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

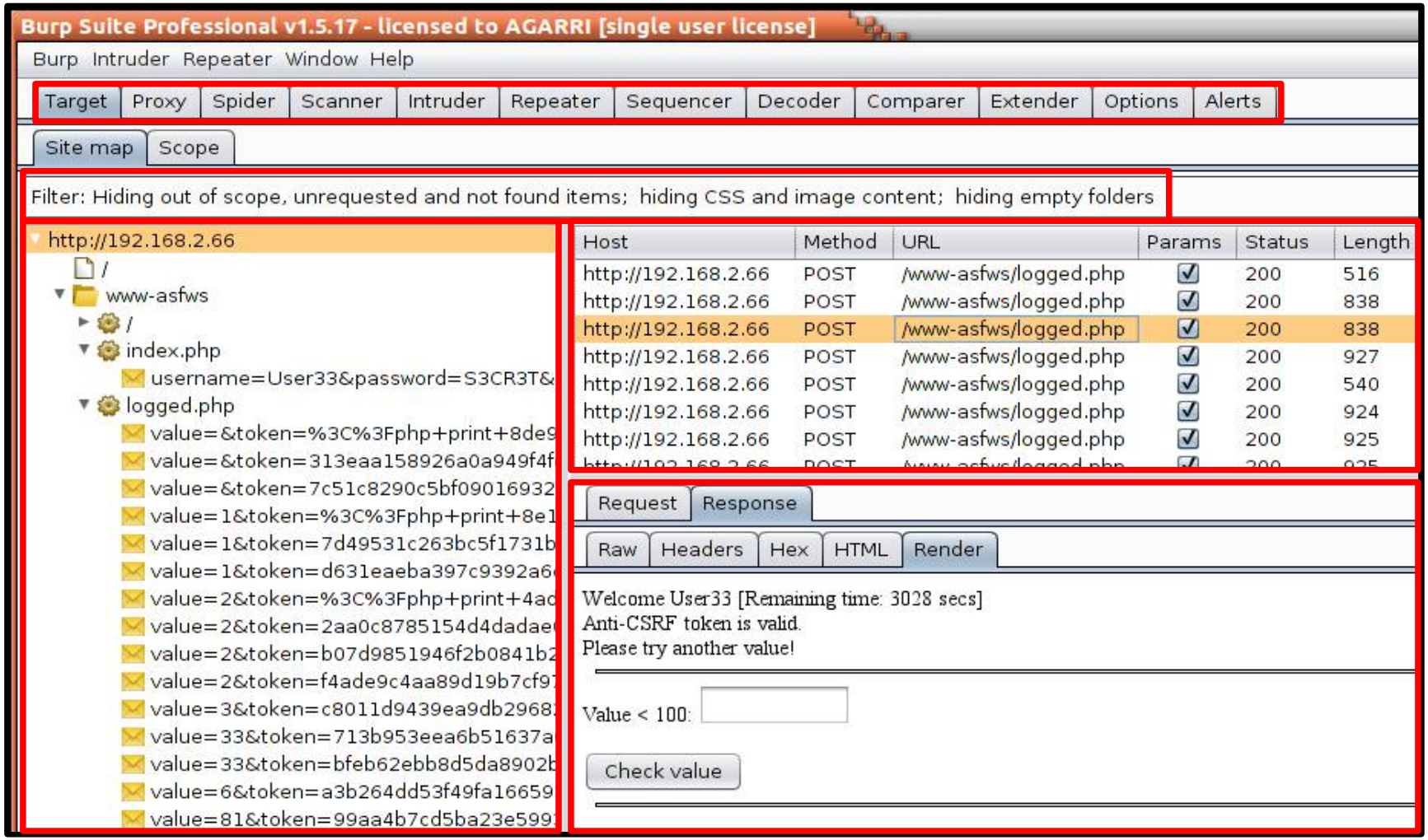
§ Se configure comme un proxy

§ 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)

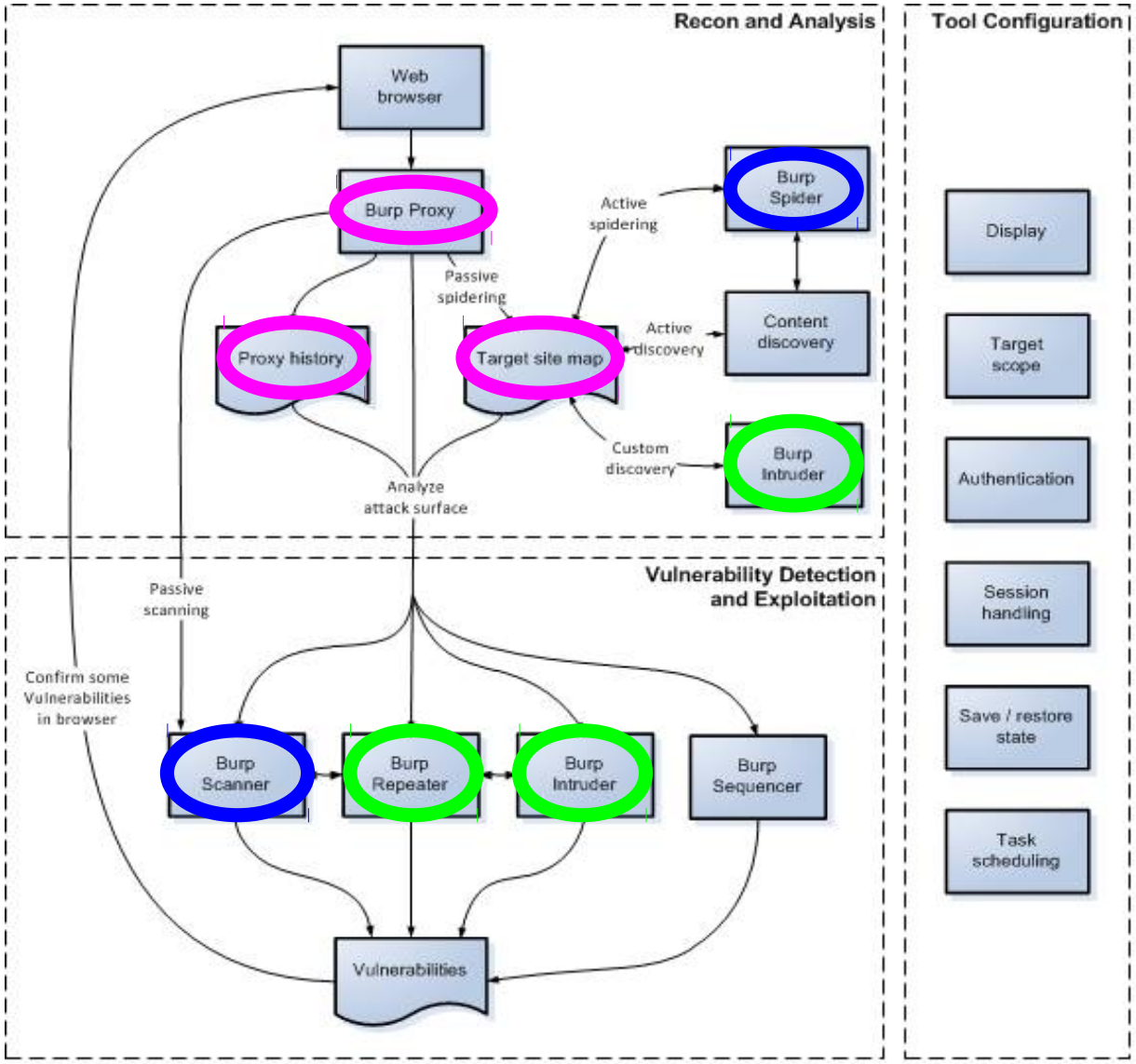
Aperçu de l'interface



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

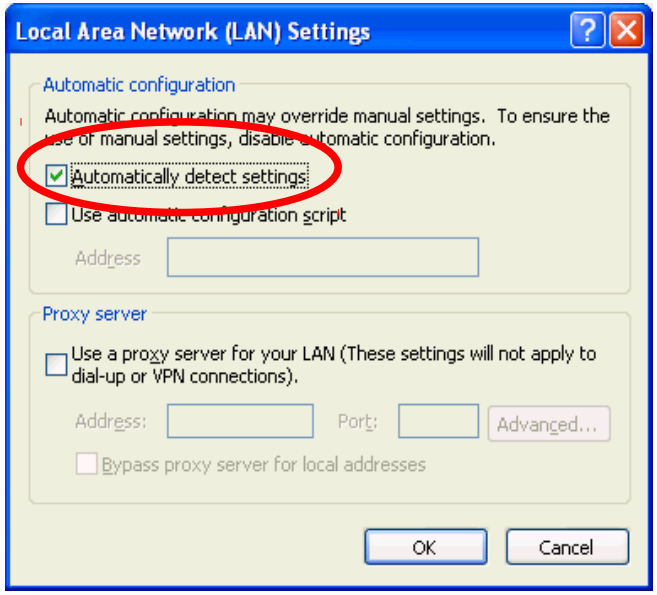
§ Test intrusif interne

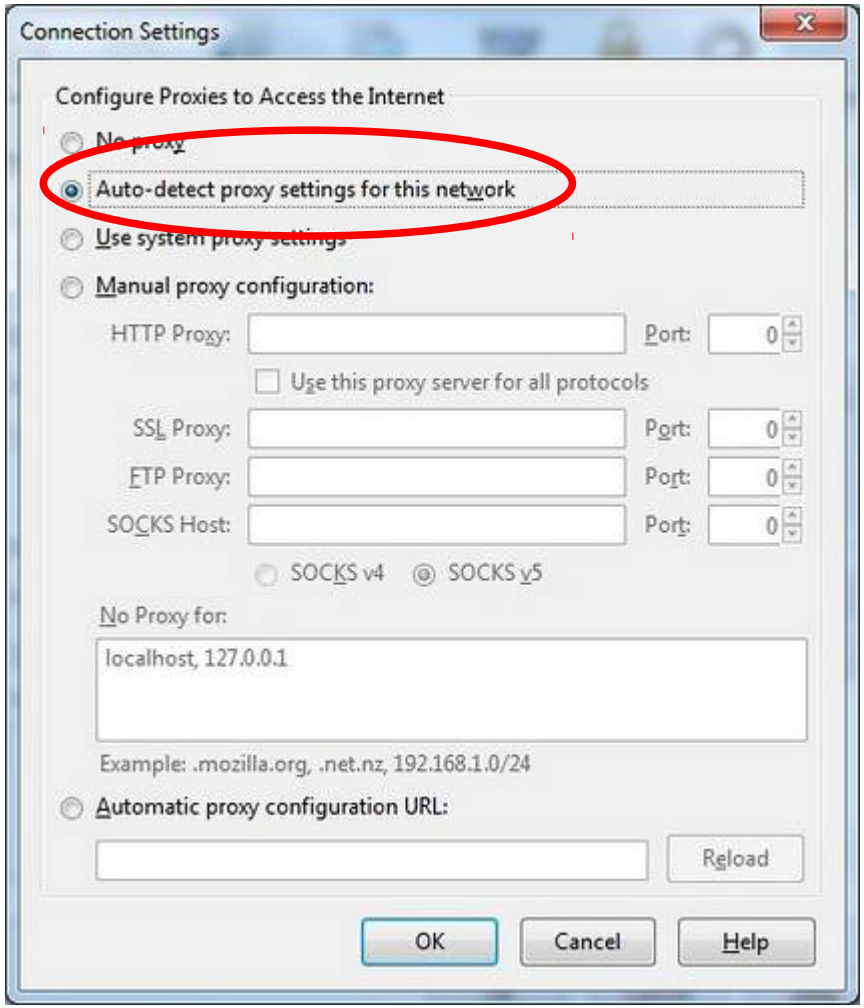
§ Mode « boîte noire »
§ Pas d'information sur le réseau
§ Pas d'information sur le domaine Windows

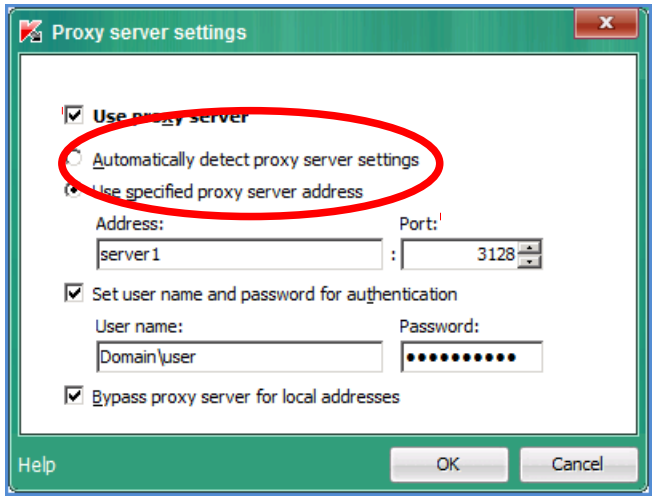
§ Administrateurs compétents et vigilants
§ Besoin de discrétion (surtout au début)

§ 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+)

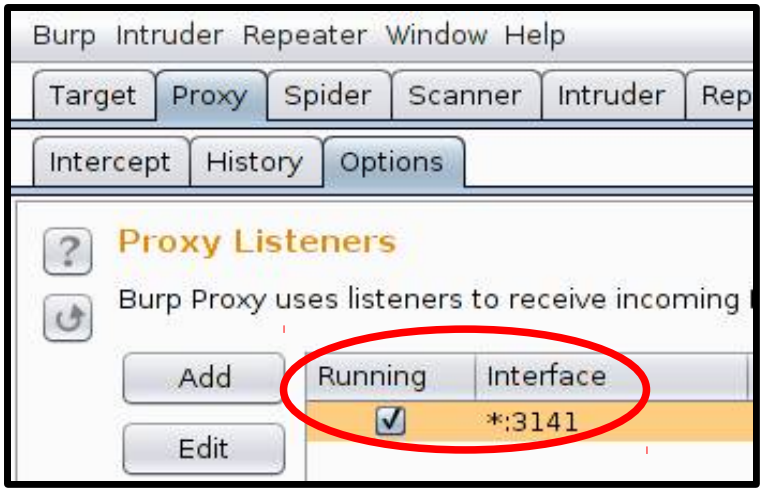
§ Si NBT-NS ou LLMNR, la requête est envoyée en *broadcast* !

