0...	261-0073225-55...	false
session-token	.amazon.fr	/	Tue, 01 Jan 2036 08:00:01...	Tue, 14 Nov 2017 14:40:0...	FIGj8cWVifR1cj...	false
ubid-acbfr	.amazon.fr	/	Mon, 31 Dec 2035 23:00:0...	Tue, 14 Nov 2017 14:40:4...	261-4730583-99...	false
x-wl-uid	.amazon.fr	/	Mon, 31 Dec 2035 23:00:0...	Tue, 14 Nov 2017 14:40:4...	1gdnwKR5z9uX...	false

▼ Données

csm-hit: "Y2R4VHWBT9VGEW1T...8j1510670852949"

CreationTime: "Tue, 14 Nov 2017 14:29:57 GMT"

Domain: "www.amazon.fr"

Expires: "Tue, 21 Nov 2017 14:32:06 GMT"

HostOnly: true

HttpOnly: false

LastAccessed: "Tue, 14 Nov 2017 14:47:32 GMT"

Path: "/"

Secure: false

L'état des cookies <https://fr.wikipedia.org/wiki/Wikip%C3%A9dia> sur **Firefox**:

Cookies		+						Filtrer les éléments	Filtrer les valeurs
https://fr.wikipedia.org		Nom	Domaine	Chemin	Expire le	Dernier accès le	Valeur	HttpOnly	Données
Stockage de session	CP	fr.wikipedia.org	/	Session	Tue, 14 Nov 2017 14:40:19 GMT		H2	false	CP : "H2" CreationTime : "Tue, 14 Nov 2017 14:40:19 GMT" Domain : "fr.wikipedia.org" Expires : "Session" HostOnly : true HttpOnly : false LastAccessed : "Tue, 14 Nov 2017 14:40:19 GMT" Path : "/" Secure : true
Stockage cache	GeolIP	.wikipedia.org	/	Session	Tue, 14 Nov 2017 14:40:19 GMT		FR:NOR:Mont-...	false	
Indexed DB	WMF-Last-Acc...	.wikipedia.org	/	Sat, 16 Dec 2017 12:00:00 ...	Tue, 14 Nov 2017 14:40:19 GMT		14-Nov-2017	true	
Stockage local	WMF-Last-Acc...	fr.wikipedia.org	/	Sat, 16 Dec 2017 12:00:00 ...	Tue, 14 Nov 2017 14:40:19 GMT		14-Nov-2017	true	

L'état des cookies <https://www.fnac.com/> sur **Firefox**:

- https://fnac-by.accengage.net
- https://csync.smartadserver.com
- https://ad.turn.com
- https://ads.pubmatic.com
- https://ssum-sec.casalemedia.com
- https://rtb-csync.smartadserver.com
- https://image4.pubmatic.com
- https://image2.pubmatic.com
- https://simage2.pubmatic.com
- https://connectivity.net
- https://halc.iadvize.com
- https://www.fnac.com
- https://www4-fr.fnac-static.com

- Stockage de session
- Stockage cache
- Indexed DB
- Stockage local

+ ↺
⌵ Filtrer les éléments
⌵ Filtrer les valeurs

Nom	Domaine	Chemin	Expire le	Dernier accès le	Valeur	HttpOnly
ADRU _M _BT1	www.fnac.com	/	Tue, 14 Nov 2017 14:54:1...	Tue, 14 Nov 2017 14:53:4...	R:22[j;1118351]e...	false
ADRU _M _BTa	www.fnac.com	/	Tue, 14 Nov 2017 14:54:1...	Tue, 14 Nov 2017 14:53:4...	R:22[g;e20cce9...	false
OrderInSession	.fnac.com	/	Session	Tue, 14 Nov 2017 14:53:4...	1	false
ORGN	.fnac.com	/	Fri, 24 Nov 2017 14:53:49 ...	Tue, 14 Nov 2017 14:53:4...	fnac_google	false
PageOriginBro...	.fnac.com	/	Session	Tue, 14 Nov 2017 14:53:4...	search	false
SID	.fnac.com	/	Sun, 13 May 2018 13:53:4...	Tue, 14 Nov 2017 14:53:4...	f1acb2d8-e13c-...	false
UID	.fnac.com	/	Sun, 13 May 2018 13:53:4...	Tue, 14 Nov 2017 14:53:4...	025881303-6d7...	false

Données

ADRU_M_BT1 : "R:22[j;1118351]e:70"

CreationTime : "Tue, 14 Nov 2017 14:53:49 GMT"

Domain : "www.fnac.com"

Expires : "Tue, 14 Nov 2017 14:54:19 GMT"

HostOnly : true

HttpOnly : false

LastAccessed : "Tue, 14 Nov 2017 14:53:49 GMT"

Path : "/"

Secure : false

Valeur analysée

ADRU_M_BT1 : Array

0: "R"

1: "22[j"

2: "1118351]e"

3: "70"

length : 4

__proto__: Array

Sur **TOR**, nous n'avons aucun cookie de stocké, en revanche sur Firefox nous avons 4 cookies du domaine `fr.wikipedia.org` et 1 du domaine « wikipedia.org » :

fr.wikipedia.org

CP : Contient la valeur H2.

WMF-Last-Access : Contient la date de dernier accès au site.

frwikiGeoFeaturesUser2 : Contient une valeur hexadécimale

frwikimwuser-sessionId : Contient une valeur hexadécimale (avec le nom on devine que c'est l'identifiant de session).

wikipedia.org

GeoIP : Contient l'endroit depuis lequel on accède au site.

Remarque :

Le navigateur fait 86 requêtes à [Wikipédia] (<https://fr.wikipedia.org>), sur 3 sous domaines différents.

Pour complètement charger le site de la [Fnac] (<http://www.fnac.com/>), le navigateur effectue 2 requêtes sur notre navigateur.

Description des attributs des cookies :

- ✓ **Secure** : Définie si le cookie ne doit être envoyé que sur du Https car il contient des données confidentielles.
- ✓ **HttpOnly** : Définie si le cookie est accessible à d'autre protocole que HTTP. Par exemple si le cookie est disponible via JavaScript.
- ✓ **Expires** : Date de fin de validité du cookie.

Same Origin Policy

Cela permet d'éviter qu'un site tiers utilise ou supprime notre cookie. Par exemple, un cookie mis en place sur un nom de domaine « **origin.site.com** » n'est utilisable que sur le même sous domaine et le même nom de domaine.

C'est à dire que notre cookie mis en place sur « **login.site.com** » n'est utilisable que sur « **origin.site.com** » et `site.com` mais pas sur « **autre.site.com** » ou « **autresite.com** ». Idem pour les ports : un cookie déposé sur le port 80 n'est utilisable que sur le port 80.

Chercher les requêtes sur le site ` <https://www.fnac.com/> `

2 requêtes mènent vers cette adresse, et ces requêtes sont principalement des requêtes vers des outils de tracking.