



WAVESTONE

Website security - a benchmark review

*Analysis of 155 sites belonging to France's largest
companies*

October 2017



In a world where continuous evolution is the key to success, we enlighten and partner our clients in their most strategic decisions.



Tier one clients,
leaders in their
industry



2,600 employees across
4 continents



Among the leading independent
consultancies in Europe, and
number one in France.

Paris | London | New York | Hong Kong | Singapore * | Dubai *
Brussels | Luxembourg | Geneva | Casablanca
Lyon | Marseille | Nantes

* Through partnerships



WAVESTONE

WAVESTONE AND CYBERSECURITY AUDITS

Wavestone: unique expertise in cybersecurity audits



350 security audits a year

A wide range of activities: websites, physical penetration testing, social engineering; configuration, code, and industrial IS reviews, etc.

Over 100 different clients

Largely major French companies, operating in national or international markets

Covering all business sectors

Banking/insurance, retail, medical, energy, services, telecoms, transport, defense, public bodies, etc.

2017 Benchmarking on website vulnerabilities




**155
websites
tested**

155 penetration tests carried out on websites between June 2016 and June 2017: 117 public websites and 38 sites on private corporate networks



**70
organizations
involved**

All business sectors were covered: banking, health, defense, energy public bodies, services, e-commerce, telecoms, transport, etc.



**47 potential
flaws tested
each time**

Identical methodologies were used for each test – generating comparable results.

Flaws tested included access control, encryption quality, dissemination of unnecessary technical information, communications handling, etc.

Confidentiality was maintained: the data used for benchmarking was anonymized – the analysis generated aggregate statistics.



WAVESTONE

THE RESULTS

4 striking findings on website security

1 **100%** of websites tested proved vulnerable, regardless of business type or sector.

2 **50%** of sites openly accessible via the internet had at least one serious flaw.

3 **40%** of the sites that had already undergone a security audit were still vulnerable.

4 **90%** of sites tested were already online when our security audits were carried out.

And these findings apply to all business sectors assessed...

No site was perfect!



The figure

100%

As in 2016, all websites tested in 2017 (155) had **at least one** security flaw

A neglect of security issues over time

More than **40%** of the sites tested remain vulnerable, with at least one serious flaw, despite having been previously audited.

Little implementation of corrective measures, and the development of new features without applying good security practices.