§ 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



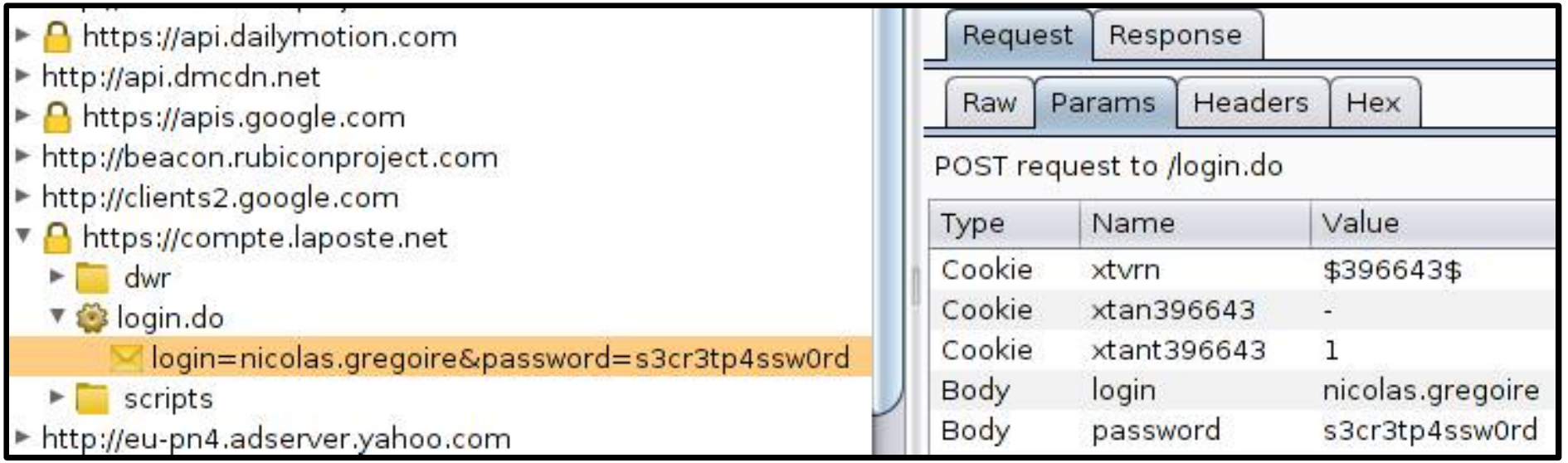
§ Rediriger le trafic WPAD vers Burp

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

Nous écoutons le trafic proxyfié !

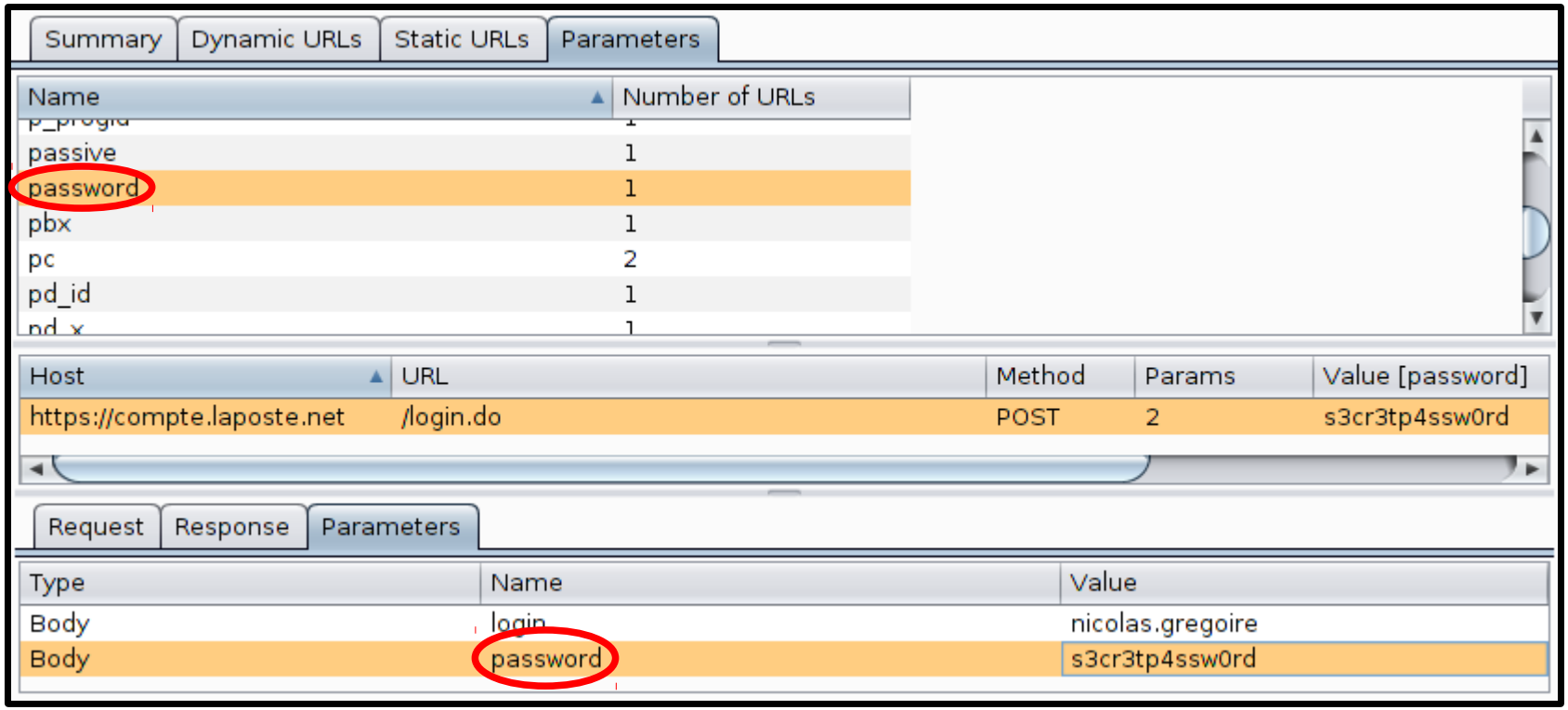
Analyse du trafic

§ Le trafic Web intercepté est visible dans :
- « Target » / « Site Map »
  - Présentation arborescente (site / URL / paramètres)
- « Proxy » / « History »
  - Ordre chronologique (principalement)



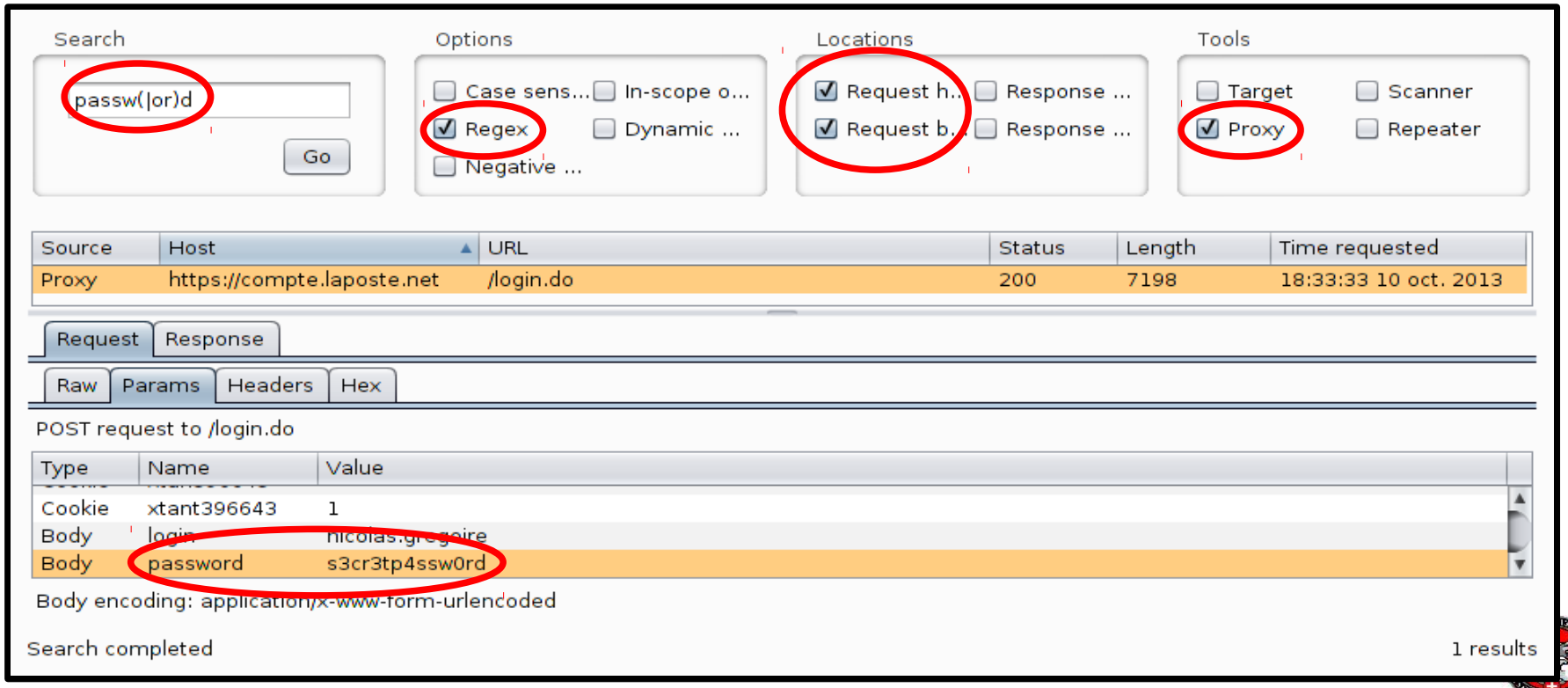
Analyse du trafic

§ Fonctionnalités avancées de recherche dans « Target » / « Site Map »
- Bouton droit puis sous-menu « Engagement tools »
  - « Search »
  - « Analyze target »



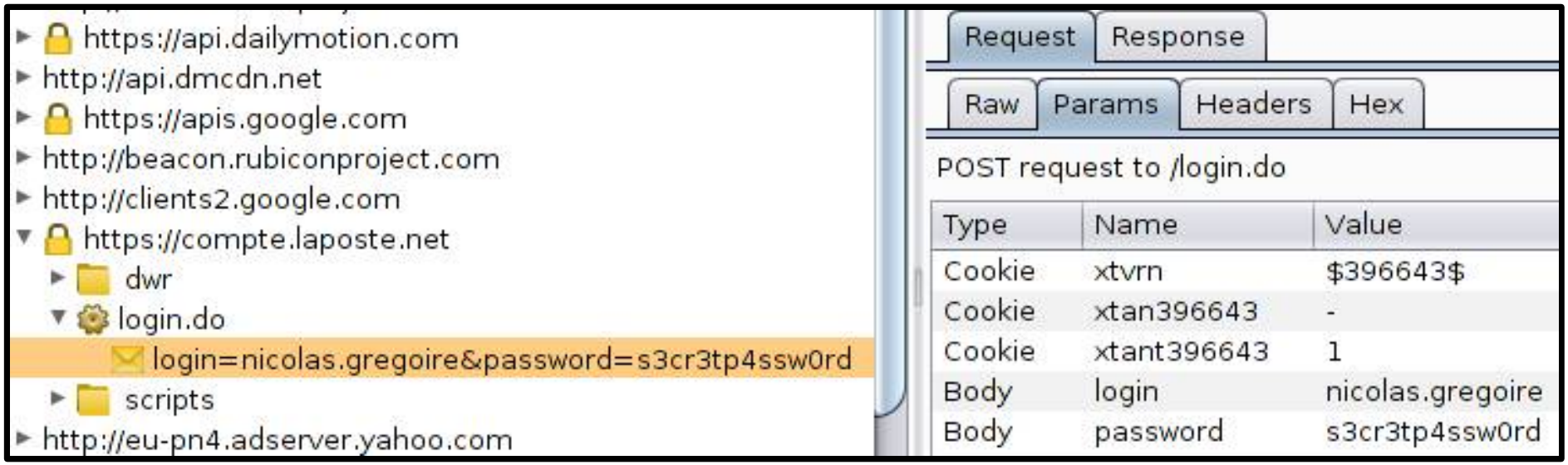
Analyse du trafic

§ Fonctionnalités avancées de recherche dans « Target » / « Site Map »
- Bouton droit puis sous-menu « Engagement tools »
  - « Search »
  - « Analyze target »



Mais ...

