Security for Developers

Review on Basics

Soheil Hashemi

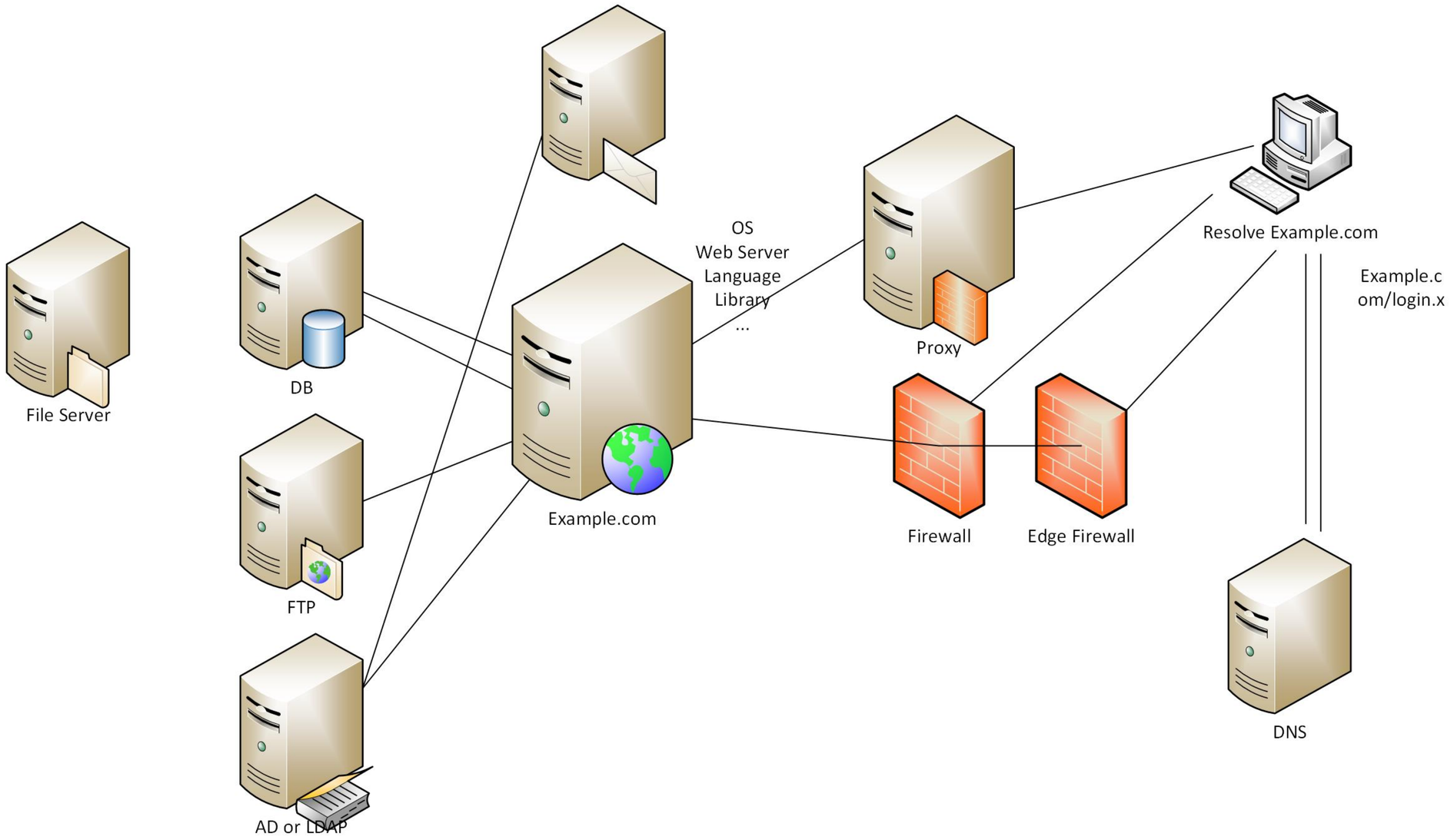
About Me

- Soheil Hashemi
- MSc in Network Computers
- Network Administrator, Penetration Testing
- Ashiyane Digital Security Team AKA “Xenotix" [2012]
- https://linktr.ee/soheilhashemi

Headlines

- Landscape on WA and security

Web Application Landscape



Problems

- Web Application , library , Rate limit , https
- DNS [recursion , misconfiguration bypass Proxy find IP]
- Web Server [Permissions, hardening]
- OS , Service , App , Accessibility [RDP,SSH]

What should to Do?

- Secure Coding -> Best Practice
- Hijack Execution flow [include hash prevent running malicious library]
- Valid Accounts[make sure do not store sensitive data or credentials insecurely]
- Access Notification [avoid place sensitive data on text notification]
- Access sensitive Data in Device Logs [avoid log sensitive data such as credit card]
- Screen Capture [FLAG_SECURE]
- URI Hijacking [prevent intercepting and redirect]
- Devsecops -> Design -> Build -> Test -> Deploy [Automate Test(Vulnerability Scan) before build decrease cost of Penetration Testing] - Burpsuite Enterprise integrate with JIRA
- Pentest

MITRE

- Tactic 12
- Technique initial Access with Phishing
- Procedure using xlxs for attachment