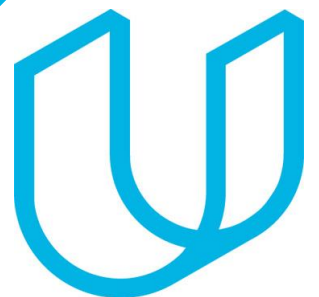


Udajuicer: Threat Report



YOUR NAME:

DATE



How to use this Template

- Make a copy of this Google Slide deck.
- We have provided these slides as a guide to ensure that you submit all the required components to successfully complete your project.
- When presenting your project, please only think of this as a guide. We encouraged you to use creative freedom when making changes as long as the required information is present.
- **Remember to delete this and all** of the other example slides before you submit your project.
- **Remember to add your name and the date** to the cover slide

Reference slide remove
before you submit

Purpose of this Report:

This is a threat model report for **Udajuicer**. The report will describe the threats facing Udajuicer. The model will cover the following:

- Threat Assessment
 - Scoping out Asset Inventory
 - Architecture Audit
 - Threat Model Diagram
 - Threats to the Organization
 - Identifying Threat Actors
- Vulnerability Analysis
- Risk Analysis
- Mitigation Plan



Section 1

Threat Assessment

1.1: Asset Inventory

Components and Functions

- ***[Part Name Here]:*** [Part Function Here]
- ***[Part Name Here]:*** [Part Function Here]
- *[Add extra parts and functions as necessary.]*

1.1: Asset Inventory

Explanation of How A Request Goes from Client to Server

[Response Here]

1.2 Architecture Audit

Flaws

- *[Flaw 1 Here]*
- *[Flaw 2 Here]*
- *[Flaw 3 Here]*
- *[Add extra flaws as necessary]*

1.3 Threat Model Diagram

Using OWASP Threat Dragon, build a diagram showing the flow of data in the Juice Shop application and identify 3 possible threats to the Juice Shop. Make sure to include the following components:

- **Client**
- **Web Server**
- **Application Server**
- **Database**

1.3 Threat Model Diagram

Insert Threat Model Diagram Here:

1.4 Threat Analysis

What Type of Attack Caused the Crash?

[Name of Attack Here]

What in the Logs Proves Your Theory?

[Proof Here]

1.5 Threat Actor Analysis

Who is the Most Likely Threat Actor?

[Type of Threat Actor Here]

What Proves Your Theory?

[Proof Here]



Section 2

Vulnerability Analysis

2.1 SQL Injection

Insert Screenshot of Your Commands Here:

2.1 SQL Injection

Insert Screenshot of Account Settings Showing You as Admin Here:

2.2 XSS

Insert Screenshot of Your Commands Here:

2.2 XSS

**Insert Screenshot of `alert()` popup saying "Hacked!"
Here:**

Optional Task:

Extra Vulnerabilities

- *[Vulnerability 1 Here]*
- *[Vulnerability 2 Here]*
- *[Add more vulnerabilities as necessary]*



Section 3

Risk Analysis

3.1 Scoring Risks

| Risk | Score <i>(1 is most dangerous, 4 is least dangerous)</i> |
|--|---|
| <i>[Name of Attack Identified in 1.3 Here]</i> | |
| Insecure Architecture | |
| SQL Injection | |
| XSS Vulnerability | |

3.2 Risk Rationale

Why Did You Choose That Ranking?

[Rationale Here]



Section 4

Mitigation Plan

4.1 Secure Architecture

Insert Image of Your Secure Architecture Here:

4.2 Mystery Attack Mitigation

What is Your Mitigation Plan?

[Plan Here]

4.3 SQL Injection Mitigation

What is Your Mitigation Plan?

[Plan Here]

4.4 XSS Mitigation

What is Your Mitigation Plan?

[Plan Here]