

Conclusions

pretty tough place this web, huh...

Rough Overview

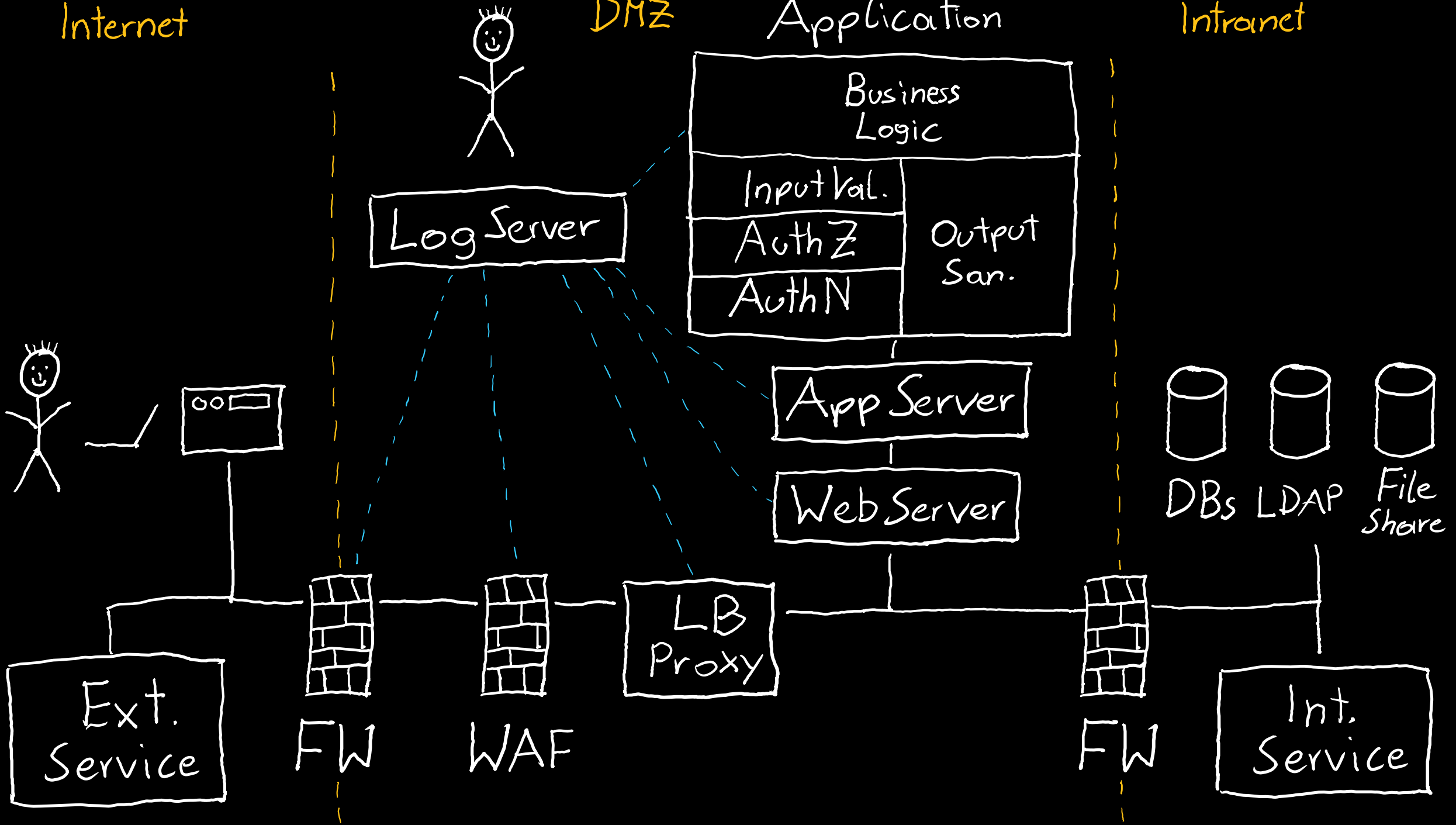
1. Introduction
2. Basic Principles and Resources
3. Architecture & Basic Web Procedure
4. Authentication and Session Management
5. Authorization
6. Server and Backend Attacks
7. Remaining Client Attacks
8. General Topics
9. >> Conclusions <<

Internet

DMZ

Application

Intranet



Security Principles

Earn or give, but never assume, trust.