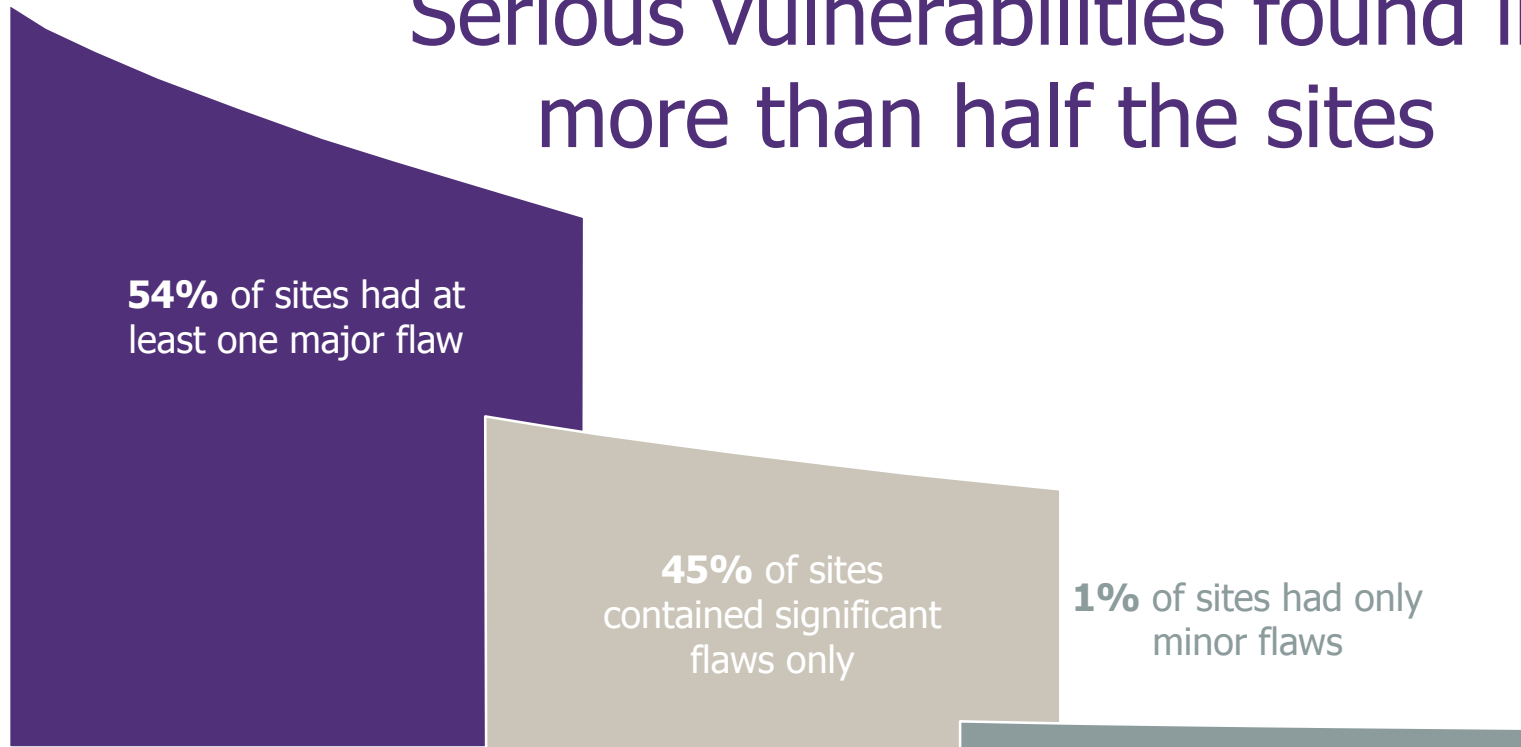
All business sectors are at risk

Percentage of websites (per sector)
with at least one serious vulnerability



Sectors were selected from at least 30 sites to form a representative sample.
53% of all sites in the other sectors – defense, health, real estate, etc. – had serious vulnerabilities

Serious vulnerabilities found in more than half the sites



Compared with 60% in 2016

Major flaw enables access to all site content and/or the compromise of servers
Access to all site data, code execution via the server, User A having access to User B's data, etc.

Compared with 39% in 2016

Significant flaw enables access to information from other users, but this is limited or complicated to manipulate
Theft of a user's session, weak encryption, actions can be carried out without a user's knowledge, etc.

Compared with 1% in 2016

Minor flaw mainly provides information that can be used to continue the attack
Unnecessary technical messages, lack of cookie security, ineffective user disconnection, etc.

