WAVESTONE

Bilan de la sécurité des sites web en France

Retour sur 3 ans d'analyse de la sécurité des sites de grandes entreprises

Gérôme BILLOIS
Partner
gerome.billois@wavestone.com
+33 (0)6 10 99 00 60
@gbillois

Yann FILLIAT
Manager – Responsable offre audit de sécurité
yann.filliat@wavestone.com
+33 (0)6 24 76 08 67

Dans un monde où la capacité à se transformer est la clé du succès, nous éclairons et guidons nos clients dans leurs décisions les plus stratégiques

Des clients leaders dans leur secteur

2 800 collaborateurs dans 8 pays

Parmi les leaders du conseil indépendant en Europe, n°1 en France

Paris | Londres | New York | Hong Kong | Singapour* | Dubaï* | São Paulo*
Luxembourg | Madrid* | Milan* | Bruxelles | Genève | Casablanca | Istanbul* | Edimbourg
Lyon | Marseille | Nantes

* Partenariats

WAVESTONE

WAVESTONE ET LES AUDITS EN CYBERSECURITE

Wavestone : un retour d'expérience unique sur les audits en cybersécurité

350 audits de sécurité par an

Périmètres d'interventions variés : sites web, tests d'intrusion physiques, ingénierie sociale, revue de configuration, de code, SI industriel, red teams, etc.

Plus de 100 clients différents

Essentiellement des très grandes entreprises françaises, présentes sur le marché national ou international

Tous les secteurs d'activité couverts

Banque, Assurance, Distribution, Médical, Énergie, Service, Télécom, Transport, Défense, Institutions Publiques, etc.

Benchmark de 2016 à 2018 des failles des sites web

Tests d'intrusion de sites web réalisés au cours de l'année (de juin à mai) sur des sites accessibles depuis Internet et des sites sur des réseaux privés d'entreprise.

2018 : 139 sites testés
2017 : 155 sites testés
2016 : 128 sites testés

De multiples secteurs d'activités : banque, santé, ministère, énergie, télécom, services et transport.

2018 : 75 organisations
2017 : 70 organisations
2016 : 82 organisations

Des tests respectant la même méthodologie, pour des résultats comparables.
Des failles incluant le contrôle d'accès, la qualité du chiffrement, la diffusion d'informations techniques superflues, le traitement des communications, etc.

47 points de contrôle testés chaque année

WAVESTONE

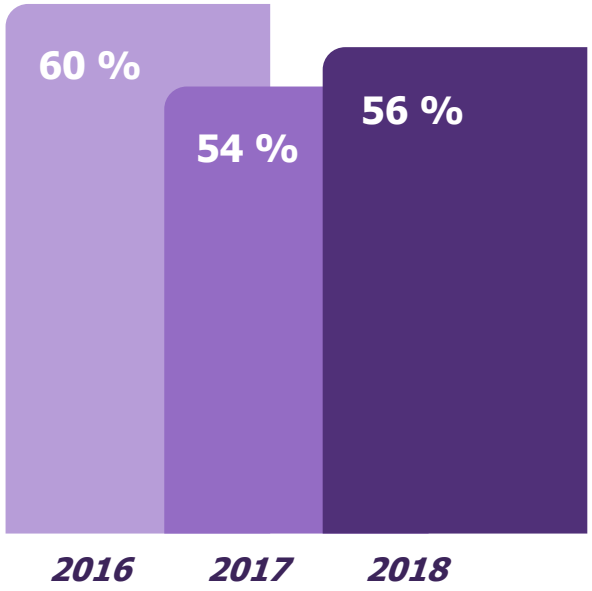
LES RESULTATS

Aucun site parfait !

