- Filename: eccouncil-ceh31250-v12-14-2-1-owasp-top-10-web-application-attacks-2021.md
- Show Name: CEHv12 (312-50)
- Topic Name: Web Application Hacking - Hacking Web Applications
- Episode Name: OWASP Top 10 Web Application Attacks (2021)
  ==

OWASP Top 10 Web Application Attacks (2021)

Objectives:

- What is OWASP and what are the 'Top 10' lists?

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

- A1: Broken Access Control

  - Failure implement/properly configure mechanisms for controlling access to sensitive information

    - Compromise CIA

      - IDOR
      - CSRF
      - Force Browsing to pages they don't have permission to

    - Unauthenticated users can access authenticated pages

      - Authenticated non-admin user can access administrative areas/data

- A2: Cryptographic Failures

  - Was "Sensitive Data Exposure"

    - This topic is specific to Encryption

      - Lack of encryption
      - Use of weak encryption
      - Not enough entropy

  - Strong encryption should be always used for data like PII/PHI
  - Data At-Rest/In-Motion/In-Use

    - CC#s on a file server
    - PHI being send via email/API/file transfer
    - PII being accessed by an application

- A3: Injection

  - Malicious user-provided data is allowed and accepted

    - No input sanitization
    - No prepared statements

      - Command Injection
      - Code Injection
      - Query Injection

- A4: Insecure Design

  - New for 2021
  - Lack of security consideration and implementation during SDLC

    - Secure tools and code libraries
    - No Threat Modeling done
    - Security testing/retesting done throughout SDLC

- A5: Security Misconfiguration

  - Using default creds
  - Unnecessary or unused services installed/running
  - Allow overly verbose errors/stack traces

    - Directory listing
    - Open cloud storage

- A6: Vulnerable and Outdated Components
    - Speaks for itself
        - Apache Struts vulnerability
- A7: Identification and Authentication Failures
    - Auth doesn't effectively validate user's:
        - Identity
        - Authentication
        - Session
    - Allows Brute-Force
    - Allows weak or default creds
    - Allows Session token/ID reuse
        - Doesn't invalidate sessions
    - No MFA/2FA
- A8: Software and Data Integrity Failures
    - Software utilizes 3rd-party plugins, repositories, modules, etc
        - These elements may be insecure, introducing security flaws
            - May come by way of "auto-updates"
                - If element source is compromised, then supply-chain attack
    - Insecure deserialization
- A9: Security Logging and Monitoring Failures
    - No auditing, logging, or monitoring being done
        - At all
        - or on all systems, APIs, etc
    - Logs are difficult to understand
    - System is slow to alert
    - Alerts are not effectively configured
    - No backups and/or replication
- A10: Server-Side Request Forgery (SSRF)
    - Web application makes requests for internal or remote assets
        - Internal systems trust server requests
    - No request validation