UNIVERSITY of WASHINGTON

Hacking 310

Lesson 02: Pentesting Process, Continued

Review

- Questions
- Lab Access (Credentials to be sent out)

Learning Objectives

After completing this lesson, students will be able to:

- Describe legal implications of penetration testing and ethical hacking,
- Recognize the various types of Web Applications Security Vulnerabilities and exploit vectors,
- Describe and give examples of threat modeling,
- Distinguish the differences between OCTAVE, DREAD, CVSS, and STRIDE for threat modeling,
- Explain the differences between exploitation and post-exploitation.

Legal/Ethical Limitations

- Federal / State / Local Laws
  - Computer Fraud & Abuse Act (CFAA) of 1984
- Contracts
- Impersonation
- What is Ethical?

Intelligence Gathering

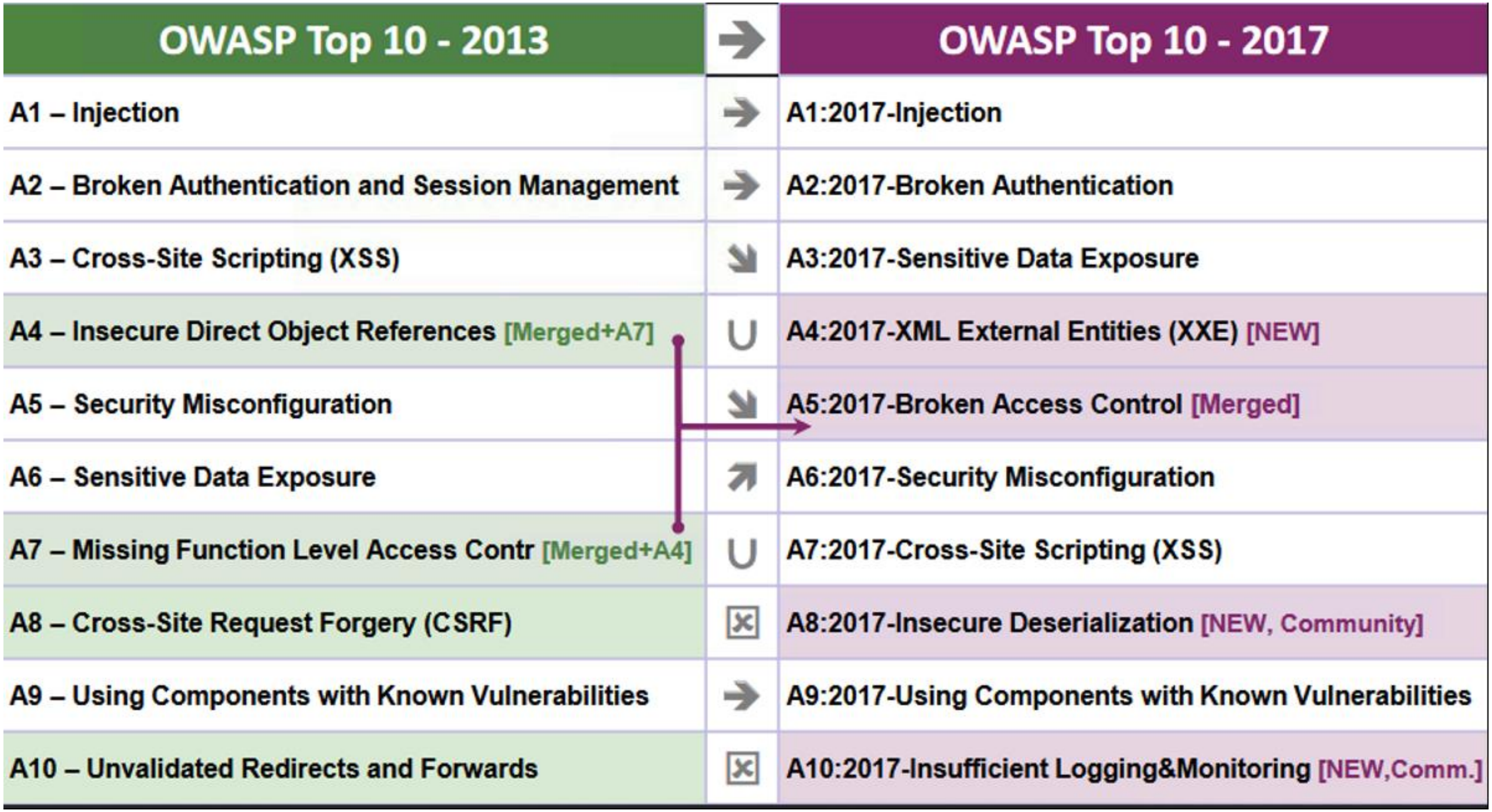
- What is needed to conduct Intelligence Gathering?
  - Target Selection
    - IP Addresses
    - Domain Names
    - Single Address
  - OSINT
    - Social Media: LinkedIn, Facebook, Twitter
    - Google Dorks (Google Hacking Database)
  - Covert Gathering
    - ShodanHQ, Censys, scans.io
  - Footprinting
    - Verify target ranges
    - Whois lookup (domain and IP)
    - BGP looking glass
    - Active footprinting

