The Positive Way

WAVESTONE

LA SÉCURITÉ DES SITES DE GRANDES ORGANISATIONS

BILAN 2019

La cybersécurité, un enjeu central pour les organisations

Les dernières cyber-attaques (Altran, M6, Betclic…) *ont démontré que la sécurité des sites et applications mobiles représente plus que jamais un enjeu crucial pour les organisations, tant leurs impacts peuvent être colossaux.*

Depuis 2016, le cabinet Wavestone présente chaque année son benchmark de la sécurité des sites web de grandes organisations françaises.

Plus de 200 sites des plus grandes organisations ont été passés au crible des défaillances cyber cette année.

Le présent benchmark sert un double objectif :

- Apporter un éclairage sur les failles de sécurité rencontrées par les grandes organisations ces 4 dernières années.
- Alerter et sensibiliser sur l'un des sujets les plus stratégiques du moment.

Un retour d'expérience unique sur les audits en cybersécurité

400 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.

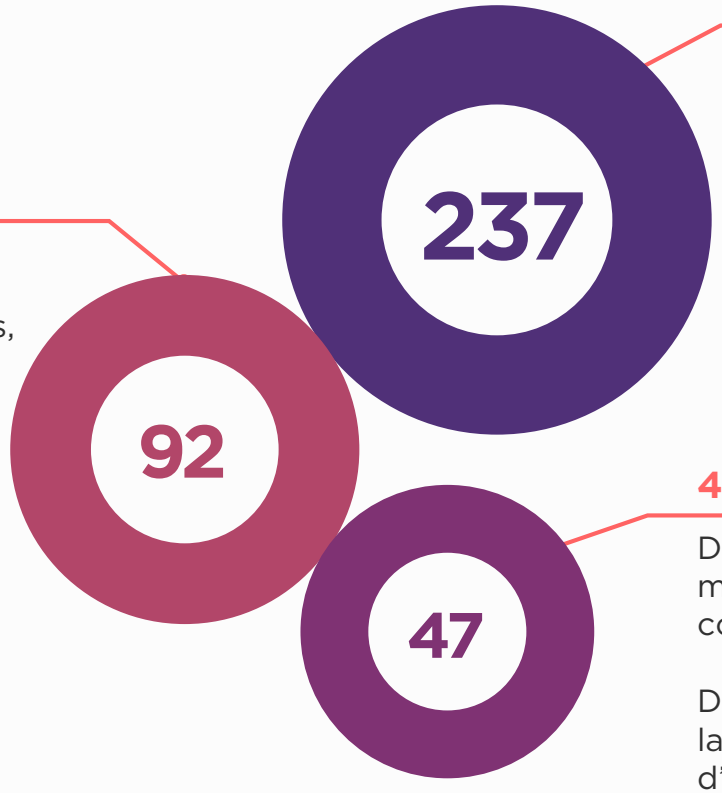
Plus de 120 clients différents

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 2019 des failles de sites web de grandes organisations



237 Sites web

Tests d'intrusion de sites web réalisés au cours de l'année (de juin 2018 à juin 2019) sur des sites sur Internet et des sites sur des réseaux privés d'organisations.

92 organisations

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

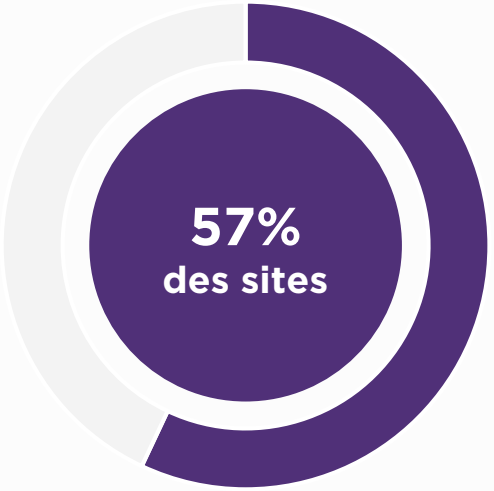
47 Points de contrôle

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.

Des failles graves dans plus de la moitié des cas

Une faille grave permet d'accéder à l'ensemble du contenu du site et/ou de compromettre les serveurs.

