Introduction to AppSec (OWASP top 10)

By Aastha Sahni

Overview

Speaker Introduction	Explain Application Security (AppSec)	Importance of AppSec (attacker mindset)	Introduction to OWASP and CyberSecurity
OWASP Top 10 Vulnerabilities	Injection	Insecure Logging	Known Vulnerabilities
AppSec Tools	Learning Resources	Communities	Career value of secure development skills

Speaker Introduction

Aastha Sahni

- Security Training Awareness Specialist |Instructor| Coach
- Founder- CyberPreserve
- Lean In: Breaking Barriers- Founder & Lead
- Communities – OWASP, InfosecGirls

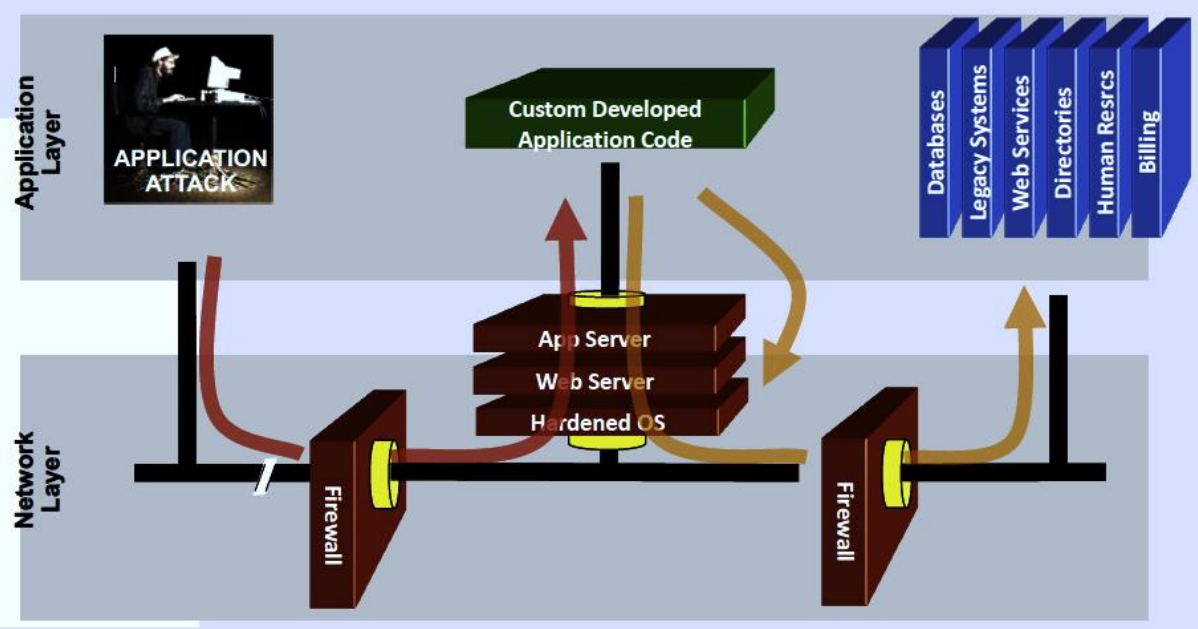
What’s a Web App?

- Stored on remote server
- Delivered over Internet through browser Interface

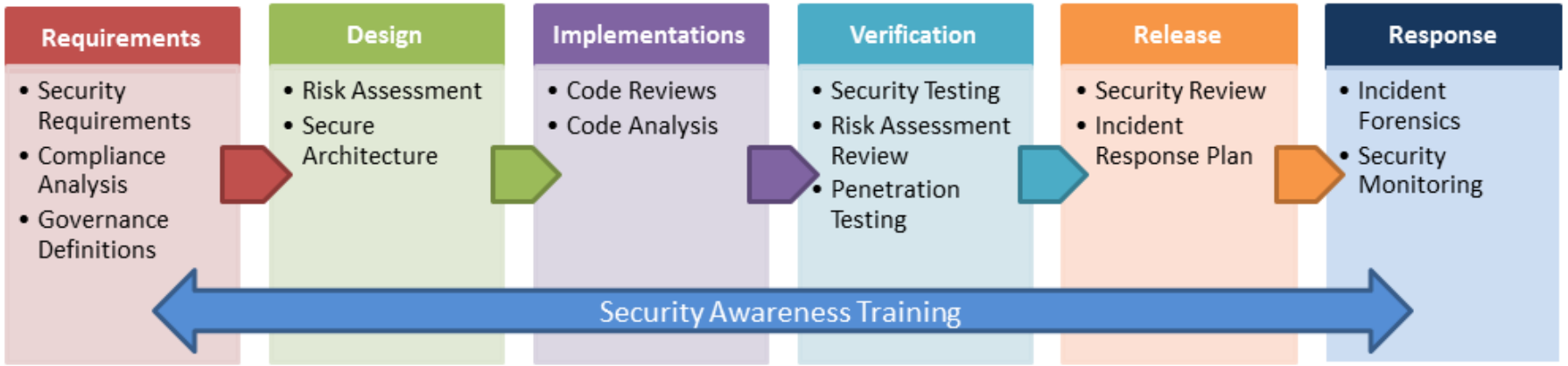
- **Architecture**

- Interactions between app components
- Client-Server app
- User Interfaces (UIs)
- Databases

Web Application Architecture



Secure SDLC


Requirements
• Security Requirements
• Compliance Analysis
• Governance Definitions
Design
• Risk Assessment
• Secure Architecture
Implementations
• Code Reviews
• Code Analysis
Verification
• Security Testing
• Risk Assessment Review
• Penetration Testing
Release
• Security Review
• Incident Response Plan
Response
• Incident Forensics
• Security Monitoring
Security Awareness Training

Introduction to OWASP and CyberSecurity

The Open Web Application Security Project (OWASP) is a nonprofit foundation that works to improve the security of software.

