Conclusions

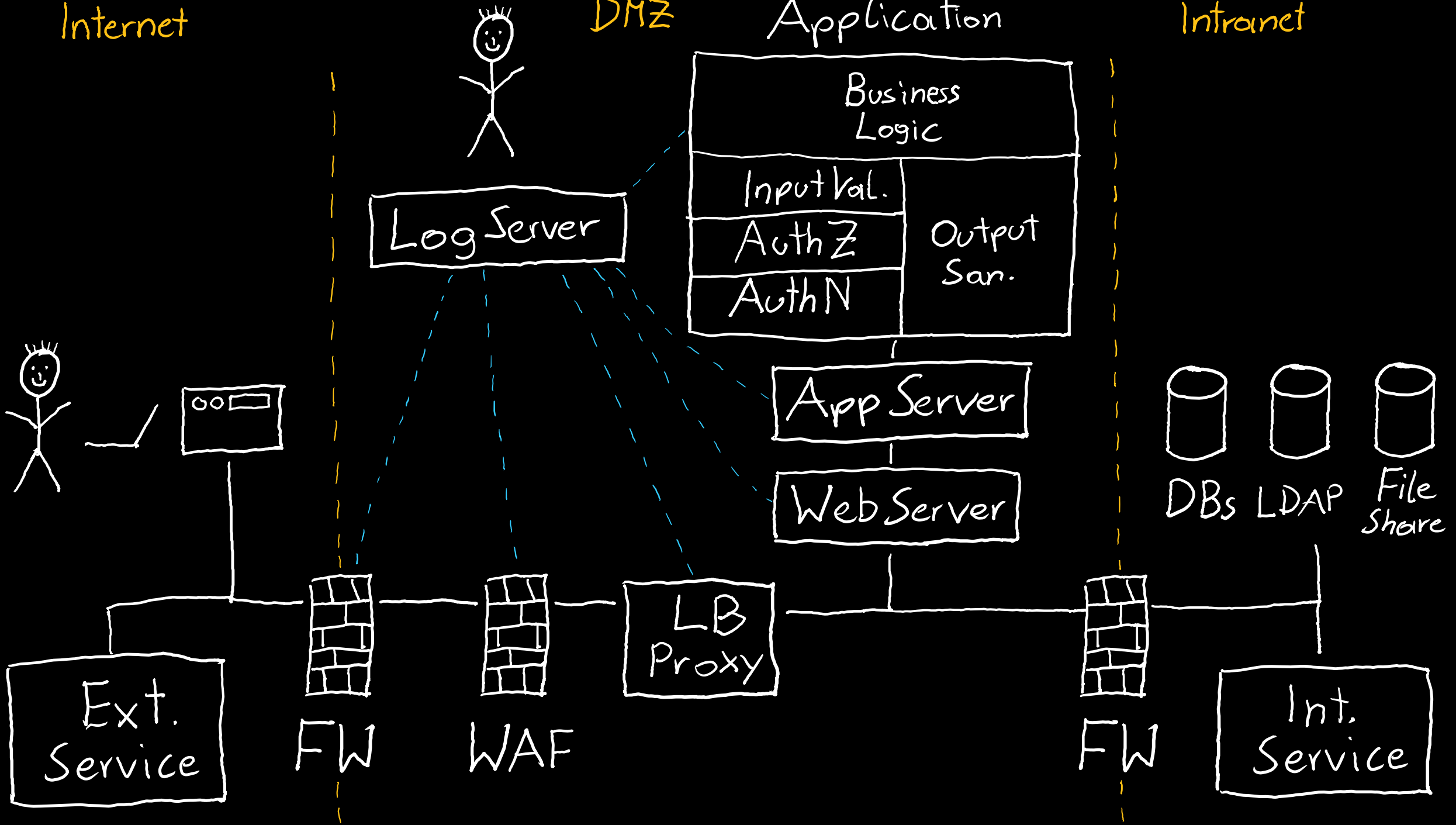pretty tough place this web, huh...