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

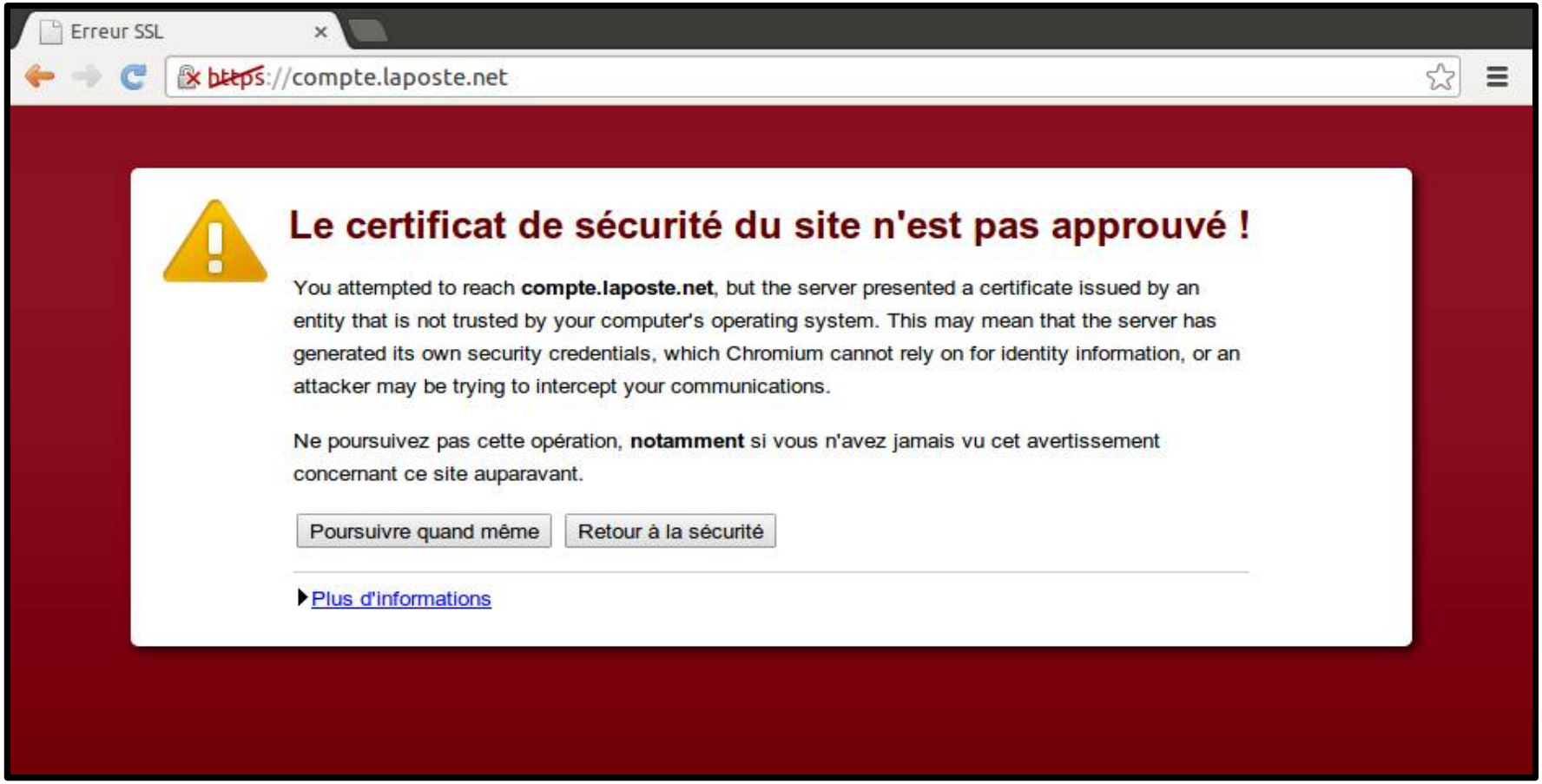


§ Le contenu des échanges HTTPS est visible !

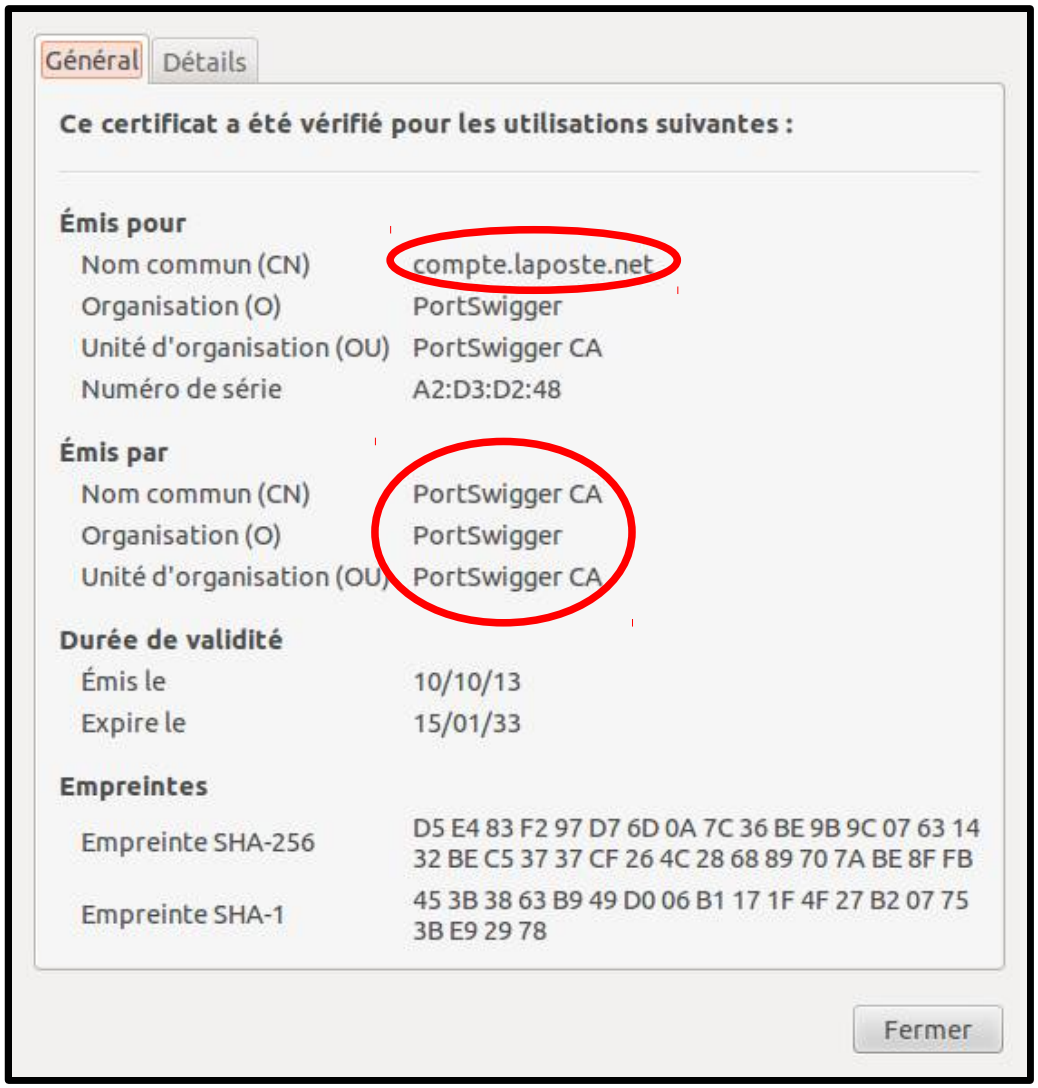
- Pratique mais très peu discret

Besoin de discrétion ?

Certificat SSL invalide

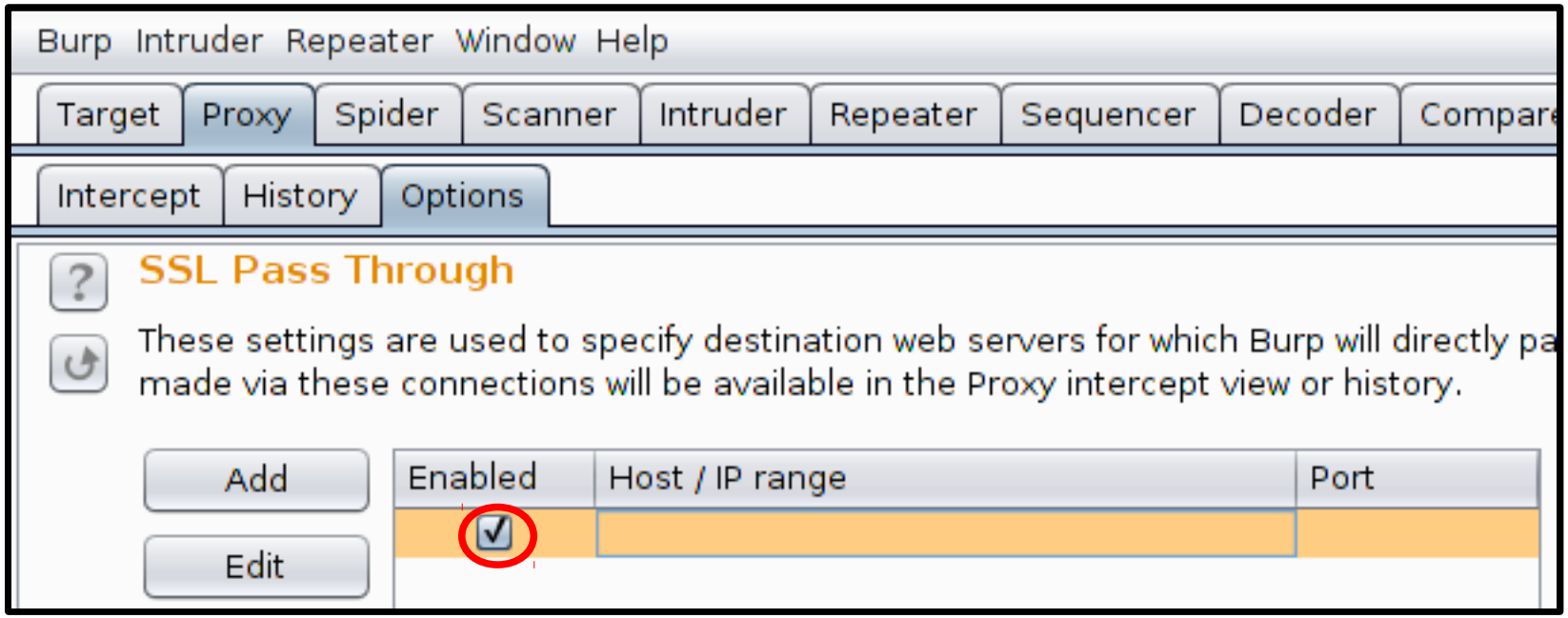


Certificat SSL invalide



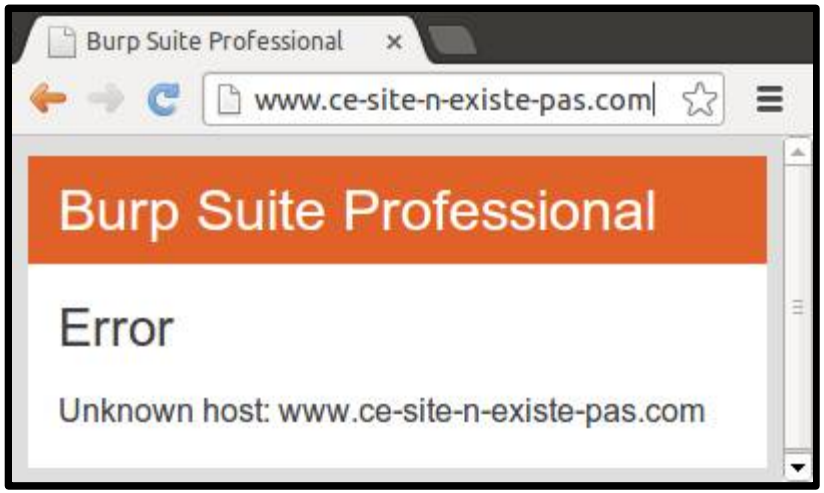
Non-rupture des sessions SSL

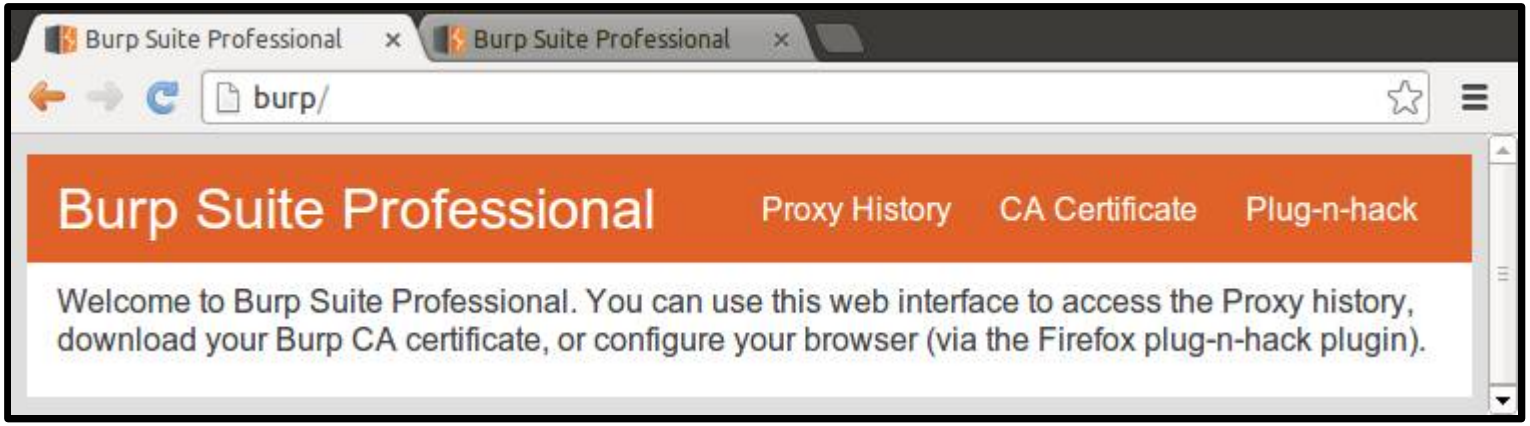
- Fonctionnalité « SSL Pass Through » introduite en v1.5.15 (Sept. 2013)
- Une seule entrée vide suffit
- Evidemment, le trafic HTTPS ne sera plus visible



