Udajuicer - Threat Report

December 12, 2023

Introduction

This project serves to address issues with an insecure web application at Udajuicer - a very big juice shop in the world. The site would constantly go down and the people at Udajuicer weren't sure what the issue was.

As a security analyst rom a world-renown cybersecurity consulting firm, I will get to the bottom of the issue and find out why the Juice Shop site keeps going down.

- I will build a threat model for Udajuicer's website.
- Using an internal threat model template provided, I will go through the process of helping Udajuicer mitigate their current issue and build a secure application.

1 Assessment

Despite being a big company, it is quite alarming that the system architecture at Udajuicer is poorly designed as shown in FIG 1.

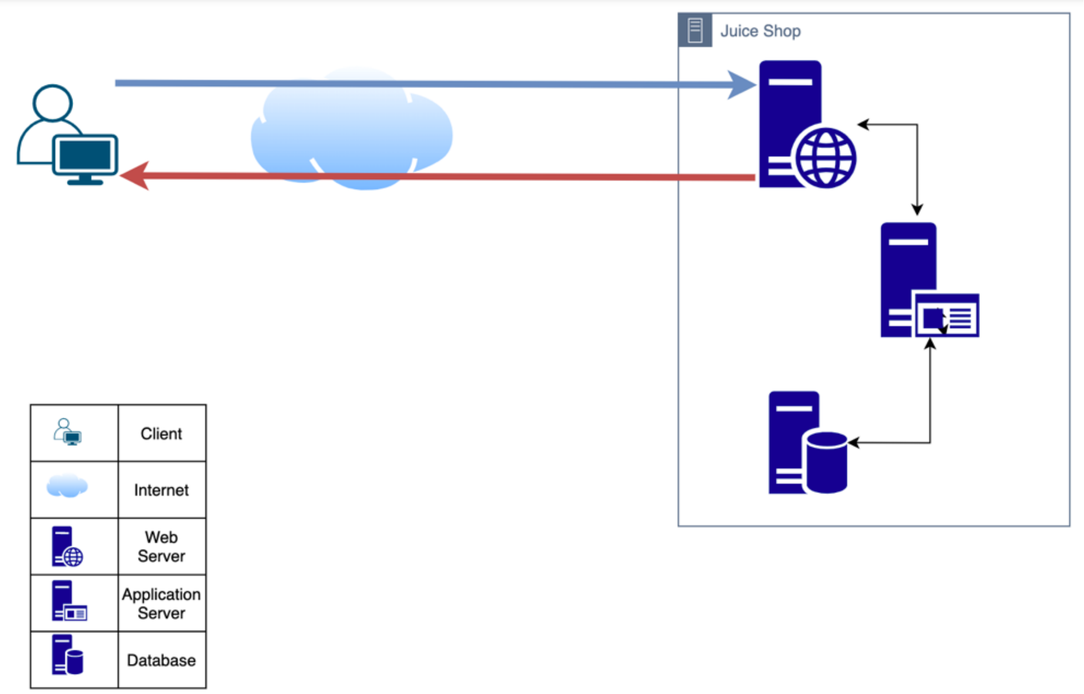

Figure 1: Udajuicer's Poorly Designed Architecture.

1.1 Asset Inventory

The first part of our threat model is being able to identify all the assets at Udajuicer. Looking at the architecture diagram, we can identify three components of the architecture: Web Server, Database Server and Application Server.

1.1.1 Web Server

A web server is a software application or hardware device that stores, processes, and serves website content to users over the World Wide Web, using the Hypertext Transfer Protocol (HTTP) to communicate. Key functions of a web server include:

- **Processing Requests**: Web servers handle incoming requests from clients (typically web browsers) and respond by serving the requested content.
- **Storing Content**: Web servers store website files, such as HTML documents, images, CSS stylesheets, and other multimedia files.
- **Communication**: Web servers communicate with clients using the HTTP (Hypertext Transfer Protocol) or its secure version, HTTPS. HTTP defines how messages are formatted and transmitted, and HTTPS adds a layer of security through encryption.
- **Hosting**: Web servers host websites and make them accessible to users on the Internet. Websites can be hosted on dedicated servers, virtual private servers (VPS), or through cloud-based services.

These dynamic functionality makes web servers an interesting target for attackers. Web servers are very common, and anyone can set one up, but doing it correctly without leaving doors open for attackers is a challenge.

1.1.2 Application Server

An application server is a software framework that provides an environment for running and managing applications. Key functions of an application server include:

- **Middleware Services**: Application servers often provide middleware services, such as messaging services, transaction processing, and connection pooling, to facilitate communication and coordination between different components of an application.
- **Application Execution**: They host and execute application code, allowing developers to deploy and run their applications in a controlled and managed environment.
- **Security**: They implement security features, including authentication and authorization mechanisms, to control access to applications and sensitive data. **Integration with Databases**: Application servers often integrate with database servers to retrieve and store data, providing a seamless connection between the application layer and the database layer.

Application server supports various communication protocols, such as HTTP, HTTPS, and others, making them suitable for web-based applications.

1.1.3 Database Server

A database server is a computer system that is dedicated to managing, storing and retrieving data from databases, and providing access to a database. Key characteristics and functions of a database server include:

- **Data Storage**: The database server stores data in a structured format, typically using a relational database management system (RDBMS) like MySQL, PostgreSQL, or Microsoft SQL Server.
- **Data Retrieval**: It allows users or applications to retrieve and manipulate data stored in the database through SQL (Structured Query Languages) queries and transactions.

In a typical architecture, applications or services interact with the database server to store and retrieve data. The database server manages the underlying data storage, indexing, and retrieval processes, providing a centralized and organized structure for efficient data management.