Rough Overview

1. Introduction
2. Basic Principles and Resources
3. Architecture & Basic Web Procedure
4. Authentication and Session Management
5. Authorization
6. Server and Backend Attacks
7. Remaining Client Attacks
8. General Topics
9. >> Conclusions <<

Security Principles

Principle	Attacks
Earn or give, but never assume, trust.	DNS Hijacking Plaintext Transmission Client-side Manipulation (of cookies) CSRF Forceful Browsing XML External Entitiy (XXE) SSRF Clickjacking Security Logging and Monitoring Failures Insecure Design
Use an authentication mechanism that cannot be bypassed or tampered with.	Authentication Automation Attacks
Authorize after you authenticate	Forceful Browsing TOCTOU (Race Condition)
Strictly separate data and control instructions, and never process control instructions received from untrusted sources.	SQL Injection XPath Injection OS Command Injection Cross-Site Scripting (XSS)
Define an approach that ensures all data are explicitly validated.	Path Traversal Insecure File Upload Unverified/Open Redirects/Forwards Software and Data Integrity Failures
Use cryptography correctly.	Insecure Password Storage Passwords in Source Code
Identify sensitive data and how they should be handled.	Information Disclosure Session Hijacking Session Fixation
Always consider the user.	
Understand how integrating external components changes your attack surface.	Vulnerabilities in 3rd Party Components
Be flexible when considering future changes to objects and actors.	Insecure Design

OWASP Top 10 2017

A1:2017-Injection	SQL Injection XPath Injection OS Command Injection
A2:2017-Broken Authentication	Authentication Automation Attacks Session Hijacking Session Fixation
A3:2017-Sensitive Data Exposure	Information Disclosure Plaintext Transmission Insecure Password Storage Passwords in Source Code
A4:2017-XML-External Entities (XXE)	XML External Entitiy (XXE)
A5:2017-Broken Access Control	Client-side Manipulation (of cookies) Forceful Browsing Path Traversal TOCTOU (Race Condition)
A6:2017-Security Misconfiguration	Information Disclosure
A7:2017-Cross-Site Scripting (XSS)	Cross-Site Scripting (XSS)
A8:2017-Insecure Deserialization	Software and Data Integrity Failures
A9:2017-Using Components with Known Vulnerabilities	Vulnerabilities in 3rd Party Components
A10:2017-Insufficient Logging&Monitoring	Security Logging and Monitoring Failures
Not in OWASP Top 10 2017	DNS Hijacking CSRF Insecure File Upload Unverified/Open Redirects/Forwards Clickjacking SSRF Insecure Design

OWASP Top 10 2021

A01:2021-Broken Access Control	Client-side Manipulation (of cookies) Forceful Browsing Insec. Direct Object References Path Traversal TOCTOU
A02:2021-Cryptographic Failures	Plaintext Transmission Insecure Password Storage Passwords in Source Code
A03:2021-Injection	SQL Injection XPath Injection OS Command Injection Cross-Site Scripting (XSS)
A04:2021-Insecure Design	Insecure Design
A05:2021-Security Misconfiguration	Information Disclosure XML External Entity (XXE)
A06:2021-Vulnerable and Outdated Components	Vulnerabilities in 3rd Party Components
A07:2021-Identification and Authentication Failures	Authentication Automation Attacks Session Hijacking Session Fixation
A08:2021-Software and Data Integrity Failures	Software and Data Integrity Failures
A09:2021-Security Logging and Monitoring Failures	Security Logging and Monitoring Failures
A10:2021-Server-Side Request Forgery	Server-Side Request Forgery (SSRF)
Not in OWASP Top 10 2021	DNS Hijacking CSRF Insecure File Upload Unverified/Open Redirects/Forwards Clickjacking