Le chiffre

100% Comme en 2016 et en 2017, nos tests de sites web en 2018 ont révélé la présence d'**au moins une** faille de sécurité

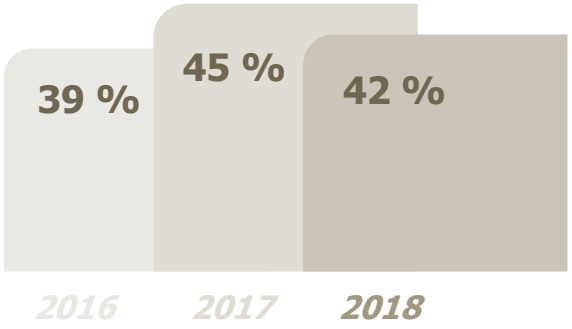
Une situation qui ne s'améliore pas



% de sites touchés par au moins une faille grave

Permet d'accéder à l'ensemble du contenu du site et/ou de compromettre les serveurs

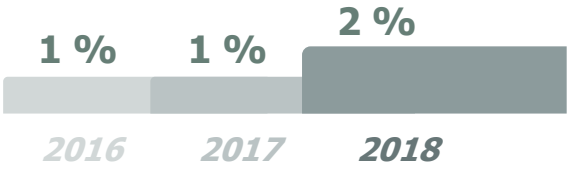
Accès à l'ensemble des données du site, exécution de code par le serveur, utilisateur A ayant accès aux données de B, etc.



% de sites n'étant touchés que par des failles importantes

Permet d'accéder aux informations d'autres utilisateurs mais en nombre limité ou de manière complexe

Vol de session d'un utilisateur, faiblesses dans le chiffrement, possibilité de faire réaliser des actions à l'insu de l'utilisateur, etc.



% de sites n'étant touchés que par des failles mineures

Permet principalement d'obtenir des informations pour continuer l'attaque

Messages techniques superflus, absence de sécurisation des cookies, déconnexion utilisateur non efficace, etc.

Des failles graves sur Internet, comme en interne

2016	2017	2018
50%	**50%**	**52%**

des sites accessibles à tous depuis Internet ont au moins une faille grave

2016	2017	2018
75%	**68%**	**66%**

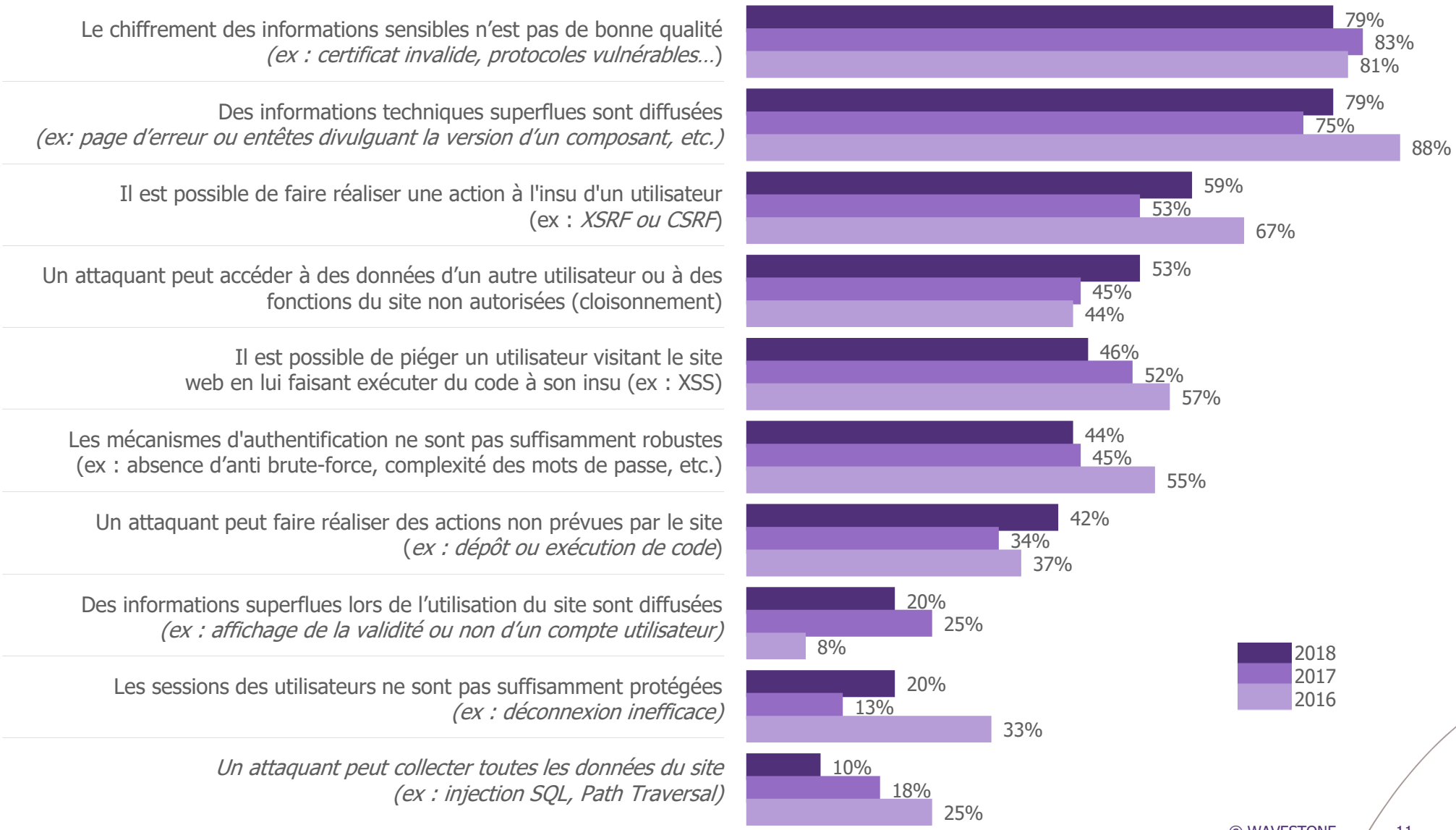
des sites web internes réservés aux collaborateurs ont au moins une faille grave

