WAVESTONE

Website security – a benchmark review

Analysis of 1029 vulnerabilities discovered on the websites of large organisations

Yann FILLIAT
yann.filliat@wavestone.com
Head of Security Audit offer

Gérôme BILLOIS
gerome.billois@wavestone.com
Senior Manager
@gbillois

In a world where permanent evolution is key to success,
we enlighten and partner our clients in making their most critical business decisions

Tier one clients
leaders in their industry

2,500 professionals
across 4 continents

Among the leading independent
consultancies in Europe

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

Wavestone Cybersecurity & Digital Trust

Win the **digital race** with **digital trust**

Building Digital Trust in your organisation is an **essential business enabler** for success in the race for **digital transformation**

400+
Consultants
& Experts

1,000+
Engagements
per year in
20+ countries

Our clients
Board, Business,
CDO, CIO, CISO, BCM

PROVEN EXPERTISE

- Digital Risk Strategy and Compliance
- Safe Business Transformation
- Security Design and Program Management
- Identity, Fraud and Trust Services
- Penetration Testing and Incident Response
- Business Continuity and Resilience

ACTIONABLE INSIGHTS

- Industry-specific risk mapping
- AMT Master plan methodology
- Startups and Innovation Radars
- CERT-W

Wavestone: a unique expertise on security audits

300 security audits per year

100 different clients

8 business sector verticals

Breadth of audit scope: websites, physical penetration tests, social engineering, configuration review and code review

Global organisations, mainly headquartered in France, addressing local and international markets

Financial Services, Retail, Health, Energy, Services, Telecom, Transport and Public Bodies

A website vulnerabilities benchmark

128 tested websites

85 Internet
43 private

Audits and penetration tests were performed on websites between June 2015 and June 2016

All data was anonymised to protect participant data and confidentiality

82 organisations took part in the benchmark

Participants represented the full range of industry and included financial services, health, energy, telecoms, transport and public sector organisations

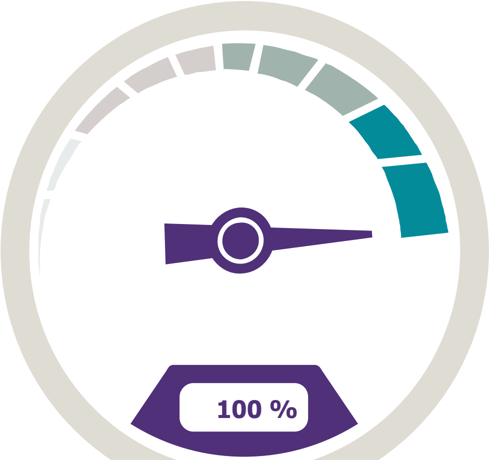
47 vunerability tests for each audit

A standardised test approach was used to evaluate each website for access control, encryption strength and quality, unnecessary display of technical information, communication exchanges and other potential vulnerabilities

90 % of sites online before the test

Although some organisations used the penetration tests to evaluate the security of proposed systems, the majority of tested websites were already in production environments

All tested websites were vulnerable!