Most important security techniques

Most vulnerabilities can be avoided by a combination of

- strong authentication and session management

SQL Injection	Client-side Manipulation (of cookies)
XPath Injection	Forceful Browsing
OS Command Injection	Path Traversal
XML External Entitiy (XXE)	TOCTOU (Race Condition)
Authentication Automation Attacks	Cross-Site Scripting (XSS)
Session Hijacking	Software and Integrity Failures
Session Fixation	Vulnerabilities in 3rd Party Components
Information Disclosure	Security Logging and Monitoring Failures
Plaintext Transmission	DNS Hijacking
Insecure Password Storage	CSRF
Passwords in Source Code	Unverified/Open Redirects/Forwards
Insecure File Upload	Server-Side Request Forgery
Clickjacking	Insecure Design

Most important security techniques

Most vulnerabilities can be avoided by a combination of

- strong authentication and session management

SQL Injection	**Client-side Manipulation (of cookies)**
XPath Injection	Forceful Browsing
OS Command Injection	Path Traversal
XML External Entitiy (XXE)	TOCTOU (Race Condition)
Authentication Automation Attacks	Cross-Site Scripting (XSS)
Session Hijacking	Software and Integrity Failures
Session Fixation	Vulnerabilities in 3rd Party Components
Information Disclosure	Security Logging and Monitoring Failures
Plaintext Transmission	DNS Hijacking
Insecure Password Storage	CSRF
Passwords in Source Code	Unverified/Open Redirects/Forwards
Insecure File Upload	Server-Side Request Forgery
Clickjacking	Insecure Design

Most important security techniques

Most vulnerabilities can be avoided by a combination of

- strong authentication and session management

- consistent authorization checks

SQL Injection	**Client-side Manipulation (of cookies)**
XPath Injection	**Forceful Browsing**
OS Command Injection	**Path Traversal**
XML External Entitiy (XXE)	**TOCTOU (Race Condition)**
Authentication Automation Attacks	Cross-Site Scripting (XSS)
Session Hijacking	Software and Integrity Failures
Session Fixation	Vulnerabilities in 3rd Party Components
Information Disclosure	Security Logging and Monitoring Failures
Plaintext Transmission	DNS Hijacking
Insecure Password Storage	CSRF
Passwords in Source Code	Unverified/Open Redirects/Forwards
Insecure File Upload	Server-Side Request Forgery
Clickjacking	Insecure Design

Most important security techniques

Most vulnerabilities can be avoided by a combination of

- strong authentication and session management

- consistent authorization checks

- strict input validation

- context-sensitive output handling

SQL Injection	**Client-side Manipulation (of cookies)**
XPath Injection	**Forceful Browsing**
OS Command Injection	**Path Traversal**
XML External Entitiy (XXE)	**TOCTOU (Race Condition)**
Authentication Automation Attacks	**Cross-Site Scripting (XSS)**
Session Hijacking	**Software and Integrity Failures**
Session Fixation	Vulnerabilities in 3rd Party Components
Information Disclosure	Security Logging and Monitoring Failures
Plaintext Transmission	DNS Hijacking
Insecure Password Storage	CSRF
Passwords in Source Code	**Unverified/Open Redirects/Forwards**
Insecure File Upload	**Server-Side Request Forgery**
Clickjacking	Insecure Design