Une sécurité négligée dans la durée

Cette année, plus de **50%** des sites testés restent vulnérables avec au moins 1 faille grave, et cela malgré la réalisation d'audit par le passé.

Des corrections peu appliquées et des nouvelles fonctionnalités développées sans prendre en compte les bonnes pratiques de sécurité.

Un top 10 des failles qui évolue peu

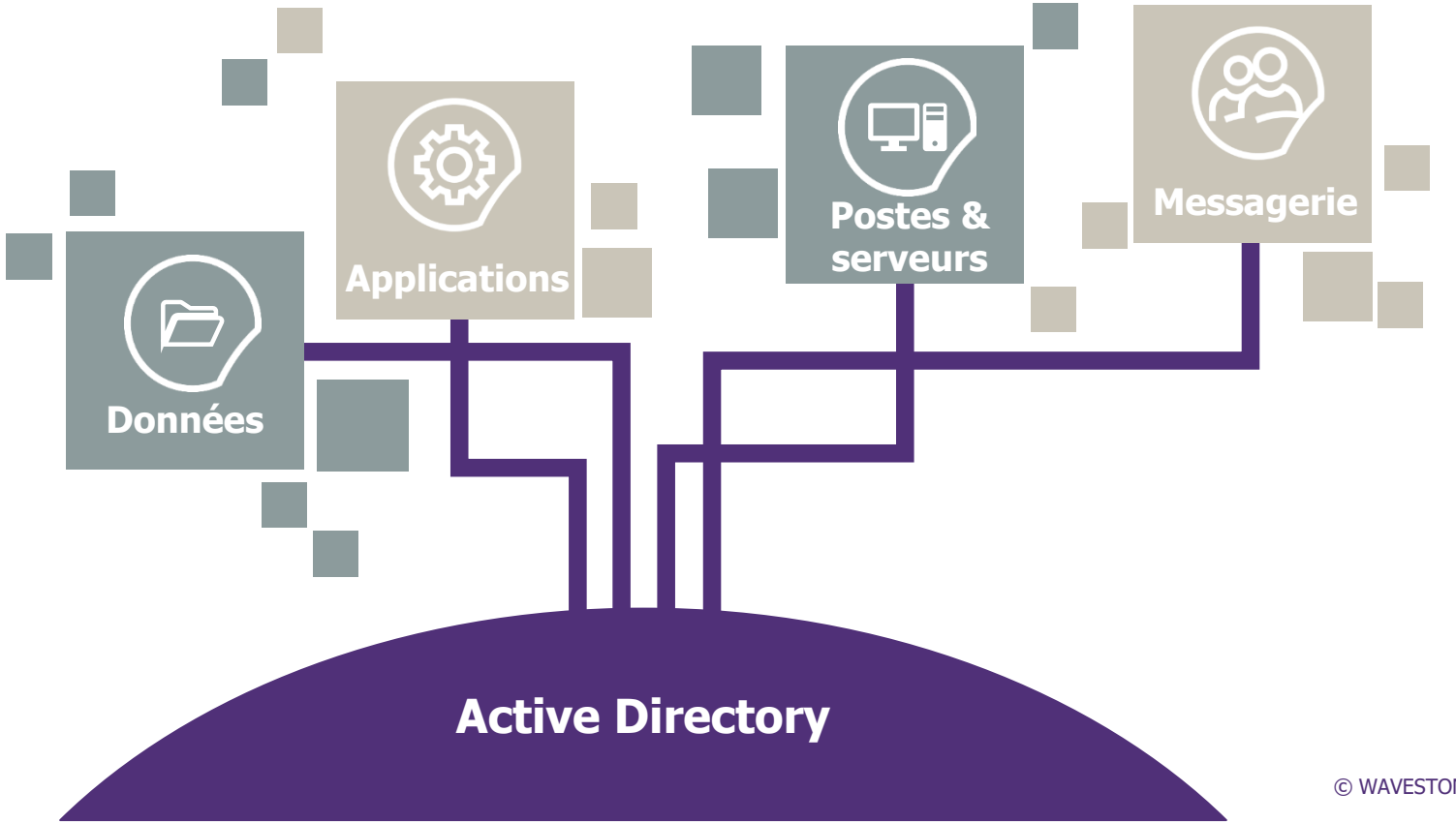


WAVESTONE

FOCUS 2018
La sécurité des systèmes d'information des entreprises

Quel niveau de sécurité pour les systèmes d'information des entreprises ?

Les systèmes d'information reposent sur une **infrastructure centrale**, usuellement Active Directory. Sa compromission permet de prendre le contrôle de l'ensemble **des systèmes et des données** des entreprises.

