GDPR - Websites: security, privacy, performance and quality

Use the following table to test if a website is unsafe (can not be said to be safe!).
See the notes below (including links) to understand the rationale for these tests.
There is a script that streamlines the tests, "GDPR-IsMyWebsiteInSecure".

Category	Test	Tool	Metric
security	yes	https://pentest-tools.com/network-vulnerability-scanning/tcp-port-scanner-online-nmap https://nmap.org/ (-sV | -v -A url)	tcp/443
security	Yes	https://www.wpsec.com/	no vulnerabilities
security	yes	https://sitecheck.sucuri.net/	no malware no outdated software
security	yes	https://www.ssllabs.com/ssltest/index.html	A
security	yes	https://observatory.allizom.org/	A
security	yes	https://internet.nl/	90
security	yes	https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project	no vulnerabilities
security	(*)	https://www.arachni-scanner.com/	no vulnerabilities
security	(*)	http://sqlmap.org/	no vulnerabilities
privacy/cookies	yes	https://www.ezigdpr.com/products/gdpr-website-compliance-checker	no action required
privacy/cookies	(*)	https://www.cookiebot.com/en/	no action required
performance	yes	https://batchspeed.com/	90
performance	yes	https://developers.google.com/speed/pagespeed/insights/	90
performance	(*)	https://developers.google.com/web/tools/lighthouse/ (test mobile, desktop)	90
performance	(*)	https://gtmetrix.com/	90
performance	(*)	https://www.webpagetest.org/	B
quality	yes	http://validator.w3.org/	no errors
quality	yes	https://jigsaw.w3.org/css-validator/	no errors
quality	yes	https://website.grader.com/	90
quality	(*)	https://www.dareboost.com/	90

Grades:

- use only if authorized
- security is a necessary but not sufficient requirement to ensure that a website is GDPR "compliance"
- all websites must have a digital certificate applied and all urls must use https
- in the "Content Security Policy Header" 'unsafe-inline' and 'unsafe-eval' are not allowed
- sites with high risk vulnerabilities should be placed immediately "out of service" and all vulnerabilities corrected
- sites with medium or low risk vulnerabilities should be immediately corrected
- pages with syntactic errors (html, css, etc.) should be corrected immediately
- if the minimum score is not reached, the tests must continue, for each of the categories, with the tools marked with (*)

(c)2019 v1.2 Oscar Azevedo

GDPR - Websites: security, privacy, performance and quality

Use of "utilities" or platforms

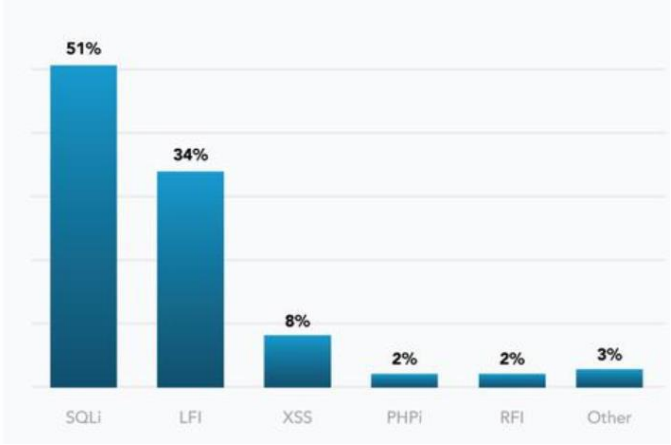
The use of "utilities" (jQuery, Bootstrap, etc.), frameworks or platforms (Wordpress, etc.) in the development of websites should only be applied, once accepted by the client, when standard languages are not sufficient or effective, by themselves carry a security risk and should be guaranteed by those who develop the following:
- the use of the latest versions
- upgrade to the latest version or release at no additional cost during the term of the agreement or warranty period

Compliance with requirements / specifications

Validation of the tests (safety, privacy, performance and quality) does not ensure that the development complies with the functional requirements or specifications of the project (website / portal).

Cybersecurity

"Web applications are becoming more interesting targets for adversaries as more businesses and firms are becoming dependent on web services, both in revenue and reputation".
"Web based attacks continued to be observed as one of the most important threats due to their wide spread surface across the threat landscape, from general ad related spamming campaigns to banking trojans117 and multiple Advanced Persistent Threat (APT) groups118 facilitating such attacks as their techniques to target victims. This threat is expected to increase as more malware and exploitation techniques rely more heavily on it, as a delivery mechanism, during the end-to-end attack path."



source: ENISA Threat Landscape Report 2018 January 2019, 15 Top Cyberthreats and Trends

https://www.enisa.europa.eu (ENISA - European Union Agency For Network and Information Security)
https://www.nist.gov/cyberframework (NIST - National Institute of Standards and Tecnology, U.S. Department of Commerce)
https://www.iso.org/isoiec-27001-information-security.html (ISO 27001 - information security)
https://www.iso.org/news/2012/10/Ref1667.html (ISO 27032 - Guidelines for cybersecurity)

https://infosec.mozilla.org/guidelines/web_security
https://infosec.mozilla.org/fundamentals/security_principles.html
https://developers.google.com/web/fundamentals/security/csp/
https://content-security-policy.com/
https://www.hacker101.com/videos
https://kali.training/
https://www.owasp.org/index.php/OWASP_Secure_Headers_Project#tab=Headers
https://scotthelme.co.uk/hardening-your-http-response-headers/
https://developers.google.com/web/fundamentals/performance/why-performance-matters/

GDPR

https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=EN#d1e40-1-1
(GDPR - General Data Protection Regulation)
https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=EN#d1e4234-1-1
(GDPR, art. 32 treatment safety)

(c)2019 v1.2 Oscar Azevedo