Cybersecurity is the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information.

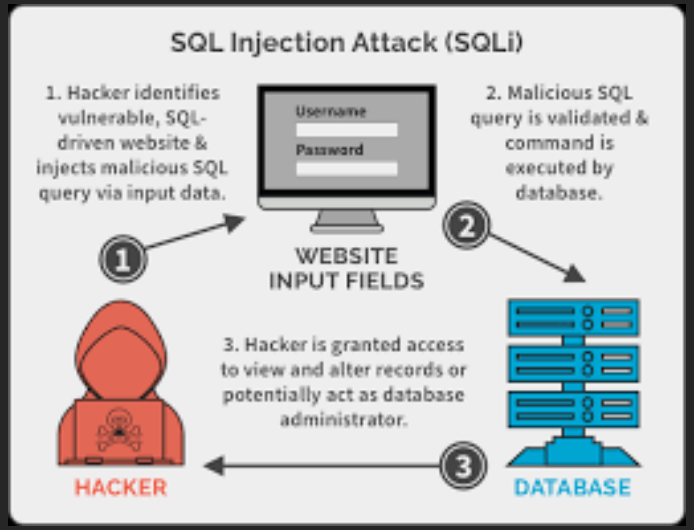
CIA TRIAD


CONFIDENTIALITY
INTEGRITY
INFORMATION
SECURITY
AVAILABILITY

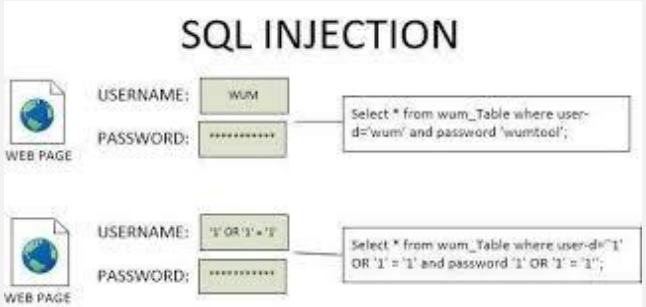
OWASP Top 10

OWASP Top 10 2017		change	OWASP Top 10 2021 proposal	
A1	Injections	**as is**	A1	Injections
A2	Broken Authentication	**as is**	A2	Broken Authentication
A3	Sensitive Data Exposure	**down 1**	A3	Cross-Site Scripting (XSS)
A4	XML eXternal Entities (XXE)	**down 1 + A8**	A4	Sensitive Data Exposure
A5	Broken Access Control	**down 1**	A5	Insecure Deserialization **(merged with XXE)**
A6	Security Misconfiguration	**down 4**	A6	Broken Access Control
A7	Cross-Site Scripting (XSS)	**up 4**	A7	Insufficient Logging & Monitoring
A8	Insecure Deserialization	**up 3 + A4**	A8	**NEW:** Server Side Request Forgery (SSRF)
A9	Known Vulnerabilities	**as is**	A9	Known Vulnerabilities
A10	Insufficient Logging & Monitoring	**up 3**	A10	Security Misconfiguration

A1: Injection



- Injections are at the head of the OWASP Top 10 and Injection flaws, particularly SQL Injection, are common in web applications



A7: Insufficient Logging and Monitoring

Auditable events like logins,failed logins and transactions are not logged.

Warnings and errors generate inadequate or unclear log messages.

Logs of applications and related APIs are not monitored correctly. (do not detect suspicious activities)

Logs are stored locally

A9: Known Vulnerabilities

01

Using old versions or incompatible versions of certain components.

02

Failed to scan vulnerabilities regularly.

03

Developers failed to test the availability of updated, upgraded or patched libraries.

04

If Software used is vulnerable due to old or outdated version.

AppSec Tools

Proxies

- Burp Suite
- ZAP Proxy

Offensive Security OS

- Kali Linux

Intentionally Vulnerable Web Apps

- OWASP Juice Shop

FREE LEARNING RESOURCES

https://owasp.org/www-project-top-ten/

https://www.sans.org/top25-software-errors

https://www.iso.org/standards.html

https://network-tools.com/

https://linuxhint.com/list_essential_linux_security_commands/

Communities

- OWASP - https://owasp.org/membership/
- ISSA - https://www.issa.com/member-benefits
- ISACA - https://www.isaca.org/membership
- ISC2 - https://www.isc2.org/Membership
- **Women** – *WiCyS , WoSEC, InfosecGirls, Breaking Barriers Lean-In Circle etc.*

Mentorship Programs

CyberPreserve

Mentorship programs offer trainings as well as right set of guidance in your career path.

CyberPreserve aims to provide the same with comprehensive foundational training along with mentor support.

To know more visit our website - https://www.cyberpreserve.com

Career Value: Dev + Security

- Development and Security goes hand in hand.
- Developing an application, component or software requires secure coding measures to be implemented.
- Security knowledge provides additional skill to your career.
- Keep you updated with the recent security trends and development.

P.S. - Security Awareness is mandatory.

Reach out to me!

Stay Connected

- **Email**: aastha.cyberpreserve@gmail.com
- **Twitter**: @aastha1891
- **LinkedIn:** /aastha-sahni/
- **CyberPreserve**: https://www.cyberpreserve.com