The figure

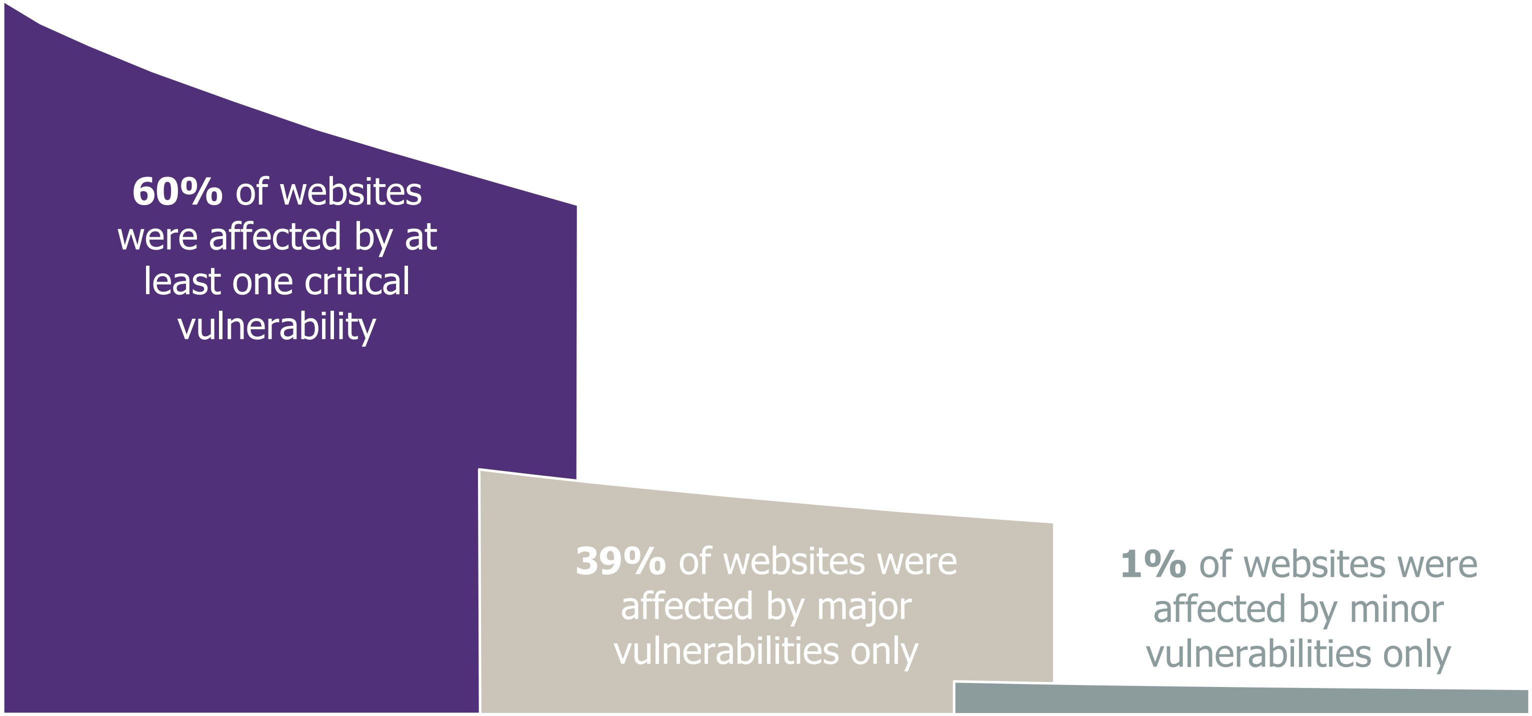
100% On all 128 tested websites, **at least one** vulnerability has been discovered during each test campaign

1 **All** tested websites were vulnerable, across all contexts and business sector

2 **50 %** of public (Internet) facing websites had at least one **critical** vulnerability

3 **75 %** of internal websites for employees had at least one **critical** vulnerability

Critical vulnerabilities existed in 60% of cases



60% of websites were affected by at least one critical vulnerability

39% of websites were affected by major vulnerabilities only

1% of websites were affected by minor vulnerabilities only

Critical vulnerability
Allows full access to website content and/or server compromise

Access to all data from the website, code execution on server, user A accessing data from user B, etc.

Major vulnerability
Allows access other users' data on a reduced scope or only with a complex technique

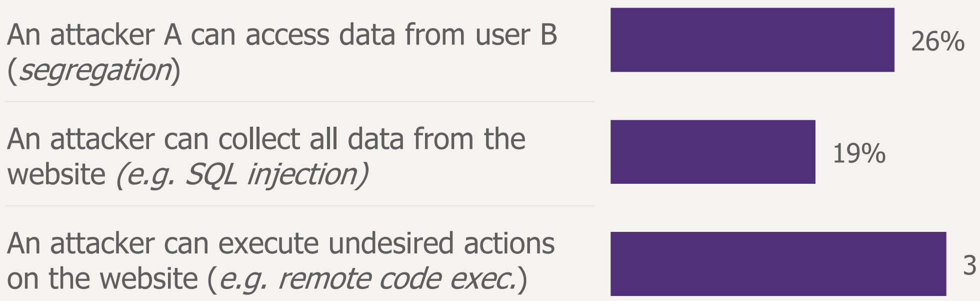
Session theft, weakness in encryption protocol, unwanted actions performed by users, etc.