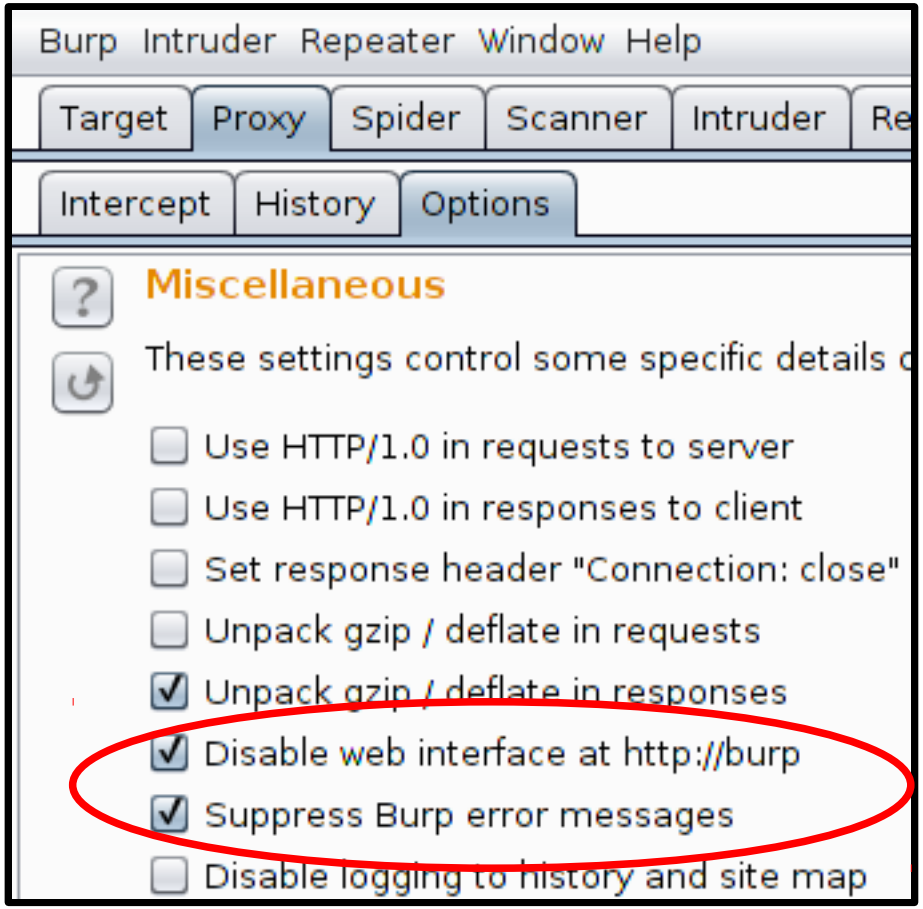
Nous écoutons le trafic HTTP !

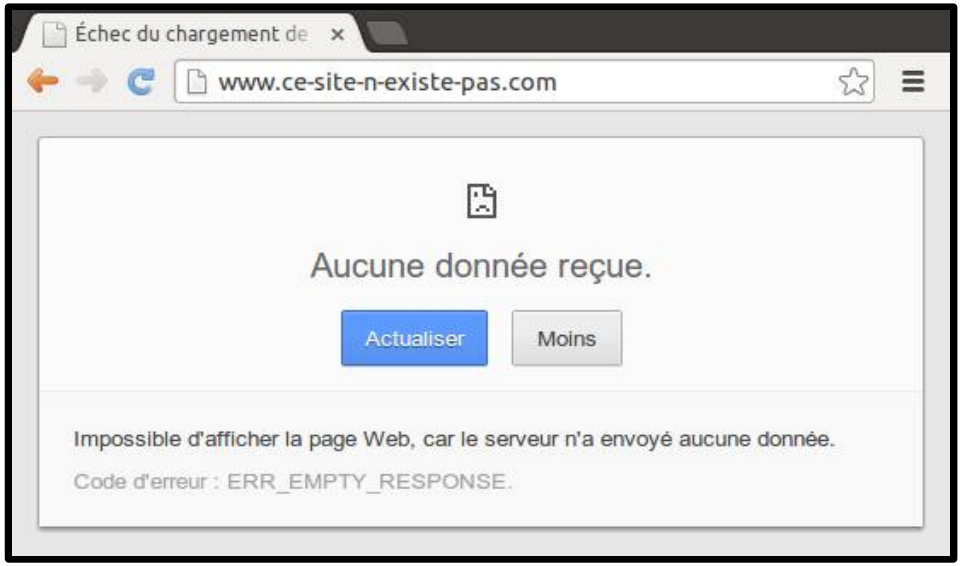
Artefacts


Burp Suite Professional
www.ce-site-n-existe-pas.com
Burp Suite Professional
Error
Unknown host: www.ce-site-n-existe-pas.com


Burp Suite Professional
Burp Suite Professional
burp/
Burp Suite Professional
Proxy History
CA Certificate
Plug-n-hack
Welcome to Burp Suite Professional. You can use this web interface to access the Proxy history, download your Burp CA certificate, or configure your browser (via the Firefox plug-n-hack plugin).

Artefacts


Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Re
Intercept History Options
Miscellaneous
These settings control some specific details
Use HTTP/1.0 in requests to server
Use HTTP/1.0 in responses to client
Set response header "Connection: close"
Unpack gzip / deflate in requests
Unpack gzip / deflate in responses
Disable web interface at http://burp
Suppress Burp error messages
Disable logging to history and site map


Échec du chargement de
www.ce-site-n-existe-pas.com
Aucune donnée reçue.
Actualiser
Moins
Impossible d'afficher la page Web, car le serveur n'a envoyé aucune donnée.
Code d'erreur : ERR_EMPTY_RESPONSE.

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 »

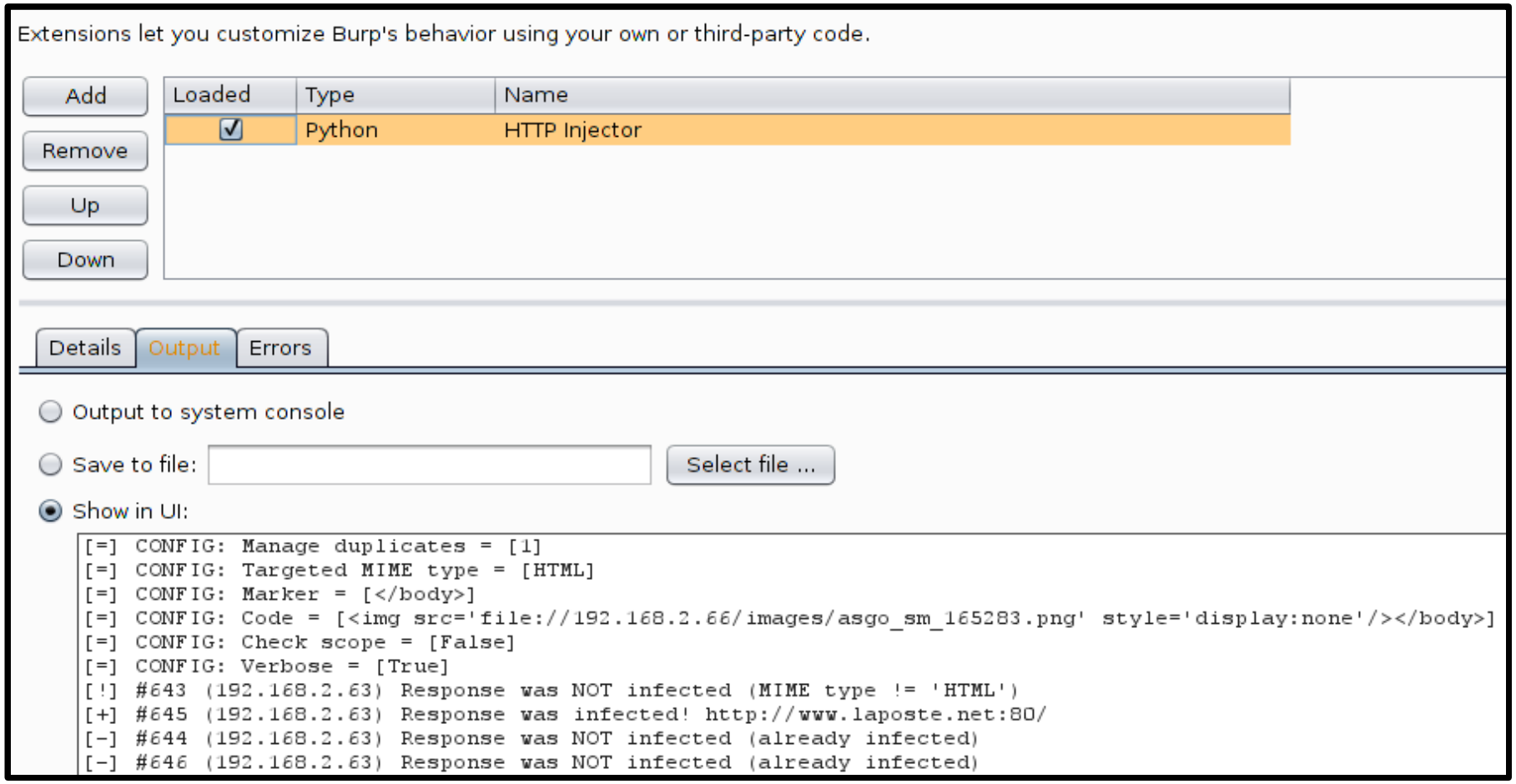
§ Burp n'intègre pas de fonctionnalité de manipulation complexe des réponses
- D'où une extension dédié : « HTTP Injector »

§ 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)

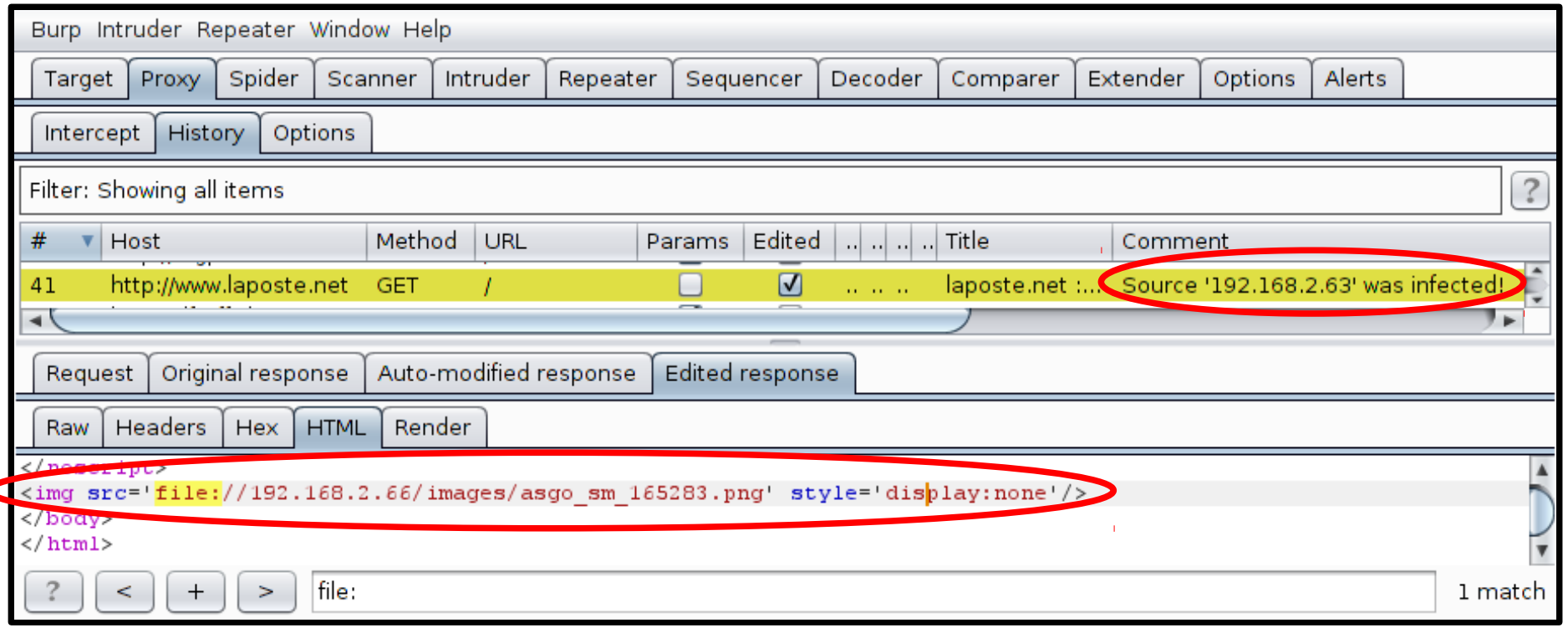
§ Cas d'usage
- Insertion de code JavaScript (BeEF, FireBug Lite)
- Insertion d'images ou d'*iframes*
- Et tout ce qui vous passe par la tête, c'est du Python !

