Assignment #2: Questionnaires

Ignacio Nieto Vidaurrázaga, 50757986-E
inietv00@estudiantes.unileon.es

Diseño y programación seguras
Máster Universitario en Ciberseguridad
Universidad de León (Spain)

I. Purpose

- The objective of this report is to make a brief analysis and comparison between some questionnaires used to secure information systems. I have chosen two questionnaires and the ASVS as a framework of reference. That three objects of study have interesting differences but it is not attempted to delve into any them nor assert which one is better. Each of them could be recommended depending on the needs of the organization.

  I've chosen the ASVS although it is not strictly a questionnaire, and that's because its items to be checked are a reference for almost all questionnaires nowadays, to the point that ASVS has become a de facto standard.

II. Comparison table

- In this section the three questionnaires are shown in a table format because it is the most visual way to perform the analysis and see the differences. The first two samplings are from the educational environment, Purdue University and University of California Irvine. And the last one, the Application Security Verification Standard by the OWASP Foundation, is more than a questionnaire as it is considered as a standard of secure application development.

	University of California Irvine	Purdue University	ASVS by OWASP
ID	Security Risk Assessment Questionnaire - v1.5 (09/04/2018) https://security.uci.edu/security-plan/plan-resources.html	Vendor Security Questionnaire v8.2 (no date of release found) https://www.purdue.edu/securepurdue/services/solution-services-review.php	OWASP Application Security Verification Standard v4.0.3 (october 2021) https://github.com/OWASP/ASVS
GOAL	Self-assessment tool designed to help Unit's understand the security posture of the University systems.	Protect University Resources and Information assets when it is started a procedure of purchasing software.	The primary aim is to provide an open application security standard for web apps and web services of all types. Normalize the range in the coverage and level of rigor available in the market when it comes to performing Web application security verification using a commercially-workable open standard.
TARGET USERS	Generic individuals willing to understand the security posture of their system and to identify ways to make their systems more secure. It is designed to protect University of Calfornia IT Resources whose unauthorized disclosure or modification could result in moderate to severe fines or modifications, losses or deletions that could result in moderate damage to that university	These kind of issues are mostly related to the PDF viewer, they will not appear in a print version of the document.	All software developers who need a list of requirements for secure development.

	University of California Irvine	Purdue University	ASVS by OWASP
DESCRIPTION	20 main sections with **almost 150 security and verification questions**: 1. Input Validation 2. Output Escaping/Encoding 3. Authentication and Password Management 4. Session Management 5. Authorization and Access Control 6. Cryptographic Practices 7. Error Handling, Auditing and Logging 8. Data Protection 9. Communication Security 10. System Configuration/Hardening 11. Database Security 12. File Management	The questionnaire is within a scheduled process that concludes with the approval or denial of the purchase of software. This process involves in the filling of the questionnaire by the vendor, technical stuff and employees of the University. All those actors must fill **more than 220 questions** and cells divided in 4 four tabs: 1) Project Information. 2) Data security. 3) Vendor Hosted. 4) Purdue Hosted. With all the information the IT software is scored.	Its composed by **286 points to be checked**. It covers all phases in development with their potential risks and is divided in 14 sections: 1) Architecture, Design and Threat Modeling. 2) Authentication 3) Session Management 4) Access Control 5) Validation, Sanitization and Encoding 6) Stored Cryptography 7) Error Handling and Logging 8) Data Protection 9) Communication 10) Malicious Code 11) Business Logic 12) Files and Resources 13) API and Web Service 14) Configuration
PROS AND CONS	Well structured and very generic so it can be applied for most IT systems. The web page is clear and help potential users to follow the questionnaire. It has Only 6 versions since 2012, that gives us an idea of the lack of a strong community that contributes to develop this document. No GitHub or other official and verified repositories. Probably due to lack of employees designed to maintain this we can find unforgivable errors such as a users guide only for the version released in 2012.	Once the questionnaire is submitted, Purdue University ensure that the purchase is rated and approved or denied within 30 days. Thats a quality characteristic since there are recommendations in the review report and not only a rating. There is another interesting Purdue's document, the Cloud Computing Consumer Guidelines, which provide guidance on operational and contractual requirements when is a Cloud service purchase. There are no indications of different levels of security, so there is no distinction between small software and huge developments, all of then will have to fulfil the same requirements in the questionnaire.	Strong community of contributors involved in the project and supported by an organization that is a reference in security. Furthermore is a non profit organization so it cant be focused to personal interests as other private companies or Universities. Also is a reference for every IT institution than tend to follow OWASP recommendations and adapt them in their processes and questionnaires. The biggest disadvantage of ASVS is the level of detail and thoroughness that requires. This requires more and harder efforts from the companies that wanted to apply it. And over all it is needed qualified IT staff that can lead the entire process of security.

	University of California Irvine	Purdue University	ASVS by OWASP
OTHERS	Some resources are offered by the UCI in order to attach correct format documents (data flow and network diagrams for example) to the questionnaire: https://wiki.oit.uci.edu/display/public/SRAQ+Network+Diagram+and+Data+Flow+Diagram+Examples	The questionnaire, the instructions, the version history and the reviewer scoring are unified in a single document. This can help to clarify the process of evaluating.	In older versions there were 4 levels of security but the level 0 has been cancelled since this standard want to apply minimum levels of thoroughness in development. ASVS requirement lists are made available in CSV, JSON, and other formats which may be useful for reference or programmatic use.

III. Conclusion

- The three questionnaires are very useful when trying to adopt good practices in IT security. The two first are internal documents that help the universities in their purchases processes. The ASVS is more global and pretend to be a standard (in fact it is, because is referenced by almost all organizations developing web-based applications. UCI questionnaire refer it).

  You must take into consideration the ASVS when developing or acquiring software but undoubtedly there are other questionnaires that are easier to fill and can be enough for some simple applications. If you want to implement the higher levels of security and thoroughness and consequently minimize risks you ought to implement OWASP ASVS.