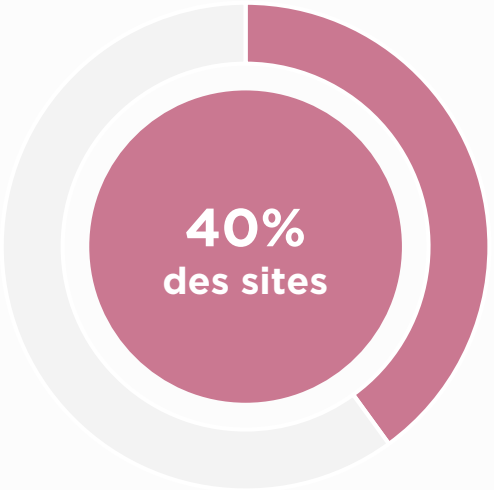


sont touchés par au moins 1 faille grave

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

Des failles importantes qui nuisent à la sécurité des données personnelles

Une faille importante permet d'accéder aux informations d'autres utilisateurs mais en nombre limité ou de manière complexe.

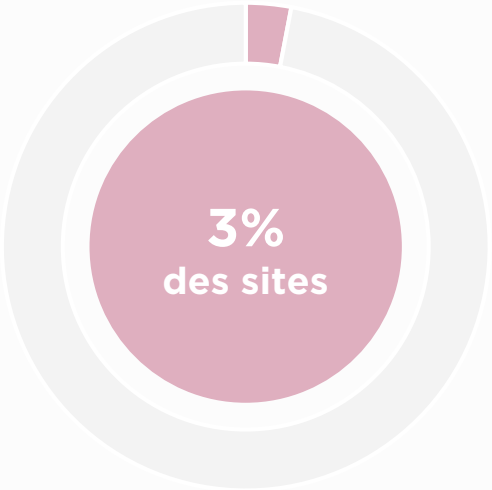


sont touchés par des failles importantes

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

Des failles mineures qui permettent de prolonger l'attaque

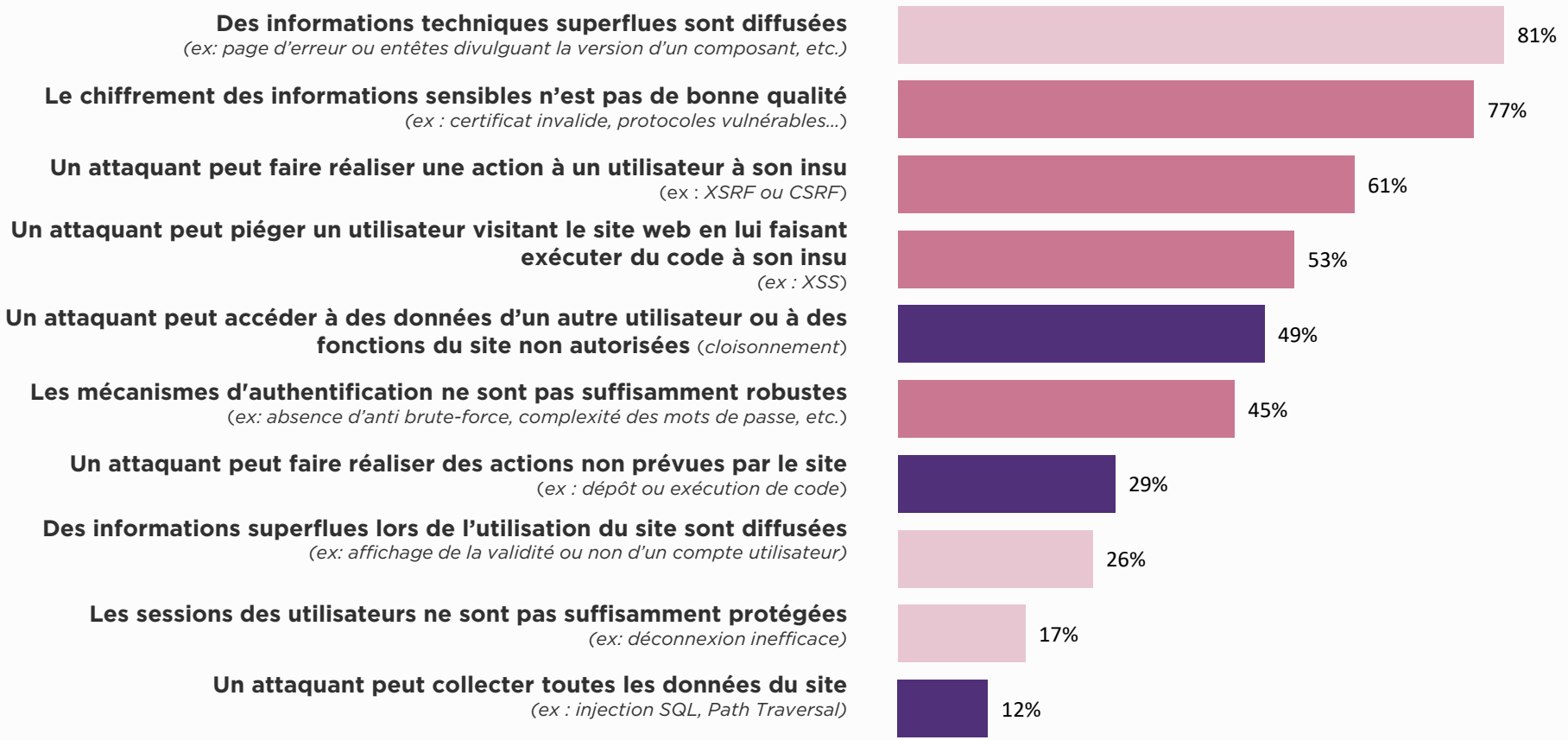
Une faille mineure permet principalement d'obtenir des informations pour continuer l'attaque.



