Hong Kong Tree Watch Security Manifesto

Outline of Security

Updated June 1st, 2023

All team members:

Database (Maria DB, MYSQL)

- Role-based access control
- Install a trusted digital certificate using
- Enable firewall rules
- No plaintext passwords are stored in the backend hashed using SHA-256
- Removed sa accounts and disabled open ports
- Regular review of user permissions.
- Data integrity with correct data types, use of rollback transactions, primary and foreign keys
- Use of stored procedures to hide unintended data
- Separation of roles and powers.
- Centralized input validation routine
- Encode data to the common character before validation
- Verify header validates and origin request (same domain request)
- Implement lease privilege, restrict users to only functionality
- Use strongly typed parameterized queries

-

Server (EC2 AWS NGINX Server)

- Install TLS 1.2 Certificate with Let's Encrypt, renewable 90 days
- All inputs are untrusted and validated on the server side
- Prevent master secrets from being logged
- All logging should only be accessed by Admin
- Do not store plain text passwords in logs
- Use a cryptographic hash function to validate log entry integrity (SHA 256)

Client

- XSS Prevented with input sanitization
- JSON web tokens for role-based authentication
- Strong & Unique passwords requirement
- Require authentication for all /dash pages
- Cookie is checked with every request and sent to the backend server for verification
- JWT Tokens validity is valid for 60 mins
- Use only HTTP Post to transmit authentication credentials
- Notify users if the password reset
- Stretch goal (MFA)
- Implement encryption for the transmission of all sensitive data (TLS)
- Connection strings should not be hardcoded; use backend to connect to database

Repository

- .gitingore file makes sure certain files are not checked in to repository
- Lockdown GitHub to a private repo
- All team members have access
- Do not commit any keys to repo; use environmental variables instead.

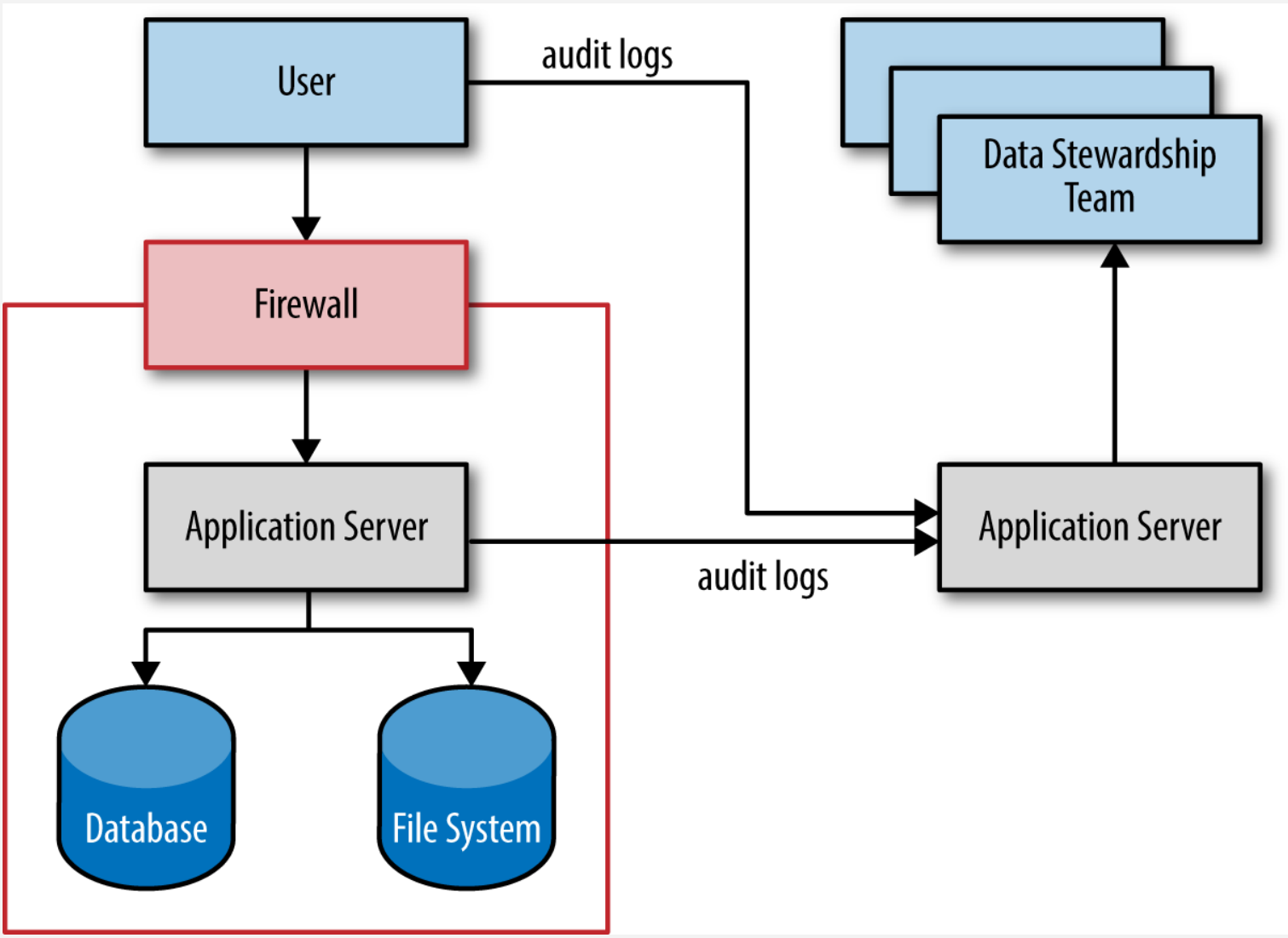

Fig .1 https://www.oreilly.com/content/security-architecture/

Team references 👍

Appendix A: External References: 1. Cited Reference Sans and TippingPoint "The Top Cyber Security Risks" http://www.sans.org/top-cyber-security-risks/ Web Application Security Consortium http://www.webappsec.org/ Common Weakness Enumeration (CWE) http://cwe.mitre.org/ Department of Homeland Security Build Security In Portal https://buildsecurityin.us-cert.gov/daisy/bsi/home.html CERT Secure Coding http://www.cert.org/secure-coding/ MSDN Security Developer Center http://msdn.microsoft.com/en-us/security/default.aspx