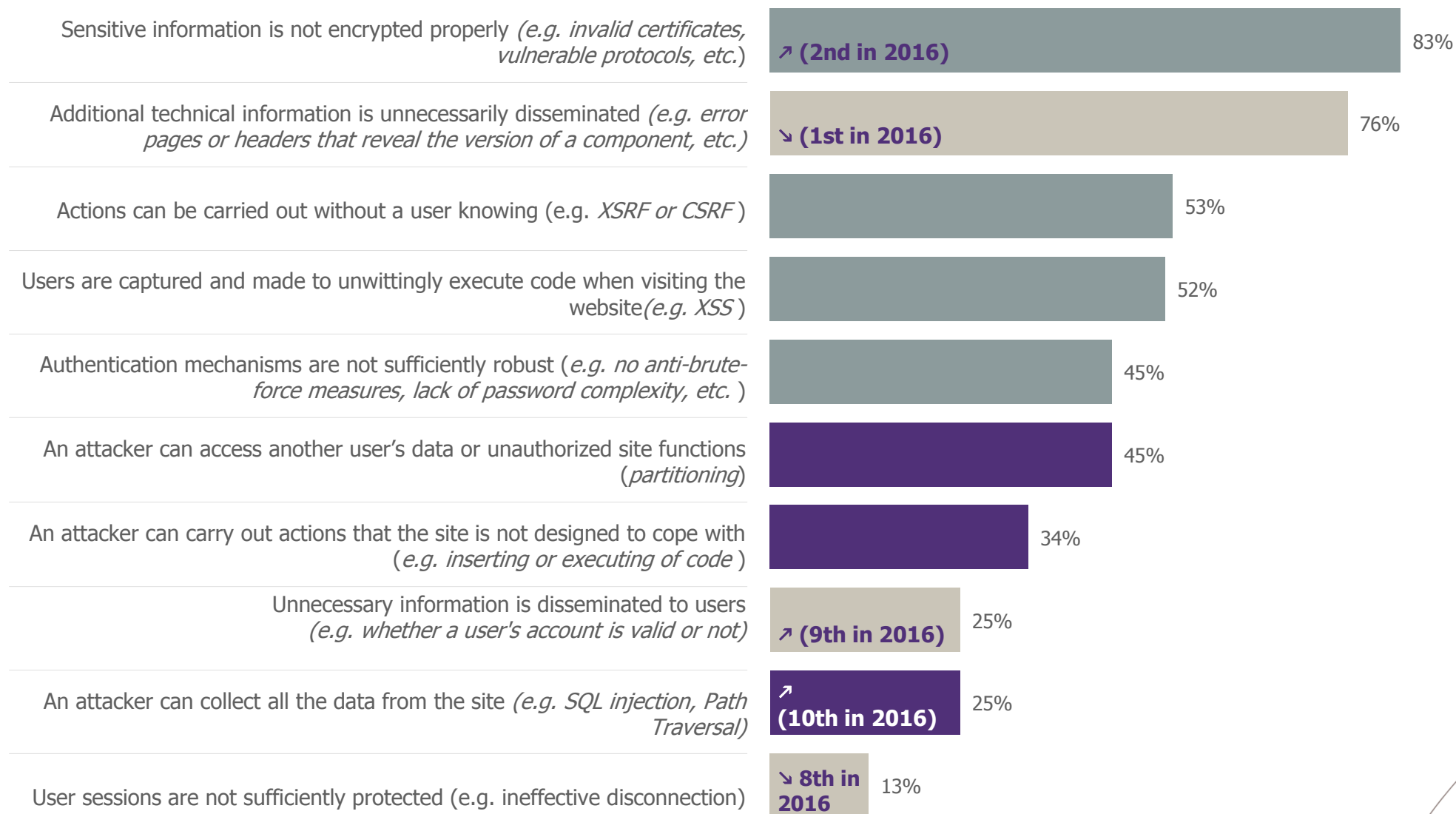
Serious vulnerabilities found on both websites and company intranets

50% of sites openly accessible via the internet had at least one serious flaw



68% of the company intranets had at least one serious flaw

Little change in the top 10 vulnerabilities





WAVESTONE

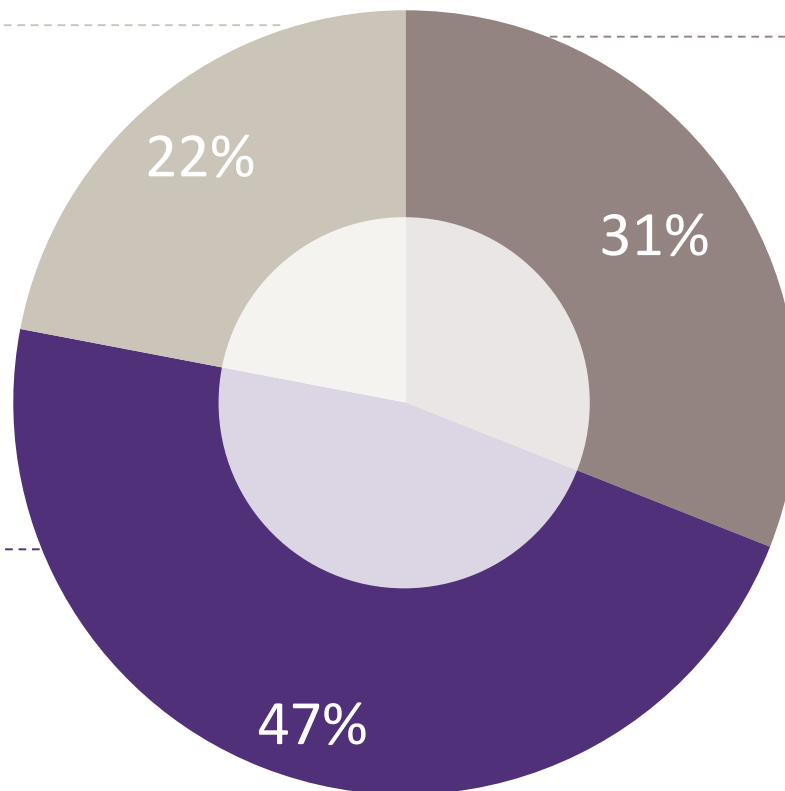
AND NOW?