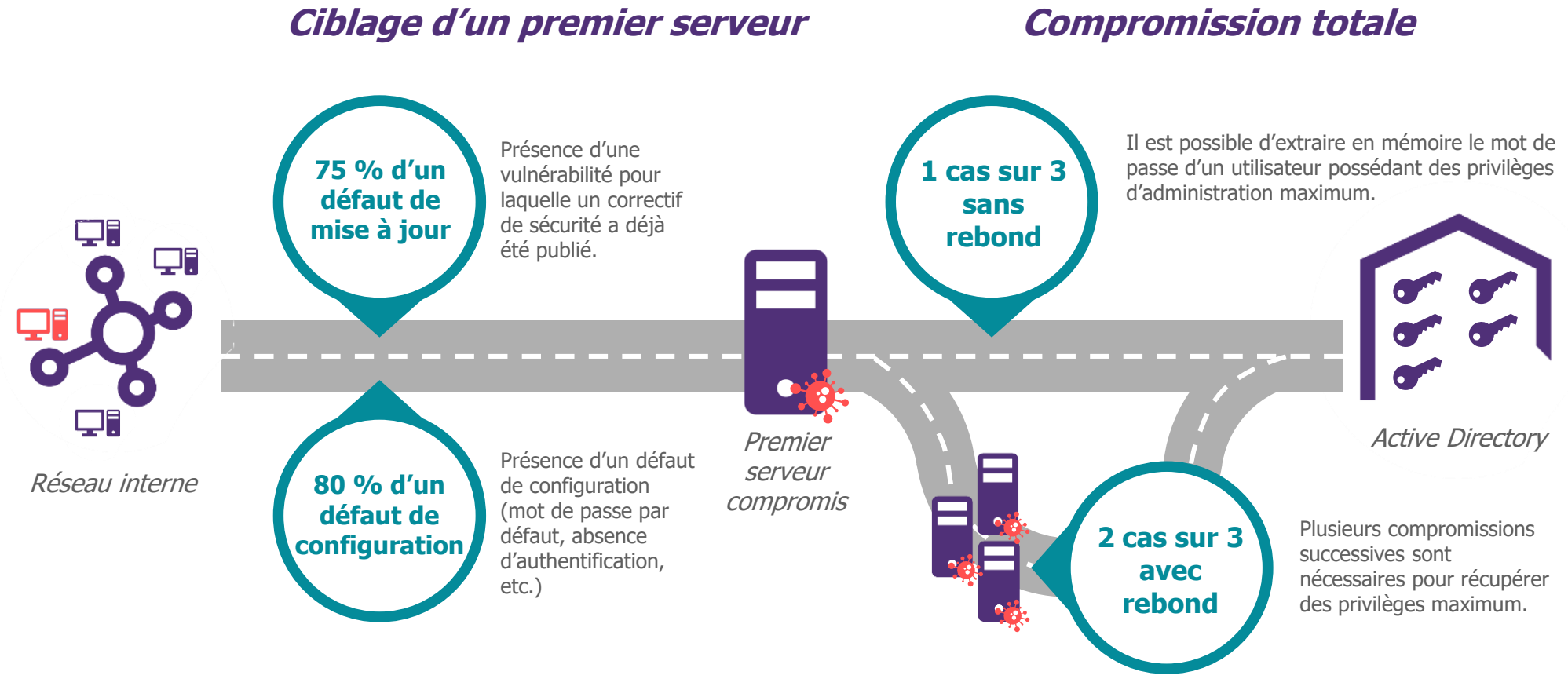


La quasi-totalité des systèmes d'informations sont vulnérables

Wavestone a réalisé sur 2017 et 2018, des tests d'intrusion sur 25 systèmes d'information de grandes entreprises.

96% se sont soldés par la **compromission de l'Active Directory**

Quels chemins pour compromettre le SI ?



**Dans 80 % des audits réalisés,
la compromission est totale en moins de 24h**

WAVESTONE

RECOMMANDATIONS

Des résultats qui ne s'améliorent pas, une prise de conscience nécessaire au plus haut niveau de l'entreprise sur 4 axes

Conception

Intégrer la sécurité dans toutes les phases des projets, dès les réflexions amonts

Acteurs

Mobiliser et objectiver les développeurs mais aussi les donneurs d'ordre sur la sécurité

Contrôle

Définir des référentiels de contrôles clairs et les appliquer dans toutes les phases de développement

Vérification continue

S'assurer de la prise en compte dans toutes les phases de vie des applications et des sites

ANNEXES

Un contrôle d'accès pas toujours contrôlé…

53% des tests réalisés en mode **boite grise** (utilisation d'un compte utilisateur standard) ont permis de contourner le cloisonnement applicatif pour accéder à des données ou des fonctions (escalade horizontale ou verticale) non autorisées

2016	2017
44%	45%

Dépôt de fichier ? Attention danger !

2016	2017
37%	34%