DNS Hijacking
Plaintext Transmission
Client-side Manipulation (of cookies)
CSRF
Forceful Browsing
XML External Entity (XXE)
Clickjacking
Insufficient Logging and Monitoring

Use an authentication mechanism that cannot be bypassed or tampered with.

Authentication Automation Attacks

Authorize after you authenticate

Forceful Browsing
Insec. Direct Object References
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
Insecure Deserialization

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.

OWASP Top 10

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 Entity (XXE)
A5:2017-Broken Access Control	Client-side Manipulation (of cookies) Forceful Browsing Insec. Direct Object References 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	Insecure Deserialization
A9:2017-Using Components with Known Vulnerabilities	Vulnerabilities in 3rd Party Components
A10:2017-Insufficient Logging&Monitoring	Insufficient Logging and Monitoring
Not in OWASP Top 10 2017	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	Insec. Direct Object References
XML External Entity (XXE)	Path Traversal
Authentication Automation Attacks	TOCTOU (Race Condition)
Session Hijacking	Cross-Site Scripting (XSS)
Session Fixation	Insecure Deserialization
Information Disclosure	Vulnerabilities in 3rd Party Components
Plaintext Transmission	Insufficient Logging and Monitoring
Insecure Password Storage	DNS Hijacking
Passwords in Source Code	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	Insec. Direct Object References
XML External Entity (XXE)	Path Traversal
Authentication Automation Attacks	TOCTOU (Race Condition)
Session Hijacking	Cross-Site Scripting (XSS)
Session Fixation	Insecure Deserialization
Information Disclosure	Vulnerabilities in 3rd Party Components
Plaintext Transmission	Insufficient Logging and Monitoring
Insecure Password Storage	DNS Hijacking
Passwords in Source Code	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
- consistent authorization checks

SQL Injection	Client-side Manipulation (of cookies)
XPath Injection	Forceful Browsing
OS Command Injection	Insec. Direct Object References
XML External Entity (XXE)	Path Traversal
Authentication Automation Attacks	TOCTOU (Race Condition)
Session Hijacking	Cross-Site Scripting (XSS)
Session Fixation	Insecure Deserialization
Information Disclosure	Vulnerabilities in 3rd Party Components
Plaintext Transmission	Insufficient Logging and Monitoring
Insecure Password Storage	DNS Hijacking
Passwords in Source Code	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
- consistent authorization checks
- strict input validation
- context-sensitive output encoding/sanitization

SQL Injection	Client-side Manipulation (of cookies)
XPath Injection	Forceful Browsing
OS Command Injection	Insec. Direct Object References
XML External Entity (XXE)	Path Traversal
Authentication Automation Attacks	TOCTOU (Race Condition)
Session Hijacking	Cross-Site Scripting (XSS)
Session Fixation	Insecure Deserialization
Information Disclosure	Vulnerabilities in 3rd Party Components
Plaintext Transmission	Insufficient Logging and Monitoring
Insecure Password Storage	DNS Hijacking
Passwords in Source Code	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
- consistent authorization checks
- strict input validation
- context-sensitive output encoding/sanitization
- constant TLS usage