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

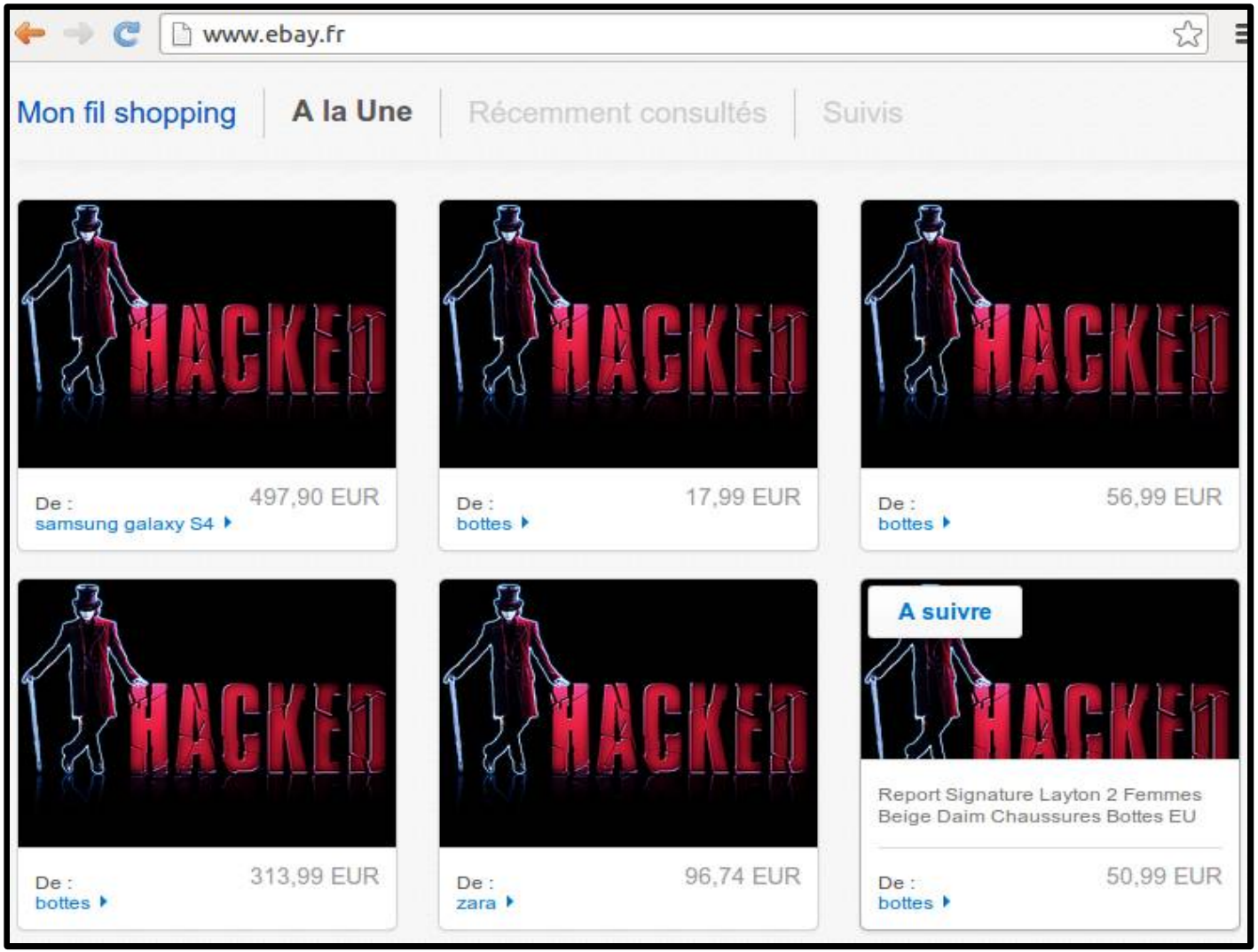
Extension « HTTP Injector »



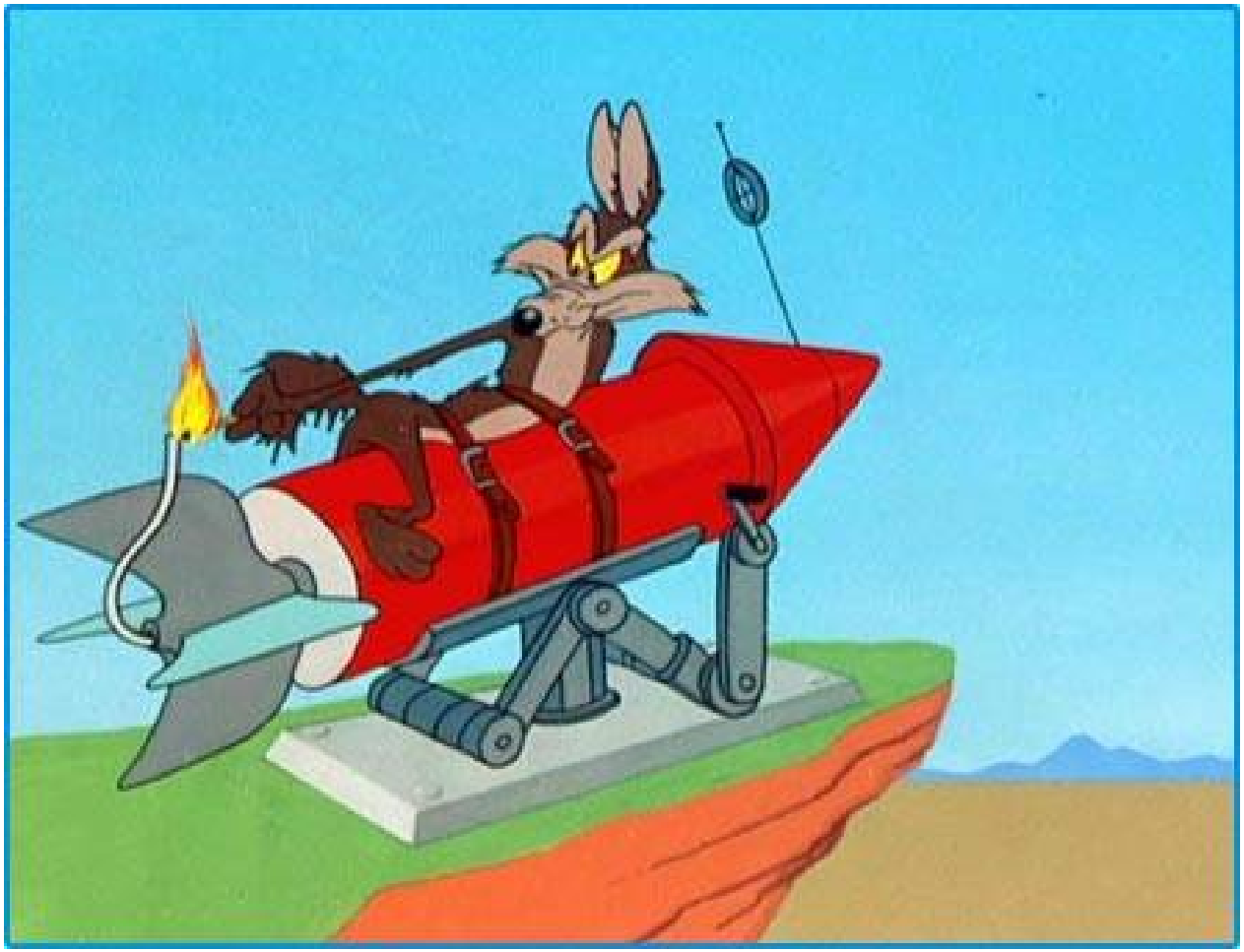
Extension « HTTP Injector »



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

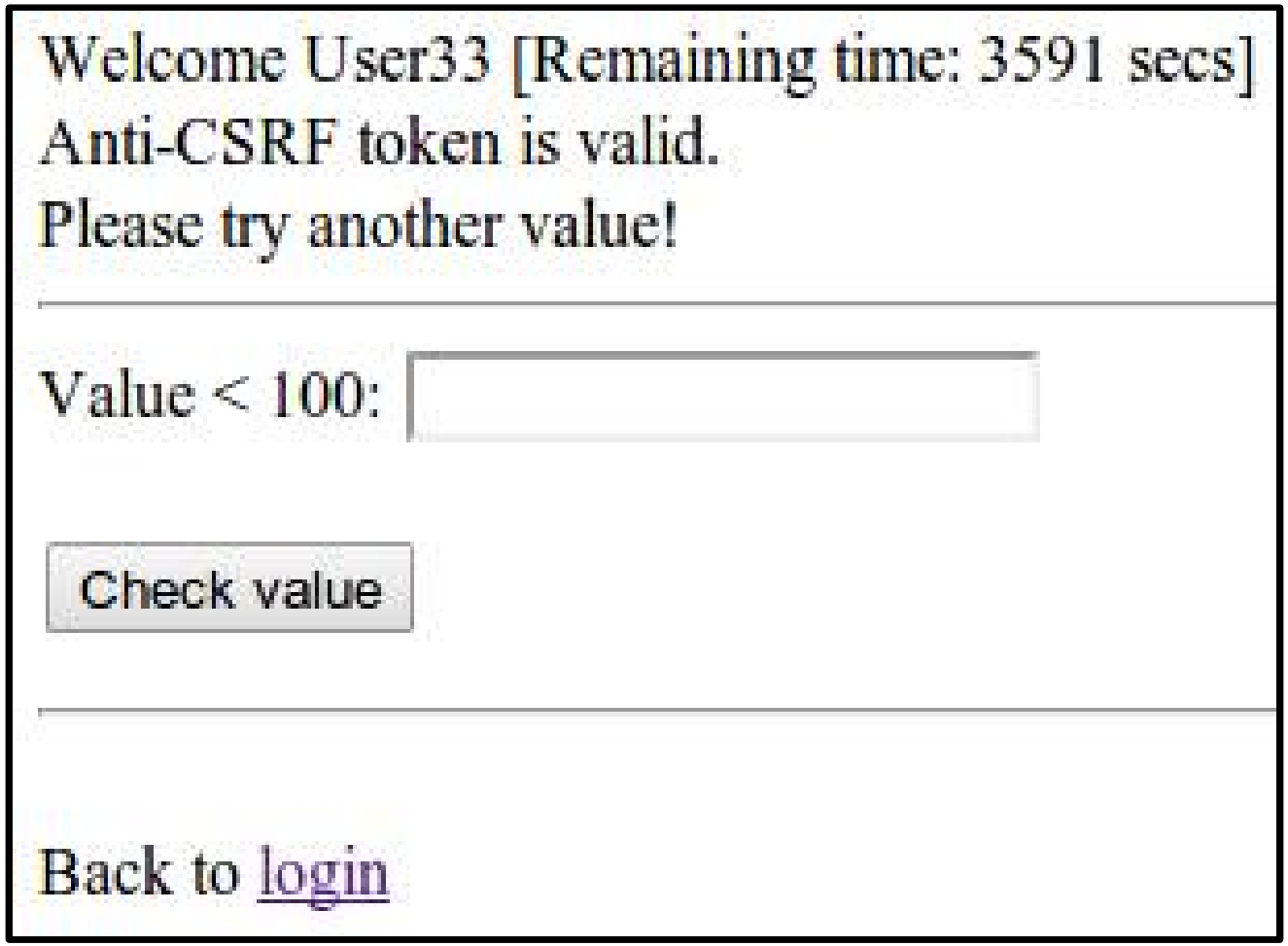
- § Introduction à Burp Suite
- § Test intrusif interne : WPAD
- § Sessions brèves et jetons anti-CSRF

