Project: Insecure Juice Shop

Section 1: Threat Assessment

Success Criteria	Specifications
Identify all components of the Juice Shop application and explain their function	Looking at the architecture diagram, identify all the components that make up the Juice Shop and document them in the Assessment Inventory section of your report. Explain each component's function on the slide.
Conduct an architecture audit of UdaJuicer	Reference the secure architecture best practices and identify at least 3 flaws in the Udajuicer architecture.
Build a Threat Model and identify threats or vulnerabilities	Build a Threat Model of the Juice Shop and identify at least 3 possible threats or vulnerabilities that could affect the Juice Shop. Make sure to include in your Threat Model: • Web Server • Application Server • Database • Client Browser
Identify what sort of attack is taking place by looking at web server logs	Identify which type of attack is causing the Udajuicer site to crash. Based on the data in the logs, explain why you think it is this type of attack.
Identify the possible threat actor and their motivation for wanting to take down the Udajuicer's website	Identify the most likely threat actor for the attack. Provide reasoning for your theory in at least 3 sentences.

Section 2: Vulnerability Analysis

Success Criteria	Specifications
Login as Admin on the UdaJuicer site by exploiting a SQL injection vulnerability	After loading up the Udajuicer website navigate to the login page and exploit a SQL Injection vulnerability to gain admin access. Submit a screenshot of the injection you typed to perform the exploit and a screenshot of you logged in as admin.
Exploit a XSS Vulnerability	After gaining access to the site as admin perform a reflected xss attack in the search bar to get a message box to pop up saying "Hacked!" Submit a screenshot of your command and the message box showing the reflected XSS.

Section 3: Prioritization of Risks

Success Criteria	Specifications
Rank risks based on the negative impact on the organization	Rank the following risks: • *Name of Attack Identified in 1.3* • Insecure Architecture • SQL Injection Vulnerability • XSS Vulnerability
Explain the rationale behind the risk ranking	Give a justification for how you ranked each of the risks. Your answer must be reasonable based on the content of the course and based on learned content, not hypothetical scenarios.

Section 4: Mitigation Plan

Success Criteria	Specifications
Design a secure architecture for the website	Use draw.io to draw a secure architecture. Reference secure architecture best practices and make sure your design fixes the issues initially highlighted in your audit.
Build a countermeasure for the identified attack Udajuicer is facing	Choose one or more of the prevention methods we've covered in the course and describe how implementing this would prevent further attacks.
Suggest possible solutions to prevent SQL Injection attacks and how their prevention method works	Choose one or more of the prevention methods we've covered in the course and describe how it would prevent further SQL Injection attacks.
Suggest possible solutions to prevent XSS attacks and how their prevention method works	Choose one or more of the prevention methods we've covered in the course and describe how it would prevent further XSS attacks.