A10

Always Secure. Always Available.

狙われやすいAPIを保護する –

A10のAPIセキュリティ対策

A10ネットワークス株式会社

API 利用の拡大

API通信　＝　アプリがネット上にあるサービスと連携するためのインタフェース

各種サービスとの連携

- 決済
- SNS
- 位置情報
- 天気予報
- 地図
- 配車

等

モバイルアプリ

- 必要な機能をAPIで呼び出すことで開発コストを低減
- 機能ごとに分離することで更新・メンテナンスがしやすい
- 標準的で実装が容易
- 外部アプリを利用することで簡単に機能追加
- 生成AIとの連携機能追加なども要因
  - コンテンツ生成
  - 文章校正
  - 画像生成
  - プログラミング支援

インターネット上のトラフィックの半分以上がAPIのトラフィック

APIの脆弱性

OWASP API Security Top 10

出典：https://owasp.org/www-project-api-security/
OWASP：Webセキュリティのコミュニティ

API1: オブジェクトレベル認可の不備(BOLA)
例：IDを他人のものに書き換えるだけで、他人の個人情報等を閲覧・操作可能になってしまう（個別のデータの権限不備）

API2: 認証の不備
例：認証の仕組みが不十分で、攻撃者がパスワードを推測したりキーを盗んだりして、他の利用者になりすます

API3: オブジェクトプロパティレベルの認可の不備
例：APIが非公開の項目（例: Adminフラグ）を漏洩させたり、不正な更新リクエストを受け入れたりしてしまう

API4: リソース消費の制限の不備
例：ページ指定やファイルサイズに上限がなく、大量のリクエストでサーバーのリソースを枯渇させる

API5: 機能レベルの認可の不備（BFLA）
例：一般ユーザーが、管理者しか使えないはずのAPIをURL直接指定などで呼び出せてしまう問題（API機能の権限不備）

API6:機密性の高いビジネスフローへの無制限アクセス
例：APIを自動で高速に呼び出し、チケットの買い占めや在庫確認のようなビジネス上の問題を発生させる。

API7: Server-Side Request Forgery
例：攻撃者が指定したURLにサーバーがアクセスしてしまい、本来非公開の内部システムの情報が漏洩する。

API8: セキュリティの設定ミス
例：詳細すぎるエラー表示、不要なHTTPメソッドの許可など、設定ミスによる脆弱性

API9: 不適切なインベントリ管理
例：古いAPIやテスト用APIが放置され、セキュリティパッチが適用されず攻撃の標的になること

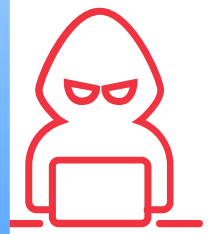
API10: 安全でない API の使用
例：連携先の外部APIを信用しすぎ、応答に含まれる悪意あるデータを無害化せずに利用してしまう問題。

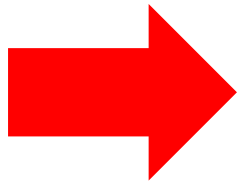
APIの実装には脆弱性対策が必須

APIへの攻撃：攻撃者の行動

時間経過

- ＜偵察＞ 通常のアクセスで基本的なデータ収集
- ＜スキャン＞ 既知の脆弱性に対する応答を調査
- ＜構造調査＞ 弱点を見つけるためにアプリの構造を調査
- ＜不正アクセス＞ パスワード推測・総当たり等でアクセスを試みる
- ＜サービス侵害＞ 権限奪取による不正操作等でアプリを侵害
- ＜悪用＞ アプリの弱点を悪用・機密情報取得
- ＜足場固め＞ 侵害されたサーバ上でアクセス権や制御を維持





攻撃対象のAPI

攻撃者は段階的・戦略的にAPIを狙う