Minor vulnerability
Largely limited to providing more information to allow continued attack

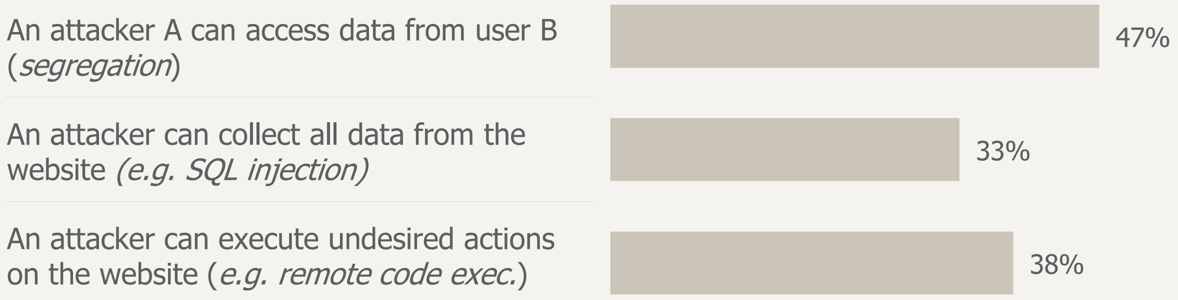
Unnecessary technical messages, unsecure cookies, incomplete disconnection, etc.

Breakdown of **critical** vulnerabilities on Internet and intranet websites

#2: 50% of public (Internet) facing websites had at least one **critical** vulnerability



#3: 75% of internal websites for employees had at least one **critical** vulnerability



Website design was often a critical factor

4 key design issues relating to critical vulnerabilities were recurring themes in the TOP 10 most encountered vulnerabilities

1 **Access control**

An attacker can, with a basic user account, access data from all users

2 **File upload**

File upload functions frequently allow an attacker to fully take control of a website

3 **Sessions**

An attacker can, with an open tab, interact with a website opened in another tab

4 **Language**

The development language does not change the amount of vulnerabilities… but their criticality!

An access control
not always under control…

44% of tests performed in **grey box** mode (where a standard user account was available) demonstrated a bypass access control vulnerability, allowing access to unauthorised data or functions (horizontal or vertical privilege escalation)

File upload?
Dangerous cross road!

37 %

In **37%** of 68 cases where a file upload function was available, a vulnerability was identified that allowed custom code to be placed and executed on the web server

This type of vulnerability provides an attacker with the means to jump from the web server to other information system devices

Browsing multiple websites is bad for your own security

2/3 of websites tested were vulnerable to CSRF* (or XSRF*):

- ➔ While using a sensitive website, you decide to open a new browser tab
- ← The website in this new tab, if malicious, is capable performing actions without your consent on your sensitive website, such as changing the **email address** used to re-set your **password**

**CSRF or XSRF: Cross Site Request Forgery*

67 % of websites were vulnerable to XSRF*

The web server scripting language used did not change the amount of vulnerabilities… but did change their criticality

