INTER-Mediatorが備える
セキュリティ機能

2019/08/24
INTER-Mediator《大》勉強会 2019

松尾篤（株式会社エミック）

株式会社エミック

Agenda

- Webアプリで見つかりやすい脆弱性
- INTER-Mediatorのセキュリティ機能
- INTER-Mediator Training Course

Webアプリで

見つかりやすい脆弱性

Webアプリの脆弱性を知る

- 安全なウェブサイトの作り方を参照

https://www.ipa.go.jp/security/vuln/websecurity.html

見つかりやすい脆弱性

- SQLインジェクション
- OSコマンド・インジェクション
- ディレクトリ・トラバーサル
- セッション管理の不備

見つかりやすい脆弱性

- クロスサイト・スクリプティング（XSS）
- クロスサイト・リクエスト・フォージェリ（CSRF）
- HTTPヘッダ・インジェクション

見つかりやすい脆弱性

- メールヘッダ・インジェクション
- クリックジャッキング
- バッファオーバーフロー
- アクセス制御や認可制御の欠落

INTER-Mediatorの
セキュリティ機能

XSS対策

- INTER-Mediatorはデフォルトで HTML出力時にエスケープ処理を考慮

```
<td colspan="3" class="grayback" data-im="messageauth@message">
```

innerHTMLプロパティ

- 仕様上エスケープ処理をしない場合に
はinnerHTMLプロパティに代入

<td colspan="3" class="grayback" data-
im="messageauth@message@innerHTML">

CSRF対策

- params.phpで$webServerNameを設定
  - デフォルトでは未設定
  - Webアプリケーションが稼働しているホストのドメイン名もしくはFQDN（完全修飾ドメイン名）を配列で指定

CSRF対策

- params.phpでの$webServerName設定例

```
$webServerName = array('inter-
mediator.com', 'inter-mediator.info');
```

CSRF対策

- リクエストヘッダーにX-Fromおよび
Originを利用する手法を利用

http://hasegawa.hatenablog.com/entry/20130302/p1

クリックジャッキング対策

- params.phpで$xFrameOptionsを設定
  - デフォルトでは未設定
- 設定例

```
$xFrameOptions = 'SAMEORIGIN';
```

INTER-Mediatorの認証機能

- INTER-Mediatorでの認証やアクセス権設定では、ユーザーやグループを使用
- authuser、authgroup、authcorのそれぞれのテーブルに記録しておくのが基本
- 認証をチャレンジ-レスポンスによって行うためのissuedhashテーブルも必要

INTER-Mediatorの認証機能

- ネイティブ認証
  - データベースエンジンに組み込まれたユーザーを利用する方法
- ユーザー認証
  - データベースに含まれるテーブルあるいはビューを利用する方法

認証は定義ファイルで設定

特定ユーザーのみログイン

レコード単位のアクセス権

- authenticationキーの配列の中で、操作名をキーにした配列で、targetキーとfieldキーを指定

その他の設定項目

- params.phpで記述するセキュリティ関連の設定項目
  - $contentSecurityPolicy
  - $generatedPrivateKey
  - $passwordPolicy

詳細

- 詳細はINTER-Mediator Training Courseの Chapter 7「セキュリティと認証・アクセス権」を参照

その他知っておきたいこと

- 暗号化通信のためのSSL/TLS

SSL/TLSの利用

- HTTPでは通信は暗号化されない
- 用途・目的に応じてHTTPではなく
  HTTPSの利用を検討（常時SSL）
  - 認証局からSSLサーバー証明書を購入
  - 最近では無料の証明書も存在

INTER-Mediator Training Course

トレーニングコース

- INTER-Mediatorの開発手法を演習形式で自習する有償のトレーニングコース
  - ePub形式の電子出版物
  - INTER-Mediator-Server VMを利用しながら演習を進められる

サーバーサイドで出力調整

サーバーサイドで出力調整

- 詳細はINTER-Mediator Training Courseの Chapter 8「サーバーサイドでのプログラミング」を参照

まとめ

まとめ

- Webアプリケーションの脆弱性をなくす一般的な解決策を知る
- フレームワークが提供するセキュリティ機能と前提条件を把握する
- データベースソフトウェアが備えるセキュリティ機能を理解する