Active Footprinting

- Port scan
- Banner grabbing
- SNMP sweep
- DNS enumeration / DNS zone transfers
- SMTP bounce back
- Web application discovery
- Identify lockout threshold
- Compile target list

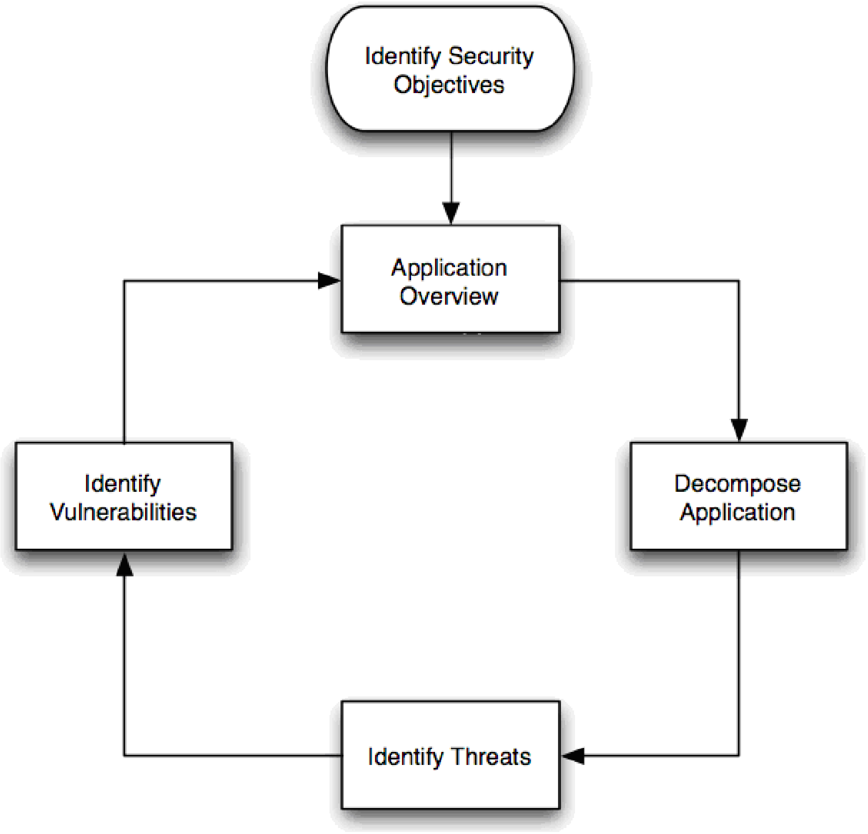
Web Vulnerabilities

Open Web Application Security Project (OWASP) Top 10 Vulnerabilities



OWASP Top 10 - 2013	→	OWASP Top 10 - 2017
A1 – Injection	→	A1:2017-Injection
A2 – Broken Authentication and Session Management	→	A2:2017-Broken Authentication
A3 – Cross-Site Scripting (XSS)	↘	A3:2017-Sensitive Data Exposure
A4 – Insecure Direct Object References [Merged+A7]	∪	A4:2017-XML External Entities (XXE) [NEW]
A5 – Security Misconfiguration	↘	A5:2017-Broken Access Control [Merged]
A6 – Sensitive Data Exposure	↗	A6:2017-Security Misconfiguration
A7 – Missing Function Level Access Contr [Merged+A4]	∪	A7:2017-Cross-Site Scripting (XSS)
A8 – Cross-Site Request Forgery (CSRF)	☒	A8:2017-Insecure Deserialization [NEW, Community]
A9 – Using Components with Known Vulnerabilities	→	A9:2017-Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards	☒	A10:2017-Insufficient Logging&Monitoring [NEW,Comm.]