≠

Java

39%

of vulnerabilities

PHP

44%

of vulnerabilities

Java

40%

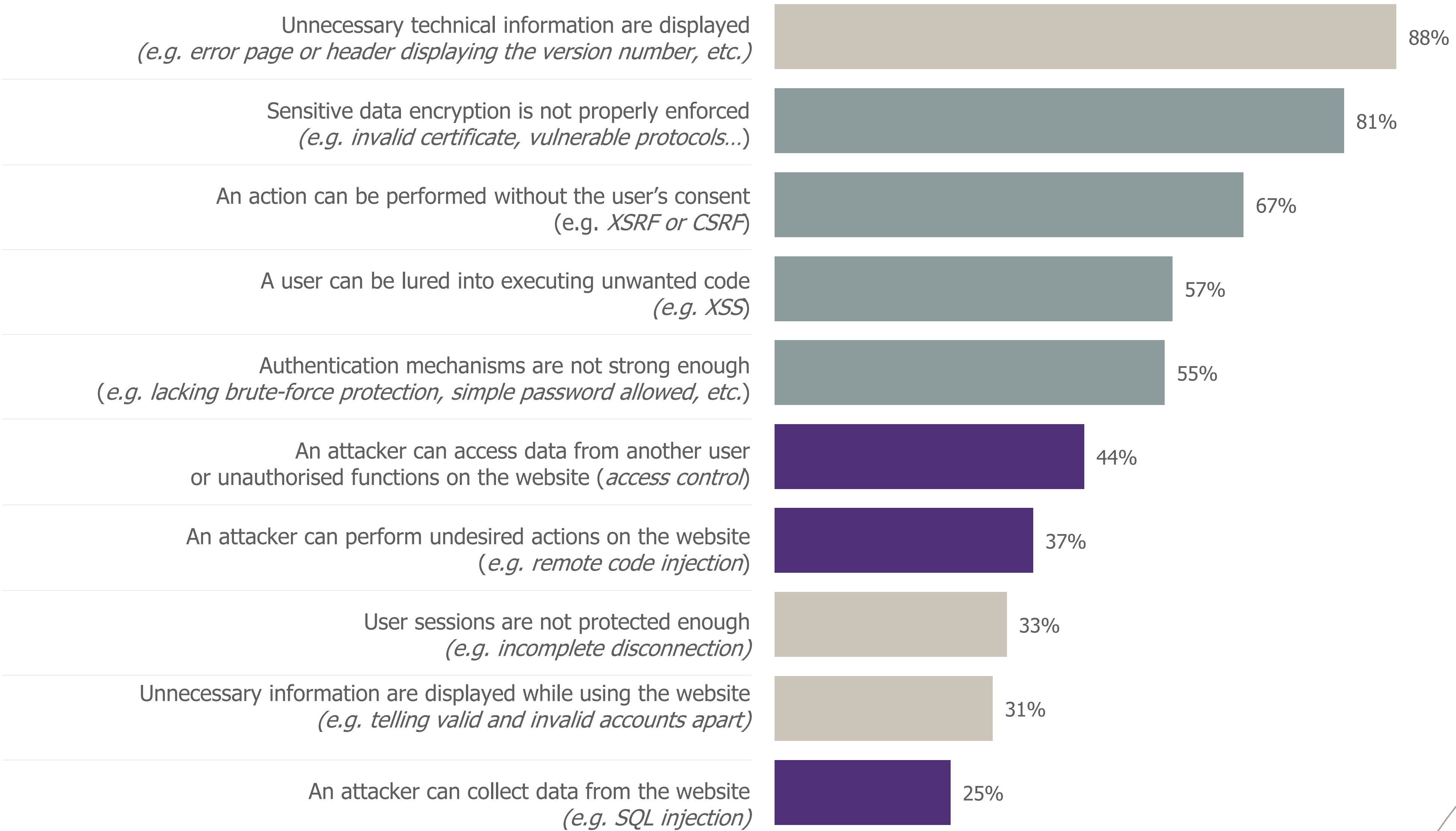
of websites had at least a critical vulnerability

PHP

75%

of websites had at least a critical vulnerability

Top 10 most encountered vulnerabilities



Vulnerabilities leading to ■ Critical ■ Major ■ Minor security risks

And now, what's next?

Improve project mindsets

It is alarming that critical vulnerabilities were discovered in 60% of the websites which were already in production

Project management currently leaves no room for security: for urgent projects, websites are often deployed with little or no security controls or testing

Embedding security from the beginning of all projects is one way to improve this situation

Adapt to the disruption of digital methodologies

The pace of release is increasing with new Agile methodologies, DevOps…

Would you be able to perform a penetration test every 15 days in a world where it is already difficult to have 1 before being deployed in production?

This is the opportunity for a change: embed continuous security in the development process by bringing pentest and engineering teams closer together.

Implement improved governance

Security will not be delivered only through buying new security solutions or through carrying out retrospective audits

It is now time to invest in improving team skills, particularly engineering teams, for security to be less of a (rarely) observed step in a process and more of a day-to-day reality.

WAVESTONE

Yann FILLIAT
Manager – Head of Security Audit offer
M +33 (0)6 24 76 08 67
yann.filliat@wavestone.com

Etienne CAPGRAS
Manager – Head of Security Audit offer
M +33 (0)6 67 49 45 35
etienne.capgras@wavestone.com

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

RI riskinsight-wavestone.com
@Risk_Insight

SI securityinsider-wavestone.com
@SecuInsider

wavestone.com
@wavestone_

PARIS

LONDON

NEW YORK

HONG KONG

SINGAPORE *

DUBAI *

BRUSSELS

LUXEMBOURG

GENEVA

CASABLANCA

LYON

MARSEILLE

NANTES

* Strategic partners

WAVESTONE