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

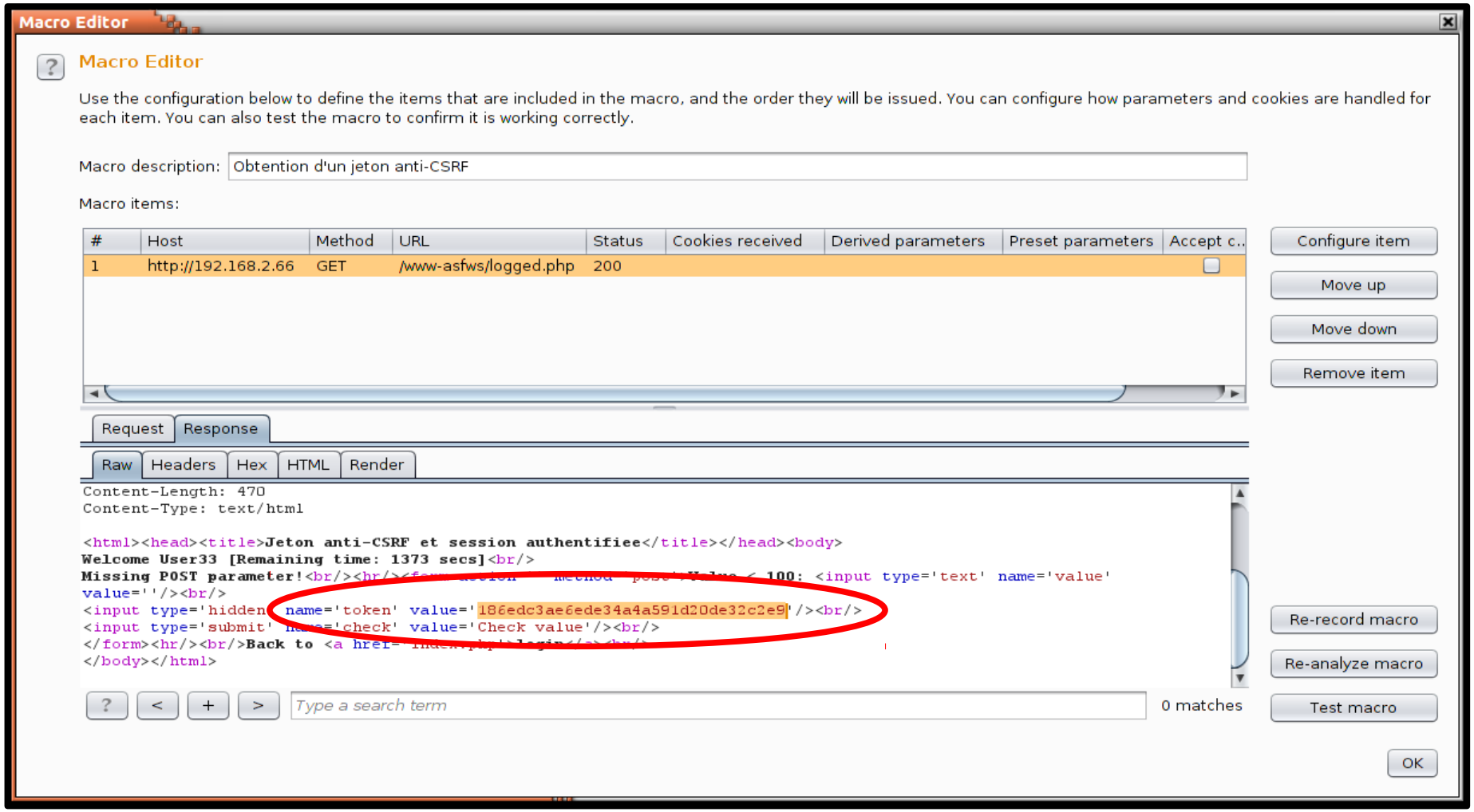
Macro de collecte du jeton

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

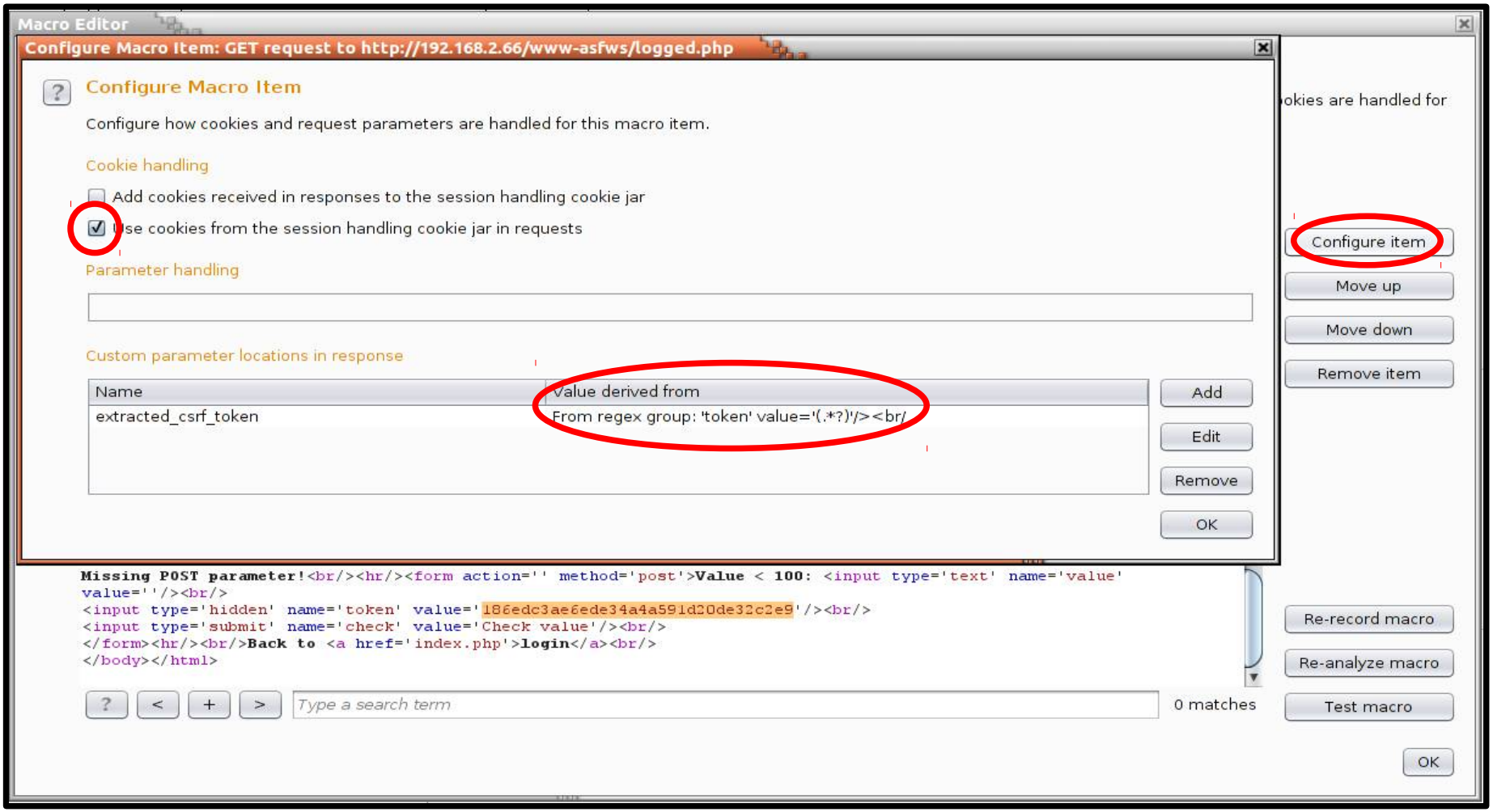
§ Configuration :

- 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 de collecte du jeton



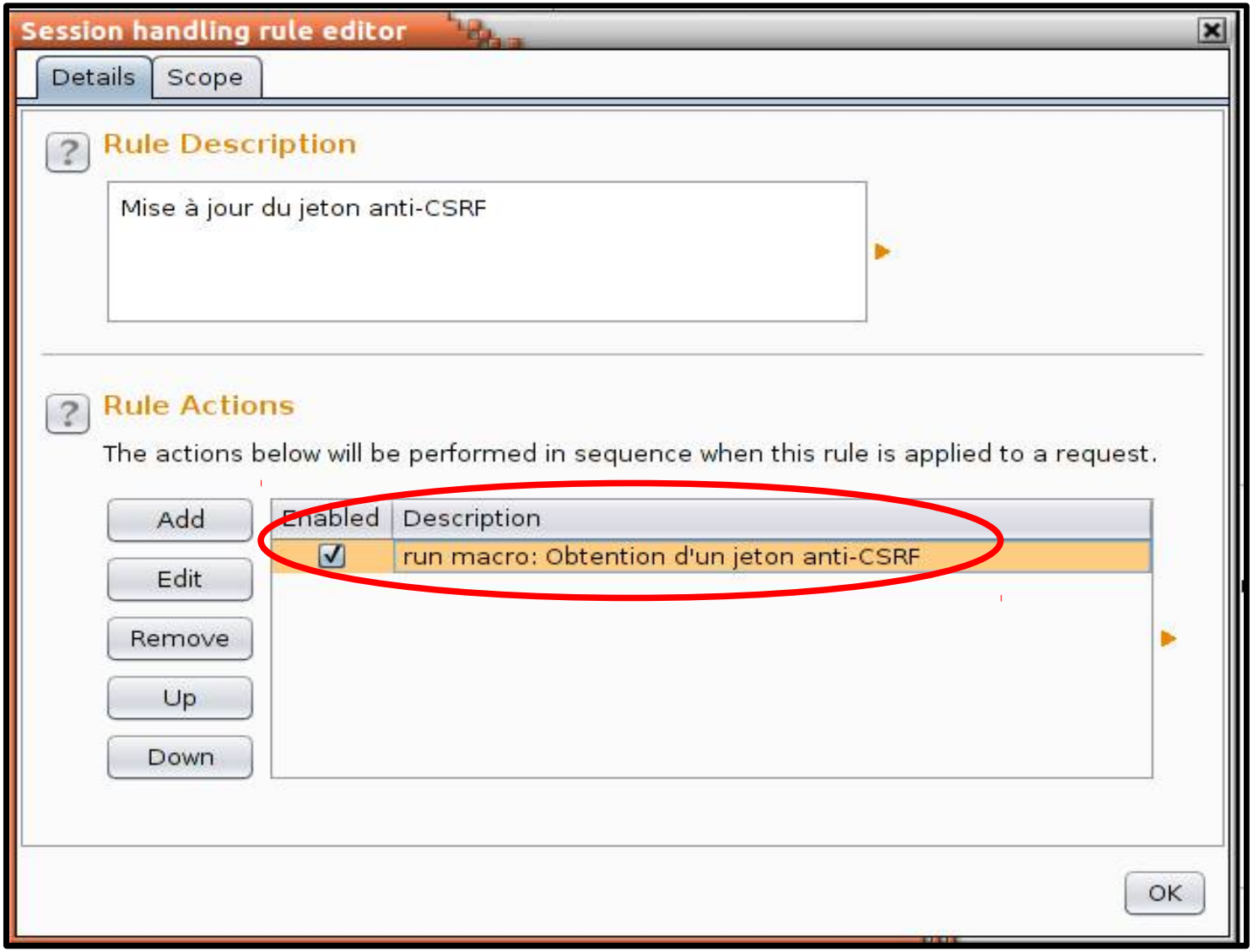
Règle de gestion de session

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

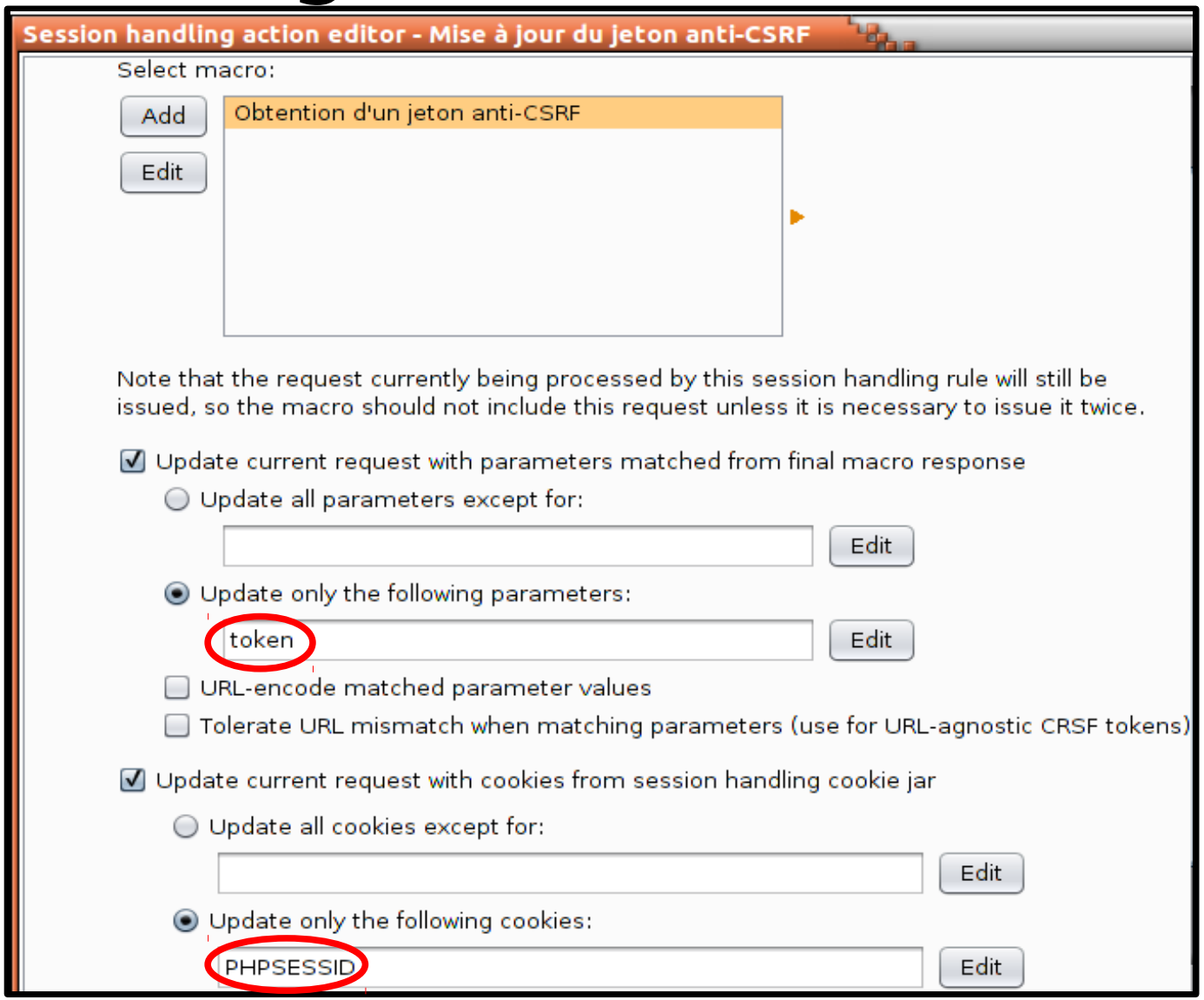
§ Configuration :

- 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



Règle de gestion de session

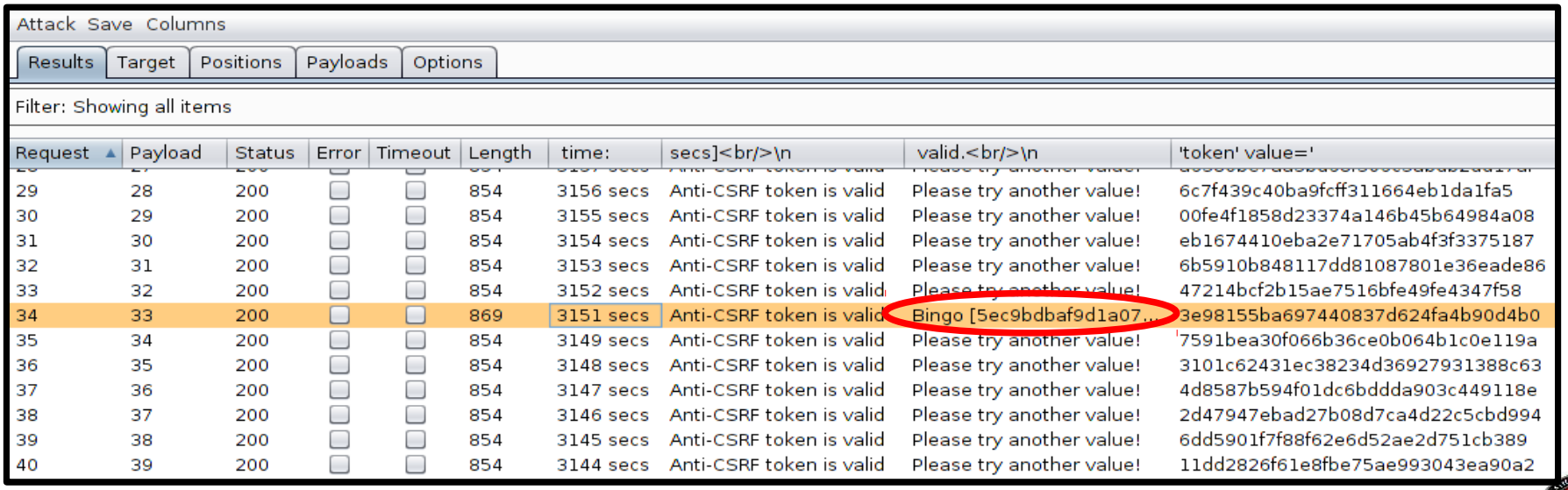


Usage

§ Un seul thread !