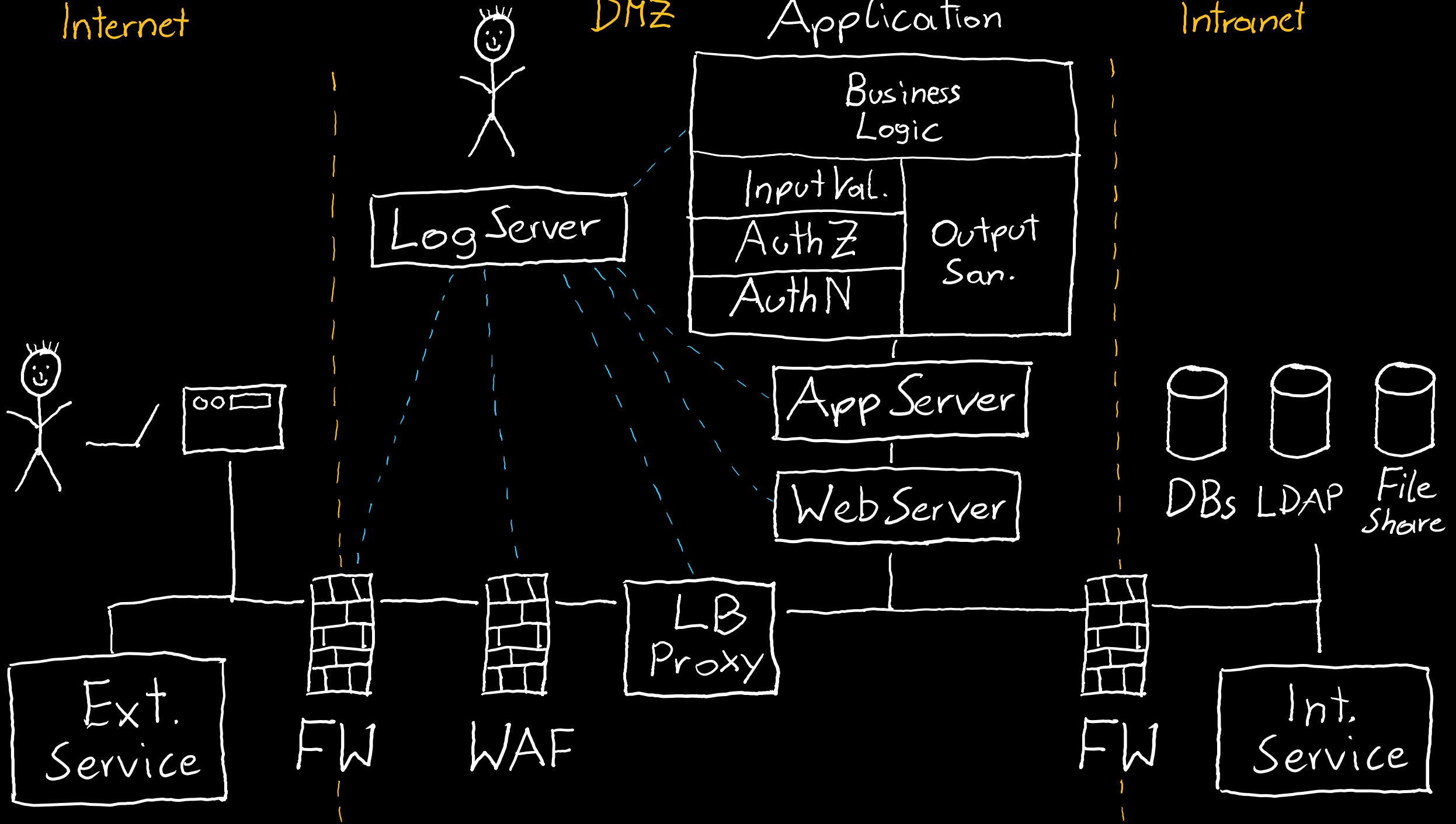
SQL Injection	Client-side Manipulation (of cookies)
XPath Injection	Forceful Browsing
OS Command Injection	Insec. Direct Object References
XML External Entity (XXE)	Path Traversal
Authentication Automation Attacks	TOCTOU (Race Condition)
Session Hijacking	Cross-Site Scripting (XSS)
Session Fixation	Insecure Deserialization
Information Disclosure	Vulnerabilities in 3rd Party Components
Plaintext Transmission	Insufficient Logging and Monitoring
Insecure Password Storage	DNS Hijacking
Passwords in Source Code	CSRF
Insecure File Upload	Unverified/Open Redirects/Forwards
Clickjacking	

Internet

DMZ

Application

Intranet



and of course...

**THE CLIENT,
YOU MUST NEVER TRUST**



MY YOUNG PADAWAN