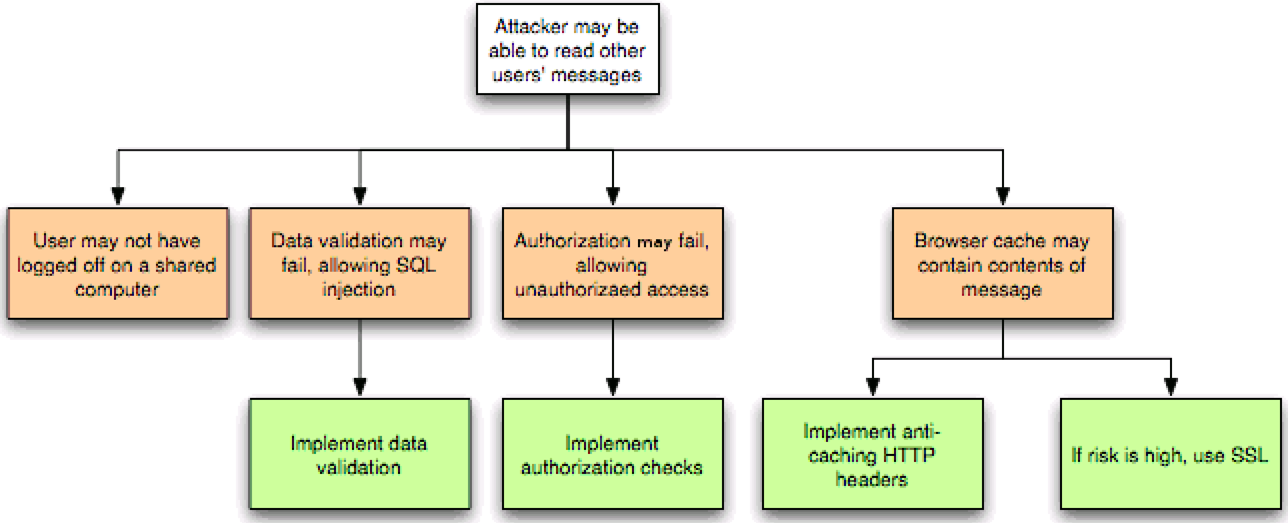
Threat Modeling



Threat Modeling - Process

- Assessment Scope
- System Modeling
- Identify Threats
- Identify Vulnerabilities
- Examining the Threat History
- Evaluation or Impact on the Business
- Developing a Security Threat Response Plan

Threat Model - Microsoft



Attacker may be able to read other users' messages

User may not have logged off on a shared computer

Data validation may fail, allowing SQL injection

Authorization may fail, allowing unauthorizaed access

Browser cache may contain contents of message

Implement data validation

Implement authorization checks

Implement anti-caching HTTP headers

If risk is high, use SSL

Threat Modeling - Frameworks

- STRIDE
- DREAD
- CVSS
- OCTAVE

Exploitation

- Purpose / Objective
- Bypass Countermeasures / Evasion
  - Anti-Virus
    - Encoding
    - Packing
    - Encrypting
    - Whitelist Bypass
    - Process Injection
    - Purely Memory Resident
  - Data Execution Prevention (DEP)
  - Address Space Layout Randomization (ASLR)
  - Web Application Firewall (WAF)
  - Intrusion Detection System (IDS) / Intrusion Prevention System (IPS)

Exploitation - Continued

- Exploits
  - Packaged
  - Tailored Customization
  - Zero-Day
    - Fuzzing
    - Source Code Analysis
    - Types
      - Buffer Overflow
      - SEH Overwrites
      - Return Oriented Programming
    - Traffic Analysis
    - Physical Access
      - Social Engineering
      - PC Access
    - Proximity Access
      - Wireless

Post-Exploitation

- Rules of Engagement
  - Protect the Client
  - Protect Yourself
- Infrastructure Analysis
  - Resources
    - MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK)
  - Network Configuration
  - Network Services
  - Sensitive Data
  - User-Information
  - System Configuration
- High Value Targets
- Data Exfiltration
- Persistence
- Further Penetration
- Cleanup