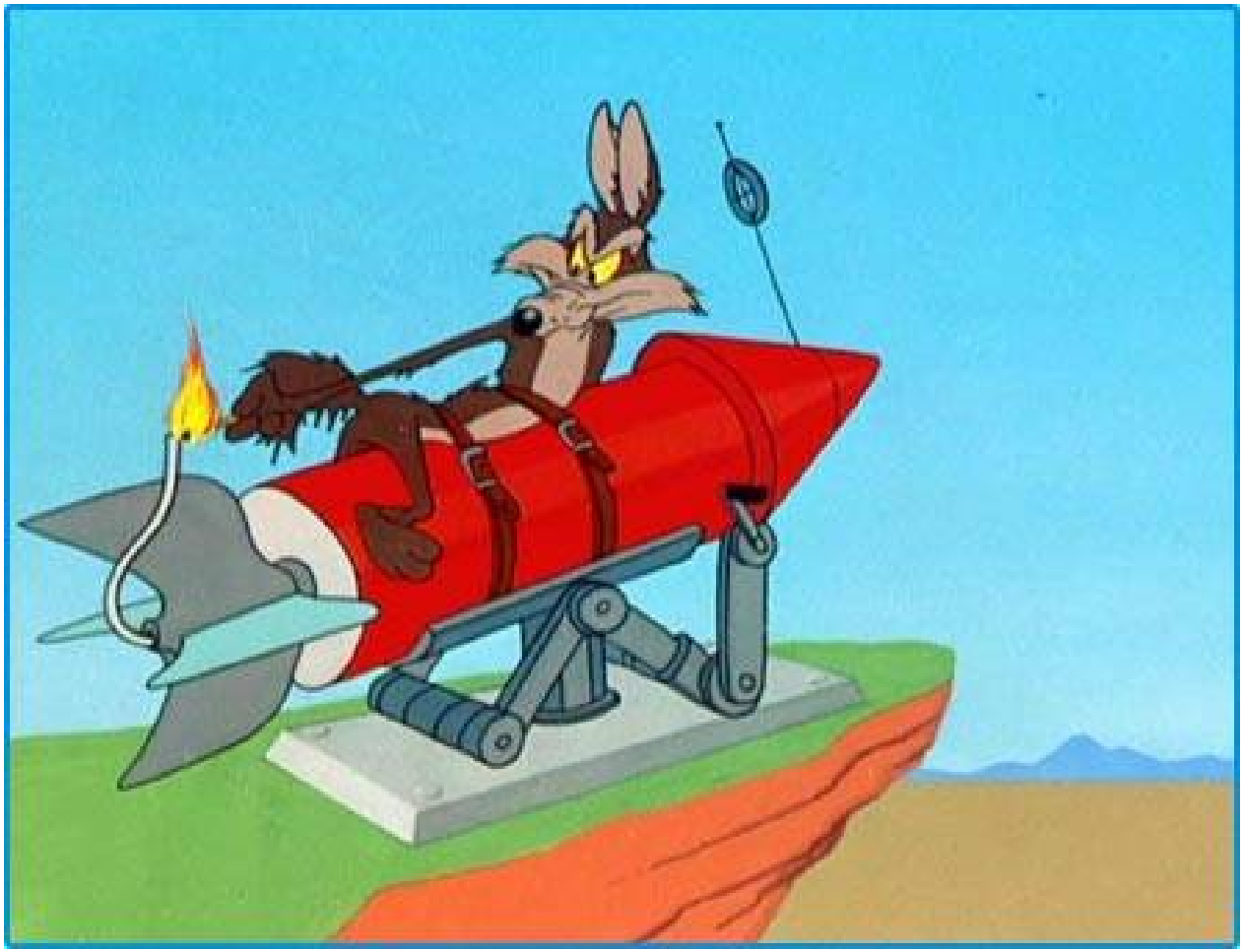
§ Dans l'outil « Repeater » :
- Utilisation transparente, si le scope des règles de session est bien défini
- Conseil : tester les macros et règles de gestion de session dans cet outil

§ Dans l'outil « Intruder » :
- Désactivation de l'option « Make unmodified baseline request »
- Utilisation de « Grep – Extract » afin de suivre l'avancement



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)

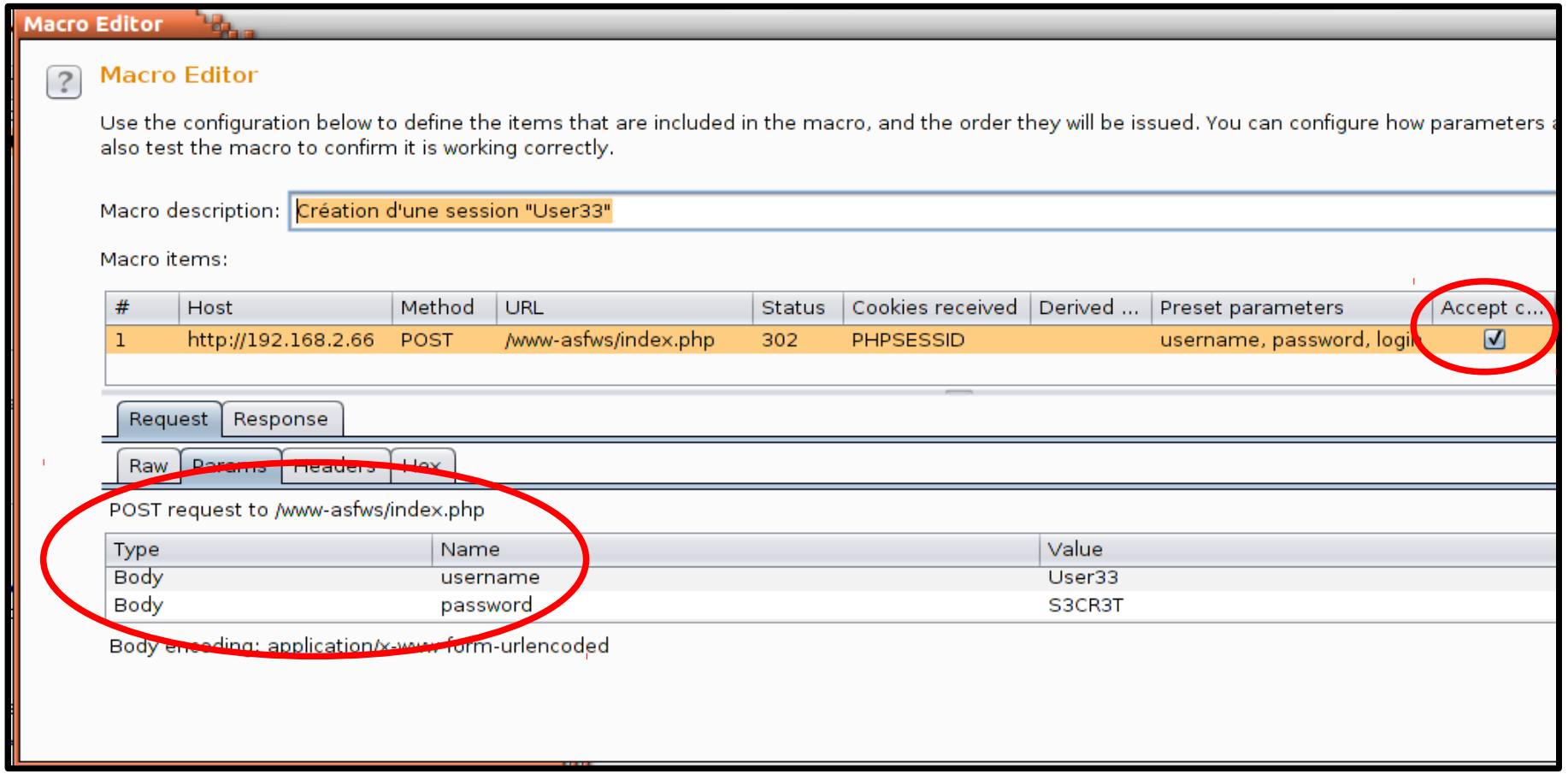
Macro de création de session

§ 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 boite à biscuits

Macro de création de session



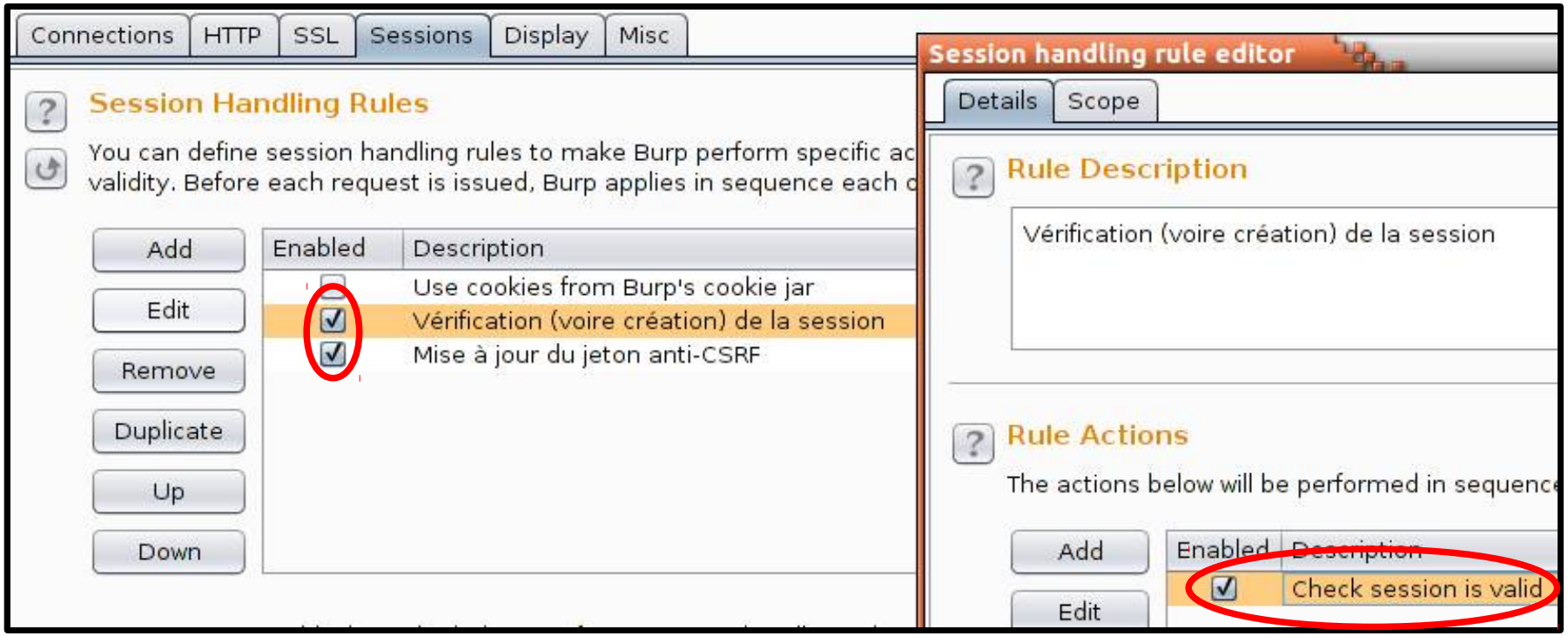
Règle de gestion de session

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

§ Configuration :