ne sont touchés que par des failles mineures

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

Top 10 des failles en 2019



La sécurité des sites web reste un enjeu majeur pour les organisations

Notre expérience en réponse à incidents vient confirmer la criticité de la sécurisation des sites web.

*Dans 1 cas analysé sur 3 *, l'attaquant a exploité une application web vulnérable afin de pénétrer le système d'information d'une organisation. Il est urgent de mettre en œuvre les mesures de sécurisation de la surface visible des organisations.*

Yann FILLIAT
responsable de l'offre
audit de sécurité

* Etude « Cyberattaques en France : quelle situation sur le terrain ? » publiée par Wavestone en Septembre 2019, synthétisant l'analyse de 40 incidents de sécurité majeurs chez les grandes organisations, ayant mené à l'interruption d'activités métiers ou une compromission avancée du système d'information.

Interprétation des résultats

4 ans après les premiers tests menés par Wavestone, 100% des sites web analysés sont toujours touchés par une faille de sécurité et 57% contiennent une faille grave.

Tout comme les années précédentes, le benchmark cybersécurité a révélé la présence d'au **moins une faille de sécurité sur l'ensemble des sites web analysés.**

Malgré la réalisation d'audits par le passé, **57% des sites testés précédemment restent vulnérables** en 2019 avec au moins une faille grave.

Parmi ces failles, **56% des sites analysés et accessibles à tous depuis Internet contiennent des failles graves** pouvant mener à la fuite d'informations, à l'accès au contenu et à différentes données du site, ou à la prise de contrôle des serveurs.

Toutefois, si moins de sites sont touchés par des failles graves, ils restent touchés par des **failles dites « importantes »** (40% en 2019 vs 42% en 2018).

Les failles importantes permettent d'accéder aux informations d'autres utilisateurs mais en nombre limité ou de manière complexe (vol de session, faiblesse dans le chiffrement, réalisation d'action à l'insu de l'utilisateur…).

Retrouvez les éditions précédentes : 2018 2017 2016

WAVESTONE

Dans un monde où savoir se transformer est la clé du succès, Wavestone s'est donné pour mission d'éclairer et guider les grandes entreprises et organisations dans leurs transformations les plus critiques avec l'ambition de les rendre positives pour toutes les parties prenantes. C'est ce que nous appelons « The Positive Way ».

Wavestone rassemble plus de 3 000 collaborateurs dans 8 pays. Il figure parmi les leaders indépendants du conseil en Europe, et constitue le 1er cabinet de conseil indépendant en France.

Wavestone est coté sur Euronext à Paris et labellisé Great Place To Work® .

Découvrez notre expertise en cybersécurité et confiance numérique

- Management du risque & stratégie
- Conformité numérique
- Cloud & Sécurité nouvelle génération
- Tests d'intrusion et audits de sécurité
- Réponse à incidents
- Identité numérique (pour les utilisateurs et les clients)

En particulier dans le domaine des services financiers, de l'industrie 4.0, de l'IoT et des biens de consommation.

Contacter nos experts