- Filename: eccouncil-ceh31250-v12-14-9-1-apis-and-webhooks.md
- Show Name: CEHv12 (312-50)
- Topic Name: Web Application Hacking - Hacking Web Applications
- Episode Name: APIs and Webhooks
  ==

APIs and Webhooks

Objectives:

- What is an API?
    - A single web service that can facilitate multiple online sources
        - Less complexity
    - API Services
        - SOAP
        - REST (REpresentational State Transfer)
            - RESTful
        - XML
        - JSON
- What is a Webhook?
    - Push notifications
- API Security Risks
    - OWASP Top 10 API Security Risks
        - https://owasp.org/www-project-api-security/
    - SQLi
    - IDOR
    - Auth/Access insecurity
    - DDoS
- API Hacking Methodology
    - Identify the Target
    - Detect security standards
    - Identify the attack surface
    - Launch Attack
- Security countermeasures for APIs and Webhooks
    - API
        - Sanitize User Input
        - Firewalls
        - Rate-Limiting
        - Parameterized Statements
        - Pagination
        - Rate-limiting and throttling
        - MFA
    - Webhooks
        - Require authentication
        - Blacklist calls from unauthorized sources
        - Webhook signing
        - Timestamps
            - X-Cld-Timestamp (timing attacks)
            - X-OP-Timestamp