Most important security techniques

Most vulnerabilities can be avoided by a combination of

- strong authentication and session management

- consistent authorization checks

- strict input validation

- context-sensitive output handling
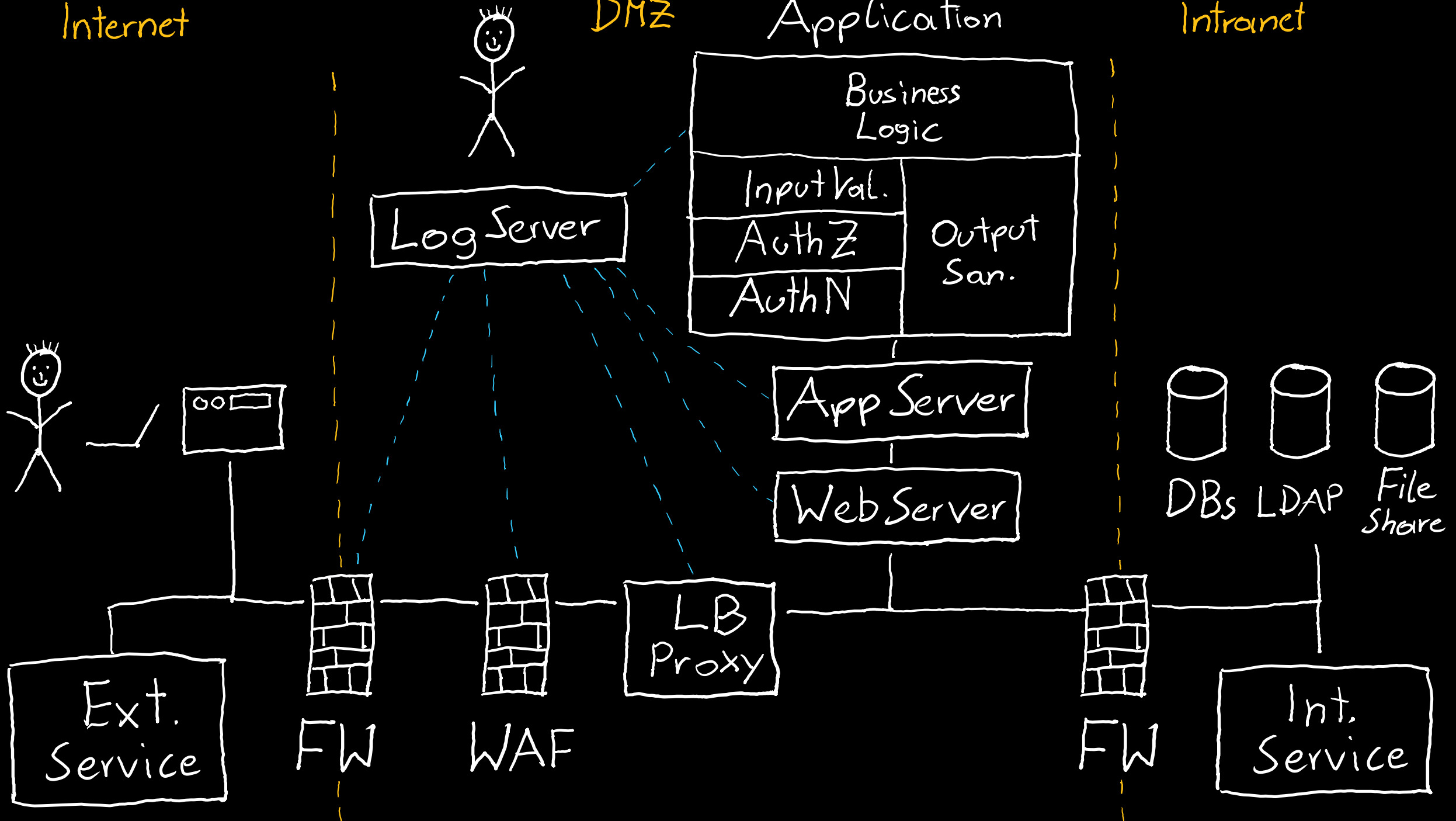
- constant TLS usage

SQL Injection	**Client-side Manipulation (of cookies)**
XPath Injection	**Forceful Browsing**
OS Command Injection	**Path Traversal**
XML External Entitiy (XXE)	**TOCTOU (Race Condition)**
Authentication Automation Attacks	**Cross-Site Scripting (XSS)**
Session Hijacking	**Software and Integrity Failures**
Session Fixation	Vulnerabilities in 3rd Party Components
Information Disclosure	Security Logging and Monitoring Failures
Plaintext Transmission	**DNS Hijacking**
Insecure Password Storage	CSRF
Passwords in Source Code	**Unverified/Open Redirects/Forwards**
Insecure File Upload	**Server-Side Request Forgery**
Clickjacking	Insecure Design

Internet · DMZ · Application · Intranet

Business Logic

Input Val.

AuthZ

AuthN

Output San.

Log Server

App Server

Web Server

DBs LDAP File Share

Ext. Service

FW

WAF

LB Proxy

FW

Int. Service

and of course…