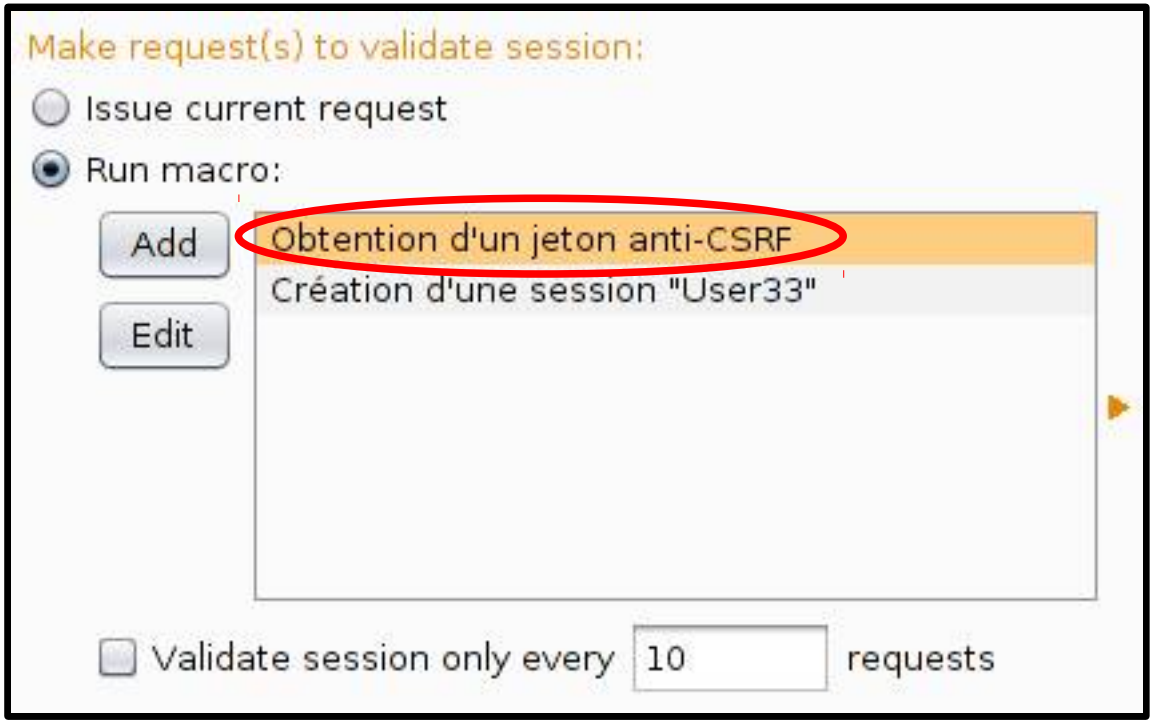
- Action : « Check session is valid »
- Requête à émettre : n'importe quel accès à la partie authentifiée
- Inspection de la réponse
  - Lieu : corps de la réponse
  - Motif : « Remaining time: (..+) secs »
  - Type de motif : expression régulière
  - Si le motif est trouvé, alors la session est valide
- 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



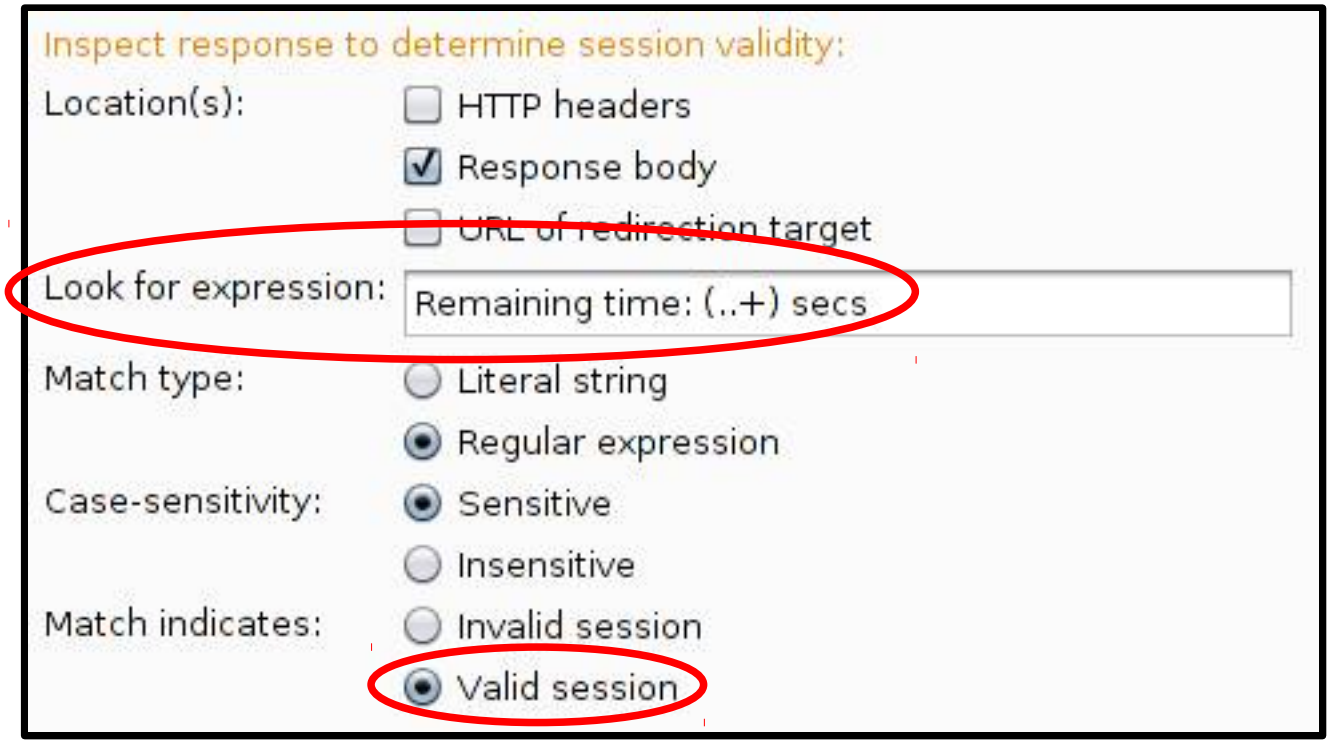
Règle de gestion de session

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



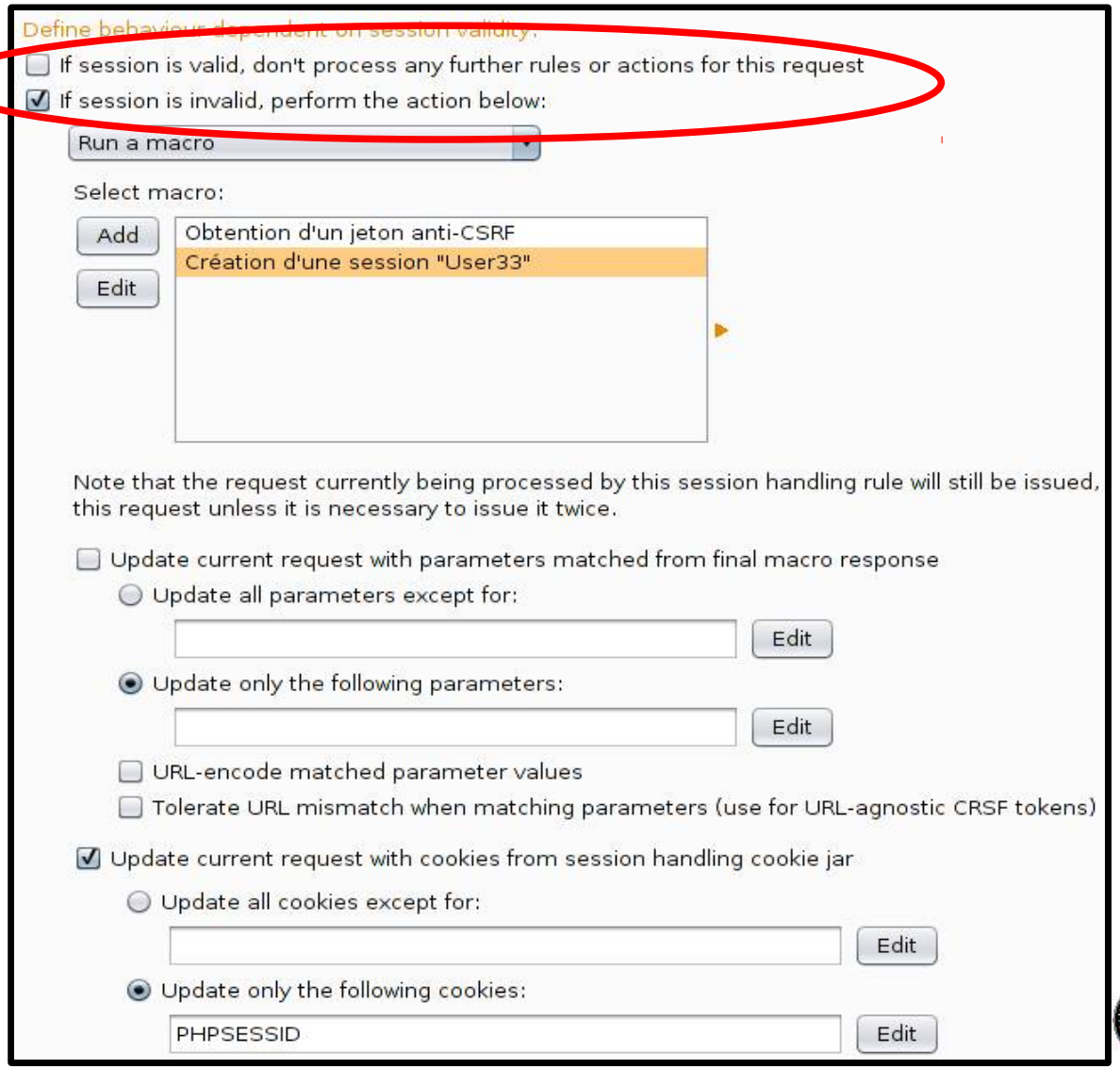
Règle de gestion de session

§ Inspection de la réponse



Règle de gestion de session

- Selon validité de la session



Usage

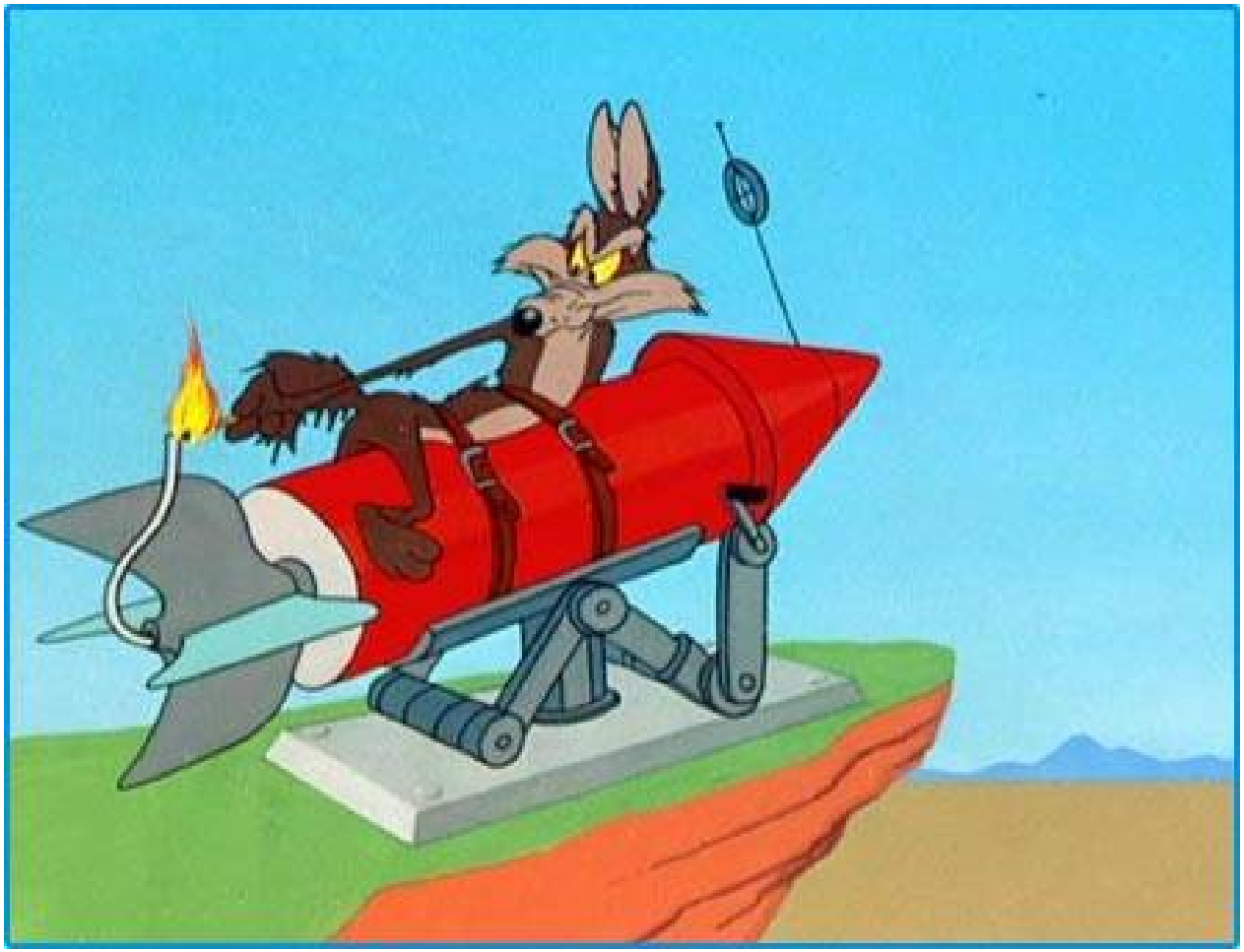
Request	Payload	Status	Error	Timeout	Length	time:	secs] \n	valid. \n	'token' value='
30	29	200			855	12 secs	Anti-CSRF token is valid	Please try another value!	2f07b17df953c3893b2c6d45f6ab5119
31	30	200			855	10 secs	Anti-CSRF token is valid	Please try another value!	4596f38fd8736f37a9b4c41f88568948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