Corrective actions that need significant effort

A concrete example showing the number of XSS vulnerabilities (code execution in a visitor's browser) identified per site

An oversight

Where a single parameter is vulnerable, corrective action is simple.



Everything needs to be reviewed

The majority of the parameters (dozens or hundreds) are affected; significant action has to be envisaged for the entire site.

A number of shortcomings

A small number of parameters (five to ten) are vulnerable; only a handful of pages will need to be modified.

A change of approach is needed

A dangerous dash for new functionality

The results are indefensible: serious flaws identified on more than 50% of websites already in production...

The current approach to project management leaves little room for security: pressure from the business, urgent needs to go into production, projects that only come to light as they go live, etc.

And the pace continues to accelerate with the rise of agile methods, DevOps, etc.

Learn from mistakes and harness innovations

It's disappointing to see that the situation is not improving over time. Integrating security at the start of the project is a key plank in improving these figures.

Recent technological developments offer the opportunity to apply what has not, so far, been possible: the integration of security into the development process – by bringing security measures within the scope of developers.

The need to invest in skills

The answers won't come just from investments in new security measures, retrospective testing, etc.

Investing in the skills of teams, especially developers, is more important than ever if security is to move from being a mere stage in the process to being an integral part of it.



WAVESTONE

**SPOTLIGHT 2017
CONNECTED OBJECTS
AND THE IoT**

Are connected objects better secured than websites?



Yes, for connected objects developed in France. Wavestone performed ten penetration tests on representative connected objects without finding a flaw that allowed a large-scale attack (although the potential for local attacks was frequently observed)

No, for "low-cost" connected objects which contain numerous flaws, something borne out by the large number of incidents observed in 2016 and 2017



WAVESTONE

ANNEXES

Let's not reinvent the wheel!



50% of sites using PHP without a recognized content management system (CMS) were affected by at least one serious flaw.



Only **30%** of the ones using a recognized CMS were affected, because these also provide security features

Selection of tests carried out on 55 sites using PHP technology

Access controls that don't provide much control...

45% of **gray-box** tests (using a standard user account) allowed application partitioning to be bypassed and access to unauthorized data or functions (horizontal or vertical escalation)

*Compared with **44%** in 2016*



Attach a file? Danger ahead!



In **56%** of the cases where a feature, such as "attach a file" was offered, flaws allowed code to be placed on the server.

In **34%** of cases, this allowed code to be executed on the server.



This provides a perfect opening to use the server as a springboard for the manipulation of other IS components.

37% for attachments in 2016

Surfing several sites in parallel severely compromises security

1/2 of the sites were vulnerable to CSRF* (or XSRF*):

- ➔ While using a sensitive website, you decide to open a new tab for further surfing.
- ⬅ If the website displayed on this new tab contains an attack, it can carry out actions – without your knowledge – on the sensitive website: *changing your contact address to reset the password, for example...*

*Compared with **67%** in 2016, with the difference mainly due to developments in the sample (ASP technology).*



*CSRF or XSRF: Cross Site Request Forgery

WAVESTONE

Yann Filliat
Security Audit Team Manager

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

