Project: Juice Shop Vulnerabilities Report

Report Design and Language

Success Criteria	Specifications
Communicate risk and vulnerabilities in a professional, meaningful, concise, and methodical way.	The submission follows a reporting flow that includes the following sections: 1. Cover Page 2. Security Engagement Summary 3. Significant Vulnerabilities Summary 4. Significant Vulnerabilities Detail 5. Security Analysis Methodology

Communicate technical information in tone and language appropriate to intended audiences.	The report is written for its intended audience and can be easily consumed by multiple functions of the organization; each section of the report is written in the appropriate tone and language according to its intended audience.
	
	• **Executive Language**
	  • Security Engagement Summary
	• **Technical Management Language**
	  • Significant Vulnerabilities Summary
	  • Significant Vulnerabilities Detail
	• **Practitioner Technical Language**
	  • Security Analysis Methodology

Executive Engagement Overview, Scope, and Analysis

Success Criteria	Specifications
Propose appropriate frequency, scope, and type of vulnerability assessments/penetration testing.	Report includes discussion of the necessity of the tasked project and if the task was a recurring assessment. If the task is a recurring assessment, the report discusses if modifications are warranted on the frequency of assessment.
Analyze the results of a vulnerability assessment or penetration test and identify overall business risk impact.	Report includes an overall risk associated with the identified vulnerabilities during the engagement. These risks are presented in common-language consumable by executive-leadership who can use this information to direct appropriate action. The overall risk should be presented in terms of HIGH | Medium | Low | Information. The overall risk rating is discussed.
Analyze the results of the vulnerability assessment and provide an executive recommendation for remediation.	Report includes a brief discussion regarding a recommendation of remediation efforts. This discussion should provide enough information (facts) that an executive could determine if

Success Criteria	Specifications
	remediation efforts are warranted and what action they should take to begin remediation efforts. It should not include specific details or remediation details.

Vulnerability and Risk Analysis (Managerial Summary)

Success Criteria	Specifications
Analyze the results of a vulnerability assessment or penetration test and identify business risk impact.	Report includes an overall discussion of the scanning results and selects specific significant vulnerabilities that warrant further research or validation. Report considers the risk of at least 2 significant vulnerabilities. These vulnerabilities have been summarized and added in a dedicated section of the report.
Determine the probability that a vulnerability associated with a threat will result in a compromise of integrity or system breach.	Report includes a discussion of the probability that a vulnerability could be exploited. Report considers the probability of exploit of at least 2 significant vulnerabilities. These vulnerabilities have been summarized and added in a dedicated section of the report.
Analyze the results of a vulnerability assessment or penetration test and identify appropriate remediation / mitigation / hardening actionable items.	Report includes a discussion of the potential remediation / mitigation / hardening / action items related to a vulnerability. Report includes this discussion for at least two significant vulnerabilities.
Prioritize mitigation/remediation efforts according to vulnerability risk and probability.	Report includes a summary of vulnerabilities and a section that identifies significant vulnerabilities that includes a discussion of each. These significant vulnerabilities are presented in descending order according to priority.
Research, propose, and deploy mitigating or remediation processes to eliminate a vulnerability.	Report includes a discussion of each highlighted vulnerability and includes information on potential remediation. Specific technical remediations are not necessary, but may be linked as references for further research by the reader.
Determine the users, departments, workflows, and business continuity potentially impacted by a vulnerability’s risk.	The report includes a summary of vulnerabilities and a section that identifies significant vulnerabilities that includes an analysis of the users, departments, workflow and/or business continuity potentially impacted by the vulnerability’s risk. These significant vulnerabilities are presented in descending order according to priority.

Assessment Methodology (Practitioner Detail)

Success Criteria	Specifications
Identify the appropriate tools and/or techniques to identify vulnerabilities in a technology.	Report includes a list of tools appropriate for the specified assessment. At least one vulnerability scanning tool had been identified.
Identify vulnerabilities associated with technologies deployed in an environment.	Report includes a methodological process of the process of configuring and executing the vulnerability scan. Use of technical language in this section is expected; it may include technical jargon and is intended for practitioner's consumption. The tone of this section of the report is statements of facts, roughly documented in a chronological or story-board order. The methodology includes sufficient detail to allow another security analyst to arrive at the same conclusions as summarized earlier in the report. The Report methodology includes evidence that the assessment tool was executed and its output was reviewed. The Report includes either evidence of validation of specific vulnerabilities and/or a detailed discussion of the vulnerabilities impact within the environment.