GDPR - Websites: security, privacy, performance and quality

Utilize a seguinte tabela para testar se um website é inseguro (não se pode afirmar que é seguro!).
Veja as notas infra (incluindo links) para perceber a fundamentação destes testes.
Existe um script que agiliza os testes, "GDPR - Is my Website inSecure?"

Categoria	Testar	Ferramenta	Critério / Pontuação mínima
security	sim	https://pentest-tools.com/network-vulnerability-scanning/tcp-port-scanner-online-nmap https://nmap.org/ (-sV | -v -A url)	unicamente porta tcp/443
security	sim	https://sitecheck.sucuri.net/	low risk, no software outdated
security	sim	https://www.ssllabs.com/ssltest/index.html	A
security	sim	https://observatory.allizom.org/	A
security	Sim	https://internet.nl/	100%
security	sim	https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project	zero risco elevado, médio e baixo
security	(*)	https://www.arachni-scanner.com/	zero risco elevado, médio e baixo
security	(*)	https://pentest-tools.com/website-vulnerability-scanning/sql-injection-scanner-online http://sqlmap.org/ (utilizar unicamente se for autorizado)	zero risco
privacy/cookies	sim	https://www.ezigdpr.com/products/gdpr-website-compliance-checker	No Action Required
privacy/cookies	(*)	https://www.cookiebot.com/en/	No Action Required
performance	sim	https://batchspeed.com/	90
performance	sim	https://developers.google.com/speed/pagespeed/insights/	90
performance	(*)	https://developers.google.com/web/tools/lighthouse/ (testar c/ opção mobile e desktop)	90, 90, 90, 90
performance	(*)	https://gtmetrix.com/	90%, 90%
performance	(*)	https://www.webpagetest.org	B
quality	sim	http://validator.w3.org/	zero erros, zero avisos
quality	sim	https://jigsaw.w3.org/css-validator/	zero erros, zero avisos
quality	sim	https://website.grader.com/	90
quality	(*)	https://www.dareboost.com/	90%

Nota(s):

- a segurança é um requisito necessário mas não suficiente para garantir que um Website é GDPR "compliance"
- todos os websites devem ter um certificado digital aplicado e todos os urls devem utilizar https
- na configuração do "Content Security Policy Header" não são permitidos 'unsafe-inline' e 'unsafe-eval'
- sites com vulnerabilidades de risco elevado devem ser colocados imediatamente "fora de serviço" e as todas as vulnerabilidades corrigidas
- sites com vulnerabilidades de risco médio ou baixo devem ser imediatamente corrigidos
- páginas com erros sintáticos (html, css, etc.) devem ser corrigidas de imediato
- se não for atingido o score mínimo os testes devem prosseguir, para cada uma das categorias, com as ferramentas assinaladas com (*)

Utilização de "utilitários" ou plataformas

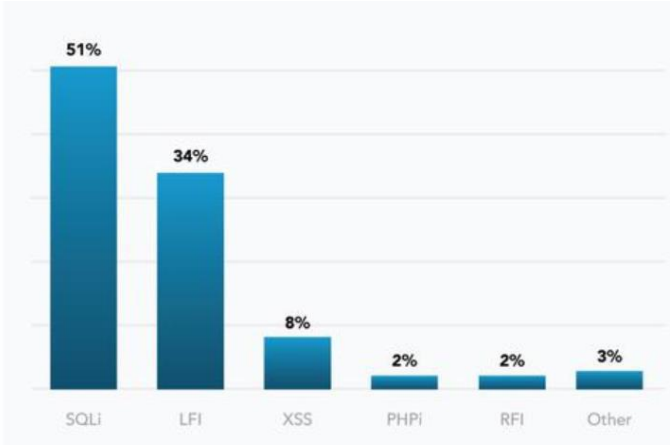
A utilização de "utilitários" (jQuery, Bootstrap, etc.), frameworks ou plataformas (Wordpress, etc.) no desenvolvimento de websites só deve ser aplicada, após aceite pelo cliente, quando as linguagens standard não forem suficientes ou eficazes, sendo que por si só acarretam um risco de segurança pelo que deve ser garantido por quem desenvolve o seguinte:
- a utilização, sempre, das últimas versões
- o upgrade para a última versão ou release, sem qualquer custo adicional, durante a vigência do contrato ou do período de garantia

Conformidade com os requisitos/especificações

- A validação dos testes (segurança, privacidade, desempenho e qualidade) não assegura que o desenvolvimento esteja de acordo com os requisitos ou especificações funcionais do projeto (website/portal).

Cibersegurança

"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 - segurança da informação)
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 - Websites: security, privacy, performance and quality

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.º 32 segurança do tratamento)