Dans **41%** des cas où une fonctionnalité de type « dépôt de pièce jointe » était offerte, une faille a permis de déposer du contenu non autorisé sur le serveur.

Dans **42%** des cas, cela a permis d'exécuter du code sur le serveur.

C'est une voie royale pour rebondir depuis ce serveur vers d'autres composants du SI.

Surfer sur plusieurs sites en parallèle nuit gravement à la sécurité

Plus de **1/2** des sites sont vulnérables à du CSRF* (ou XSRF*) :

- ➔ Pendant l'utilisation d'un site web sensible, vous décidez d'ouvrir un nouvel onglet pour surfer.
- ➔ Le site web de ce nouvel onglet, s'il contient une attaque, est capable de réaliser des actions à votre insu sur le site web sensible : *modifier votre adresse de contact pour réinitialiser le mot de passe par exemple…*

2016	2017
67%	**53%**

59 % des sites vulnérables à du XSRF*

*CSRF ou XSRF : Cross Site Request Forgery

WAVESTONE

Yann FILLIAT
Manager – Responsable offre audit de sécurité

M +33 (0)6 24 76 08 67
yann.filliat@wavestone.com

Gérôme BILLOIS
Partner

M +33 (0)6 10 99 00 60
gerome.billois@wavestone.com

riskinsight-wavestone.com
@Risk_Insight

securityinsider-wavestone.com
@SecuInsider

wavestone.com
@wavestone_

PARIS

LONDRES

NEW YORK

HONG KONG

SINGAPOUR *

DUBAI *

SAO PAULO *

LUXEMBOURG

MADRID *

MILAN *

BRUXELLES

GENEVE

CASABLANCA

ISTANBUL *

LYON

MARSEILLE

NANTES

* Partenariats

WAVESTONE